Astalavista Group Security Newsletter
Issue 27 – 31 March 2005
http://www.astalavista.com/
security@astalavista.net

- Programming language inventor, or serial killer?
- The Web Hacking Incidents Database
- The PHP Security Consortium

[01] **Introduction**

Dear readers,

Issue 27 of **Astalavista's Security Newsletter** is out! Check out our additions of important security events, associated commentaries, recommended resources that made it on our site during the month, two articles, "**Establishing an internal security awareness culture – the basics** ", "**How do I figure out who's attacking me?**" and an exclusive interview with **Roberto** from the **Zone-H.org's** team, a site that hopefully doesn't need an introduction at any point.

Enjoy the issue, and fell free to send us your feedback as usual. Till next month!

Check out the Geeky Photos section :

http://www.astalavista.com/index.php?section=gallery and of course our additions for March only :

http://www.astalavista.com/index.php?section=gallery&cmd=showCat&cid=47

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

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

Previous issues of Astalavista Security Newsletter can be found at:

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

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

[02] **Security News**

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

---

[**OFFSHORE OUTSOURCING CITIED IN FLORIDA DATA LEAK**]

Florida state's People First payroll and human resources system was "improperly subcontracted to a company in India", and as a result,

state employees are being informed that personal information may have been compromised. More than 100,000 people may be affected through the subcontracting error, although no identity fraud has been blamed on the situation as yet.

More information can be found at :

http://www.computerworld.com/securitytopics/security/story/0,10801,109938,00.html

Astalavista's comments :

So what's the bottom line? Keep up a call center and pray you don't forget yourself and let them talk to your most valuable clients, or outsource, or be naïve and outsource your entire HR management to cut costs? No matter how financially sound your business might be, at the bottom line it's the qualified, experienced, or the HR with attitude type of characters that keep the company growing. There have been numerous reported cases of security breaches involving personal information, or other scams, which doesn't mean that the rest of the companies are using exactly the same practices – what happened in here is the result of a wrong choice while choosing the third-party, and the decision to outsource HR at the very beginning. Trust is vital between partners, and so is synergetic relationship, just don't forget to do your best when choosing the parties.

[**TROJAN EXTORTION BLOCKED BY E-GOLD**]

E-Gold, a company offering digital currency backed by gold, says the creators of the Cryzip trojan did not profit from their cyber extortion. Cryzip encrypted files on infected computers and directed users to pay a ransom of $300 using E-Gold if they wanted the keys to get their data back. E-Gold says its own review process detected the multiple accounts associated with Cryzip, found them suspect, and blocked all payments to those accounts. The spread of Cryzip has been hard to track, since it is spreading slowly to avoid detection by antivirus companies. E-Gold says it cooperates with all legal requests for account data and does not want to be known as a tool for racketeering and other criminal behavior.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?NewsID=5577

Astalavista's comments :

Cryptoviral extortions or ransomware are an attractive concept from the attacker's points of view. Yet the most visible problems for it have always been the generally weak encryption algorithms used, as well as successfully enforcing the victim to pay the ransom, even wire it. Segmentation is indeed important, and I bet that these will also get very popular through localization or directly targeting a specific country(use of language). Until the malicious attackers figure out how to exploit the momentum, include self-destruction routines for those not complying (black humor), the end user is safe given recent non-infected backups are available, or their AV vendor's quite response on decrypting the weak algorithms.

[**INTERNET "CLOAKING" EMERGES AS NEW WEB SECURITY THREAT**]

Speaking at the FOSE 2006 trade show, Lance Cottrell, founder and chief scientist at Anonymizer of San Diego, reported that terrorists are beginning to "cloak" their websites to hide sensitive information from law enforcement. Terrorist websites are blocking traffic from North America or from IP addresses from English-speaking countries. They are also using the websites for counterintelligence; a federal agent posing as a terrorist sympathizer can be fed false information so terrorists can pinpoint leaks in their communications. Terrorists can also set up their computers to use a specific operating system and browser configuration; website visitors with a different configuration would be identified as law enforcement and targeted for cyberattack. Further, terrorists could watch how an investigator browses a website to see what sort of intelligence he/she is seeking. Cottrell argued that anonymizing technology, such as that sold by Anonymizer, could help law enforcement cover their own tracks when investigating terrorists.

More information can be found at :

http://www.gcn.com/online/vol1_no1/40075-1.html

Astalavista's comments :

The concept is very trendy, indeed, and with the ability to cloak yourself and mix with the local traffic of a country, might provide with an IP based "caller ID" so to speak. When it comes to the Intelligence Community, and law enforcement bodies, it is my impression that they still tend to stick to their infrastructure, whether passing through public networks or secret ones, it doesn't get routed through other customers or nodes of Anonymizer. I find IP cloaking important in cases of crawling for malicious/terrorist web sites, namely when doing reconnaissance of competitive intelligence, or plain simple intelligence with limiting the risk of revealing the actual location – greatly depends of course.

[**ISRAELI SOFTWARE FIRM ABONDONS U.S DEAL**]

Israeli software firm Check Point has withdrawn its bid to purchase Sourcefire, maker of the Snort packet sniffer program, after the companies were unable to reach an agreement with the Treasury Department's Committee on Foreign Investments in the United States (CFIUS). US officials were concerned that the acquisition could endanger some classified government systems that use Snort for intrusion detection. Both companies offered restrictions on the deal to allay government concerns, but officials continued to object. Sourcefire says it is prepared to continue operating as an independent company. The deal is one of only 25 CFIUS investigations

launched in more than 1,600 transaction reviews since the committee was formed in 1988.

More info can be found at :

http://www.guardian.co.uk/worldlatest/story/0,,-5707949,00.html

Astalavista's comments :

This is a rather ironical decline, I mean on the majority of occasions the U.S is sharing technologies with temporary partners, to later have to investigate that type of deals. Check Point is the market leader in perimeter based defense and a possible acquisition with SNORT would have been the logical development, still the U.S felt endangered out of having the free and open-source SNORT under Israeli's control. What kind of control they have in mind is rather unclear, but it's a clear indication of the U.S's espionage and national security concerns, rather a protectionist sentiments. Hint : SNORT has a deep roots within military and government networks, but it's so open source than you wouldn't need to acquire snort to execute a system call whatsoever, would it?

[**FRSIRT PUTS EXPLOITS UP FO SALE**]

The French Security Incident Response Team (FrSIRT), formerly known as K-Otik, has announced plans to sell exploits and proof-of-concept exploit code through its subscription-based Vulnerability Notification Service (VNS). FrSIRT describes itself as a "trusted center for the collection and dissemination of information related to network threats, vulnerabilities, exploits and incidents" but many software vendors accuse the organization of irresponsible disclosure. the FrSIRT VNS will offer real-time monitoring and alerts through e-mail, XML feeds, and a web portal. Pricing will vary based on the number of users. Code audits and vulnerability information are becoming profitable markets; iDefense and Tipping Point already have programs to purchase the rights to vulnerability data from independent researchers.

More information can be found at :

http://www.eweek.com/article2/0,1895,1938511,00.asp

Astalavista's comments :

The big news this month, FrSIRT is putting not "its" exploits database under closed doors, but the one acquired through submissions or aggregation from various places. Exploits are handy when doing penetration testing, the way they are handy for malicious attackers, but I'm totally missing the point of their service given how vulnerabilities turned into a commodity in today's Metasploit world. Vulnerability notification works fine given there's a "reported" vulnerability somewhere, when there isn't, it's just a reactive approach to tackle a known threat.

[**MICROSOFT CREATES PUBLIC BUG DATABASE FOR IE**]

Microsoft is for the first time encouraging people to give public feedback on Internet Explorer, with the creation of a bug database for the next version of its browser, the IE 7 beta. The company admitted that customers have often asked why it doesn't have a public

bug database, something that is standard practice for open-source projects such as Mozilla's Firefox browser. "Many customers have asked us about having a better way to enter IE bugs. It is asked, 'Why don't you have Bugzilla like Firefox or other groups do?' We haven't always had a good answer, except it is something that the IE team has never done before," Al Billings, a member of the IE project team, wrote in a Microsoft blog Friday. Security bugs and problems with earlier versions of IE should not be logged in the database, Billings said.

More information is available at :

http://news.com.com/2100-1012_3-6054198.html

Astalavista's comments :

Ground breaking, you can easily forget the hundreds of vulnerabilities that ALL previous versions of IE faced so far, but couldn't take the time and effort to keep track of them – it ultimately reflects your commitment to deal with them. The bugs and problems are already logged and have been commented on as far as you can remember yourself using IE. Ever heard of http://elsenot.com/, did they? Great initiative, but the way Microsoft are currently centering on starting a new era in security with their Vista release, the now forgotten Windows is the de-facto OS and the most obvious infection vector for malicious attackers, before you build something new, deal with the past.

[**ROOTKIT WITHDRAWN FROM SALE**]

"holy_father", has announced that he will stop selling his Hacker Defender rootkit, one of the most popular rootkits in the world. Hacker Defender modifies several Windows and Native API functions in order to hide files and processes from other applications. holy_father offered two version of Hacker Defender, a free version and a paid version with more features. holy_father says he did not develop Hacker Defender to defend hackers, but to spur the security industry to develop better technologies to counter rootkit threats. holy_father's decision will not likely affect use of the rootkit, which is available as open source.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?NewsID=5496

Astalavista's comments :

Open source malware is an emerging concept, that's resulting in a great deal of Botnet families coming from well known source code packages, Agobot and SDBot among the most popular ones. Open source has pros and cons, the way malware coders can achieve cut'n'paste rootkits implementation, the same way AV vendors can look deep into providing proactive protecting to their customers. Heuristics used to be a popular term back in the old days, whereas things have greatly changed and there're new benchmarks to compete against, anti virus signatures are definitely not a competitive factor anymore, but the response time to new pieces of malware – open source ruins the whole effect.

[DNS SERVERS HIT BY MORE DENIAL-OF-SERVICE ATTACKS]

Network Solutions, a domain-name registrar, has been targeted with a denial-of-service attack, "resulting in a brief performance degradation for customers". This type of attack, "relatively rare until now" can be critical as there is potential to affect many websites through targeting only one. The attack against Network Solution closely follows a similar attack against domain name registrar Joker.com.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?NewsID=5668

Astalavista's comments :

Among the biggest insecurities of the Internet is the current DNS system, one that is totally incapable of defending itself given the clear-text communication and concept flaws – but it's the one we use and cannot use the Web if we were to use domains not IP addresses only. DNS reflection attacks are nothing new, and people are obviously experimenting, still no one would ever want to bring down the Internet, or actually make it invisible in such a way. Can digital extortion still be an option here, or I'm just brainstorming on a worst case scenario?

More info on the attacks can be found here as well :
http://www.techworld.com/security/news/index.cfm?NewsID=5586

[POLICE DATA ON 4,400 UPLOADED VIA WINNY]

Police in Ehime prefecture in Japan have announced that sensitive data on 4,400 people was accidentally uploaded to the Internet through the Winny peer-to-peer (P2P) file sharing application. The information includes records on suspects, victims, and investigation informants. The oldest leaked datum dated back to 1984. The police will apologize to those affected by the leak and offer a free telephone consultation. The police are asking web hosts and managers of bulletin board systems to remove the data if they find it on their websites. The Ehime announcement follows a similar incident in Okayama prefecture revealed earlier in the month, which involved the data of 1,500 suspects and victims.

More information can be found at :

http://www.yomiuri.co.jp/dy/national/20060321TDY02008.htm

Astalavista's comments :

Several thoughts, why was the info available unencrypted given its sensitivity, and now that this is public (probably read by a third-party that hopefully cannot take advantage of it), how would they deal with the situation, actually protect the leaked people's data – informants are to be worried, and such events could provoke major scandals. The only fact protecting government or police entities from these increasing P2P sensitive data leaks is how

average people come across them, but what if they were to take advantage of the information?

[STATE SEIZES NEWSPAPER'S HARD DRIVES IN LEAK PROBE]

The Pennsylvania Attorney General's Office has seized four hard drives from the newsroom of the Intelligencer Journal of Lancaster in a grand jury probe. The state Supreme Court rejected the Intelligencer Journal's challenge to the subpoena, and the Attorney General's office refused the newspaper's offer to allow investigators to use the computer to find the information they seek in a less intrusive manner. The investigation seeks to determine whether Lancaster Coroner G. Gary Kirchner gave reporters his password to a restricted law enforcement site. The newspaper warns that the seizure could have a "chilling effect on newsgathering", as sources would be less likely to trust reporters if they believe the state can seize data from newspapers at will.

More information can be found at :

http://www.yorkdispatch.com/pennsylvania/ci_3608667

Astalavista's comments :

A lot of commentaries followed on this case, I think they were basically looking for a reason to go in-depth into possible government/military sources leaking information – we've witnessed quite some cases recently. And if they didn't find any sign of such evidence, it would have successfully figured out all the private correspondence, and contacts of the journalists in question – enough on free speech.

[03] **Astalavista Recommended Tools**

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

" **BURP SUITE V1.0** "

Burp suite is an integrated platform for attacking web applications. It contains all of the burp tools (proxy, spider, intruder and repeater) with numerous interfaces between them designed to facilitate and speed up the process of attacking a web application. All plugins share the same robust framework for handling HTTP requests, authentication, downstream proxies, logging, alerting and extensibility. Burp suite allows an attacker to combine manual and automated techniques to enumerate, analyse, attack and exploit web applications. The various burp tools work together effectively to share information

and allow findings identified within one tool to form the basis of an attack using another.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6483

" **ZEPPO- I386 ROOTKIT DETECTION TOOL FOR LINUX** "

Zeppoo is a tool that detects rootkits on i386 Linux. It also detects hidden tasks, modules, syscalls, corrupted symbols and hidden connections.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6463

" **SECURE FTP FACTORY V5.5** "

Secure FTP Factory is a set of Java classes for communicating with FTP servers using the FTP, SFTP (FTP over SSH), and FTPS (FTP over SSL) protocols. The components offer complete FTP functionality, including the ability to transfer files, rename files, delete files, create directories, transfer directories recursively, and more.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6450

" **DARIK'S BOOT AND NUKE (CDR/CDRW VERSION)** "

Darik's Boot and Nuke ("DBAN") is a self-contained boot floppy that securely wipes the hard disks of most computers. DBAN will automatically and completely delete the contents of any hard disk that it can detect, which makes it an appropriate utility for bulk or emergency data destruction. Please clearly label your DBAN boot media because it is dangerous.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6437

" **SQUTUN V1.1** "

SquTUN (pronounced "skew-ton") creates an AES-encrypted, SHA-1 authenticated UDP tunnel over which IP packets received from a TUN interface are encapsulated and transmitted. It is intended to replace installations that are currently using CIPE for point-to-point VPN's. Unlike CIPE, SquTUN doesn't require a custom kernel module. Furthermore, SquTUN's implementation and interface are much less complex, leading to greater confidence in its correctness.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6427

" **MICROSOFT THREAT ANALYSIS AND MODELING V2.0 BETA2** "

Microsoft Threat Analysis & Modeling tool allows non-security subject matter experts to enter already known information including business requirements and application architecture which is then used to produce a feature-rich threat model. Along with automatically identifying threats, the tool can produce valuable security artifacts such as: - Data access

control matrix - Component access control matrix - Subject-object matrix - Data Flow - Call Flow - Trust Flow - Attack Surface – Focused reports

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6382

" **SECURITY CLOAK** "

Allows you to spoof your OS in order to fool passive fingerprinting techniques (twenty different OSs are supported). Also helps prevent information leakage via timestamp options.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6372

" **QEMU-PUPPY** "

QEMU-Puppy is an OS and a set of applications on a USB memory stick. This OS can be booted natively or on top of another already installed OS. Just borrow a PC, boot your own environment, and return the PC unaffected.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6360

" **PHP OPENID V1.0.0** "

The PHP OpenID library implements the OpenID decentralized identity system. It can be used to enable single-sign-on across Web applications. The library includes examples and different options for storage back-ends.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6352

" **CREDENCE 1.4** "

Credence is a tool for combating spam and pollution in filesharing networks. It lets you vote on files in the network, analyzes the votes of your peers so that you can avoid polluted files, and automatically identifies the voters in the network that are most credible and useful. It is built as an extension to LimeWire, running on the Gnutella filesharing network.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6331

[04] **Astalavista Recommended Papers**

" **STEALING AL-QA'IDA'S PLAYBOOK** "

Our authors suggest ways to address this significant shortfall. Not only do they attempt to answer the who and what sort of questions in plain language; they also outline a highly original method for discerning the answers to these questions that has, up to now, been ignored or poorly used. One of the best places to look for information regarding the strengths and weaknesses of the jihadi movement,

Brachman and McCants argue, is in texts written by jihadi ideologues.* Of course, a number of analysts inside and outside the U.S. government read texts like these for insight into al-Qa`ida's strategic thinking. But it has been my experience that many of the most useful texts have not received attention.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6319

" **SECURITY CONSIDERATIONS FOR GOOGLE DESKTOP** "

Desktop search represents an emerging (Q1 2006) market segment designed to make searching your desktop as easy as it is to search the Internet. This paper examines, from a security perspective, one entry in this product space: Google Desktop. The goal is to provide information that can be leveraged by the University community to perform a more thorough evaluation or a more secure deployment of Google Desktop.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6336

" **PROTECTING BROWSER STATE FROM WEB PRIVACY ATTACKS** "

Through a variety of means, including a range of browser cache methods and inspecting the color of a visited hyper- link, client-side browser state can be exploited to track users against their wishes. This tracking is possible because per- sistent, client-side browser state is not properly partitioned on per-site basis in current browsers. We address this prob- lem by reopening the general notion of a "same-origin" policy and implementing two browser extensions that enforce this policy on the browser cache and visited links.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6349

" **SUBVIRT – IMPLEMENTING MALWARE WITH VIRTUAL MACHINES** "

We evaluate a new type of malicious software that gains qualitatively more control over a system. This new type of malware, which we call a virtual-machine based rootkit (VMBR), installs a virtual-machine monitor underneath an existing operating system and hoists the original operating system into a virtual machine. Virtual-machine based rootkits are hard to detect and remove because their state cannot be accessed by software running in the target system.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6365

" **ARGOS – AN EMULATOR FOR CAPTURING ZERO-DAY ATTACKS** "

Argos is a full and secure system emulator designed for use in Honeypots. It is based on QEMU, an open source processor emulator that uses dynamic translation to achieve a fairly good emulation speed.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6394

" **RFID VIRUSES AND WORMS OR IS YOUR CAT INFECTED WITH A COMPUTER VIRUS?** "

While we have some hesitation in giving the "bad guys" precise information on how to infect RFID tags, it has been our experience that when talking to people in charge of RFID systems, they often dismiss security concerns as academic, unrealistic, and unworthy of spending any money on countering, as these threats are merely "theoretical." By making code for RFID "malware" publicly available, we hope to convince them that the problem is serious and had better be dealt with, and fast. It is a lot better to lock the barn door while the prize race horse is still inside than to deal with the consequences of not doing so afterwards.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6421

" **CONTEMPORARY APPROACHES TO PROJECT RISK MANAGEMENT:ASSESSMENT&RECOMMENDATIONS** "

In order to manage risks, we have to define what risk is. From the OXFORD dictionary, risk is defined as 'possibility of meeting danger or suffering harm'. With this definition, it makes us feel that there is a need to avoid risks especially when managing projects. But unfortunately, like what all risk managers know, risk can never be avoided BUT it can be reduced and that is what management wants to hear. And unfortunately again, risks are often ignored. By abolishing constraints and reducing ambiguities, risk can be minimised to an acceptable level. Project risks may be accidentally overlooked by those who just do not have time to look into it or those who want to avoid serious delays.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6414

" **DETECTING BOTNETS USING A LOW INTERACTION HONEYPOT** "

This paper describes a simple honeypot using PHP and emulating several vulnerabilities in Mambo and Awstats. We show the mechanism used to 'compromise' the server and to download further malware. This honeypot is 'fail-safe' in that when left unattended, the default action is to do nothing – though if the operator is present, exploitation attempts can be investigated. IP addresses and other details have been obfuscated in this version.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6454

" **DNS AMPLIFICATION ATTACKS** "

This paper outlines a Distributed Denial of Service (DDoS) attack which abuses open recursive Domain Name System (DNS) name servers using spoofed UDP packets. Our study is based on packet captures and logs from attacks reported to have a volume of 2.8Gbps. We study this data in order to further understand the basics of the reported recursive name server amplification attacks which are

also known as DNS amplification or DNS reflector attacks. One of the networks under attack, Sharktech, indicated some attacks have reached as high as 10Gbps and used as many as 140,000 exploited name servers. In addition to the increase in the response packet size, the large UDP packets create IP protocol fragments. Several other responses also contribute to the overall effectiveness of these attacks.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6448

" **THE TOP 10 INFORMATION SECURITY MYTHS** "

When it comes to information security, there's a lot of popular wisdom available, but much of it is unfounded and won't necessarily improve your organization's security. Only by cutting through the hype to separate reality from myth can IT professionals help take their enterprises to the next level. Here are 10 network security myths that bear further examination.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6493

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

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

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

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

check out the special discounts!!

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

What is Astalavista.net all about?

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

Among the many other features of the portal are :

- Over **7.22 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates

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

[06] Site of the month

Secure Coding

http://www.cert.org/secure-coding/

This area describes our efforts toward developing secure coding practices that software producers can use to avoid vulnerabilities in new software.

[07] Tool of the month

VMware Virtual Machine Importer 2.0 Beta Program

http://www.vmware.com/products/beta/vmimporter/

VMware is proud to announce the Beta availability of Virtual Machine Importer 2.0, the latest desktop utility for IT professionals and software developers/testers working with virtual machines. VMware Virtual Machine Importer (VMI) is a freely available, stand-alone utility to import virtual machines from different source formats into several VMware product destinations

[08] Paper of the month

Able Danger and Intelligence Information Sharing

http://www.fas.org/irp/congress/2005_hr/shrg109-311.html

Congressional hearings, September, 2005.

[09] Astalavista Security Toolbox DVD v2.0 – Download version available!

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

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

convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=153

[10] **Enterprise Security Issues**

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

- **Establishing an internal security awareness culture – the basics -**

In this brief article I'll discuss various key points on the usefulness and basics of introducing an internal security awareness culture. Moreover, we'll also discuss how the lack of such is capable of influencing your organization in the long term.

What's the current situation?

Companies are getting more and more obsessed with perimeter based security solutions, some are actually discovering the concept with the introduction of a full-time E-business activities altogether, clearly missing the basic point that security is about applications, processes, and yes, people. These very same people are the ones sitting behind your IT infrastructure, configuring or directly taking advantage of it for their daily activities, that turns all of them into a possible attack vectors for malicious attackers. While organizations, and hopefully yours is among them, are getting more training-conscious, in the last issue of the Astalavista's Security Newsletter we covered the topic of security training and emphasized on prioritizing the people that mostly need it, given of course you somehow manage to control the environment of them as well as the others.

Why do we need such a culture?

Mostly because the risk exposure to security threats facing your organization should be shared among everyone functioning in it, and everyone is to a certain extend responsible. Employees even trying to forward sensitive data outside the organization, or impulsively clicking on every link received through email or IM aren't an example of that. Positioning and actually executing a sound strategy must turn into a commitment if you are to stay away of contingency plans, but stick to security investments only. Moreover, your employees will hopefully understand they must play a role in the process as well, which is what you're trying to achieve. Google for instance, has been the perfect case study on establishing a powerful internal culture – shared goals and level of commitment.

How to achieve it?

Start with setting clear and easily measurable objectives, but keep in mind that not all of them should be quantitative, that is, leave some space to actually figure out how are they progressing going beyond surveys, do they witness the change and put some economic thoughts into the problem. Evaluating the current situation is perhaps the first step you could take. How often do employees get spam and how often do they actually click on the links? Are there any currently enforced security policies that is access control, removable media, or for instance, host's integrity preserved? So, when you have evaluated the current situation, set clear and easily to measure both qualitative and quantitative objectives, its

- Emphasize on clear and common goals
- Don't overload everyone with security posters and creative it's like a Bunker, it's a workplace
- Set progress milestones
- Get their attention, make it personal
- Keep it both formal and informal

What if we don't?

Simple - you will continue living in the illusion that security is all about technologies, it isn't, technology is only an enabler, not an aim, what's left the panacea of security. Security is everyone's responsibility. For systematic approach on security awareness programs – not culture – you can look further at :

http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

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

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

- How do I figure out who's attacking me? –

In this brief article we'll review important things to keep in mind whenever you want to trace the host supposedly attacking you, and try to emphasize on should you be doing just that instead of putting security measures in place.

The age-old question "Who's attacking me" seems to be still often asked these days. According the FBI's 2005 Computer Crime Survey a great deal of companies are Actually trying to figure this out, and still couldn't which leaves you, the end user in a very interesting position. Port scan attempts, floods, alerts or anything else your security software generates is often a cause for alarm, that's they way it should be, what you shouldn't be actually concerned about is who's attacking or, as it's not "personal", you're a part of the Internet, you're discoverable to a certain extend. Whether you're received a suspicious email with malware of phishing, a personal threat, it always comes down to looking at headers, and reporting them, and of course they're spoofed, or actually have real IP information while sent through

That said, this again leaves the question unanswered – the hosts your see attacking are on the majority of occasions infected hosts around the world looking for more victims, forgotten zombies of old malware trying to continue their lifecycle, and tracing these – you wouldn't be able to change the world alone, but together we can still make a distributed judgment :)

Go through the following resources on :

Tracing email messages
http://gandalf.home.digital.net/spamfaq.html

Report a phishing attack
http://www.antiphishing.org/report_phishing.html

Report child pornography
http://isc.sans.org/diary.php?storyid=1193

Submit your firewall logs here
http://dshield.org/

Report a botnet:
http://www.shadowserver.org/

Free online network tools
http://www.dnsstuff.com/

[12] Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **Roberto Preatoni,** a key member of the Zone-H's team http://www.zone-h.org

Your comments are welcome at security@astalavista.net

Interview with Roberto Preatoni, http://www.zone-h.org

Astalavista : Hi Roberto, would you, please, introduce yourself to our readers and tell us something more about your experience when it comes to information security and information warfare?

Roberto : My full name is Roberto Preatoni, I'm 39 and I am Italian even though I spent the last third of my life outside my home country, the last two years specifically globetrotting for hacker conferences and hacking seminars.

I started, as almost everyone of my age with the Commodore 64 microcomputer, the best machine ever built to play hacker games (I apology with the

ZX Spectrum fans...). I started to be interested in information warfare as soon as Internet became popular, as it was clear to me that the next level of warfare *had to be* conducted on the digital level.

Astalavista : To all the folks out there that haven't heard of Zone-H, or know nothing about its aim, could you tell us what is Zone-H all about and how it has evolved during the years since it started?

Roberto : Good question. We decided to open zone-h as we saw that the other mirror website were slowly slowly dying. A mirror archive such zone-h is necessary as it shows to the public the trends and the quality of the attacks (server side). As by today we receive notifications of 2,000/3,000 defacements, on a daily base.

One of the common mistake people are doing is to judge the "defacement" a lame crime therefore judging indirectly also the mirror websites such zone-h. To all those who are thinking the same let me tell that the defacement is just a choice, behind that there are techniques that often are the same of more serious cybercrimes. Last but not least, Zone-H evolved from its original scope into something that gives to the community a lot more than news about defacements. We published a lot of self-produced advisories, we publish free hacker comics, free music tracks and we publish self written news and commentaries about hot topics.

Astalavista : What is Zone-H's team up to these days, and what are some of your future project development plans as well?

Roberto : Zone-H has grown from a simple home-made project to an international project embracing a 50 strong member crew and 4 different localized versions of the website. Soon a new version of Zone-H will be up and running, it will be more focused on warfare and geopolitic issues, a few international names in journalism (not only IT) already agreed to contribute with exclusive contents. We are also enlarging the sphere of activity of our Hands on Hacking training which is the only source of income to maintain Zone-H which is an extremely expensive "hobby" in money and time (ask to Alldas and Attrition about it...)

Astalavista : To many, Zone-H's contradictive defacement archive act as a incentive for script kiddies to keep on defacing and work on their ego knowing that the "made it to Zone-H", while it can be argued that it's the only early warning system for detecting hacktivism tensions around these days. What are your comments on your digital attacks contribution, and how do you perceive its usefulness?

Roberto : First of all, mirror websites appeared after the first Defacements happened, this should answer it all. But to this question (which is fully legit) I answer with this link:

http://www.fbi.gov/wanted.htm

The question is: is the FBI eligible to unethical conduct given that they are giving space to criminals and report their crimes to the public? Is CNN guilty of conspiracy in regards of the Sept. 11th facts, given that they showed live Bin Laden's bombing attacks?
I also want to answer posting this information: 8129 early warning subscribers (http://www.zone-h.org/en/warnlist). This is the number of the subscribers of zone-h's free early warning service. Given that a lot of websites get compromised not at the homepage level (often the cracker is creating a www.site.com/hacked subpage) how would the "normal" administrator be able to understand that the site was hacked given that the homepage wasn't substituted? The answer can be only in a service like the one zone-h is giving. In this view, we are receiving a lot of emails from thankful administrators whom got to know about their site being compromised ONLY thanks to zone-h prompt report. But yes, we also get some hate-mails as well, not too many fortunately.

Astalavista : Compared to five years ago, you would rarely see someone hacking military and government networks while looking for evidence of UFO contacts. These days, as it's all about the money. Can we still talk about hacktivism in today's profit-driven underground, what is the current situation and what are your comments on some possible future trends on hacktivism, cyber-crime and cyberterrorism?

Roberto : I am personally confident that hacktivists and hacktivism will never disappear as the power and the opportunities given by the use of the Internet for effective cyber-protests will be more and more appealing. As you said, the current underground is profit driven, we witness every day skilled people turning to the profit oriented side of the hacking but I guess this is due to the fact that where is business, there is criminality and Internet *is* business.

I would like to point out a psychological evaluation though of such fact. Interned related crimes (defacements included) are committed by a criminal hackers who are probably sitting in a cozy armchair located in their living room, having a bottle of beer in their right hand and a cigarette in the left one and acting through a bunch of hops between strategic shells. What I mean is that hacking doesn't carry along with it the "thrill" of the traditional crimes like robbing a bank. Thus, the threshold of the perceived risk is very low, this is why we should expect an overall raise in the Internet related crimes.

Astalavista : Cyberterrorism is a sexy threat these days, it provokes the imagination, and it can be argued that the speculation has a favorable effect on increasing intelligence cyberterrorism as a platform for communication.

How real do you think the threat is in respect to communication, recruitment, propaganda, fund-raising, and research?

Roberto : Well, I just published a book related to cyberterrorism and cyberwarfare, I don't want to abuse of this interview to sell more copies so I won't name the title of it but I told it just because I wanted to point out the fact that I am very sensible to the matter. We should not consider the cyberterrorism as the way to cause directly death and destruction like shutting down the SCADA system of a nuclear powerplant but there are serious evidence of the use of the Internet as a very cheap (and more effective) way to substitute the traditional Command and Control centers needed to plan terrorist activities.

The Internet has been used to collect money (fund raising campaigns) to sustain terrorists activities. I personally recall a website that was collecting the money to be used to maintain the families of the suicide bombers of the Al Aqsa martyr brigades. There are still websites that are collecting the volunteers for the martyrdom. Three Bin Laden's foundations have been funded for a long time by US's and private money to sustain campaign in favour of the Islamic culture while the same money were actually sent as a contribution of the Afghani resistance movement of the mujahedeens.

I would like also to say that the fact that the terrorists are using Internet is wrongly perceived by the media as something exceptional. Should also be considered exceptional the fact that also we are using the Internet? No, it's absolutely normal as it became a common mean of communication and an exceptional media for political propaganda. Beheading movies included.

Finally I want to point out that in one of the Al Qaeda manuals (at least so considered by the English MI6 services that translated it after it was seized by an English police raid in an apartment belonging to a suspect terrorist) there is an entire chapter related to Internet and cryptography.

But again, we shouldn't be too much surprised of that as those manuals, as most of the presumed Al Qaeda terrorist manual are a mere translation of traditional CIA manuals with an integration of ad-hoc Islamic concepts...

Astalavista : What is your attitude on the current state of commercializing vulnerability research, and what would be the most suitable model satisfying vendors, researchers and end users at the bottom line?

Roberto : I have an idea on which I am working, allow me some time to show it to the world... ;)

Astalavista : If you were to name the most worth-mentioning cases in respect to hactivism tensions, perhaps government backed one as well, for the last several years, which ones would you name?

Roberto : From my own direct experience, I would name the Chinese government sponsored round of hacking attempts and trojans that westerns servers and mail receivers enjoyed in the last quarter (one of the zone-h co-founders is currently the administrators of some of the EU servers in Bruxelles, so we have first hand evidences of it . I'd also like to name the Islamic cyber-protest for the Prophet Mohammed cartoons issue That led to the defacements of tenths of thousands of western servers, several of them Danish.

Finally in the first episode of the Hero-Z comics (Network Conspiracy http://hero-z.org/modules.php?name=Downloads&d_op=viewdownload&cid=35) we talked, much before the Electronic Frontier Foundation did, about embedded spying devices in the electronic components of everybody's computers. Science fiction or blatant vision? Up to you the judgment...

Astalavista : In conclusion, and going out of the security world, what are among the other things that motivate you enough to mention them as extracurricular activities?

Roberto : Well, the production of free comics and the related free music tracks (I saw some of them on Astalavista archives) makes me particularly proud ;) In my free time I work also on a new book about cyberwarfare and I am also a professor for an Italian University about... Internet abuses in the University's IT Security fundamentals course.

Astalavista : Thanks for your time, and keep up the good work!!

[13] IT/Security Sites Review

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

-
SplunkBase
-

http://www.splunk.com/base

Tag your logs!

-
10 Favorite Firefox Extensions
-
http://farrokhi.net/blog/archives/000572.html

Security/Privacy related firefox extensions for you

-

Programming language inventor or serial killer?

-

http://www.malevole.com/mv/misc/killerquiz/

Can you tell a coder from a cannibal?

-

The Web Hacking Incidents Database

-

http://www.webappsec.org/projects/whid/

The web hacking incident database (WHID) is a Web Application Security Consortium project dedicated to maintaining a list of web applications related security incidents.

-

The PHP Security Consortium

-

http://phpsec.org/

Founded in January 2005, the PHP Security Consortium (PHPSC) is an international group of PHP experts dedicated to promoting secure programming practices within the PHP community. Members of the PHPSC seek to educate PHP developers about security through a variety of resources, including documentation, tools, and standards.