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)