Astalavista Group Security Newsletter
Issue 20 - 30 August 2005
http://www.astalavista.com/
security@astalavista.net

[01] Introduction

Dear respected readers,

Welcome to Issue 20 of the Astalavista Security Newsletter!

In this issue, we would like to share the most spicy security events of the month; as always, we briefly summarized and featured useful security tools, and resourceful papers written during the month at **Astalavista.com.** In addition to reviewing a couple of IT/Security practical sites, which may turn into your valuable info resources, we also recommend two gorgeous articles. First, by featuring **"Security in the enterprise– HR Management",** we sincerely hope to provide company executives/decision-makers with another point of view regarding investment in security and human resources. On the other hand, **"Today's security trends – practical tips for your security – Part 2"** would give the home user four golden tips on how to protect his/her privacy. In conclusion, you will also read another great interview **from the scene –** this time with **Robert** from **CGIsecurity.com**, a site I'm sure you've all visited during the last couple of years.

Be aware and you would be secure. And, of course, keep the spirit!

Astalavista Security Newsletter is constantly mirrored at :

http://www.packetstormsecurity.org/groups/astalavista/
http://www.securitydocs.com/astalavista_newsletter/

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

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

Previous issues of Astalavista Security Newsletter can be found at:

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

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

[02] Security News

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

---

[**KEY MANAGEMENT HOLDING BACK ENCRYPTION**]

A survey of 237 large companies conducted by nCipher, a UK encryption group, concludes that while businesses are eager to encrypt data, they struggle with complex key management. While the survey indicated that encryption is quickly becoming a "mainstream technology", it also concluded that many managers knew "little or nothing" regarding key management systems. 82% of those surveyed agreed that they would be encrypting stored data within 18 months. While a growing area of encryption are hardware-based systems called Trusted Platform Modules (TPMs), the survey indicated a lack of knowledge on the part of managers about TPMs.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=4150

Astalavista's comments :

Plain-text communications and data transfer are sooner or later prone to be abused, be it locally, remotely, or in between, whereas the management of PKI infrastructure requires quite a few additional resources and HR additions? – a bit untrue though. PKI indeed greatly improves the overall level of confidentiality and authentication in an organization given it's successfully maintained and implemented. Communicating the values and benefits to an organization and its employees is something the vendors would soon start emphasizing the way they aggressively "emphasized" on VPNs. In case an organizational manager wants to see another perspective on the topic, I strongly recommend that he/she go through the following :

http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/pki_e.asp

Outsourcing the tasks instead of "reinventing the wheel" is always an option, namely using the services or a Managed Security Services Provider would definitely justify the expenses posed by the introduction of a company-wide PKI infrastructure.

I believe the companies surveyed haven't yet reached maturity in the Security industry; they still have doubts whether to encrypt or not, and a security issue becomes a problem only when such arises. The truth is that a great deal of organizations have totally lost themselves when it comes to security, perhaps due to the following reasons : lack of industry-accepted ROSI models, fix it when it happens attitude, and security breaches are justified given business performance mode of thinking resulting in complete PR mockeries.

On the other hand, KeyMan has always been handy :

http://www.alphaworks.ibm.com/tech/keyman

Yet another, resourceful page on PKI management, certificate authorities etc is available at :

http://www.pki-page.org/

[**U.S COLLEGES STRUGGLE TO COMBAT IDENTITY THEFT**]

US colleges and universities, with enormous databases, are "finding themselves on the front lines of the battle against identity theft". In 2005, almost 50% of publicized data security breaches have targeted universities, the California-based Identity Theft Resource Center reports, while other researchers claim that such institutions probably make up only 20% of total victims. However, that traditionally open academic environment may be especially easy to target, as well as "financially naïve" students on their own for the first time. Notification costs when a breach does occur can be high; Educause estimates that an example of a situation where 50,000 potentially affected individuals must be contacted can cost an institution between $300,000 to $500,000.

More information can be found at :

http://www.eweek.com/article2/0,1759,1849198,00.asp?kc=EWRSS03119TX1K0000594

Astalavista's comments :

Universities have always acted as the main playground for hacking experiments and security breaches, mainly because of their open/research nature. Students are a different crowd compared to an organization's workforce, and these networks tend to be a little bit of an open environment. On the other hand students are aware of both the dark and white side of the Internet..

What bothers me is how the heck such highly confidential information is so conveniently available?! Lack of government enforcement is perhaps one of the reasons, and while reporting for the breach is legally justified in the state, no one needs more statistics – but actions. Identity theft is on the rise; thinking from an attacker's point of view, universities indeed comprise a huge, insecure database of fresh identities; namely universities themselves should realize that securing the information is more cost-effective and ethical instead of later on notifying the people involved.

A good article on the topic "Information Security in Campus and Open Environments" is available at :

http://irongeek.com/i.php?page=security/campussec05

[**GAO : FEDERAL DATA MINING NOT OBEYING PRIVACY RULES**]

The US Government Accountability Office (GAO) has released a report finding that federal data mining has not adhered to privacy regulations. Based on a review of data mining practices at the Small Business Administration, the Agriculture Department's Risk Management Agency, the Internal Revenue Service, the State Department, and the Federal Bureau of Investigation, the GAO found that each agency practiced some, but not all, of the privacy protection measures required by law. Most agencies notify the public about the use of personal information in data mining programs, but not the purpose of the program itself. Officials fail to understand the impact data mining can have on personal privacy; none of the agencies reviewed had produced an acceptable privacy impact report.

More information can be found at :

http://www.fcw.com/article90517-08-29-05-Web&RSS=yes

Astalavista's comments :

For me it's always a matter of personal opinion where the consensus should be reached. Consider yourself a privacy activist, simply because you have something to hide and you don't like the idea of being watched, or "think BigBrother". Now consider an organization whose purpose is to protect your country, ensure terrorists don't communicate over its networks, and locate those eventually doing it. Picture a terrorist doing searches on local neighborhoods, map routes, satellite images of parts of NY, taking advantage of GPS services, and communicating with his folks with the help of PGP or any other publicly available encryption tool, and yes they communicate on attacking your city!

From a governmental point of view, I see several options. Monitor everything, BUT detect only predefined patterns of information, ensure their technological advantage in breaking the algorithms and be always a step ahead - a relatively weak option given the increasing use of steganography, and quantum cryptography, or think marginally. The Australian government is perhaps aware they cannot break the so called strong encryption though brute forcing, which is why they might take advantage of browse based vulnerabilities to plot Trojans, spyware and get access to private keys etc.

I like my privacy, but I also know I live in a digitalized world, where privacy tends to be a different word, given today's technologies for storing and processing information. And even though sacrifices are important, I know that every time I take advantage of this digitalized world, I sacrifice some of my privacy.

Data mining as a concept is perfectly fine given that there's at least a slight degree of transparency about how information is gathered; TIA was perhaps too motivated, a bit desperate project to try to gather; analyze and detect possible terrorist information, while I'm certain there's a working or at least an alternative in development.

Consider reading the following publications when it comes to terrorists, Internet and data mining :

http://www.astalavista.com/index.php?section=directory&linkid=4683
http://www.astalavista.com/index.php?section=directory&linkid=4689
http://www.astalavista.com/index.php?section=directory&linkid=4282
http://www.astalavista.com/index.php?section=directory&linkid=4783
http://www.astalavista.com/index.php?section=directory&linkid=4858

[**PIRACY CRACKDOWN SPURS SHIFT IN ONLINE FILE SHARING**]

Internet analysis firm CacheLogic has released a study that finds decreased use of BitTorrent in the United States since the movie industry's crackdown on piracy sites using the technology, and greater use of the eDonkey peer-to-peer (P2P) file sharing software. eDonkey has long been a popular P2P program in Europe and South Korea. CacheLogic chief technology officer Andrew Parker describes the shift in platforms as "a game of P2P hide-and-seek" between pirates and content holders. About 60% of internet traffic is used for P2P, according to CacheLogic.

More info can be found at :

http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,104239,00.html

Astalavista's comments :

I'm rather surprised by this study, as you can't deal with P2P by simply shutting down sites – they will appear later on and its new life cycle will only depend on its popularity. Content is easily distributed these days, what's left for torrents when home users are transferring gigabytes of data on a daily basis. While on the other hand there's indeed a trend of "a game of P2P hide-and-seek", it's not because of the fact that certain web sites have been shut down, but because a matter of choice, P2P application popularity and needed content availability.

The industry is fighting a war against itself, they cannot fight the technology, what they try to fight is the distribution and development practices of the content – the main factors for having so much copyrighted works available even before their trailers have become public.

[**ANTI-SPYWARE FIRM WARNS OF MASSIVE ID THEFT RING**]

On August 4, 2005, Florida-based anti-spyware vendor Sunbelt Software discovered a "massive ID theft ring" that is systematically breaking into and stealing information from computers on a global scale. The organized group of identity thieves uses a variant of the browser hijacking tool "CoolWebSearch" (CWS) to redirect users to Web sites that then collect information from the infected computers. Sunbelt said it found a large file located on a remote server containing "user names, addresses, account information, phone numbers, chat session logs, monthly car payment information and salary data". While the domain in question is registered in China, the server itself appears to be located in the United States. The FBI is investigating.

More information can be found at :

http://www.networkworld.com/news/2005/080505-id-theft.html?fsrc=netflash-rss

Astalavista's comments :

The trends are indeed becoming more aggressive and the one-to-one advertising streaming and intelligence gathering approach doesn't seem to be as satisfying as it used to be in the past, but due to what? As spyware and adware have gotten a lot of attention recently, the "vendors" are having hard time trying to infect, even maintain infected users. Realizing the possibility of loosing these forever, they try to take the maximum out of having total access to someone's PC, id's, logins, bank details, or anything else of financial, personal value. It's getting harder and harder for spyware vendors to keep as many infected victims as they used to at the very beginning, and what we're about to witness soon is the coordinated work between spyware, malware and spammers in a way that it will totally test the response of the industry and the Internet as a whole.

[**HACKER FEAR FUELS OUTSOURCED SECURITY SPEND**]

Global demand for outsourced security services is "strong and growing fast", fuelled by increasing fear of viruses, malware, spyware and hacking, combined with the complexity of rolling out security systems in house. According to the latest market size and forecast report from Infonetics Research, demand for virtual private network (VPN) services continues to grow strongly, driven by the productivity improvements and cost savings that secure VPNs can offer remote workers.

More information is available at :

http://www.vnunet.com/vnunet/news/2140767/hacker-fear-outsourced-security

Astalavista's comments :

It is great to see companies outsourcing risks with the help of MSSPs, but as always, you shouldn't rely on a single protection layer, namely the MSSP for taking care of your entire infrastructure. Consider MSSPs as partners and consultants taking the bulk out of your work, while take into consideration that in-house security teams still justify the investment, they way you(in case you're not naïve) would rather hear the opinion of two doctors instead of listening to just one.

[**MICROSOFT'S HONEYMONKEYS PROVE PATCHING WINDOWS WORKS**]

Microsoft unveiled details of its Strider HoneyMonkey research, a project that sniffs out sites hosting malicious code, and hands the information to other parts of the company for patching or legal action. he HoneyMonkey concept, said Yi-Min Wang, the manager of the Cybersecurity and Systems Management Research Group, is completely different from the better-known honeypot approach to searching for malicious exploits. "Honeypots are looking for server-based vulnerabilities, where the bad guys act like the client. Honeymonkeys are the other way around, where the client is the vulnerable one."

More information can be found at :

http://www.desktoppipeline.com/167600732

Astalavista's comments :

Cheers for the Microsoft team for bringing and developing the HoneyMonkeys initiative!

Although the concept for trusted web in terms of exploits-free and verified web sites has always been around, I'm surprised an anti-virus, anti-spyware vendor hasn't come up with it earlier, at least in terms of PR. Client-based honeypots are perhaps the next trend when it comes to honeypots as with the increasing browser based and end user based vulnerabilities.

An interesting aspect to consider is the manual feeding of potentially malicious web sites, whereas the eventual localization of link hubs and the use of PageRank concepts would provide a researcher with realistic and timely information for the poisoned side of the WWW.

Perhaps a future option to be considered is integrating the feature into all-in-one appliances or end users' applications in order to ensure that a site, any site in this case, is free of exploits before visited – just a small product development tip!

[HACKING THE HOTEL THROUGH THE TV]

The "inverted security model" of hotel connections allows Adam Laurie to avoid paying for movies, the minibar and phone calls, as well as hack into other guests' accounts and set wake-up calls or follow their internet surfing. Laurie presented his findings at the Defcon security conference in Las Vegas on July 30, 2005. Laurie connects the hotel TV cable into a USB TV tuner connected to his laptop. He warns that as hotels increase amenities, such as allowing payment through the TV system or adding webcams, the security situation will worsen.

More information can be found at :

http://news.com.com/Hacking+the+hotel+through+the+TV/2100-1029_3-5812598.html?part=rss&tag=5812598&subj=news

Astalavista's comments :

Impressive example of what a security-minded person can research given the advances hotels offer to guests these days. Should hotels seriously start thinking about security?! Not at all, just make sure they've taken care of downright genius issues in case they want to avoid huge damages to their reputation. On the other hand the possibilities for abuse could be compared to those of hacking celebrities cell phones.

[LINUX BLUETOOTH HACKERS HIJACK CAR AUDIO]

Injecting or recording audio signals from passing cars whose occupants are running insecure Bluetooth hands-free units is possible, using the "Car Whisperer" tool developed by Trifinite. The hacker group demonstrated the process at the "What the Hack" meeting in The Netherlands. The issue appears to be "implementation problems", as opposed to true security protocol problems, as many auto makers use easy to guess passkeys such as "0000" or "1234".

More information can be found at :

http://www.securityfocus.com/news/11266

Astalavista's comments :

It's great to see yet another release from the Trifinite group, authors of some of the prominent bluetooth security tools and research publications. Car and mobile phone manufacturers should start seriously cooperating with security researchers in order to ensure devices are distributed "secure by default", as these days it's a public secret that Bluetooth devices are way too insecure, but as always when it comes to security, the fix it when it happens mode of thinking prevails.

What to do about it? – Consider testing the tool!

[GOOGLE EARTH "COULD AID TERRORISTS"]

Frans Weekers and Aleid Wolfson, two members of the Dutch parliament, have questioned whether terrorists could use Google Earth to plan attacks. Google Earth uses a collage of satellite photos to give users a bird's eye view of locations all around the world; some locations have enough detail for users to see a swimming pool or shed in backyards. Terrorists could use this data when plotting attacks. The lawmakers have asked how other countries are reacting to potential threats enabled by Google Earth. A Google official says the software is built from open source data that anyone can collect, and that the benefits far outweigh possible harms. The Dutch Ministry of Justice is examining the issue.

More information can be found at :

http://www.smh.com.au/news/breaking/google-earth-could-aid-

terrorists/2005/08/18/1123958137040.html

Astalavista's comments :

Slowly, but at least realizing, government entities are considering the largest publicly available database as a feature that could greatly assist the plotting of terrorist attacks. It will save a potential terrorist the need to be physically walking around (now tell me, how you're about to justify all the surveillance cameras budgets you've felt so secure about?!)

From a Google's point of view, it's common sense, not corporate PR which is they maintain an open-topic privacy policy, thereby ensuring data can be gathered and later on datamined with other sources for the eventual detection of terrorist patterns given the other variables.

[03] **Astalavista Recommends**

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

" **KOJONEY – SSH HONEYPOT**"

Kojoney is an easy of use, secure, robust, and powerful Honeypot for the SSH service. It includes other tools such as kip2country (IP to Country) and kojreport, a tool to generate reports from the log files.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4819

" **CHATSNIFF V1.0** "

ChatSniff is an easy to use program that monitors, or "sniffs" networks for AIM, ICQ, MSN, Yahoo!, and Jabber instant messages.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4866

" **WINDOWS TCP/IP STACK HARDENING TOOL** "

The following tool was designed to harden the Windows TCP/IP stack against different types of DoS attacks. The tool also provides a simple to use GUI. The tool has been tested to work under all versions of Windows XP and Windows 2000.

http://www.astalavista.com/index.php?section=directory&linkid=4886

" **IRCD – THE INCIDENT RESPONSE COLLECTION REPORT** "

The Incident Response Collection Report is a script to call a collection of tools that gathers and/or analyzes data on a Microsoft Windows system. You can think of this as a snapshot of the system in the past. Most of the tools are oriented towards data collection rather than analysis.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4890

" **BASTED – HONEYPOT FOR SPAMMERS** "

BASTED is a free tool/solution, that acts as a honeypot for spammers, who use spambots to harvest email addresses from websites. BASTED has been designed to become a powerful tool for system administrators willing to gather information about the data-flow in the spam process.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4916

" **PEBROWSE** "

PEBrowse (Crash Dump Analyzer, Professional and Professional Interactive) provides a multitude of functionality on the Windows platform. Including: * PE File Analysis * Disassembling * Debugging

http://www.astalavista.com/index.php?section=directory&linkid=4927

" **CRYPTKNOCK – ENCRYPTED PORT KNOCKING TOOL** "

Cryptknock is an encrypted port knocking tool. Unlike other port knockers which use TCP ports or other protocol information to signal the knock, an encrypted string is used as the knock. This makes it extremely difficult for an eavesdropper to recover your knock (unlike other port knockers where tcpdump can be used to discover a port knock).

http://www.astalavista.com/index.php?section=directory&linkid=4928

" **CYBERDUCK V2.5** "

Cyberduck is an SFTP (SSH Secure File Transfer) and FTP browser licenced under the GPL. It has been built from the ground up with usability in mind, having the same consistent graphical user interface for both SFTP and FTP browsing.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4992

" **NINJA – A PRIVILLEGE ESCALATION DETECTION AND PREVENTION SYSTEM** "

Ninja is a privilege escalation detection and prevention system for GNU/Linux hosts. While running, it will monitor process activity on the local host, and keep track of all processes running as root. If a process is spawned with UID or GID zero (root), ninja will log necessary information about this process, and optionally kill the process if it was spawned by an unauthorized user.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4966

" **SPAMSTATS** "

Spamstats is a Perl script that analyses spamassassin+mailer logs in order to extract useful informations about spam traffic. It displays scores, volumes, and spamassassin analysis times for spam/non-spam/both. It also extracts top spammed mailboxes. Its

time options let it be used in conjunction with SNMP to generate near realtime graphs. Currently supported mailers are Postfix, Exim, and Sendmail.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=4923

[04] **Astalavista Recommended Papers**

" **A HARDWARE BASED PROGRAM AND DATA PROTECTION MECHANISM** "

Validy Technology is a protection mechanism achieving a high degree of security by having a protected program execute a small fraction of its instructions in a coprocessor. The coprocessor works on a set of integer registers and manipulates them in a secure way to prevent hacking. An important feature of the coprocessor is its ability to detect program or data tampering and to stop working when this happens, leaving the program with missing information and forcing it to stop.

http://astalavista.com/index.php?section=directory&linkid=4827

" **HOWTO BUILD YOUR OWN SMALL WARDRIVER BOX** "

It's very easy, but this is not a step by step HOWTO, only a guide to build your own box. To start, you need a small up and running OpenBSD System on an Intel based System. This Sytem can run on in VMWare or on a older PC System (i use a 500 Mhz Pentuim System with 4 GB HD and 128 MB Ram) For installing OpenBSD, Order the CD-Rom's and install OpenBSD. For More detailed Information go to www.openbsd.org and then RTFM (read the famous manual)

http://astalavista.com/index.php?section=directory&linkid=4836

" **CREDIT CARD DATA PROCESSING – HOW SECURE IS IT?**"

Hearings on the topic of "Credit Card Data Processing: How Secure Is It?"

http://astalavista.com/index.php?section=directory&linkid=4841

"**PROTECTING PRIVACY FROM CONTINUOUS HIGH-RESOLUTION SATELLITE SURVEILLANCE**"

This paper argues that the high resolution geospatial images of our earth's surface, produced from the earth observing satellites, can make a person visually exposed, resulting in a technological invasion of personal privacy. We propose a suitable authorization model for geospatial data (GSAM) where controlled access can be specified based on the region covered by an image with privilege modes that include view, zoom-in, overlay and identify. We demonstrate how access control can be eficiently enforced using a spatial indexing structure, called MX-RSquadtree, a variant of the MX-CIF quadtree.

http://astalavista.com/index.php?section=directory&linkid=4857

" **DATABASE SECURITY EXPLAINED** "

Working from the outside into the crunchy database center, we'll cover: - The types of security problems. What should you worry about? - Server placement. Where should you put your MySQL server to protect it from TCP exploits? How can you provide secure

access for database clients? - Database server installation. What version of MySQL should you use? What are the best file/directory ownerships and modes? - Database configuration. How do you create database user accounts and grant permissions? - Database operation. How do you protect against malicious SQL and bonehead queries? What are good practices for logging and backup?

http://astalavista.com/index.php?section=directory&linkid=4872

" **VULNERABILITY DISCLOSURE FRAMEWORK** "

The goal of this report is to achieve a common understanding and develop standard practices for disclosing and managing vulnerabilities in networked information systems.

http://astalavista.com/index.php?section=directory&linkid=4894

" **A KNOWLEDGE DISCOVERY APPROACH TO ADDRESSING THE THREATS OF TERRORISM** "

Ever since the 9-11 incident, the multidisciplinary field of terrorism has experienced Tremendous growth. As the domain has benefited greatly from recent advances in information technologies, more complex and challenging new issues have emerged from numerous counter-terrorism-related research communities as well as governments of all levels. In this paper, we describe an advanced knowledge discovery approach to addressing terrorism threats. We experimented with our approach in a project called Terrorism Knowledge Discovery Project that consists of several custom-built knowledge portals.

http://astalavista.com/index.php?section=directory&linkid=4858

" **HOME SURVEILLANCE WITH INTERNET REMOTE ACCESS** "

As with seemingly everything else, the Internet has revolutionized what you can build for remote surveillance and security. Low-cost video cameras, driven by the market for desktop video conferencing and webcams, have improved to where they generate reasonably high-quality video and provide embedded video compression. Broadband Internet access offers both speed advantages and a permanent connection to the net, making it suitable for remote monitoring. The global reach of the Internet means that you can monitor your home from Abu Dhabi, if you happen to be there.

http://astalavista.com/index.php?section=directory&linkid=4940

" **MYFIP – INTELLECTUAL PROPERTY THEFT WORM ANALYSIS**"

Myfip is a network worm discovered in August of 2004. It didn't get an extreme Amount of attention at the time, just a few articles talking about a new worm which stole PDF files. It wasn't terribly widespread or damaging, so it didn't rate very high on the antivirus companies' threat indicators. However, it is still worth paying attention to because the potential for damage to a company can actually be greater than with other worms. A Slammer or Blaster outbreak might take the network down for a while, but an incident like that can be recovered from. If the wrong document leaves your network it could have devastating consequences.

http://astalavista.com/index.php?section=directory&linkid=4933

" **TIMING ATTACKS ON WEB PRIVACY** "

We describe a class of attacks that can compromise the privacy of users' Web-browsing histories. The attacks allow a malicious Web site to determine whether or not the user has recently visited some other, unrelated Web page. The malicious page can determine this information by measuring the time the user's browser requires to perform certain operations. Since browsers perform various forms of caching, the time required for operations depends on the user's browsing history; this paper shows that the resulting time variations convey enough information to compromise users' privacy.

http://astalavista.com/index.php?section=directory&linkid=4905

[05] **Astalavista.net Advanced Member Portal v2.0 – Become part of the community today!**

Become part of the **community** today. **Join us!**

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

http://www.astalavista.net/v2/?cmd=tour&page=top10

and our **30%** discount this month

http://www.astalavista.net/v2/?cmd=sub

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering an enormous database of **very well-sorted and categorized Information Security resources - files, tools, white papers, e-books.** At your disposal are also thousands of **working proxies**, **wargames servers**, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs.

Among the many other features of the portal are :

- Over **5.5 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

[06] **Site of the month**

GData : An Online MD5 Hash Database

Database currently contains **12,291,785** unique entries.

http://www.gdataonline.com/

[07] **Tool of the month**

BiDiBLAH – An Automated Assessment Tool

Find more about the tool at :

http://www.sensepost.com/research/bidiblah/what_is_bidiblah.pdf

Get it at :

http://www.astalavista.com/index.php?section=directory&linkid=4835

[08] **Paper of the month**

How to build your Business with open-source

Think high-priced commercial software is your only option? Don't be so sure. Free alternatives are available in a wide range of enterprise software categories, including some that may surprise you.

http://www.astalavista.com/index.php?section=directory&linkid=4869

[09] **Free Security Consultation**

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

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

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

Question : Hi folks at Astalavista!! Amazing work from your team when it

comes to real security or hacking content, keep up the good work and don't get caught! I've been recently confronted with the difficult task to keep myself up-to-date with the latest patches released given the many software programs that I use. Reading through various publications I have come to believe that patching is indeed quite important and no firewall can protect me against an unpatched system.

Answer : A little bit of common sense and a couple of publications can come handy in your case, as a matter of fact we've decided to feature this question due to the many other similar ones we keep on getting – all about patching. As far as "getting caught" is concerned – I honestly believe the only thing we could "get caught" about is bringing one of the most resourceful security portals to the world for free..

Patching is essential for keeping yourself safe out of associated vulnerabilities, Whereas a 0-day exploit cannot be taken care of patches since it's still unknown. What you should keep in mind is that patching has proven useful to protecting against any kind of vulnerabilities and worms – given that the patch has been applied. Whenever you use certain software, you will usually find security and patch updates on its site, even better, the majority of sites often provide you with a free alert based service, usually through a newsletter. As you've already stated that you're a Windows user – keep an eye at Microsoft's TechNet and especially the security bulletins :

http://technet.microsoft.com/default.aspx

Windows Update will also take care of quite a few issues whenever such arise :

http://windowsupdate.microsoft.com/

Consider also keeping an eye on the following, which provide great filtering features so you will get the results you need :

Bugtraq - http://www.securityfocus.com/archive/1
X-Force Database - http://xforce.iss.net/xforce/search.php
SecurityTracker - http://www.securitytracker.com/
SecuriTeam - http://www.securiteam.com/
FrSIRT - http://www.frsirt.com/english/
CVE - http://www.cve.mitre.org/

Question : Managing an SMB with couple of hundred workstations causes a lot of trouble when fighting viruses and all the pests my employees download or somehow get infected with. I wanted to ask you for any other particular recommendation besides having anti-virus scanners on every computer – it's still causing a lot of troubles.

Answer : There are quite a lot of factors contributing to these problems, for instance, are you aware how many of the anti-virus scanners are actually active, are they constantly updated, both signatures and patches for the software itself, do you keep a track of what's been infecting your organization so that you would be able to develop a strategy specifically for your type of users? What you should consider is that patching workstations is very important when it comes to exploits-based web sites and that application based firewalls are a must have,

besides having a server based and host based anti-virus solution. Keep an eye on users bringing laptops inside the network and make sure your system administrator would be on alert for infected PCs so that these would be blocked Backups(data,system) are also a must have, as even though today's malware isn't as destructive as it used to be, you will definitely face a situation with lost data, or totally messed up configurations. Above all – educate them on the most common malware attack patterns.

Question : I have been recently doing a research on the abuse of Port 80 from an enthusiast's point of view. What bothers me is the fact that whatever I do I simply cannot control the use/abuse of this port, as this is the port my and pretty much every other public server operates on. Add some dynamic content, sophisticated databases and all my other security measures, even my ISPs one become useless. How to deal with this problem?

Answer : Web based vulnerabilities are attracting a lot of attention from malicious attackers, mainly because of the reasons you mentioned – easy to execute, but with devastating consequences if successful. Based on the profile of your site(I assume it's a low one), it would be more cost-effective to put in action a web vulnerabilities scanning tool or get help from a professional consultant/auditor with experience in web application vulnerabilities.

On the other hand, looking at web server logs, and with the right IDS Configuration (can again be abused of course) will provide you with a surprisingly relevant information on how often, and to what extent your web security is being attacked – it will motivate you even more on securing it.

Check out http://www.owasp.org on the other hand, it will provide you with a lot of info!!

[10] Astalavista Security Toolbox DVD v2.0 - what's inside?

Astalavista's Security Toolbox DVD v2.0 is considered **the largest and most comprehensive Information Security archive available offline**. As always, we are committed to providing you with a suitable resource for all your security and hacking interests - in an interactive way!

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=3

[11] Enterprise Security Issues

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

- **Security in the enterprise** – **HR Management -**

This brief article will provide a company's manager with a discussion on the benefits, problems and recommendations when it comes to attracting and utilizing the workforce, or the blood that goes through the veins of your organization, not only when it comes to security, but to its long-term prosperity as well.

As the information security industry is steadily growing, there're a countless number of opportunities in each and every of its sectors, code auditors, malware analysts, consultants, auditors, and many more. A great number of standardization oriented institutions and entities have been established to provide best practices about the education and training of the workforce. Managers are still conveniently looking for all-in-one solution to securing their enterprise, even worse, thinking that's it's a one time investment, whereas trying to capitalize on the benefits of today's E-commerce technologies.

Finding the right candidate for the right job is always a tricky job, what is "right" anyway? Are you an organization on the level of survival, profitability or perhaps innovation? The three of these and other stages will greatly reflect the way you hire, with an "filling the positions" mode of thinking, or talent scouting approach, if any.

Some of the most common obstacles to HR management in the enterprise I'm aware of are the **technical wizards versus the strategical thinkers conflicts**. The benefits of having these are obvious, the technical wizards will do code miracles, whereas they will lack the strategical/business, perhaps pragmatic mode of thinking. On the other hand the strategical thinkers wouldn't be able to technically execute an idea. Whenever hiring make sure each of these individuals possess some of the other one's qualities, or consider taking care of the productive interaction between such individuals, otherwise you will face a situation like where an engineer in love with his creation or sophistication cannot communicate with a marketer or product manager trying to convince him/her that there are better, time-effective, and market-driven basis for developing or postponing an idea.

Lack of incentives will also result in a total stagnation of your workforce, and in security, folks, vision and dental insurances just doesn't fit in. InfoSec experts want to be valued, respected and most importantly given the necessary credit for the realization of any project, free conferences tickets, asking for major decision-making idea and comments, the opportunity to participate in an impact-driven project, and not another product/service extension.

Another common problem that I have encountered is the promotion of **inside-the-box thinking culture**, namely following procedures, company hierarchy and too

much bureaucracy, seek open spaces, comments and actually takes these into consideration, promote diversity!

Possible solutions to any of these might be to outsource these tasks to an External company, such a managed security services provider who will take the bulk out of managing a security infrastructure and motivating/taking care of employees. In case you want to take an indirect approach when dealing with such problems, you can consider trying to find the most talented and exception individuals, but how? Don't go and search out for them, let THEM search for you, through professional and socially-oriented security initiatives your company will establish itself as the number one choice for a future employer, thus easily attract outstanding people from everywhere.

As far as spotting the right candidate is concerned, yes, experience is a must, but don't go for the usual "at least 3 years experience" requirement for an exceptional and just graduated candidate. Look for passion for work, self-starters usually go beyond the required tasks, and most importantly, **don't try to cultivate them – empower them!**

An organization's HR in the security industry, and not only, is perhaps the most valuable investment that a wise and visionary manager can make; stick to the people not to the numbers and in the long-term you'll have both the "numbers" and the people's respect, highlighting yet another important fact – if you're to build a business with an exit strategy – don't even start it, be a company that's "here to stay!".

[12] **Home Users' Security Issues**

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- **Today's security trends – practical tips for your security – Part 2** -

This article will deal with today's major security issues from an end user's point of view and would not only reveal their importance, but also provide the reader with recommendations on how to deal with them.

1. Identity theft

Make sure you protect your sensitive information and do not store sensitive or complete package of info regarding your identity or financial abilities, both offline and online. The more it takes to locate your PIN and your credit card the harder it would be to get these stolen. Try to stay spyware and malware free, and constantly monitor your online financial activities. Shred any confidential information and don't just throw it away, it could be abused. Make sure you have the latest version of your browser, and consider a bank that promotes the use of alternatives to Internet Explorer a security-conscious one. Think twice and always be suspicious whenever doing E-banking, and do not ever follow direct links from emails pretending to be a bank, any bank whatsoever.

2. Social engineering attacks

Keep in mind, that each and every communication over the Internet can be sniffed, and that anonymity online simply does not exist. Something else to consider is that whenever you use the Internet, certain leads are always there, and be suspicious in case someone starts pointing them out in a direct or an indirect way. Don't be naïve, and try to "sense" is the person on the other side of the communication indeed the one you're talking to. As far as social engineering attacks are concerned, these are present everywhere, phishing, malware infected emails, so watch out, and don't everything you receive in your mailbox way too personally! Don't be so talkative to strangers, and consider strangers even people you've met weeks ago online, have respect for your privacy and as they say "anything that you say may be used against you" fully applies in this situation.

3. Malware

Consider avoiding the download of programs from sites whose origin is unknown, and always try to locate the associated program with the help of Google, thus getting a better picture of how eligible it really is. Avoid directly opening attachments even from known people and try to spot anything that seems unusual in your communication. Never trust a programs icon for whatsoever reason, as these are easily changed. Don't accept tricky programs and hot tools from strangers over IM networks, IRC etc.

4. Wireless networks/nodes

Perhaps rather common sense, but consider turning off your equipment when you don't use it , make sure default passwords and logins are removed, ensure the strongest level of encryption is in use, as well as that a firewall or wireless nodes monitor is active, so that in case you notice someone else is connecting through your network, you would be able to take measures, namely block them, or improve your knowledge on how they managed to do it(pretty easy though). Make sure you often change your WEP encryption keys and that they're as long as possible.

Best of all, check out the following collection of vulnerabilities :

http://new.remote-exploit.org/index.php/Wlan_defaults

[13] **Meet the Security Scene**

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **Robert** from **CGISecurity.com**

Your comments are welcome at security@astalavista.net

Interview with Robert, http://www.cgisecurity.com/

Astalavista : Hi Robert, would you, please, introduce yourself to our readers and share some info about your profession and experience in the industry?

Robert : I first started to get interested in the hacker/security aspect of computers in the 90's in high school where I had my first brush with a non 'windows/mac system' called 'VMS' (a VAX/VMS system to be exact). A yearlater I *finally* got access to an internet connection and to my amazement discovered that it was possible to break into a website with nothing more than your browser which was something I found to be rather interesting. This *interest* grew into a website I originally hosted on xoom (some free hoster I forget which :) that later became CGISecurity.com in September of 2000 where I've published numerous articles and white papers pertaining to website security.

In 2003 I 'sold out' (get paid to do what you'd do for free) and was hired to perform R&D and QA on a Web Application Security Product where I am to this day. In 2004 I Co Founded 'The Web Application Security Consortium' (**http://www.webappsec.org**) with Jeremiah Grossman (**http://www.whitehatsec.com**) to provide an outlet for some projects that multiple people we knew where interested in participating in. A year later I created 'The Web Security Mailing List' (**http://www.webappsec.org/lists/websecurity/**) as a forum where people can freely discuss all aspects of Web Security where I am currently the lead list moderator.

Astalavista : Recently, there's been a growing trend towards the use of automated code auditing/exploitation tools in web applications security. Do you believe automation in this particular case gives a false sense of security, and provides managers with point'n'click efficiency, compared to a structured and an in-depth approach from a consultant?

Robert : Scanners provide a good baseline of the common types of issues that exist but are not magic bullets. It shouldn't come to a surprise to you but many of these consultants use these automated scanning tools (Both freeware and commercial) in conjunction with manual review and simply verify the results. The skill of the person using any specialized product greatly impacts the end result. Someone with a good security understanding can save immense amounts of time by using such an automated product. If your organization doesn't have a 'security guy' then a consultant may be the best solution for you.

Astalavista : Phishers are indeed taking a large portion of today's e-commerce flow. Do you believe corporations are greatly contributing to the epidemic, by not taking web security seriously enough to ensure their web sites aren't vulnerable to attacks in favour of online scammers?

Robert : Phishing doesn't *require* that a website be vulnerable to anything it just simply requires a look alike site exploiting a users lack of security education and/or patches. I wouldn't say they are contributing towards it, but I do think that educating your user (as best as you can)

is a requirement that should be in place at any online organization.

Astalavista : What are you comments on the future use of web application worms, compared to today's botnets/scams oriented malware? What are the opportunities and how do you picture their potential/use in the upcoming future?

Robert : In 2005 we saw a rise in the use of search engines to 'data mine' Vulnerable and/or suspect hosts. Some of the larger search engines are starting to put measures in place such as daily request limitations, CAPTCHA's, and string filtering to help slow down the issue. While these efforts are noteworthy they are not going to be able to prevent *all* malicious uses a search engine allows. I think the future 'web worms' will borrow methodologies from security scanners created to discover new vulnerabilities that will have no patches available. While the downside of this is to slow infection rates and lots of noise, the upside is infecting machines with no vendor supplied patch available because the 'vendor' may be a consultant or ex employee who is no longer available.

Worms such as Nimda infected both the server and its visitors making it highly effective and I expect this user/server trend to increase in the future. I also suspect a switch towards 'data mining' worms, that is worms that are trying to steal useful data. Modern day versions of these worms steal cd keys to games and operating systems. The use of worms to seek and steal data from a server environment, or user machine is only going to grow as credit card and identity theft continue to grow.

While investigating a break-in into a friends ISP I discovered the use of a shopping cart 'kit' left behind by the attacker. This kit contained roughly 8 popular online shopping carts that where modified to grab copies of a customers order, a 'shopping cart rootkit' if you will. I suspect some type of automation of either auto backdooring of popular software or uploading modified copies to start creeping its way into future web worms.

In 2002 I wrote an article titled 'Anatomy of the web application worm' (**http://www.cgisecurity.com/articles/worms.shtml**) describing some of these 'new' threats that web application worms may bring to us.

Astalavista : Is the multitude and availability of open-source or freeware web application exploitation tools benefiting the industry, resulting in constant abuse of web servers worldwide, or actually making the situation even worse for the still catching up corporations given the overall web applications abuse?

Robert : This entirely depends on the 'product'. There are tools that allow you to verify if a host is vulnerable without actually exploiting it which I consider to be a good thing while some of these 'point and root' tools are not helping out as many people as they are hurting. In the past few years a shift has started involving 'full disclosure' where people are deciding not to release ./hack friendly exploits but are instead releasing 'just enough detail' for someone to verify it. This 'shift' is something that I fully support.

Astalavista : CGISecurity.com has been around for quite a few years. What are your plans for future projects regarding web security, and is it that you feel the industry is lacking right now - awareness, capabilities or incentives to deal with the problem?

Robert : Actually September 14th will be the 5th year anniversary of **CGISecurity.com**. Right now I'm heavily involved in 'The Web Application Security Consortium' where we have numerous projects underway to provide documentation, education, and guides for users. I plan on expanding CGISecurity into a one stop shop for all 'web security' related documentation where you can (hopefully) find just about anything you could ever need.

To answer the second part of your question I'd say all three with awareness (education) being the biggest problem. One of the things that the industry hasn't 'gotten' yet (in my opinion) is security review throughout an application's lifecycle. Sure developers are starting to take 'secure development' more seriously but as many of your readers know deadlines hamper good intentions and often temporary solutions (if at all) are put in place to make something work in time for release. This is why we need security review during all phases of the cycle not just during development and post production. I think that a much overlooked aspect of the development cycle is Quality Assurance. QA's job is to ensure that a product works according to requirements, identify as many pre release (and post release) bugs as possible, and to think about ways to break the product. I think that more companies need to implement 'QA security testing' as a release requirement as well as train their testers to have a deeper understanding of these 'bugs' that they've been discovering. You've heard the term 'security in layers' so why can't this process be implemented throughout most development cycles? Developers get busy and may overlook something in the rush to meet the release date which is why (before release) they need someone double checking their work (QA) before it goes production.

Astalavista : In conclusion, I would like to ask you what is your opinion of the Astalavista.com's web site and, in particular, our security newsletter?

Robert : I first discovered astalavista in my 'referrer' logs when it linked to one of my articles. Since then I've been visiting on and off for a few years and only recently discovered the newsletter which I think is a great resource for those unable to keep up with all the news sites, and mailing list postings.

[14] IT/Security Sites Review

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

-

RobotsTXT.org

-

http://www.robotstxt.org/wc/active.html

The most comprehensive and well-sorted achive of web robots sorted by name, type, contact details etc.

-
AV-Comparatives.org
-
http://www.av-comparatives.org/

On this site you will find independent comparatives of Anti-Virus software.

-
NeedScripts.com
-
http://www.needscripts.com/

The one stop web development resource with over 30,786 resources and growing.

-
Owasp.org
-
http://www.owasp.org/

The Open Web Application Security Project (OWASP) is dedicated to finding and fighting the causes of insecure software. Our open source projects and local chapters produce free, unbiased, open-source documentation, tools, and standards.

-
I-Hacked.com
-
http://i-hacked.com/

Electronics are everywhere, and technology drives pretty much everything we do in today's world. We show you how to take advantage of these electronics to make them faster, give them added features, or to do things they were never intended to do.

[15] **Final Words**

Dear readers,

Thank for going though issue 20 of the Astalavista Security newsletter, or though your favourite sections only!

We value and read each of your comments/suggestions. Please, share your impressions – positive or negative, they will be highly appreciated.

Till next issue of the **Astalavista.com's Security Newsletter**!

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net