Astalavista Group Security Newsletter
Issue 24 - 31 December 2005
http://www.astalavista.com/
security@astalavista.net

[01] **Introduction**

Dear readers,

Merry Christmas, and Happy New 2006!!

Issue 24 of the Astalavista Security Newsletter has just turned two years!!

During each and every month of 2005, we provided you with a very resourceful and up-to-date overview of the latest developments in the security world. We have also including hundreds of new additions to our **Security Directory**, and have restored the tradition of the **Geeky Photos** section, whose contributions are amazingly creative!

We also had the chance to interview key people whose projects and initiatives motivate the rest of world, that as a matter of fact, is directly, or indirectly benefiting out of them. To sum up, we had chats with key figures such as :

SnakeByte - http://www.snake-basket.de/
Björn Andreasson - http://www.warindustries.com/
Bruce - http://www.dallascon.com/
Nikolay Nedyalkov - http://www.iseca.org/
Roman Polesek - http://www.hakin9.org/en/
John Young - http://www.cryptome.org/
Eric Goldman - http://www.ericgoldman.org/
Robert - http://www.cgisecurity.com/
Johannes B. Ullrich - http://isc.sans.org/
Daniel Brandt - http://google-watch.org/
David Endler - http://www.tippingpoint.com/

Folks, keep up the good work!!

What's else to note is that during 2005, **Astalavista.com** attracted the attention of the W32.Ahker worm family, and was blocked to infected victims, right next to important anti-virus and government sites. That's a gesture, and a result of the hard work, the **Astalavista Team Members** did during the year, namely providing even more knowledge, awareness, and tools on important security issues.

Astalavista.NET v2.0 went live, and we are sure you have had the chance to take a look at all of its new features though the screenshots accessible at the site.

Have a productive, visionary and inspiring 2006, and make sure you think what you wish for, cause it can easily become a reality!

Enough wisdom from us, have something to say?!

Drop us a line at security@astalavista.net

In Issue 24 of the Astalavista Security Newsletter, you'll find :

- significant security events during the month, and associated commentaries
- Part 2 of our "**Breaking through security myths**" article
- The threats posed by P2P software for end users
- and an interview with **Vladimir (3APA3A)** – http://www.security.nnov.ru/

Enjoy and share your comments!!

Check out the Geeky Photos section :

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

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

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

Previous issues of Astalavista Security Newsletter can be found at:

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

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader – Yordanka Ilieva
danny@astalavista.net

[02] **Security News**

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

----

[**HACKERS STEAL CUSTOMER DATA FROM GAMING COMPANY**]

White Wolf Publishing, maker of such popular role-playing games as "World of Darkness" and "Vampire: The Requiem," shut down its online store for four days after hackers sent a message saying they had penetrated the company's defenses, stealing e-mail addresses, user names and encrypted passwords, and demanding money for

not posting the data on the web. When White Wolf refused to pay, the hackers emailed individual White Wolf customers "to tell them they can buy the stolen information for $10." The hackers exploited a flaw in White Wolf's security software, which they have fixed. The company advised users to change their passwords but does not believe any credit card information was stolen.
The FBI is investigating.

More information can be found at :

http://news.com.com/Hackers+steal+customer+data+from+gaming+company/2100-7349_3-6001566.html?tag=cd.lede

Astalavista's comments :

Blackmailing over the Net is a growing practice, courtesy of the (Cyber) Mafia, or yet another guy "in the wild" trying to make quick buck. What should be noted in this case, the the clear financial ambition behind the hack, whereas, a theft of intellectual property such as upcoming releases plans, strategies, even code, could have let to a much more serious scenario. Trying to extort money of the organization whose data has been stolen, indicates the lack of market for such kind of "goods". My point is that, in the very near future, we would witness a market especially for that kind of things. A professional, or let's just say, a visionary organization would never pay, as it will face the risk of being extorted twice, and while that's common sense, a great deal of companies actively comply in order to prevent the loss of soft dollars, such as PR fiasco's, loss of reputation etc. Look for any other alternatives, besides simply paying and thinking the trend will go it, as it wouldn't!

[**HACKERS KNOCKS TV CHANNEL OFF AIR**]

A hacker has managed to take the Kremlin-sponsored English-language television channel Russia Today off the air only two days after its launch. Margarita Simonyan, Russia Today's editor in chief, says the channel went off the air after an attempted intrusion infected the channel's systems with malware, and is unable to say when the channel will begin broadcasting again. Russia Today was created in response to what the Kremlin views as "unfairly critical" reporting in foreign media.

More information can be found at :

http://www.smh.com.au/news/breaking/hacker-knocks-tv-channel-off-air/2005/12/13/1134236031398.html

Astalavista's comments :

Information warfare to some, or a pissed of on the initiative native citizen?! I feel it's the second, and that's a story worth mentioning next to the fact that the U.S.S.R and its ex-republics, were perhaps the first, and primary source of political propaganda though malware -- obvious reasons, trying to achieve free speech. To me, this case clearly indicates two possibilities, *an outsider that did reconnaissance for the purpose, or an insider that could have made it easier to accomplish. In both cases, it's obvious knowledge individuals always find a way to express an opinion on their own!*

[**PORT SCANS DON'T ALWAYS PRECEDE HACKS**]

According to a report from the University of Maryland, only 5% of port scans are followed by a cyber attack. Many security professional view port scans as a sign of an impending attack. The study gathered evidence over 48 days from two honeypots; only 28 of 760 attacking IP addresses conducted a port scan. However, 21% of attacks were launched with a scan for a particular vulnerability. The SANS Internet Storm Center's Johannes Ullrich finds the study sound, but the analysis too simplistic, arguing that it is more important to examine the content of a scan rather than the number of packets to determine whether it is a port scan. The methodology could have led the researchers to mistake attacks for port scans.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=4991

Astalavista's comments :

Port scanning greatly evolved during the last couple of years, at least the way I see it. Banner grabbing, passive and active scans, port-knocking etc. got greatly improved as both, acceptance, and development. And with the steadily growing for the past several years rate of released vulnerabilities, vulnerabity scanners started getting a lot of attraction. An organization's network, was no longer perceived as a host from a attacker's point of view. But as a complex E-business system, whose biggest joys are actually it's biggest weaknesses. What used to be a sophisticated open source attacker, bringing on more Raw data, or is Linux or Windows secure, is the today's bored teen with poin'n'click modulation of destructive payload into his GPL malware, sad fact, but that's how I see the reality. I no longer need to know your "opened up default" Windows ports in order to exploit your network is an attitude that's resulting in the huge botnets "assembled" online today.

What I could argue though, is that integrating raw data of the originating IPs of phishing, spam, or malware containing worm, would result in a common fact -- the port scan we got from 666.666.666.666 N days ago, has already sent over 20 phishing, and malware containing emails to us.

Don't get me wrong, port scanning is important, and so is the content of packets, but the "noise" generated by script kiddies and zombies(where's the difference?!) opens up the possibilities

As far as port scanning is concerned, distributed port scanning, even "slow" scanning has been around for ages, and it can be hard to spot. But the network based understanding of port scans has greatly changed these days.

[**EBAY PULLS EXCEL VULNERABILITY AUCTION**]

An auction for "a vulnerability in Microsoft's Excel spreadsheet program" was shut down by eBay, as the online auction site says that "the sale of flaw research violates the site's policy against encouraging illegal activity". The advertised vulnerability, which "could allow a malicious programmer to create an Excel file that could take control of a Windows computer when opened", appears legitimate. Microsoft complained to eBay, resulting in the auction being stopped. eBay explained its decision as, "In general, research can be sold as a product. However, if the research were to violate the law or intellectual property rights then it would not be allowed. " While buying vulnerability research is still considered controversial, some security companies do pay independent flaw finders for information.

More info can be found at :

http://www.theregister.co.uk/2005/12/10/ebay_pulls_excel_vulnerability_auction/

Astalavista's comments :

*It's very exciting to note that in a chat I had with **Dave Endler** from the **ZeroDayInitiative**, we had a discussion on exactly the same market, a week or so before it actually happened. Sometimes, the maturity of the concept it itself prompts you to look for future developments, and the huge growth in reported vulnerabilities, is greatly influenced by the growing number of people capable of doing security vuln. research.*

The blogosphere, and some important commentators don't seem to find the legal reason for removing the auction, and there isn't as a matter of fact! What Ebay reasonably fear is not to end up in the news the way Google did with the Santy worm. Namely acting as a the vehicle for purchasing software vulnerabilities in this case.

In the sense of the article, is purchasing a vulnerability violation of intellectual property law? And if it is, why isn't MS suing everyone posting research on security Mailing lists, or beyond?! In my opinion, there are trying to keep the current full-disclosure central, thus transparent, as if it becomes decentralized(consider the possibilities of e-auctions going beyond Ebay) it would create more trouble for everyone, but the researchers in respect to competitive bids.

[**AIRPORT PASSCODES LEAKED FROM VIRUS-INFECTED PC**]

Japan Airlines has announced that a virus on the computer of one pilot has leaked security passcodes used at 16 airports in Japan and one in Guam. Airline staff typically carry lists similar to the leaked list due to the large number of security passcodes they must use at numerous airports. Twelve airports have already changed their passcodes. Japan Airlines is planning no disciplinary action against the pilot. While airline policies govern downloads of sensitive data to personal computers, airport passcodes are not included in these policies.

More information can be found at :

http://www.infoworld.com/article/05/12/09/HNairportpasscodes_1.html

Astalavista's comments :

Malware, besides spam, is the plague of the Internet. It can reach everyone, and it can get everywhere, including the computers of an airline company, or a military contractor employees. Being paranoid, if such an attack is done on purposely, it could pose a serious risk, and being even more paranoid, if information like this could be forwarded to interested parties. Ensuring that sensitive information doesn't leak out of the network is an important issue to consider. Moreover, setting actual enforcement of policies as your first strategy, and communicating how it's done, and what is still prohibited as your second, is another proven approach.

Several companies that I recently researched take both signatures of sensitive data, or monitor predefined patterns.

Vontu
Reconnex

[**EEYE ENTERS ANTI-VIRUS MARKET**]

eEye will incorporate anti-virus technology into its Blink firewall product. A beta version, to be published early in 2006, will be considered an update and available to all existing customers for free. The Blink intrusion prevention product is designed to "enforce security policies and protect clients from network-based attacks, anti-spyware and phishing attacks". Currently, Blink uses "signature-based" prevention, and the new anti-virus software will use behavior-based analysis to judge whether it is malicious. While "signature-based techniques are still the most widely used form of anti-virus detection", "they are starting to break down because of the massive amount of malicious software in circulation". Behavior-based anti-virus software "is generally not as effective as the signature-based alternatives against known attacks".

More information is available at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=4976

Astalavista's comments :

No, this isn't a vendor-sponsored ad, instead I decided to feature it because the trend deserves a lot of attention. The anti-virus industry has a lot of potential, and we see a lot of new players, serving different market, or geographical segments entering it. What's the fastest way to gather know-how and years of experience in the field, that's an acquisition, and companies you've never heard of an year *ago, are quite a catch for big vendors wanting to cover yet another area in their solutions portfolio.*

My point is that, with the lowest cost of both network and hardware infrastructure ever, you could easily turn your honeyfarm into an automatic malware collector, and generate the above mentioned signatures. Don't reinvent the wheel, license it, or continue bargaining on the fees you're currently paying to have anti virus solution offered as a feature.

What are the implications affecting you, or your organization?

Ensure your technology employs a reputable at lest in respect of years on the market, and innovative approaches solution. Also, have your CSO's or administrator's opinion acting as a leading first-hard indicator. The majority of security appliances providers offer the possibility of multiple anti-virus solutions, that give you a lot of flexibility in case of a vulnerability targeting any of these(happens quite often these days). Mostly, make sure you're not entrusting the continuity of your processes to an unproved "product extension" of your current vendor.

[**FROM PASSWORDS TO "PASSTHOUGHTS"**]

Julie Thorpe, a researcher at Carleton University in Ottawa, suggests it may be possible to develop technology to recognize 'passthoughts', passwords that users will need to only think to access a computer system. Brainwave patterns vary from person to person, allowing their use as a biometric identifier. Users could also use images or childhood memories as passthoughts. However, such a system requires better MMI (mind-machine interface) and proof that users would be able to generate the same thought on demand. Thorpe's research is primarily focused on developing computer interfaces for the paralyzed.

More information can be found at :

http://www.smh.com.au/news/breaking/from-passwords-to-passthoughts/2005/12/14/1134500895603.html

Astalavista's comments :

Users barely control their emotions, what's left for their thoughts. Doing a "mind-recalling" of a passwords, could be achievable, but would recalling a passphrase be possible, most important, practical and efficient enough to be implemented on a large scale? Would future mind-machine or cyberware experiences let us sniff someone else's thoughts, modify them in transfer, and delaying them for doing so count as e retard for instance? :)

Nanotechnologies and malware have too many things in common to mention. The air can be the propagation factor, the mind in itself can be the payload, as a matter of fact, even Hollywood picked up the future of nano viruses etc. too bad I cannot recall the movie.

Still, the geek was doing remote capacity coding for a MegaCorp, and somehow managed to has his brain under malicious "brainware" attack.

[ADOBE MOVING TO MONTHLY SECURITY PATCHES]

Adobe "has decided to follow Microsoft's lead and begin releasing security patches on a predictable monthly basis". The regular updates will begin "within in the next six months and are expected to cover most, if not all, of Adobe's products". Although "most software companies have not moved to this kind of regular patching cycle" some analysts predict that "it is likely to become an industry standard".

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=5010

Astalavista's comments :

That's such a long-term strategy, mainly because no software vendor has accountability for timely or proactive releases of vulnerabilities. And until change isn't made in here, the today's Windows dominated world, two times, where the second is the "windows of opportunity" acting as the main driving factor for security threats. Money incentives count as well. Let's even for a sec. imagine that within half an year they manage to dedicate the time and effort to do it. Than, all of a sudden, an 0day vulnerability would ruin the whole effect, if any.

In this six months timeframe, it would be great if any code auditing, or ensuring timely response to full disclosure is also taken into consideration. Just in between.

[ARE FACELESS BANKS MAKING TROUBLE FOR THEMSELVES]

The "rapid growth of automated banking facilities, such as online banking, telephone banking and now mobile phone banking, is creating a situation where banks are losing touch with their customers and potentially exposing them to fraud". While younger customers continue to call for more mobile banking, research by the Henley Centre shows that increased remote banking is causing banks to lose the "chance to offer their customers tailored advice as well as the opportunity to cross-sell products.

More information can be found at :

http://www.silicon.com/financialservices/0,3800010322,39155194,00.htm

Astalavista's comments :

Do the costs of E-crime outpace the revenues of E-commerce? No, they don't, as if there were we wouldn't be witnessing the birth of Web 2.0, would we? You wouldn't, or perhaps shouldn't expect your customers to pop up at your branch they way they'll do at a Levi's story. And making payments, getting cash, *even wiring over mobile, is a feature we can currently take advantage of on our mobile phones. Getting back to costs mentioned, it would cost a bank or any institution lost employees' productivity doing to performing tasks which are automated, or ones related with hiring extra staff to achieve the objectives desirable. The best cost-effective way(one needed for survival and profitability these days!) is to utilize the number of clients that are currently using the E-services of the bank, and expose them to the rest of your offerings. Engage them, provide them with as many contact points as possible, as some current or potential important customers, wouldn't use email for certain requests. Yet, if you "sense" what they might be up to, treat them in the right way, and direct them further the process of obtaining the necessary information, you'll close a deal. And do it online. I feel the benefits of E-commerce outpace the inevitable insecurities of the current approaches, and would greatly improve with the time.*

[03] **Astalavista Recommended Tools**

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

" THOR – IE DRIVEN TOOL FOR MANUAL WEB APPLICATION TESTING "

Thor is Internet Explorer driven tool for manual web application testing. Both security professionals and testers found it useful while testing web applications. You can control (intercept and change) what web forms submit to web servers, see the source code of the page and/or manipulate cookies.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5691

" WINPOOCH – OPEN SOURCE ANTI-SPYWARE AND TROJAN PROTECTION "

Winpooch is a Windows watchdog, free and open source. Anti spyware and anti trojan, it gives a full protection against local or external attacks by scanning the activity of programs in real time.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5710

" TTYRPLD – KERNEL BASED KEYLOGGER "

ttyrpld is a Kernel-based keylogger and screenlogger for Linux, FreeBSD and OpenBSD, and includes a real-time, tail-following log analyzer. It supports most tty types, including vc, bsd and unix98-style ptys (xterm/ssh), serial, isdn, etc.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5748

" **NESSUS 3.0 – LATEST RELEASE** "

Nessus 3.0 benefits include: -- Vastly increased performance, -- Access to over 9,000+ quality vulnerability checks with vulnerability update subscription options from Tenable Network Security, -- Support for CVSS (Common Vulnerability Scoring System), -- Ability to audit Windows, Unix, Linux hosts and more

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5744

" **BFILTER V.0.10.2** "

BFilter is a smart filtering HTTP proxy. It removes ads, webbugs, and popups. Unlike the majority of similar tools, it doesn't rely on a list of blocked URLs, but instead parses HTML on the fly, and detects ads using a set of heuristic rules. BFilter has a built-in JavaScript engine which detects popups and js-generated ads.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5789

" **BETA – BINARY DATA ENCODING TOOL** "

BETA was developed to convert raw binary shellcodes into text that can be used in Windows exploit code's sources. BETA can also convert raw binary data to a large number of encodings.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5782

" **OPENSWAN – IPSEC FOR LINUX** "

Openswan is an implementation of IPsec for Linux. It supports kernels 2.0, 2.2, 2.4 and 2.6, and runs on many different platforms, including x86, x86_64, ia64, MIPS and ARM.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5765

" **EIGRP TOOLS** "

This is a custom EIGRP packet generator and sniffer developed to test the security and overall operation quality of this brilliant Cisco routing protocol. Using this tool requires a decent level of knowledge of EIGRP operations, packets structure and types, as well as the Layer 3 topology of an audited network.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5805

" **MINDTERM 3.0.1** "

MindTerm is a complete ssh-client in pure Java. It can be used either as a standalone Java application or as a Java applet. Three packages of importance are provided (terminal, ssh, and security).

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5811

" **NETDISCOVER – ACTIVE/PASSIVE ADDRESS RECONNAISSANCE TOOL** "

Netdiscover is an active/passive address reconnaissance tool, mainly developed for those wireless networks without dhcp server, when you are wardriving.
It can be also used on hub/switched networks.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5771

[04] **Astalavista Recommended Papers**

" PRIVACY PRESERVING WEB-BASED EMAIL "

The Internet is hemorrhaging unimaginable amounts of user data. In addition to information leaked through tracking cookies and spyware, users are often required to allow the providers of online services such as web-based email access to their data. We argue that it is possible to protect this information from the dangers of data mining by external sources regardless of the arbitrary privacy policies imposed by these services.

http://www.astalavista.com/index.php?section=directory&linkid=5688

" TRANSLATION-BASED STEGANOGRAPHY "

This paper investigates the possibilities of steganographically embedding information in the "noise" created by automatic translation of natural language documents. Because the inherent redundancy of natural language creates plenty of room for variation in translation, machine translation is ideal for steganographic applications.

" BOTNETS AS A VEHICLE FOR ONLINE CRIME "

This analysis of real-world botnets indicates the increasing sophistication of bot malware and its engineering as an effective tool for profit-motivated online crime.

http://www.astalavista.com/index.php?section=directory&linkid=5694

" INFORMATION POLICY IN THE 21ST CENTURY : A REVIEW OF THE FREEDOM OF INFORMATION ACT "

Hearing before the subcommittee on government management, finance, and accountability.

http://www.astalavista.com/index.php?section=directory&linkid=5698

" ECONOMIC EVALUATION OF A COMPANY'S INFORMATION SECURITY EXPENDITURES "

The paper will address why justify security expenditures, what methods have been used within the security industry, what caused the move to justify the security expenditures, and what is the general perception of the information security community and how are they embracing the new methods?

http://www.astalavista.com/index.php?section=directory&linkid=5707

" QUNTIFYING NATIONAL INFORMATION LEAKAGE "

The Internet has been become a global communication medium that transcends national boundaries. However, few empirical studies have explored how this network without borders impacts a nation's ability to limit access and control over the information it entrusts to the Internet. In this paper we present our work addressing one facet of this issue: national information leakage.

http://www.astalavista.com/index.php?section=directory&linkid=5737

" CAN THE GOVERNMENT TRACK YOUR CELL PHONE'S LOCATION WITHOUT PROBABLE CAUSE? "

When is the government allowed to track your cell phone's location? What legal standards must the government meet before a judge can authorize such surveillance? That's the issue in two recent cases where two federal magistrate judges, in an unprecedented move, rejected Department of Justice requests to track cell phones without a search warrant.

http://www.astalavista.com/index.php?section=directory&linkid=5732

" SETI HACKER OR IS A SETI VIRUS JUST SCIENCE FICTION? "

"With an unsuspecting receiver an electromagnetic wave can move "alien" signal across cosmos at light speed."

http://www.astalavista.com/index.php?section=directory&linkid=5728

"SIGNALS INTELLIGENCE AND HUMAN RIGHTS - ECHELON "

This report, first published today, was prepared in 2000 by Duncan Campbell for the Electronic Privacy Information Center (EPIC), but was "then ignored by EPIC director Marc Rotenberg who did not believe that such surveillance happened to Americans."

http://www.astalavista.com/index.php?section=directory&linkid=5822

" WARDRIVING IN CHINA "

I was recently in China for AVAR 2005, the annual meeting of antivirus researchers from Asia and the Pacific. While I was there I did some parallel research on wireless networks in two of China's major cities, Tianjin and Peking

http://www.astalavista.com/index.php?section=directory&linkid=5746

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

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

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

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

check out the special discounts!!

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

What is Astalavista.net all about?

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

Among the many other features of the portal are :

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

[06] Site of the month

OSVDB – The Open Source Vulnerability Database

http://www.osvdb.org/

OSVDB is an independent and open source database created by and for the community. Our goal is to provide accurate, detailed, current, and unbiased technical information.

[07] Tool of the month

Nessus 3.0 - Multi-platform Vulnerability Scanner

Nessus is the world's most popular vulnerability scanner used in over 75,000 organizations world-wide, with over 9,000+ quality vulnerability checks

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5744

[08] **Paper of the month**

The Top Speed of Flash Worms

In this paper, we revisit the problem in the context of single packet UDP worms (inspired by Slammer and Witty).

http://www.astalavista.com/index.php?section=directory&linkid=5678

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

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

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

More information about the DVD is available at:

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

[10] **Enterprise Security Issues**

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

- Breaking through security myths – Part 2

This article aims to point out 10 of the most common misunderstandings I have encountered recently among a various organizations, and what are the real issues to worry about.

In Part 2 we'll cover, VPNs, managed security service providers, compliance, behavior blocking, and 0day vulnerability protection.

- **VPNs**

I feel that there was a lot of hyper over VPNs during 2004 mainly because of the enterprises' growing work force, and their need to securely connect and use its resources. Don't get me wrong, the concept has its benefits, but from a management's point of view, it creates the myth of the fully secure communication channel, at least on a network level. What else should be seriously taken into consideration, is the client-side security of the participant. Namely, the hosts's integrity, that is lack of malware to somehow take advantage of the accounting data, even take active screenshots of it. Also, even though certain solutions/appliances provide the ability to integrate an IDS within such an infrastructure (if you cannot have an IDS working due to encrypted traffic, it's a huge trade-off), ensure that encrypted traffic going in and going on, can still be analyzed, and accountability for any actions can be kept track of.

- **managed security service providers**

Managed security service providers are a logical business choice for any company that doesn't want to heavily invest in security infrastructure and personnel, at least at a certain point of stage. I often say that if you don't take care of your destiny, someone else will. And, I feel that philosophy greatly applies to the concept of MSSPs. Such providers cannot guarantee you total security, so ignore the hype, but look for such that offer you a guarantee in case of an intrusion. Mind you, an MSSPs would never take fully responsibility for what's going around your infrastructure. Ensure your MSSP is a value-driven company, as the majority of today's MSSPs are simply responding to the need of managed security, namely mainly profit-driven organizations actively reselling licenses to services, or access to a set of appliances etc. Sooner or later though, your organization would eventually grow, and being the 567?th customer of a large MSSP, it is a great idea to build an infrastructure on your own, why, because it's getting even more cheaper and qualified work force is much more often found these days.

- **compliance**

Compliance is a buzz word, companies spend millions to comply with legal regulations, and again, get broken into. A lot of folks that I know, have expressed a great level of optimism towards the overall state of security due to the process. And while true, today's threats and concepts used to malicious attackers change on a daily basis. And you simply need to keep track of that in one way or another.

Make your point, compliance tells you what has to be done, not how to do it. How it's actually done is entirely up to you, or the consultants you've hired. There are a great deal of compliance tools available, and it's a common myth that you can buy your security and keep going. You simply cannot, so make sure the tools you use aren't the type of MSSPs I mentioned above, profit-driven ones, and not that I have troubles with these, but in the long-term it's a serious organization you're interested in working with.

- **behavior blocking**

Concept that's been around for a decade, and while there's a great logic into spotting malicious activity in a software, you should also keep in mind, is how easy it is for a malicious action to get executed through a legitimate program. Ensure does your blocker merely monitors certain events, or a sequence of events to figure out whether malicious or not. What's else to note is how the concept is actually executed, if you were to allow every end user to participate in the process, instead of doing your best to enforce it, you might experience certain trouble.

Don't ignore the availability of such a feature, but look for the total package of intrusion detection and prevention services. You'd better prevent, instead of curing it later on.

- **0day vulnerability protection**

No company can provide you a total 0day vulnerability protection, no matter of the terms and abbreviations used to describe their technology. They cannot protect you from a vulnerability they are not aware of. They can though, theoretically try to prevent the most widely used concepts, ensure minimal damage is done in case of an attack, and actually open up their deep-pockets to purchase vulnerabilities and disclose them exclusively to you as customer only.

Ensure unprivileged accounts dominate, adapt to your workforce, yet achieve the balance, and try to survive because the threats you're not aware of, are the ones that actually exist.

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

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

- Threats posed by P2P software -

This brief article will discuss the most common threats posed by the use of P2P, excluding law enforcement prosecutions in case the service is illegal in itself. It will also try to provide you with practical tips on how to deal with these threats.

Even though the recording industry is currently suing teens for sharing of intellectual property, these aggressive law enforcement practices have resulted in a slight decline in the overall use of P2P. It is my opinion that the majority of P2P networks ended up so poisoned, that end users started willing to purchase songs.

Yet, some of the threats you should consider while using P2P networks are :

- **bundled spyware, adware, EULA abuse practices**

There's no such thing as a free lunch, given it's not a promotion of course :) Expecting to simply download, let's say, "content" without testing your systems security measures is false. Before using any P2P, do a little research, and find out what the others say about its hidden features. Consider checking out Spywareinfo's list of clean and infected P2Ps, the thing is, at any time, any of these can change their practices.

http://www.spywareinfo.com/articles/p2p/

EULA's are all these lengthy terms of agreement you automatically concept thinking they are the common terms of agreement you come across in other software(given you even read them at all). I remember a company that paid a couple of thousands dollars To the first that came across the message in the EULA, just to Figure out who's actually reading them, the truth is no one. And it opens up huge business opportunities, if I can legally comply with ensuring I've provided you with info on storing third party programs on your PC, and you agreed, that's a bad thing.

I recommend you either read EFF's EULA guide

http://www.eff.org/wp/eula.php

or consider using the EULAlizer, a great tool with the help of which I have come across great discoveries.

http://www.javacoolsoftware.com/eulalyzer.html

- **the degree of malicious content on the network**

Certain P2P networks are so poisoned(yes, the RIAA has made their contributions as well!) that you should simply avoid them. The P2Ps full of junk can be either the most popular ones, or those desperately trying to generate revenues and work with malware authors to accomplish it. The increase of vulnerabilities targeting multimedia extensions is growing, and P2P is the first distribution method attackers use.

- **unintentional sharing of sensitive information**

Simply make sure you know what exactly you are sharing, and that certain preferences as limit of connections etc. are in place. What you should also consider is the possibility of an unintentional sharing of content, so watch out!

No P2P network is free of malicious content, but BitTorrent's concept solves both, the awfully slow transfers and some of the other P2P's software weaknesses. In the future, I'm sure that anonymous P2P networks will get even more attention by end users, so in case you are interested in evaluating the current solutions, check out http://www.anonymous-p2p.org/

[12] **Meet the Security Scene**

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **Vladimir, 3APA3A,** from http://www.security.nnov.ru/

Your comments are welcome at security@astalavista.net

Interview with Vladimir, aka **3APA3A** http://www.security.nnov.ru/

Astalavista : Hi Vladimir, would you please introduce yourself to our readers, and share some info on your background and experience with information security?

Vladimir : OK. I'm 31, I'm married, and we have two daughters. For last 10 years I'm support service head for middle sized ISP in Nizhny Novgorod, Russia. As so, I'm not occupied in IT security industry and I'm not security professional. It's just a kind of useful hobby. And that's the reason why I use nickname though I have no relation to any illegal activity. Everyone who is interested can easily find my real name. In addition to my primary job, I give few classes a week on computer science in Nizhny Novgorod State University.

I started on the Russian scene in the late 90s with the article on HTTP chats security. 'Cross site scripting' was quite new vulnerability class and the term itself arrived few years after. Later I began to publish some articles on the Bugtraq. Because my previous nickname taken from Pushkin's personage was not understandable abroad, I used gamer's nick '3APA3A', 'zaraza' in Cyrillic, it means infection. It also has a meaning of English 'swine' :). No, there is no relation with famous 3APA3A. ZARAZA virus, it was few years before.

I'm not 'bug digger', as one may think. Some bugs were discovered in the process of troubleshooting, while others were found in attempt to discover new vulnerability class or exploitation approach. And I'm proud to catch a few :)

Astalavista : What are some of your current and future projects?

Vladimir : Since 1999 http://www.security.nnov.ru/ is the only project I'm constantly involved in. Sometimes, I patch old bugs and create new ones within **3proxy** http://www.security.nnov.ru/soft/3proxy/.

Astalavista : How would you describe the current state of the Russian security scene? Also, what are you comments on the overall bad PR for, both, Russia, and Eastern Europe as a hackers' haven?

Vladimir : "hack" is an opposite to technology for me. The industry with technology is a conveyor, while the hack works only here and now. Hacking is the process of creating something to solve one particular problem without enough money, resources and, most important, without knowledge. In the best case it's something new for everyone and nobody to share knowledge and resources with you.

If you mean a lack of money, resources and knowledge - yes, Russia is hackers' heaven :)

We had interesting discussion on this topic with David Endler (from your Newsletter #23) Of cause you know how many viruses originated from Russia and you know some "famous" virus writing teams. Do you know any software written here? Well.. may be after some research you can find Outpost and Kaspersky Antivirus you have never used... That's all. You think. Lets look at the city I live. Many really interesting things from Quake II graphical drivers and Intel debugging and profiling tools to Motorola and Nortel firmware were written here. It's not largest city and Russia is large country. Same goes to Eastern Europe, India and China.

We have a lot of unknown programmers and few famous virus writers, that's the problem :)

The security scene in Russia is really hard question. Of course, there are few professionals, they are well-known buddies, who work for well-known companies. They publish their really useful books and write their really professional articles and receive their really good money. There are old-school hackers who do not speak Russian for few years. There are "underground" e-zines, none of them are living enough to spell correctly. There are "security teams" known by defacing each over and publishing up to 6 bugs in PHP scripts. Teenage #hax0r1ng IRC channels. And, of cause, guys who do their business with trojans and botnets and prefer to stay invisible.

That's all, folks. There is no scene. No place to meet each over. No Russian Defcon.

Astalavista : What are the most significant trends that happened with vulnerability researching as a whole since you've started your project?

Vladimir : Any new technology arrives as a hack, but grows into industry. It was with computers, software, network security and finally it happens with vulnerability research. This fact changes everything. No place left for real hacking. The guys on this scene became professionals. If you enter this without knowledge, all you can is to find some bugs in unknown PHP scripts.

Astalavista : Do you think a huge percentage of today's Internet threats are mainly posed by the great deal of window of vulnerabilities out there, and how should we respond to the concept of 0day by itself? Patching is definitely not worth it on certain occasions from my point of view!

Vladimir : Imagine a 100,000,000 of purely patched default configuration Fedora Core machines with users running their Mozilla's from root account. That's what we have in Windows world. Did you know that, 99% of Windows trojans/viruses/backdoors will not work if executed from unprivileged account? Life could be much more secure if only administrator with special license (like driver's one) might configure system and get penalties in case of virus incidents :)

Did you know that, most ISPs do not monitor suspicious activity from their customers and can not stop attack from their network within 24 hours? It's almost impossible to coordinate something between providers. There are non-formal organizations, like NSP-SEC, but it only coordinates large providers from few countries. Coordination and short abuse response time would be another step.

Astalavista : What is your attitude towards an 0bay market for software vulnerabilities? And who wins and who loses from your point of view?

Vladimir : On the real market both sides win. No doubt, the fact there is now a legal market for 0days is a good news for researches and end users, because it rises vulnerability price and establishes some standards. This "white" market is in it's beginning. There are only few players.

Who can value 0day Internet Explorer bug? First of all, Microsoft. But for some reason it does not. The second, IDS/IPS vendors and security consulting companies to make signatures and PR. Bugtraq posting is really good PR. If vulnerability is then exploited in-the-wild, it raises the article in Washington Post. It's even better PR.

Astalavista : Do you also, somehow picture a centralized underground ecosystem, the way we are currently seeing/intercepting exchange of 0day vulnerabilities on IRC channels, web forums. But one with better transparency of its content, sellers and buyers?

Vladimir : And, of cause, underground market is always ready to pay. Exploits are required to install a trojan. Trojan is required to create a botnet. Botnet is required for spamming, DDoS and blackmailing, phishing, illegal content hosting. It's definitely a kind of ecosystem with different roles and specializations and it's money cycle as a basement.

With some dirty games with 0day Internet Explorer vulnerability you can make a new car on the botnet market or (and?) just few thousands dollars with PR. Underground market is not centralized and lies on private contacts. Forums and IRC channels you can find are the top of the iceberg. It makes it less vulnerable. I bet last WMF exploit was sold without any IRC channels and forums.

Astalavista : Can there ever be a responsible disclosure, and how do you picture it?

Vladimir : According to Russian legislation, a vendor may not sell product without informing customer about any known defect or limitation on it. I bet different countries have similar legislations. I don't understand why it doesn't work with computer software. Vendor should either timely inform customers on defect in software or should stop to sell it.

Of cause, disclosing information without informing vendor is just stupid and non-profitable for everyone. From other side, if vendor has not eliminated vulnerability after few months and has not informed customers there is nothing non-responsible in publishing this information. I never saw vendor who blames researchers in non-responsible disclosure to stop selling defective product.

There were few attempts to standardize disclosure policy, RFPolicy is the first one.

Astalavista : Can a vulnerability researcher gets evil if not treated properly, and what could follow? :)

Vladimir : Sure. Imagine a situation you want to get money from vendor for vulnerability information you discovered. There is nothing bad in getting money for your work and vendor should be interested in buying this information on the first place. But it can be just a blackmail if not "treated properly".

Astalavista : In conclusion, I wanted to ask on some of your future predictions for 2006 concerning vulnerability research, and the industry as a whole?

Vladimir : One year is small period. May be we will see vendors to buy vulnerabilities. "Vulnerability researcher" may be scripted on somebody's business card and become profession by this way. "Vulnerability researching" as University course... No, let's wait for another 2-3 years :)

Astalavista : Thank you for your time!

[13] **IT/Security Sites Review**

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

-

OpenNetInitiative.net

-

http://www.opennetinitiative.net

Documenting Internet Content Filtering Worldwide

-

Ohnorobot.com

-

http://www.ohnorobot.com/

Oh No Robot comics search

-

Gateway to Intelligence

-

http://www.au.af.mil/au/awc/awcgate/awc-ntel.htm

Very resourceful!!

-

Hackaday.com

-

http://www.hackaday.com/

The Revenge of the Geeks :-)

-

Av-test.org
-
http://www.av-test.org/

Want to evaluate one anti virus vendor's solution, next to another? Look here!

[14] **Final Words**

Dear readers,

See you all in 2006, and keep on visiting our portal!!

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader – Yordanka Ilieva
danny@astalavista.net