Astalavista Group Security Newsletter
Issue 26 – 31 February 2006
http://www.astalavista.com/
security@astalavista.net

[01] **Introduction**

Dear readers,

Our second issue for 2006 is finally out!

As always you'll find a coverage of security news, recommended tools and research papers, articles, and a chat with a key participant, in this case **Martin Herfurt**, a core member of the Trifinite group, http://trifinite.prg/

- "**What is your position in the emerging market for software vulnerabilities?**" a brief introduction of the trends to consider, the benefits and threats to keep in mind, as well as several possible positions to take. Vulnerability research is getting commercialized, and as any a reputable organization, you simply cannot not to dive yourself in.

- "**If you don't take care of your Security, someone else will**" a brief article that will try to bring some do-it-yourself security attitude in our numerous end users!

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

Check out the Geeky Photos section and get the chance to win a .NET membership with your quality shots :

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

[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

---

[**RESEARCHERS : POPULAR APPS HAVE MISMANAGED SECURITY**]

Two Princeton researchers have released a report arguing that makers of popular softwares need to be more security-conscious in their programming. An analysis of such popular applications as Photoshop and America Online's Instant Messenger shows that they make changes to Windows or run with too many privileges, possibly allowing an attacker to bypass certain security features. Sudhakar Govindavajhala, a Ph.D. student and one of the paper's authors, notes that an attacker would need an account on a machine to exploit these vulnerabilities. The SANS Institute points out that hackers have been moving away from direct attacks against Windows toward exploiting flaws in applications. America Online and Adobe have fixed the problems Govindavajhala and co-author Andrew Appel discuss in the paper, though flaws sill remain in other products.

More information can be found at :

http://www.networkworld.com/news/2006/020606-application-security.html

Astalavista's comments :

That's a minor trend worth mentioning, while I feel the idea of diversifying the security attacks and exploiting third-party software to increase the number of possible entry points into a system, has been around for years.

Vendors are so into pushing latest product releases to meet customers' or stock market's expectations, while whenever it comes down to achieving a balance between user-friendliness and security, they have nothing to say besides yet another PR statement on how concerned about the security and privacy of our customers we really are. Are you are the bottom line? A very interesting study that I recently read, namely "Economic Analysis of the Market for Software Vulnerability Disclosure" argues that a profit-maximizing vendor delivers a product that has fewer bugs than a social-welfare maximizing vendor. However, the profit-maximizing vendor is less willing to patch its software than its social-welfare maximizing counterpart.

And while software quality has mostly to do with integrity and performance nowadays, the concept of secure coding is an important factor for, both, the short and long-term success of the product itself. Wish there was more accountability for unacceptable windows of opportunity from the vendor's side, that have nothing to do with a third-party researcher releasing detailed information on a vulnerability with the idea to enforce the vendor to actually patch it, cause that's how it works these days.

[**BEWARE OF THE 'POD SLURPING' EMPLOYEE**]

Security researcher Abe Usher is warning companies about the threat of "pod slurping" and employee data theft in

general. Usher has created an application that allows an iPod to scan corporate networks for files likely to contain sensitive business data and download them, potentially stealing 100 megabytes in a few minutes. An insider threat would only need to plug the iPod into a computer's USB port, normal use for an iPod – no keyboard use is required. A 60 GB iPod could potentially hold every sensitive document in a medium-sized business. While companies are aware of and protect themselves against hackers and malware, few realize the threat posed by a malicious employee with an iPod.

More information can be found at :

http://news.com.com/Beware+the+pod+slurping+employee/2100-1029_3-6039926.html

Astalavista's comments :

Insiders are a major problem for any industry. But dedicating too much measures may affect productivity and most importantly, creativity. A major problem is organizations lacking an implemented security policy on how sensitive/any company information travels across inside and outside the network.

The automated nature of the tool, and the iPod's storage capabilities, turns it it a threat to a certain extend, while blocking removable media, and fortifying another possible exit point – web traffic, would make its impact for sure. Another important feature is how it can be even activated without the need for a keyboard.

Removable media has always been a threat, therefore ensuring the confidentiality of the information, as well as detecting possible leakage in progress is what you should aim at achieving.

Does this mean you should not leave your friends hang around your PC/PCs farm with their iPods? Not unless you manage the threat.

[**FEDS : GOOGLE'S PRIVACY CONCERNS UNFOUNDED**]

The US Justice Department filed a court brief arguing that receiving data it requested from Google would not compromise the privacy of its users. The brief is a response to Google's claims that disclosing the requested information -- a week's worth of search terms and one million pages from Google's index -- would harm the company by violating user privacy and revealing trade secrets. The government is seeking the search data for use in a lawsuit brought by the American Civil Liberties Union (ACLU) against he 1998 Child Online Protection Act (COPA), an Internet pornography law, hoping to show that content filters are ineffective for preventing minors from accessing adult material. Justice says it only wants aggregate information that would not compromise privacy, criticizes Google for failing to show how disclosure would compromise trade secrets,

and argues that the government's right to access information outweighs Google's arguments. Justice requests that Google be given 21 days to comply with the subpoena.

More information can be found at :

http://news.com.com/Feds+Googles+privacy+concerns+unfounded/2100-1028_3-6043338.html

Astalavista's comments :

I honestly feel it's about time Google becomes a pioneer member of the EFF and get an in-depth review of the real-life privacy violations due to this misjudged request. I like the idea of how Google used the trade secrets issue as a possible negative effect on the business, whereas, can their enforcement of Chinese state censorship over its services be considered the same? The DoJ's request, and Google's entry in China with its Google.cn domain, prompted a lot of debate over Search engine's practices for censorship, and future subpoenas to be served.

What I don't like it how the rest of the search engines silently complied, compared to Google who immediately informed the general public. What is it that matter at the bottom line? Who's getting uncensored results, or any results at all, who's providing personally identifiable information to law enforcement under questionable subpoenas, or who simply has to do this in order to maintain operations?

[**POLITICALLY MOTIVATED ATTACKS SOAR in 2005**]

Web server attacks and website defacements rose 16 per cent last year, according to an independent report. Zone-h, the Estonian security firm best known for its defacement archive, recorded 495,000 web attacks globally in 2004, up from 393,000 in 2003.

Mass defacements (371,000) were by far the largest category in 2005. More targeted attacks on individual servers numbered 124,000. Zone-h reports an increase in politically motivated attacks. It notes a growing number of attacks were launched from Muslim countries, especially Turkey. By contrast, the majority of attacks launched in 2004 originated in Brazil. The most active defacer last year was Iskorpitx, from Turkey, who's bagged 90,000 websites over the last two years.

More info can be found at :

http://www.theregister.co.uk/2006/02/27/defacement_report_2005/

Astalavista's comments :

Shared hosting is quite common, you have these companies that offer unlimited bandwidth and often attract quite a lot of people. Politically motivated attacks have always existed, and the outbreak usually starts out of real-life events. Defacements are still on the rise, while there has also been evidence that web servers are sold to

phishers for more effective attacks. The FBI's 2005 Computer Crime Survey indicate that companies are still losing millions of dollars on average due to web site defacements. There have always been hacktivists and will always be, as Cyberspace seems to be an attractive place to express your reaction on real-life events. People sometimes question the usefulness of initiatives such as the Zone-H's one in respect to acting as an incentive for defacers, it isn't like that from my point of view, as I feel it's better to have a centralized place to keep track of what's going on instead of having to put extra efforts in doing it. Another point to consider is that they way a government responds to its defacers(check out the statistics) for me, that's a benchmark for evaluating their overall understanding of the problem. Defacers create tensions, and even worse, hordes of script kiddies interested and inspired to contribute with exactly the same.

[**IS YOUR CELL PHONE DUE FOR AN ANTIVIRUS SHOT?**]

As antivirus companies begin offering products to protect cell phones, they are discovering resistance from major cell carriers. Verizon Wireless says it sees no need for antivirus on its customers' phones. Gartner reports a total of 812 million mobile devices sold in 2005, and expects the number to break a billion by 2008. A number of viruses already target cell phones, but so far the risk has remained low, Nonetheless, Gartner expects a widespread mobile virus attack by the end of 2007. Symantec, McAfee, and F-Secure already offer mobile antivirus, but cell carriers prefer to combat viruses on the network level rather than on the phones themselves. Fortinet estimates that 10% of all MMS traffic carries a virus, with Commwarrior proving one of the most common. Gartner warns the cell industry to only use device protection as a last resort, arguing that the best results against viruses will come from protecting the network.

More information can be found at :

http://news.com.com/Antivirus+looks+to+get+locked+into+cell+phones/2100-7349_3-6042745.html

Astalavista's comments :

Mobile malware is on the rise, or at least according the majority of AV vendors with mobile security products and the mainstream media that's generating more buzz then ever. Is there anything to worry about at the bottom line? At least not for now, you see, mobile malware as a concept started from the release of a proof of concept code that had mainly to do with the propagation mechanisms. The current defenses are mainly generic, and while the yearly fees might seem attractive, I'm not in a rush for buying such a solution. I find R&D initiatives in mobile malware a very sound business investment, but generating buzz over scanners with less than 500, mind you, signatures,

when the majority of attacks actually happen due to social engineering, is how I see it at the bottom line. The recent case where the Mobile Antivirus Research Association wasn't interested in forwarding a signature of a 0day malware that spreads from PC's to mobile devices is a great example of the current situation -- there is active research, and so is a lot of buzz generated, stay away from it.

[**SMILE! YOU'RE ABOUT TO GET HACKED**]

Consultants Robert Baldwin and Kevin Kingdon, speaking at the RSA Conference, predicted that video and audio files could become the next big attack vector. Copy protection software embedded in video files can prevent security scans from working, making video files a likely vector for malware. Many video consumers have a trusted source for content, such as cable television and iTunes, but many are circulating content downloaded from random source on the Internet. Enterprises may begin to see video threats as they begin using more video in business presentations and other operations.

More information is available at :

http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1168617,00.html

Astalavista's comments :

That's a very good issue to raise more awareness on given the demand for video, be it long movies or microchunks on the Internet these days. There's been a lot of discussion on the current practices of downloading multimedia, how it lags the whole Internet, and with the incentive to target pretty much everyone out there resulting in severe vulnerabilities. While I doubt iTunes spoofs will emerge, a vulnerability in a popular media format, given a malicious sample is somehow distributed across the Net(P2P is still soo active!), it could cause a lot of headaches for everyone. Malicious attackers have always been trying to diversify, that is, not always try to exploit Microsoft products' related vulnerabilities, but popular software, even file formats' ones. Today, end users know they should not click on executable attachments, but they are not even given the chance to react, and while many enterprises block untrusted media content sites, be it out of bandwidth worries, others, proactively think employees' productivity and possible entry points.

[**STARTUP TRIES TO SPIN A SAFER WEB**]

A startup called SiteAdvisor is aiming to crawl the Internet looking for websites that surreptitiously install software on users' computers and track use of e-mail addresses for spam. The service simulates a user and browses websites and hands out "user" information, using honeypots to track where the spoof user's information ends up. This allows SiteAdvisor to document the effects of using a website so consumers can be warned about the potential dangers. SiteAdvisor will offer general service for free, with premium features reserved for paying customers.

More information can be found at :

http://www.securityfocus.com/news/11376

Astalavista's comments :

I find the idea of malware crawling a very relevant one, given the potential of not just spotting 0day piece of code, but mapping bad sites and their neighborhoods. Compared to back in 1998, today's Web is so huge, even Google with its over 150 000 servers cannot seems to be able to catch up. While SiteAdvisor can indeed evaluate how safe a site is, it can do this for a past period of time only, they way it takes a little while for Google to pick up the latest content that appears on the Web. Moreover, once checked, a site's practices could change in between and unless they start taking advantage of the buzz generated around them, and have their users push questionable sites to be checked on-the-fly, malicious sites will still find a way to bypass their three-step evaluation process. Great initiative, hope they can scale enough to make it an effective one.

[MAC ATTACK A LOAD OF CRAP]

Conventional wisdom holds that while Apple's Mac OS X is stronger built than Microsoft Windows, it is still vulnerable and has largely avoided major attack due to its small market share; as Mac OS X becomes more popular, Mac users will start facing bigger security issues. However, Kahney dismisses the threat posed by two worms targeting Mac OS X. Leap-A does not exploit a flaw in the operating system, but instead used a social engineering attack, which can work on any platform. Kahney also dismisses the threat posed by a new flaw in the Safari browser, since it is not an exploit. Kahney argues that any system has vulnerabilities, and the discovery of a Safari flaw without an exploit has been hyped by the press into a bigger threat than it really is.

More information can be found at :

http://www.wired.com/news/columns/0,70257-0.html

Astalavista's comments :

The MAC is under attack, proof of concept worms, hacking challenges, while at the bottom line I can argue which one is more secure, does it matter, and which OS is popular, thus more targeted. The MAC still remains rather unpopular compared to any of MS's products and this fact would remain the main driving force behind the lack of serious research, until someone releases a POC vulnerability that would be the corner stone of generation of attacks for months to come. MAC users aren't safe because OS X is more secure than Microsoft's products, they're safe because "security through obscurity" works on a certain of occasions.

[DDOS ATTACKS TARGET PROMINENT BLOGS]

Distributed denial of service (DDoS) attacks have targeted political as well as "financially successful" bloggers recently, and speculation is that these "digital extortionists" are expanding their range, previously limited to attacking such sites as online betting services and payment gateways.

More information can be found at :

http://news.netcraft.com/archives/2006/02/28/ddos_attacks_target_prominent_blogs.html

Astalavista's comments :

Follow the lead where the money goes, simple but effective when it comes to DDoS extortion I guess. The concept is fully working, while I believe trends are shifting towards providing the service on demand, so that a third-party can actually take care of the attack. DDoS extortion is both noisy and the malicious botnet herder simply gets too much attention, whereas exploiting the momentum, and targeting the right company seems to be working. And as cyber insurers are starting to ensure, and actually pay for such extortions, it will definitely not get unnoticed, which as a matter of fact is a totally wrong practice right from the very beginning.

[MUSLIM CARTOON PROTEST]

Zone-H.org reports over 600 defacements of Danish websites, plus attacks against websites in other European countries and Israel, carrying messages denouncing Denmark for the publication of twelve cartoons Muslims deem offensive for depicting the prophet Mohammed. One defacement by a group calling itself the "Internet Islamic Brigade" threatened bombings in Denmark similar to the London subway bombings of July 2005. Most of the defacements contain pictures of messages in Arabic with English text related to the cartoons.

More information can be found at :

http://www.eweek.com/article2/0,1759,1921048,00.asp

Astalavista's comments :

On the majority of occasions journalists are often confronted with strict deadlines, and the lack of cultural understanding, and the rush of affiliates to reprint your work -- huge problems happen. Free speech and freedom of the press is an important issue, and while Muslims tend to be very sensitive on people even talking about their prophet, releasing such cartoons in the mixed-salad called the EU is the dumbest thing ever possible. Embassies evacuation, street riots, hacktivists defacing the entire country's Web presence, and again, more tension in key regions across the world. Bill Clinton wanted a legal prosecution of the journalists, while they were simply expressing their bla bla bla, he is so good at seeing the big picture, that while I don't fully agree, they must somehow

face professional consequences, and I bet they already did. Yahoo! responded in another way, as the name Muhammad was banned on their IM network, they recently removed the ban, so anyone can use the nick and its variations.

[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**

" **SURI PLUMA V1.0.1**"

Suri Pluma is a satellite image processing tool and visualizer. It can open the most common image formats without importing to an internal format and minimizing the memory required for visualization. It is designed to be modular and extensible. It has a meassurement tool (distance and areas with error estimation) and geographical and map coordinate information.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6138

" **BACKTRACK LIVE CD** "

BackTrack is a Slackware based live CD that contain many security related tools such as sniffers, enumeration tools, exploits, scanners fuzzers and more.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6149

" **KOFFIX BLOCKER** "

Koffix Blocker is a powerful ally in the fight against web sites involved in questionable practices, such as changing your home page or downloading software to your computer without clear and upfront disclosure.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6204

" **WAPIRCGW 0.1.5** "

wapircgw allows a WAP-capable mobile phone to easily connect to IRC networks. The only thing needed is a Linux box with an Internet connection to act as a gateway between the phone and IRC networks. Users can join multiple channels and talk to others privately just like when using a real IRC client.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6219

" **NHIDE 1.63** "

nHide is an open source window hider from featuring multiple window hiding, remembering of hidden windows, and a hide hotkey for instant stealth, this program is the perfect addition to any bored employees or teenagers arsenal.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6144

" **BOBCAT – SQL INJECTION EXPLOITATION TOOL** "

BobCat is a MS Windows based tool to aid a security consultant in taking full advantage of SQL injection vulnerabilities. It is based on a tool named "Data Thief" that was published as PoC by appsecinc. BobCat can exploit SQL injection bugs/opportunities in web applications, independent of language, but dependent on MS SQL as the back end DB.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6147

" **BLUE FROG ANTI SPAM V1.7** "

Blue Frog actively fights spam and makes spammers leave you alone. Blue Frog automatically posts complaints on the sites advertised by the spam you receive. Report your spam from any desktop email client or let Blue Frog report Gmail, Hotmail and Yahoo spam directly from the Firefox browser. Filtering spam is not enough. Blue Frog protects your email accounts or your entire mail domain by making spammers remove your from their mailing lists.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6152

" **CAIN FOR POCKETPC (ARM) V1.2** "

Features: - Rainbowcrack-online client (works with any Internet connection available such as GPRS, ActiveSync ....). - Dictionary Attacks for the following hash types: MD2, MD4, MD5, SHA1, RIPEMD160, CiscoPIX, MySQL v3.23, MySQL v3.23 + challange, MySQL SHA1, MySQL SHA1 + challange, LM, LM + challange, NTLM, NTLM + challange, NTLM Session Security. - Hash Calculator. - Base64 Password Decoder. - Cisco Type-7 Password Decoder. - Cisco VPN Client Password Decoder. - VNC Password Decoder. - Microsoft Messenger Password Decoder. - Internet Explorer Password Decoder. - ActiveSync Password Decoder.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6156

" **BUG HUNT SEQUENCE FILE** "

Here is a copy of the R-20 .icf file that I wrote, and which caused a some folks to get extremely upset as few weeks back.Essentially what you do is take this file, download it into your Icom R-20, and it will find bugs... lot of bugs... from pretty far away. You can also use it to find covert video camera by listening for the raster buzz. I also programmed it so that you can hit popular bug bands if you choose.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6160

" **SANDBOXIE 2.3** "

Sandboxie requires neither the disabling nor blocking of functions available to Web sites through the browser. Instead, Sandboxie isolates and quarantines the outcome of whatever the Web site may do to your computer, including the installation of unsolicited software. There is no trade-off of functionality for security: the Web site can use the full range of active content tools, and if it uses these tools maliciously to install software or otherwise make changes in your computer, then these changes can be easily undone.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6318

[04] **Astalavista Recommended Papers**

" **HOW FILESHARING REVEALS YOUR IDENTITY** "

Following the death of Napster, all of the file sharing networks that rose to main-stream popularity were decentralized. The most popular networks include Gnutella (which powers Limewire, BearShare, and Morpheus) and FastTrack (which powers KaZaA and Grokster). The decentralization provides legal protection for the companies that distribute the software, since they do not have to run any component of the network themselves: once you get the software, you become part of the network, and the network could survive even if the parent company disappears.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6154

" **MOZILLA'S BUGFIX RATE – THE LAST 3 YEARS** "

Today's post marks the second in what I hope will be a series of similar analyses. This one looks back over a similar three-year period to see how long it took Mozilla to issue patches for self-assigned "critical" security holes in its various open source products, including the Mozilla Suite, the Firefox Web browser, and its Thunderbird e-mail software.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6161

" **THE EVOLUTION OF MALICIOUS IRC BOTS** "

This paper will examine the core features of popular IRC bots and track their evolution from a single code base. This analysis will demonstrate how many of the common IRC bots such as Agobot, Randex, Spybot, and Phatbot actually share common source code. In addition, interesting techniques utilized by specific variants will also be presented.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6177

" **A CRAWLER-BASED STUDY OF SPYWARE ON THE WEB** "

Malicious spyware poses a significant threat to desktop security and integrity. This paper examines that threat from an Internet perspective. Using a crawler, we performed a large-scale, longitudinal study of the Web, sampling both executables and conventional Web pages for malicious objects. Our results show the extent of spyware content. For example, in a May 2005 crawl of 18 million URLs, we found spyware in 13.4% of the 21,200 executables we identified. At the same time, we found scripted "drive-by download" attacks in 5.9% of the Web pages we processed. Our analysis quantifies the density of spyware, the types of threats, and the most dangerous Web zones in which spyware is likely to be encountered. We also show the frequency with which specific spyware programs were found in the content we crawled. Finally, we measured changes in the density of spyware over time; e.g., our October 2005 crawl saw a substantial reduction in the presence of drive-by download attacks, compared with those we detected in May.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6202

" **THE FINANCING OF TERRORISM THROUGH CAPITAL FROM A LEGITIMATE SOURCE** "

We present the full version of the study on international terrorism financing schemes anticipated by the previous article of Simona Sapienza.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6197

" **NATIONAL RECONNAISSANCE – FIRST UNCLASSIFIED ISSUE, 2005** "

This publication represents the first unclassfied issue of National Reconnaissance - Journal of the Discipline and Practice.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6235

" **MODELING BOTNET PROPAGATION USING TIME ZONES** "

Time zones play an important and unexplored role in malware epidemics. To understand how time and location affect malware spread dynamics, we studied botnets, or large coordinated collections of victim machines (zombies) controlled by attackers. Over a six month period we observed dozens of botnets representing millions of victims. We noted diurnal properties in botnet activity, which we suspect occurs because victims turn their computers off at night. Through binary analysis, we also confirmed that some botnets demonstrated a bias in infecting regional populations.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6224

" **WEB FORMS AND UNTRACEABLE DDOS ATTACKS** "

We analyze a Web vulnerability that allows an attacker to perform an email-based attack on selected victims, using standard scripts and agents. What differentiates the attack we describe from other, already known forms of distributed denial of service (DDoS) attacks is that an attacker does not need to infiltrate the network in any manner—as is normally required to launch a DDoS attack. Thus, we see this type of attack

as a poor man's DDoS. Not only is the attack easy to mount, but it is also almost impossible to trace back to the perpetrator. Along with descriptions of our attack, we demonstrate its destructive potential with (limited and contained) experimental results.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6220

" **TRACKING DATA OVER BITTORRENT** "

Bit Torrent has a reputation of being difficult to find out who is downloading movies, games, documentation, and other information. This is not necessarily true in all cases; any Peer-to-Peer system at some point relies on IPv4 and TCP/IP to make its connections. Because of that, the sender and the receiver can be well known to anyone who is using a program or programs that have robust logging, and other programs that help geolocate where those IP addresses are physically located. Anyone who produces or protects data that is confidential or otherwise protected by statute or law should have an understanding of bit torrent networks, how they work, and how they route.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6281

" **TRANSPARENT ACCOUNTABLE INFERENCING FOR PRIVACY RISK MANAGEMENT** "

There is an urgent need for transparency and accountability for government use of large-scale data mining systems for law enforcement and national security purposes. We outline an information architecture for the Web that can provide transparent access to reasoning steps taken in the course of data mining, and accountability for use of personal information as measured by compliance with rules governing data usage. Legislative debates and judicial oversight will determine how large and how fast the expansion of data mining power available to homeland security and crime prevention efforts will be. Our approach to the privacy challenges posed by data mining is to concentrate on transparency and accountability in the use of personal information.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6278

[05] **Astalavista.net Advanced Member Portal v2.0 – Special Discounts!!**

Become part of the **community** today. **Join us and take advantage of this month's special discounts!**

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

Plain-text.info

http://www.plain-text.info/index/

This website is a distributed cracking system powered by rainbowtables, wordlists and other techniques.

[07] Tool of the month

HoneyDVD - Bootable Honeypots on DVD

This work will enable Honeynet technology to spread much further by substantially decreasing the investment needed to run a Honeynet. With the recent commercial interest in Honeypot technology there is potential to further develop the project into an product. Also the project will help to gather further knowledge on real world applications of virtual computers, a field of increasing interest in the commercial and in the academic world.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6234

[08] **Paper of the month**

The Domain Name Service as an IDS

How can DNS be used for detecting and monitoring badware in a network?

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6275

[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!

- What is your organization's position in the emerging market for software vulnerabilities? -

As we are currently witnessing the development of this market, with already, three informediaries paying vulnerability researchers for their successful efforts, it's wise to think about how would your organization take advantage from the pros(if any), and avoid the cons(if any, again). In this brief article we'll review some of the possible scenarios as far as successfully positioning yourself is concerned, as well as avoiding common myths related to the current and future model of the market.

Many of you actively outsource their security needs to a MSSPs, or

invest in the development of an in-house security team. No matter the type of security solution, an anti virus, an IDS or a firewall, they themselves often suffer from software vulnerabilities. Ironical, or not, that's the plain truth at the bottom line. Vulnerabilities are slowly turning(given they've never been?) into the currency of today's security industry, and the transparency achieved during the last couple of years in respect to documentation, HOWTO's and the quality and number of tools capable of easily turning a vulnerability into an exploit, are among the driving forces of the trend. Proactive companies, or ones interested in their long-term survival have already started monitoring the trend, what many wonder is which position should they stick to, and how should they react to the threat posed by 0days as a concept themselves.

There are a couple of possible scenarios, and these could be :

- start participating by becoming a client of one/all of the informediaries with the idea to be the first to receive a notification of a vulnerability before the industry itself has

While this may seem to be the smart approach to chose, it stands for a "false feeling of security", and a certain degree of dependence. Given you can live with the second, and actually find the use of the first, go for it. But hold your breath for a little while, presuming that you want to participate you will have to spot the most active intermediary, that happens to be iDefense. Now, adding a little bit of exclusiveness to a vulnerability submitted, and given you are among the "chosen ones", I mean, the paying ones, you've won a very temporary battle. Paying to have information on how to fix the latest IE 0day may protect you for the time being, but it wouldn't be coincidence if IE suffers another vulnerability on that very same day, and this time the details are sent for everyone to see at Full Disclosure mailing list. Rethink the big picture of the offering, and make up your mind

- "Fall in love" with the myth of an IPS solution in place

Whether a myth or not, that seems to be the obvious evolutionary response, while on the other hand, I wish all vulnerabilities had to do with buffer overflows only, which they don't. Any IPS solution is doomed to failure if wrongly configured and maintained if we exclude the flood of false detection alarms. There's a great chance they are active IPSs in your organization right now, and while its purpose is to prevent attacks, and is often marketed as 0day prevention system, it isn't the panacea of 0day vuln. security.

- continue enforcing your current security program and naturally, evaluating its effectiveness

100% is impossible, not even desirable in respect to aiming to achieve the 99% rate and leave 1% for the uncertainty in every of our actions. Ignoring the development of such a market may or may not compromise any of your current security strategies'

objectives, yet it may put you in unfavorable position given you ignore it. Intrusions are inevitable, no matter what you do, you will suffer them, what's important is what happens from there. Has the confidentiality of important information been breached through an 0day vulnerability, what would the state of your information be even in a case of intrusion?

To conclude, as the concept has always been there, I believe at this very particular moment 0days are traded either for money, or out of someone's egocentric ambitions, the point is some of them might be targeting your software or your security solutions. It is my personal opinion that soon, the industry will find itself bidding for someone's research given it doesn't want to create decentralized and hard to keep track of secondary markets. What you, as an organization can do is to better understand the uniqueness of your network infrastructure and ensure that no matter what happens the CIA of your assets remain in place. Anticipate the trade-offs and raise your expectations, moreover, don't think products, but actual understanding of the problem so that you'll find the balance.

[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.

- If you don't take care of your Security, someone else will -

Loading yourself with firewalls, AV and anti-spyware scanners, and thinking your secure is so untrue that many people regret to admit it. And while 100% security cannot be achieved, as well as, that, it's better to have these solutions in place compared to none at all -- ensuring you stay up to date with the latest threats, and employ the right security measures is what truly matters. In Issue 25 of the Astalavista's Security Newsletter we covered some tips for enhancing your brower's security. In this issue, we'll take another, of course, novice approach towards the security of your PC, namely that simply purchasing any of the security products we've mentioned is highly advisable, still, if you don't put some personal efforts into protecting your PC, someone else will -- while trying to breach it one way or another.

Keeping yourself up-to-date

I often get the question on how should I keep myself up to date with the latest threats? And the real question, which sites should I visit in order to do so. I bet you already visit the majority of mainstream one, but sometimes miss what you were looking for – info on the latest malware, new worms or vulnerabilities to patch etc. One of the places that provides

real-time information I highly recommend you to keep an eye on is the Internet Storm Center - http://isc.sans.org/, as far as malware is concerned, http://viruslist.com/ and perhaps F-Secure's World Map would come handy http://worldmap.f-secure.com/. Whenever there's a virus outbreak, on the majority of occasions different anti virus companies give the malware a different name, so at the bottom line, you may think you're reading about a new piece of malware, that is actually the same but under a different name. This is where the Common Malware Enumeration comes into place, with the idea to summarize information from different vendors and give it a common CME number. In case you want to avoid misunderstandings, consider visiting it http://cme.mitre.org/

Be suspicious, but always try to verify

No site is to be trusted given the flood and possibilities of XSS attacks, still, I doubt you will Google around for CNN.com in order to verify has it been spreading malware, BUT, do it for another site you feel suspicious about, or see if SiteAdvisor hasn't picked it up yet http://www.siteadvisor.com/analysis/ Suspicious about a file itself, try http://www.virustotal.com/ and Norman's sandbox, as an alternative method to scan a file. What's more to mention is that signatures themselves cannot provide 100% protection. So, I recommend you to go through a well summarized document on the features to look for in a good anti virus scanner.

DIY attitude

Wish we could solve all our security problems with the push of a button, or the purchase of a product, and while that is what Microsoft is aiming for with its OneCare service to be be released out of BETA anytime now, that's simply not possible. By having a DIY attitude I mean approaches as using the least privilege accounts one http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/luawinxp.mspx, doing your howework on Internet scams before you start calling your bank http://www.banksafeonline.org.uk/, and ensuring that no matter the 0day threat your browser is blocking the majority of potential threats http://www.cert.org/tech_tips/securing_browser/. Don't just want for someone else to secure you, secure yourself!

[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 **Martin Herfurt,** from the Trifinite Group http://trifinite.org/

Your comments are welcome at security@astalavista.net

Interview with Martin Herfurt, http://trifinite.org/

Astalavista : Hello Martin, would you, please, introduce yourself to our readers, and share with us some info on your background?

Martin : My name is Martin Herfurt and I am a security researcher from Salzburg, Austria. I studied at the Salzburg University of Applied Sciences and Technologies and at the University of Salzburg. In 2000, I did an internship in a telecommunications research lab in San Ramon, California before I completed my Telecommunications Engineering degree in 2001. From the end of 2000 until the end of 2005, I worked as a full time researcher in an Austrian research facility where I participated in several EU-funded projects in the area of network quality and software agents. At the end of 2005, I left Salzburg Research in order to concentrate on my Bluetooth security research.

Astalavista : How did the idea for Trifinite start, and how did you form the group? Moreover, what are some of your current and future projects worth mentioning?

Martin : When I first started getting involved in Bluetooth security, I was still employed as a full time researcher. Even though I tried to associate Salzburg Research as a small research company with my work in a lot of newspapers and magazines, my work didn't get appreciation from the management. After all, I was asked to stop working on Bluetooth security during my office time. This was the moment when the idea to start a group was born. That was back in August 2004. Collin Mulliner was the first member and after this Adam Laurie and Marcel Holtmann also joined the group. Over time, Mark Rowe, Tim Hurmann and finally, Kevin Finisterre and Joshua Wright joined the team. As one of the few groups that concentrate on Bluetooth security, we have quite a few good ideas that will come up soon. At the moment it is too early to talk about these projects, though.

Astalavista : It's a common sense that there are more mobile phone users than PC ones, and do you believe this would be among the important driving forces of security research on mobile devices in the future? What would some of the other trends be from your point of view?

Martin : If you take a look at the IT research landscape at the moment, you will find a lot of efforts in the area of mobile technologies. European research initiatives like 'The Disappearing Computer' and efforts in the area of Ubiquitous Computing and Ambient Intelligence are speaking a clear language in point of a future, where the majority of devices that are connected to the internet will be in somebody's pocket. As devices start to have multiple interfaces it enables them to exchange information via different means, so there is a big point in spending efforts in the area of mobile security research in the future.

After people get used to the idea of consuming information on their mobile devices, they will surely start to use their devices to generate information as well. At this point, when user sensitive passwords and other user information is stored on the device, it becomes necessary to protect the data on the devices even more.

Astalavista : What is the current state of mobile devices security market, can we talk about monocultures, clumsy vendors' responses,

and where's the weakest link from your point of view?

Martin : Mobile device security is getting a topic for an increasing number of research groups. Many auditing approaches from traditional security research do also apply to mobile device security research. For example, the Phenoelit group recently presented very interesting findings on the RIM BlackBerry infrastructure. Moreover, vendors of mobile devices start to realize that security becomes an important selling point and therefore most manufacturers have already started handling these incidents in a more co-operative way.

Astalavista : The cost-effective compared to GPS, "assets tracking" over mobile phones is already gaining grounds. What are your comments on this trend, as well as the use of physical location obtained through mobile phone in respect to any government or company's ambitions?

Martin : I see this trend and I have mixed feelings about it. On one hand, there are a lot of benefits especially for fleet management in large logistics companies. Tracking of children on their way back home and tracking of possessions like cars when they got stolen, are also applications that I like. On the other hand, there might be applications of this technology which are used to infringe somebody's privacy. I think of situations, when people are not aware of being tracked. Different from GPS based tracking solutions where people are mostly aware of its existence, governments can force mobile service providers to locate their customers by paging their handsets without the customer's permission. This way of locating individuals is quite sneaky but cell phone users are getting aware of the fact that they can be located that easily.

Astalavista : As far as mobile malware is concerned, how do you picture its development in the next two years? Also, what are your thoughts on claims that AV vendors are currently building buzz only compared to the real state of the threat? If true, would it still inevitably benefit everyone and fuel more research in the long term? What is the main reason for the immature mobile malware scene from your point of view?

Martin : As efforts in mobile security research will increase over the next years, there will be publications and PoC implementations of malware for mobile devices that can, and will be exploited by blackhats. Of course, AV vendors are taking advantage of mobile malware. This is good marketing. At first I had the impression that mobile malware is hyped too much by the AV vendors, but I start seeing the situation differently. The things that are happening now are going to be bigger or smaller building blocks of things to come. In order to analyze and understand future, more complex mobile malware, AV vendors cannot start early enough to gather knowledge about it.

In my opinion, the mobile malware scene has just began to grow within the last two years. Looking at the desktop computer landscape, where a majority of devices is utilized by the Windows operating system, malware can spread easily due to the standard software environment. For mobile devices this is not the case. At the moment, there is a high diversity

of mobile operating systems in use that do not allow a standard way of creating malware.

Astalavista : As a member of the Bluetooth SIG Security Expert Group, I wanted to ask you, what are some of group's current activities, and what do you feel the over 4000 Bluetooth SIG member companies are missing for the time being?

Martin : Currently, the Bluetooth SIG is starting to take the security issues much more seriously. We got involved in order to provide device security auditing to Bluetooth SIG members at the UnPlugFests which are interoperability test events. We also get a lot of positive feedback from the members and hope to continue providing this service since it helps manufacturers not to release malicious firmware. The Bluetooth SIG Security Experts Group is currently working on improvements of the Bluetooth standard since new applications of the Bluetooth wireless technology require higher security standards. In this regard, we are trying to provide ideas from a practical viewpoint that is sometimes not paid attention to in the rather formal specification documents. It is true that there could be more participation from the SIG member companies. Another truth is that it is really hard and time-consuming to do decisions in a large group. For security topics it is important to have a balanced forum for the discussion of problems, and to have the ability to make up decisions in a timely fashion.

Astalavista : What is your worst case scenario on abusing a Bluetooth or Specific handset vulnerabilities on a mass scale, or should we consider Segmented attacks only? What would you advise the end users and the corporate ones, on how should they protect the CIA of their mobile devices?

Martin : A worst-case scenario for the abuse of Bluetooth security vulnerabilities could be a worm that propagates via Bluetooth/MMS and exploits vulnerabilities on handsets that are known to have issues. This blending of currently known exploits, and malwares, could have very big impact. Problem awareness is the best way of protecting users from threats. Being informed about how malware can infect or affect devices helps to prevent users from being the target of attacks.

Astalavista : In conclusion, I wanted to ask you what else do you do besides actively researching wireless devices and their security issues?

Martin : At the moment, I enjoy travelling quite a lot. There is a lot of conferences that we get invited to in order to do talks and workshops. There are also some good business ideas that I will implement in the near future. These ideas do not relate to wireless security issues.

Astalavista : Thanks for your time, Martin

Martin : You are welcome!

[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.

-
VMware Ultimate Virtual Appliance Challenge
-

http://www.vmware.com/vmtn/appliances/challenge/

Are you up for the challenge of creating the industry's most innovative virtual appliance? VMware invites you to put your skills to the test, go head-to-head with your peers, and develop the best virtual appliance the industry has ever seen. Using open source or freely distributable components and/or your own code, create the most inventive and useful virtual appliance and win the $100,000 first prize!

-
PaulDotCom's Security Podcast
-
http://www.pauldotcom.com/

Security with attitude

-
ITSecurity Podcasts you can't miss
-
http://ww6.infoworld.com/products/print_friendly.jsp?link=/article/06/02/17/75431_08OPsecadvise_1.html

More security podcasts for you to consider

-
Security reviews : PCWorld's reviews of antivirus software
-
http://www.pcworld.com/reviews/article/0,aid,124475,00.asp

Benchmarking anti virus software

-
Security Reviews : Top 10 Anti Spyware Apps reviewed
-
http://reviews.cnet.com/4520-3688_7-6456087-1.html

Often, you don't suspect anything's wrong until you sense your computer is getting slower, and slower, and slower. Fortunately, many antispyware apps are on the market today. For this roundup, CNET teamed with Download.com, with CNET reviewing the apps' feature sets and Download.com testing each product's ability to

remove specific spyware.

[14] **Final Words**

Dear readers,

Sometimes you have to delay an issue to find out about its actual readership and meet some folks, as simply wouldn't allow this to happen again, as always, your feedback, comments, remarks are much appreciated.

Stay secure, and cool!

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net