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