Astalavista Group Security Newsletter
Issue 21 - 30 September 2005
http://www.astalavista.com/
security@astalavista.net

[01] **Introduction**

Hello folks,

Welcome to Issue 21 of the Astalavista Security Newsletter!

As usual we have picked up the most interesting news stories around the month, and provided you with insightful comments on them, featured the most useful tools and publications that appeared around the scene and at Astalavista.com during the month, and highlighted our monthly picks in terms of sites, programs, consultations etc. In this issue, you're going to read an article "**What else should I worry about besides the encryption length of our VPN remote access solution?"** covering various attacks and points of discussion when it comes to secure VPN connections, as well as "**Tips for enhancing your online privacy"**, a brief article covering trendy tips and recommendations on how to, at least partly, limit the amount of sensitive data you expose online every day. You will also go through a great interview with **Johannes Ullrich**, CTO for the **SANS Internet Storm Center**, the main developer behind the **Dshield.org** project.

Enjoy!!

Our **GeekyPhotos** section is online again, dazzle us with your shots at photos@astalavista.net and consider visiting the section itself at : http://www.astalavista.com/index.php?section=gallery

We also strongly encourage you to express your data retention and government monitoring of data opinion by participating in our poll " **Do you believe breaking strong encryption, monitoring you, or actively intercepting and retaining huge amounts of data, is justified for the sake of protecting you against terrorism?** "

Keep yourselves busy, inspired and watch out for the next edition of our newsletter!

Astalavista Security Newsletter is constantly mirrored at :

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

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

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

Previous issues of Astalavista Security Newsletter can be found at:

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

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

[02] Security News

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

---

[USERS PLAY FAST AND LOOSE WITH CORPORATE PCS]

Internet security firm Trend Micro published results of an online survey of 1,200 US, German, and Japanese corporate employees. The survey found that internet users conduct riskier online behavior while at work, believing that there is better protection in the workplace from viruses, spyware and other threats. Two thirds of respondents agreed that they are "more comfortable with clicking on suspicious links or visiting suspicious Web sites" while at work, and 40 percent allowed that they visit suspicious sites because they felt that their IT department would step in and fix any resulting problems.

More information can be found at :

http://www.theregister.co.uk/2005/09/13/unsafe_computing_survey/

Astalavista's comments :

Great initiative from Trend Micro, as any organization's management needs to wake up and realize that the countless security awareness programs, anti-virus scanners and the rest of your risk mitigation approaches sometimes result in a bit of destructive behaviour due to this enterprise sense of security.

Surveys are always questioned, and even though globally accepted as a research method, the way questions are provided, and later analyzed could play a crucial role in their objectivity. My point is that I don't believe end users tend to act irresponsibly because they feel the IT dept. is going to fix it afterwards – but because they feel the work place is a much more protected environment than their home PCs – how true or false opens up yet another discussion, but what end users should consider is that their activities are under surveillance.

From an organizational point of view – education is great, policies are compulsory, but a bit of restrictive environment, yet efficient and active communication towards the consequences of abusing the workstation would perhaps make them think twice.

TrendMicro's press release is available at :

http://www.trendmicro.com/en/about/news/pr/archive/2005/pr091305.htm

[**EURO EMAIL STORAGE SCHEME 'ILLEGAL', WARNS OFFICIAL**]

The European Data Protection Supervisor (EDPS), Peter Hustinx, published his opinion on a potential European directive on data retention, including "strict conditions" any future law must meet to be deemed acceptable. Hustinex's main concern with the proposed directive, which would require retention of all internet data for six months, is privacy. He said, "The Directive has a direct impact on the protection of privacy of EU citizens and it is crucial that it respects their fundamental rights, as settled by the case law of the European Court of Human Rights. A legislative measure that would weaken the protection is not only unacceptable but also illegal."

More information can be found at :

http://www.theregister.co.uk/2005/09/26/eu_dp_sceptical/

Astalavista's comments :

Data retention is NOT A SOLUTION to terrorism and these are some of my Statements behind the opinion :

terrorists won't use net cafes to communicate with each other, I keep amusing myself with net cafes spreading warning messages that illegal activities will be reported to the police, and that if you're caught in sending spam, the same situation will follow, which is pretty much the same as emphasizing the "you're watched" policy of stores, metro stations

information can be hidden and embedded in any single audio and multimedia file, later on exchanged over an anonymous P2P network, and it can be done with 99% anonymity

*you cannot deal with both steganographic and encrypted content on a large scale, and even though a single, yet critical communication in the form of an HTTP request or embedded message in a spam email (**Spammimic.com** for proof of concept) will you retain spam too?!*

*Eventually, the institution responsible for data mining the information would end up with budget deficit the way the infamous **Total Information Awareness** program ended up while trying to provide a God's Eyes view of potential terrorists. Besides all, what is that you are trying to achieve – prevent terrorism, detect terrorism, avoid or detect emerging terrorism in the form of individual or group of individuals shaping future perceptions and interests on the topic, or trying to establish a social responsibility that indeed "everything's under control" – well it isn't*

unless you know what exactly you're trying to achieve.

Who suffers – the ISPs who would have to retain all this information, store and manage it, and the overall public having concerns about EU' s constant contradiction with its values, politics you say, good but terrorism cannot be fought with technology, as it's the use of technology and information dissemination that contributed to the overall economic growth, and it acts as a facilitator of terrorists activities these days.

*The **Digital Civil Rights in Europe** group has a lot to say on the topic :*

http://www.edri.org

and in case you are interested in signing the Data Retention is No Solution petition, do so at :

http://www.dataretentionisnosolution.com/

[**AUTHORS SUE GOOGLE**]

Google's "Print for Libraries" program is the target of a copyright infringement Lawsuit filed by the Authors Guild and former US poet laureate Daniel Hoffman. Google had started the process of scanning collections from five libraries to include selections in search engine results. The president of the Authors Guild, Nick Taylor, calls the bypassing of the author's rights a "plain and brazen violation of copyright law". Although Google halted the library digitization in August the publishers have proceeded with the suit.

More information can be found at :

http://www.theregister.co.uk/2005/09/21/authors_sue_google/

Astalavista's comments :

The search monster Google has totally scared everyone and perhaps even surpassed its own expectations on its tremendous impact on the future of searching, finding and researching information. As an author, I would feel totally ripped off, given that Google goes through my book and indexes it for future searches, while not paying me a dime, true but totally messed up .What authors are going to benefit from it is the exposure Google is going to give to their books. By the time search queries show integrated results from hard copy books, these would eventually result in a sale of the book. Google's taking its share for the promotion, and so is the publisher. From there it would depend on the author's contact and business practices in case future revenues are secured.

Authors have to wake up and realize the potential of the Internet for building up their popularity, and spread their works, while ensure they've done their homework when it comes to copyrights infringement online.

*Check out **Rupert Murdock's** comments on the growing threat to print media posed by the Internet :*

http://www.newscorp.com/news/news_247.html

[**RESEARCHERS TURN KEYBOARD CLICKS INTO TEXT**]

University of California, Berkeley, researchers have used "statistical learning theory", also called "machine learning", to translate the sounds of keyboard strikes into text with up to 96 percent accuracy. The slightly different sounds made by each key are analyzed by software, then refined through spelling and grammar correction tools. The researchers are not releasing their code, but say it was relatively easy to develop, and inexpensive to implement. Their best suggestion for defending against a possible use of this method to use background noise, such as music, to mask the keyboard sounds.

More info can be found at :

http://www.infoworld.com/article/05/09/14/HNkeyboardclicks_1.html

Astalavista's comments :

I totally enjoyed this "breakthrough", since the theory behind it came to my mind over 2 years ago. What's next, and what I've actually seen working is a remote digital camera recoding of keyboard typing though physical compromise, with the idea to gather login details, or snoop of the display. ***3M's PrivacyFilter*** *might come handy in situations like these though. What about wireless keyboards you wonder?* ***WarTyping.com*** *is a great initiative that gives you the opportunity to listen to your keypressing – over the air!*

http://www.wartyping.com/content/audio/logitech_keyboard.mp3

Future research could definitely incorporate these turning it into yet another technique in the arsenal of spies or malicious attackers with very serious reasons to compromise your information. Concerned about this new keyboard typing threat – well don't, as we are sure you enjoy loud music the way we do – secure by default!

[**BOT HERDER WEBSITES IN INTERNET TAKE-DOWN**]

F-Secure reports that a number of websites offering botware source code and botnet management tools with simple user interfaces have been shut down by authorities. Among these 'bot-herder' sites are such well known sources as ryan1918.com, 0x90-team.com, and neo-theone.com.ar. Botware sites are starting to charge fees for users who download source code. While hackers have long traded botnets and botnet usage rights, only recently have they offered hosted botnet management. Herder sites tend to be short-lived, since authorities shut them down as soon as they find them.

More information can be found at :

http://www.theregister.co.uk/2005/09/13/bot_herder_takedown/

Astalavista's comments :

Malicious source code has been distributed over the net as far as I can remember

myself, where because of leaks, for the sake of someone's ego and popularity ambitious, or "just because". Let's face the facts, modularization of malware and the availability of source codes greatly contributes to variations of the malware itself, and contributes to nothing besides yet another worm in the news. People possessing or involved with the development of these are trying to make a quick buck out of selling the source, or actually tutoring "customers" on what it does and how to improve it. It is well said that "in the future everyone will be famous for 15 minutes", picture the flood of wannabe malware authors AND the growth of the anti-virus sector!

On the other hand, my dear friend ***Anthony Aykut*** *(Frame4 Security Systems), has managed to unveil that* ***neo-theone.com.ar*** *is still pretty active, great work dude! :*

http://www.frame4.com/cms/index.php?option=com_simpleboard&func=view&catid=130&id=155#155

[**CHINA CRIMINALIZES INTERNET TELEPHONY**]

China Telecom, the largest fixed line telephone carrier in China, is not allowing its broadband customers to use Skype to make long-distance calls. Those that defy the ban will be subject to fines or even have their internet connections cut off. Currently, it is illegal in China to use network telephones, and management rights of internet telephone service falls under China's Communications Management Bureau. Recent declines in China Telecom's business have been attributed to the rise of Internet telephony.

More information is available at :

http://www.newsfactor.com/story.xhtml?story_id=38165

Astalavista's comments :

Even though the country is about to join the WTO, witnessing a true free market economy is rather doubtful given this "you cannot capitalize on innovative business concepts until we figure out how to do it first" approach of China. An interesting fact I came across in the ***Red Herring*** *magazine is that China Telecom's fixed-line business is not profitable, picture the effect of introducing Skype on the local market.*

Like any government, the Chinese government likes to feel in control but unlike any other, the country's approach supported by modern communism promotes centralization, which eventually results in more effective control and monitoring, but limits the level of innovation and competition. The implications for VoIP telephony in the country have two dimensions – from a business point of view it would devastate China's Telecom, responsible for handling 70% of the country's communications, while from a national security view, it would be inevitable resulting in loss of control when it comes to censoring or monitoring.

Chinese end users are once again caught in between figuring out how to bypass this and take advantage of Skype, while trying not to get caught for…using VoIP!

[**CISCO FLAW COULD ALLOW ROUTER WORM**]

Security researchers say they have found weaknesses in Cisco's Internet Operating System (IOS) which may enable an Internet worm to spread between Cisco routers. But Arhont Ltd. denied reports that such a worm had actually been developed.

In a post to the Bugtraq mailing list, Arhont's Andrei Mikhailovsky said his firm had discovered weaknesses in the way IOS uses the Enhanced Interior Gateway Routing Protocol (EIGRP), which handles information exchange between routers.

More information can be found at :

http://news.netcraft.com/archives/2005/09/20/report_cisco_flaw_could_allow_router_worm.html

Astalavista's comments :

Could or would? I doubt someone is that totally insane, irresponsible given the knowledge required from my point of view, not just to execute, but to actually infect, hide and realize the potential of such a superworm, attacking the very core of the Internet – its routers. The implications of such a worm require a much broader understanding of the amount and content of data can be gather, while for me it has always acted as the best example sensitive of plain-text commucations. Those interested in such a worm would include government agencies wanting to make sure they are not vulnerable, but can exploit adversaries' networks, segmentation based worms, namely those who would do their best not to generate any suspicious traffic on a world scale, and a mad man who cannot find out how to abuse the Internet and eventually decides to cause havoc.

Some of the best research papers on the topic I enjoyed reading a long time ago are:

Routing Worm : A Fast, Selective Attack Worm based on IP Address Information

http://tennis.ecs.umass.edu/~czou/research/routingWorm-techreport.pdf

[NSA GRANTED NET LOCATION-TRACKING PATENT]

Patent 6,947,978, granted Tuesday, describes a way to discover someone's physical location by comparing it to a "map" of Internet addresses with known locations.

The NSA did not respond on Wednesday to an interview request, and the patent description talks only generally about the technology's potential uses. It says the geographic location of Internet users could be used to "measure the effectiveness of advertising across geographic regions" or flag a password that "could be noted or disabled if not used from or near the appropriate location."

More information can be found at :

http://beta.news.com.com/2100-7348_3-5875953.html?

Astalavista's comments :

What I like in the approach is that it doesn't blindly try to guess the location, but matches with predefined ones. On a large intelligence scale, this, when integrated within different data gathering sensors, could link up an entire profile and provide more clarity into who's who, who's where, and who's been there and there, and who's coming from where. Their approach goes beyond

IPtoGeolocation, one in that the NSA utilizes many more, authorized or not access to HUGE network data streams, that just have to be coordinated in order to provide the NSA with a different look of the Internet.

A great research on the very same topic can be found at :

http://www.caida.org/outreach/papers/2005/fingerprinting/KohnoBroidoClaffy05-devicefingerprinting.pdf

The patent itself can be found at :

http://cryptome.org/nsa-6947978.htm

[DON'T TRUST SECURITY TO TECHIES ALONE, GARTNET SAYS]

Jay Heiser, a Gartner vice president, said the fundamental problem with a purely technical approach is that IT security professionals have no understanding of business. Speaking at this week's Gartner IT Security Summit in London, Heiser said businesses must now mature and appoint individuals who understand the complexities of business, rather than the simplicities of security.

A "risk management officer" is now more critical than the traditional security professional whose job is either a part-time distraction from network management, or to "scare money out of the CIO" or block projects that could have been beneficial to the organization, Heiser said.

More information can be found at :

http://news.zdnet.com/2100-1009_22-5868906.html

Astalavista's comments :

Even though I fully agree that security consultants and other security experts need to have at least basic understanding of the business processes, so that they would try to achieve even more balance between efficiency and security risks, you should require your consultants to have an MBA degree. What's more, I'm a firm believer in the industry's shift towards risk management instead of plain penetration testing and perimeter based consultations from people heavily investing into security auditing tools. Face the facts, the industry is flooded with security consultants with as many security certificates as there are malicious connection attempts on your networks – but lacking out a basic business understanding. That, from my point of view, will result in a much more informed and balanced solution.

[YAHOO! ASSISTS CHINESE DISSIDENT CONVICTION]

Media watchdog Reporters Without Borders has accused Yahoo! of going out of its way to help Chinese authorities to convict a "dissident journalist".

Shi Tao was sentenced in April to 10 years imprisonment for "divulging state secrets" partly on the basis of evidence supplied by Yahoo!. Reporters Without Borders said it "provided China's state security authorities with details that helped to identify and convict him".

"We already knew that Yahoo! collaborates enthusiastically with the Chinese regime in questions of censorship, and now we know it is a Chinese police informant as well," the press freedom organization said.

Yahoo! is attempting to downplay the row by saying it was simply complying with local laws in assisting the Chinese authorities. Yahoo! Spokeswoman Mary Osako said: "Just like any other global company, Yahoo! must ensure that its local country sites operate within the laws, regulations and customs of the country in which they are based."

More information can be found at :

http://www.theregister.co.uk/2005/09/07/yahoo_china_dissident_case/

Astalavista's comments :

Totally bad publicity for this anyway, outstanding brand, that like pretty much all the major international companies are trying to penetrate the Chinese market, which unlike others has many censorship related legislations to be taken care of and enforced if necessary. Sounds pretty normal from a business point of view, and obviously moral and ethics are out of the question. While the topic bugs me a lot, I can only imagine what Google have done or are currently doing when it comes to enforcements like this.

***Cryptome.org** has featured a **Yahoo! Rats** story to express their attitude towards these actions :*

http://cryptome.org/yahoo-rats.htm

[03] **Astalavista Recommends**

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

" **RULES FOR FIREWALLS** "

These rules are generated from RIPE LISTS, APNIC LISTS, LACNIC LISTS and ARIN LISTS. Therefore IP address ranges of these countries are not listed in mentioned LISTS cannot list below rules. As a consequence, note that only these lists cannot deny all IP-addresses of the above-mentioned countries. But I think if use this, in almost cases, you can completely deny direct accesses from these countries.

http://www.astalavista.com/index.php?section=directory&linkid=5025

" **OP V1.31** "

The op tool provides a flexible means for system administrators to grant access to certain root operations without having to give them full superuser privileges. Different sets of users may access different operations, and the security-related aspects of each operation can be carefully controlled.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5029

" **MASSIVE – ENUMERATION TOOSET** "

MASSIVE Enumeration Toolset, or MET, is a small tool that helps mine information from google.com. It supports Johnny's GHDB (Google Hacking Database XML Format) and Google's SOAP and Mobile APIs.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5015

" **ANALYZER – PHP SECURITY PROBER** "

Analyzer is a PHP open source script that tests and debugs any kind of PHP-Nuke based installation. Security checks are done for them, including MySQL, PHP, and PHP.INI settings such as register globals. Script can run in any OS environment that supports PHP.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5108

" **WIKID – OPEN-SOURCE SECURE TWO-FACTOR AUTHENTICATION SYSTEM** "

The WiKID Strong Authentication System is a highly scalable, secure two-factor authentication system consisting of a server, a token client, and network clients that connect a service such as a VPN or Web page to the WiKID server to validate one-time pass codes. The user enters their PIN into the token client, where it is encrypted and sent to the server. If the PIN is correct, the encryption valid, and account active, the one-time pass code is generated, encrypted, and returned to the user.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5056

" **GMAIL DRIVE V1.08** "

GMail Drive is a Shell Namespace Extension that creates a virtual filesystem around your Google GMail account, allowing you to use GMail as a storage medium. GMail Drive creates a virtual filesystem on top of your Google GMail account and enables you to save and retrieve files stored on your GMail account directly from inside Windows Explorer. GMail Drive literally adds a new drive to your computer under the My Computer folder, where you can create new folders, copy and drag'n'drop files to.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5102

" **TOOLBARCOP V3.4** "

Toolbarcop can be used to eliminate malware toolbands, toolbar icons and browser helper objects in Internet Explorer.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5006

" **THE TABLE OF QUIVALENTS, REPLACEMENTS, ANALOGS OF WINDOWS SOFTWARE IN LINUX** "

Even though a bit outdated, it may still come handy for everyone.

http://www.astalavista.com/index.php?section=directory&linkid=5026

" **RWKG RANDOM WEP/WPA KEYS GENERATOR** "

The RWKG tool can be used to generate random WEP and WPA keys. These randomly generated a strings of allowed ASCII characters are then converted to their hex format (where 5/13/16/29 characters are used to create 64/128/152/256 bits WEP keys, or between 8 and 63 characters strings to create WPA/PSK keys).

http://www.astalavista.com/index.php?section=directory&linkid=5020

" **ZEBEDEE – SECURE IP TUNNEL** "

Zebedee is a simple program to establish an encrypted, compressed "tunnel" for TCP/IP or UDP data transfer between two systems. This allows traffic such as telnet, ftp and X to be protected from snooping as well as potentially gaining performance over low-bandwidth networks from compression.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5059

[04] **Astalavista Recommended Papers**

" **DATABASE SECURITY AND CONFIDENTIALITY : EXAMINING DISCLOSURE RISK VS. DATA UTILITY** "

Managers of database security must ensure that data access does not compromise the confidentiality afforded data providers, whether individuals or establishments. Recognizing that deidentification of data is generally inadequate to protect confidentiality against attack by a data snooper, managers of information organizations (IOs)—such as statistical agencies, data archives, and trade associations—can implement a variety of disclosure limitation (DL) techniques - such as top coding, noise addition and data swapping—in developing data products.

http://www.astalavista.com/index.php?section=directory&linkid=5013

" **ADVANCED POLYMORPHIC WORMS : EVADING IDS BY BLENDING IN WITH NORMAL TRAFFIC** "

Normal traffic can provide worms with a very good source of information to camouflage themselves. In this paper, we explore the concept of polymorphic worms that mutate based on normal traffic. We assume that a worm has already penetrated a system and is trying to hide its presence and propagation attempts from an IDS.We focus on stealthy worms that cannot be reliably detected by increases in traffic because of their low propagation factor.We first give an example of a simple polymorphic worm. Such worms can evade a signature-based IDS but not necessarily an anomaly-based IDS. We then show that it is feasible for an advanced polymorphic worm to gather a normal traffic

profile and use it to evade an anomaly-based IDS.

http://www.astalavista.com/index.php?section=directory&linkid=5027

" **XCON'S PRESENTATIONS** "

Topics include : Anti-Virus Heuristics Reconfigurable Synchronization Technique, Talking About 0day, Structural Signature and Signature's Structure, Java & Secure Programming, Hacking Windows CE, Windows Kernel Pool Overflow Exploitation Demo, I want to see farther, New architecture and approach in Network Virus Detction, Advanced Trojan in Grub, New thoughts in ring3 nt rootkit Demo Security in development environment Research on Same Source Feature Measuring Technology of Software, Profiling Malware and Rootkits from Kernel-Mode

http://www.astalavista.com/index.php?section=directory&linkid=5016

" **THE CASE FOR USING LAYERED DEFENSES TO STOP WORMS** "

For this paper, we studied current worm strategies and implementations and tried to determine whether the trends point to a significant worsening of the problem in the near future. Are worm technologies improving? Are worm attacks becoming more sophisticated? We were also interested in defensive technologies that can be used to combat the worm problem. Where are defensive technologies best applied?

http://www.astalavista.com/index.php?section=directory&linkid=5052

" **THE SECURITY ARCHITECTURE FOR OPEN GRID SERVICES** "

This document proposes a strategy for addressing security within the Open Grid Services Architecture (OGSA). It defines a comprehensive Grid security architecture that supports, integrates and unifies popular security models, mechanisms, protocols, platforms and technologies in a way that enables a variety of systems to interoperate securely. The document presents a security model, describes a set of security components that need to be realized in the OGSA security architecture, and presents a set of use patterns that show how these components can be used together in a secure Grid environment.

http://www.astalavista.com/index.php?section=directory&linkid=5044

" **HOW YAHOO FUNDS SPYWARE** "

This article proceeds in three parts. First, I show examples of Yahoo ads supporting Claria, eXact Advertising, Direct Revenue, 180solutions, and various others; I also review the objectionable practices of each of these vendors. (Numerous additional examples on file.) Second, I review Yahoo's disclosures to advertisers -- finding that Yahoo has failed to tell advertisers about its controversial syndication partners, even in general terms. I conclude with recommendations to Yahoo (and other PPC search engines that allow syndication), as to how to put an end to this mess and avoid such problems in the future.

http://www.astalavista.com/index.php?section=directory&linkid=5041

" **UNDERSTANDING A HACKER'S MIND – A PSYCHOLOGICAL INSIGHT INTO THE HIJACKING**

OF IDENTITIES"

This paper explores both the scope and the intentions of hackers – and furthermore, how enterprises are victimised, especially in terms of identity theft. It was important to us to understand the minds of hackers; therefore we spent time analysing their psychological and sociological drivers as well as their intentions and methodologies. We examined recent abstracts and research projects conducted by prominent academics and experts, including an empiric study by the German Bundeskriminalamt (BKA) that aims to sensitise society in terms of identity theft, underlining theory with examples from the real world.

http://www.astalavista.com/index.php?section=directory&linkid=5055

" **HOWTO INSTALL MAC OS X ON A COMMODITY INTEL PC IN 8 STEPS** "

A guide to installing the developer Intel version of Mac OS X Tiger (Intel) on a generic PC. The amazing thing: I installed and troubleshooted the installation of Mac OS X on Intel in 8 steps."

http://www.astalavista.com/index.php?section=directory&linkid=5064

" **DETECTING TRAFFIC ANOMALIES THROUGH AGGREGATE ANALYSIS OF PACKET HEADER DATA** "

If efficient network analysis tools were available, it could become possible to detect the attacks, anomalies and to appropriately take action to contain the attacks. In this paper, we suggest a technique for traffic anomaly detection based on analyzing correlation of destination IP addresses in outgoing traffic at an egress router. This address correlation data are transformed through discrete wavelet transform for effective detection of anomalies through statistical analysis. Our techniques can be employed for post-mortem and real-time analysis of outgoing network traffic at a campus edge.

http://www.astalavista.com/index.php?section=directory&linkid=5034

" **A STRUCTURED APPROACH TO CLASSIFYING SECURITY VULNERABILITIES** "

Understanding vulnerabilities is critical to understanding the threats they represent. Vulnerabilities classification enables collection of frequency data; trend analysis of vulnerabilities; correlation with incidents, exploits, and artefacts; and evaluation of the effectiveness of countermeasures. Existing classification schemes are based on vulnerability reports and not on an engineering analysis of the problem domain. In this report a classification scheme that uses attribute-value pairs to provide a multidimensional view of vulnerabilities is proposed.

http://www.astalavista.com/index.php?section=directory&linkid=5071

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

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

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

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

and our **30%** discount this month

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

What is Astalavista.net all about?

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

Among the many other features of the portal are :

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

[06] Site of the month

Top 500 Supercomputers for June 2005

The TOP500 project was started in 1993 to provide a reliable basis for tracking and detecting trends in high-performance computing. Twice a year, a list of the sites operating the 500 most powerful computer systems is assembled and released.

http://www.top500.org/

[07] Tool of the month

EULAlyzer v1.0

EULAlyzer can analyze license agreements in seconds, and provide a detailed listing of potentially interesting words and phrases. Discover if the software you're about to install displays pop-up ads, transmits personally identifiable information,

uses unique identifiers to track you, or much more.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5082

[08] **Paper of the month**

An Illustrated Guide to IPSec

This is the first of two papers, the second of which covers key exchange, the Security Parameters Database, and other finer points of an IPSec configuration: in this paper we'll touch on them only briefly.

http://www.astalavista.com/index.php?section=directory&linkid=5046

[09] **Free Security Consultation**

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

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

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

Question : Hello folks at Astalavista, great newsletter, very informative, keep up the good work and your spirit!! I happen to maintain a relatively small network, network security budgets are a bit out of the question even though we take care of viruses and spyware by using a well known vendor's appliance. What bothers me is that recently I've received notifications computers unable to download their anti-virus updates, and also complaints from laptop users who are also having the same problems both when using our network and from home. What might be the problem?

Answer : I feel, that these very same local and remote users are actually the ones infected with some malware, which is successfully blocking their requests to major anti-virus update sites – a techniques that's very common for the majority of malware these days. Are there any integrity checking and verification practices in place, are desktops restored to their default configurations, besides all, why would an end user be given the opportunity to touch his/her HOSTS file at all? Ensure that laptop users are fist scanned and clean before any connection to the network is allowed, it would greatly reduce the risk of further infections.

Question : Hi people, I really appreciate your contributions and decided to drop you a line on a problem I have right now. I feel someone's using my bandwidth and was wondering could it be someone transferring data from my PC to someone else, or even hosting it? I would define myself as an experienced gamer, but security on my PC is taken care of a firewall and anti-virus program that a friend installed once?

Answer : There's always a real chance you could be participating in a botnetwork, and the best, and free way to check it is by visiting **Dshield.org**, a distributed security events network that would let you know if your IP address has been noticed doing something suspicious. You can also read an interview with its main developer, which we have interviewed in this issue of our newsletter. A great traffic measurement and tracking tool is usually provided by your ISP. It will provide you with a detailed overview on how much traffic you have consumed and when, just for reporting purposes and in case you're interested. Keeping an eye on this, at least though to be an independent source; given that host based traffic monitoring tools can by bypassed, you will have the chance to notice any abnormal traffic activities going on. Ensure the PC is 99% malware free and ensure your application level firewall permits only traffic that matters to you.

Question : Dear folks at Astalavista, I wanted to share a situation I had recently. I have always trusted the content of CDs and DVDs and though they are viruses free, I have different opinion on this one these days as I got myself infected from a CD that I borrowed from a friend. As it's totally freeware applications, he denies having anything to do with that. Should I always check their content, and isn't this too time-consuming, even unnecessary?

Answer : Time-consuming, perhaps if you don't have an on-the-fly virus protection, unnecessary that greatly depends on its content and how much you trust it. Freeware applications CDs always pose a risk, and several years ago I personally witnessed a flowed model for distribution of readers-coded applications on a CD, which resulted in the magazine's infected readers due to the majority of 0-day viruses on it. A decent, real-time malware protection should help you, but common sense before trusting content is your best solution.

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

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

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

the DVD!

More information about the DVD is available at:

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

[11] **Enterprise Security Issues**

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

- **What else should I worry about besides the encryption length of my VPN solution? -**

This article will give you a brief overview of the important role VPNs play in today's highly mobile workforce and constant integration between partners and suppliers. It would also provide you with an understanding of the associated flaws and practical recommendations on how to deal with them. VPNs are indeed among the most cost-effective solutions for remote and secure access to a company's organization, given they're reasonably protected.

During the last couple of years we have witnessed the development of the mobile organization, with employees, salespeople, partners and suppliers each of them eager to connect to your company's infrastructure with the idea to share data, request or syndicate such. The benefits of today's information sharing economy have had a tremendous impact on the improved levels of productivity and the transparency of the infrastructure itself, however the open nature of these networks turns them into valuable entry points in the organization's network.

Some of the associated risks with the introduction of VPNs is perhaps the myth behind the encrypted communication, one of the main purposes of the protocol, besides ensuring the right people connect to the organization over the Internet as a public network. Being "invincible" is always tricky at the end and you should consider living with the idea that every new productivity related concept has its security implications tool.

Some of the issues you should consider paying more attention to are :

Client-side attacks – as always these represent the end users themselves, naïve, irresponsible, unaware of today's tricky tactics of malicious attackers, while holding one of the keys to your internal network. Lack of understanding of physical security, irresponsible maintenance of login data would definitely cause you a lot of trouble. What's even worse – all the threats that apply to a general PC such as malware, spyware, keyloggers could be employed as well.

Ensuring Man-in-the-Middle attacks are out of the question even though malicious routers or servers transfer any of the data, could be achieved with adding yet another layer of security, namely digital certificates and IPSec

Avoid default configurations of software and hardware in case you want to sacrifice security for productivity.

The perimeter based security of your VPN device would naturally affect both its Effectiveness and security. Fingerprinting your server should be out of the question, and ensuring IDSs can analyze traffic within the tunnel, otherwise several other scenarios arise. IPSec should be considered the protocol of choice.

Authentication should be enhanced, and no information should be shared before a reliable authentication is achieved, with the help of SSL for instance.

Another crucial, but often overlooked issue, is to never allow full access to all your resources, sounds simple. It is, while it isn't as often considered as it should.

Check out the following publications closely related with the topic of VPNs and secure data transfer :

http://www.astalavista.com/index.php?section=directory&linkid=1837
http://www.astalavista.com/media/directory/uploads/openvpn.pdf
http://www.astalavista.com/index.php?section=directory&linkid=3620

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

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

- **Tips for enhancing your online privacy** -

This article will give you a basic understanding of today's level of privacy exposure, why it's inevitable, how unwanted the implications could be, and how to ensure you take advantage of the Internet without loosing what's most important to you.

Information researching is possible, mainly because of the fact that people share information. Each and every day you share information that provides you with the ability to pay your bills, do your research, register for a web services, communicate with friends, and be an active participant in the 21st century. Distinguishing between sensitive, private and unimportant data varies from person to person, whereas your exact physical location, daily habits of using the Internet, your age, sexual orientation or music preferences can all be defined as rather sensitive information given a particular situation. In order to take advantage of all the joys in this multi-connected world, you would inevitably have to sacrifice some of your privacy, the way you search and research for private topics, or the way your retailer needs to act as an intermediary while processing your credit card purchase.

The main risks associated with your privacy are the exposure of your private date, its interception over the Internet, or your ticking you into somehow

revealing it be it in from of a web form, or Internet participant. Making sure you're protected wouldn't mean you would simply have to follow these tips, but trying to understand the impact and why you should bother could prove to be successful.

Never reveal personal information to unknown or not to be trusted web sites

> Simply don't give your personal email, real address, names, zips etc unless you absolutely have to. Companies, even scammers are constantly trying to gather as much info as possible, what later one happens with this information is pretty much automated newsletter subscriptions, sold email to a spammer, or a malicious attacker trying to trick you into revealing more info about yourself.

Don't disclose personal information to strangers

> But what is a stranger these days over the Internet? Consider anything unusually suspicious, don't go into talkative mode unless you are absolutely sure who you're talking to, best of all try to link the uses/abuses of every information you give. These days it's not just about the personal privacy we're talking about, but to the balance of your credit card or the one you didn't know you actually applied for.

Consider proxies a double-edged sword

> It may come handy as a solution, or as a way to bypass certain restrictions, as proxies are available on pretty much every privacy/security web site out there. What is to be considered is that a great deal of proxies these days are acting as honey pots run by researchers, malicious users, or the Feds themselves. For absolutely no reason don't access login-based services through the use of proxies.

Always know that you may be actually watched

> Doing what, it's up to you, keeping this in mind might make you think in a constructive "what if" analysis way. What if I were watched?!

Never transfer sensitive information in plain-text

> Simple, while the simplest things are the basis of everything. If you want to be at least partly(but better than nothing!) ensured, don't send information you wouldn't want others to see in plain-text, which is like sending a letter and leaving it open, could and would be read!

Don't leave important information unencrypted while stored online/offline

> If you want to take advantage of hosting sensitive information online or offline, ensure it's encrypted and not just laying there in plain-text. The disadvantages will come with the keys, while the advantages will protect you even when having your account/security compromised.

Ensure your PC is as secure as possible from threats such as malware and spyware

Today's malware and spyware no longer collect keystrokes for the sake of their authors' amusement. Instead, financial information, transactions, research projects, logins and passwords are the topics of interest. Understanding malware and spyware, at least slightly will improve your ways of protection even more, don't just go for the tool itself, understand what it DOES, and what it DOESN'T.

Make sure you are aware of an site's/HR agency's Privacy Policy

Ok, you will say, but Google's Privacy bothers me and I simply cannot stop using it – very good point, then consider timing attacks, Google's cookie and the nature of your daily/average requests cannot be associated with you. Privacy policies are never read, whereas they might reveal shocking information on a company's practices, - did you know Gmail.com is keeping emails after they are deleted for "some period of time", open statements like these are simply unacceptable, while there's a bigger goal behind this, it's out of the topic for the purpose of this article. Make sure you know who you are sending your CV to, and what is eventually going to happen with it. What I usually do is that I digitally encrypt and leave a small unique ID that cannot be modified which I later on associate with the company I applied for, rather impractical to some, sense of security for others , but in case I see it somewhere, I would be able to immediately identify where it leaked from.

Concerns on the use of web anonymizer services

Web anonymizing services have shown a steady growth, due to the end users' concerns about privacy and hostile web sites. My advice is that if you go for such a service, keep in mind that actively searching for child pornography wouldn't stay unnoticed, and make sure you inform yourself on how anonymous it actually is. Besides all, mixing network traffic from end users, corporate and government institutions is always mixed in a way it can be proved who was who, so it doesn't end up in blaming the Justice Department for the malicious download of... ☺

Consider avoiding HTML based emails

Great interactivity, while totally unnecessary in case you don't want to open yourself to a great deal of other active attacks, as well as expose your online presence.

[13] **Meet the Security Scene**

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **Johannes Ullrich**, CTO of the **SANS Internet Storm Center**, and the main developer behind the **Dshield.org** project.

Your comments are welcome at security@astalavista.net

Interview with Johannes Ullrich, http://www.dshield.org/

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

Johannes : I started out as a physicist, and worked as a researcher for a small company for a few years. Throughout my graduate work, and in my first job, I was heavily using a computer, and having more fun with that part than the actual physics. So I decided to switch fields and took a position with a web development company. Security was always part of what I did in one way or another. After the big wave of attacks against e-bay and others in early 2000, I heard about how corporations (in particular banks at the time) attempted to setup information sharing systems. At the same time, personal firewalls became popular and I figured it would be easy for home users to exchange information in the same way. This is how DShield was born. While it took me a while after the initial idea to further think things through, I sat down for the Thanksgiving weekend in 2000 and wrote the first version of DShield.

Astalavista : How did the idea of Dshield come out, were you concerned about the acceptance of the idea, and how would you describe the project today compared to what it was when you started it?

Johannes : Probably the most obvious change is growth, and the integration of DShield into the Internet Storm Center. While it is still used by a lot of home users, DShield is now being taken serious by a lot of corporate users and governments. The Internet Storm Center provides invaluable manpower to DShield in the form of our volunteer handlers.

Astalavista : Josh Bethencourt, et al, released a paper entitled "Mapping Internet Sensors With Probe Response Attacks" at the 14th USENIX Security Symposium, highlighting various threats to sensor networks. What do you think are indeed, the biggest threats to their future?

Johannes : DShield is in so far different from some of the other data collection efforts in that it is using real life networks. In so far, the threat of sensor evasion is an opportunity. The more sensors, the less space there is left to attack. We do monitor the data carefully for the injection of false data. Up to this point, the main problem is sensor misconfiguration. We always had 'data harvesting' protections in place, and continue to refine them. Again, the main threat here are innocent mistakes with people writing automated query systems that will result in a DDOS attack.

Astalavista : Do you believe that while trying to avoid sensor networks maintained from both security researchers, vendors and projects such as Dshield and the Internet Storm Center ones, malicious attackers are ready to sacrifice speed and efficiency while they segment and localise their targets in a way it wouldn't raise anyone's eyebrows, at least globally?

Johannes : Attackers do no longer attack globally. The real threat these days is from targeted attacks against particular networks (e.g. ISP, University or Company). Our data is very valuable in this context as it provides a global background these networks can use to identify targeted attacks. I will be very happy if attackers avoid DShield sensors. One more reason to sign up today (see http://www.dshield.org/howto.php).

Astalavista : How much traffic are you processing, and how do you actually manage to analyze it? Most of all, what are the possibilities for detecting 0-day vulnerabilities though the data acquired, locally and globally?

Johannes : We do acquire about 25-30 Million lines of firewall logs each day. The data is very limited (IP Addresses, Ports, Protocols, Timestamp...). However, the purpose of the data is not to provide all the answers, but to tell use where to look closer and to be fast. An analyst will always ask for more information. But the goal of DShield is to be fast. So our trade off is to limit the fidelity of the information (which also reduces privacy issues). The data will allow us to focus. For example, DShield will tell us (like last week) that port 1030 scanning is on its way up. In itself, this tells us very little. But it prompted us to ask for more information about these scans in our daily handlers diary. Shortly after, some people submitted full packets identifying the traffic as popup spam.

Astalavista : Given the sometimes underestimated power of the masses, have you ever considered integrated Dshield within an OEM, namely firewall, IDSs vendors, with the idea to expand its reach?

Johannes : Yes. We considered it, and would very much encourage vendors to incorporate the ability to send reports. One problem in the past was that we do not have the manpower to provide much support to vendors. But essentially, they could just do it on their own.

Astalavista : How would you describe the cooperation with different countries, ISPs related to the abuse of their networks, or their practices when dealing with abusive users?

Johannes : This has been a big success story of the last couple of years. ISPs are cooperating. Most of this cooperation is "packethead to packethead" and very informal. But cooperation like this has already reduced if not fully averted some attacks. Law enforcement agencies world wide do start to cooperate more as well. But of course, they can not do this as informally as ISPs can.

Astalavista : Through initiatives like yours, quarterly reports from security Vendors etc., the industry and the public are very aware of where the threats are geographically coming from. Isn't this rather ironical, and do you believe the lack of accountability, understanding, even awareness makes the situation even worse?

Johannes : From some cursory analysis of my own, malicious activity is very much proportional to the number of Internet users. There are a few geographic anomalies that are typically caused by local issues. For example, German ISPs are not allowed to store which user owned a particular IP address at any time. As a result, abuse follow up is almost impossible. The collaborative efforts I mentioned above to help a lot to get everyone on the same page.

Astalavista : In what way have threats evolved during the last couple of years from your point of view?

Johannes : Worms and bots are all about money now (actually, worms kind of disappeared). Also, we do see more attacks against client applications like browsers and e-mail clients. For servers, more attacks target applications running on top of the actual service (e.g. attacks against awstats vs. attacks against Apache).

Astalavista : What is your attitude towards full-disclosure?

Johannes : Responsible full disclosure if very important. I am overall against keeping secrets. Once a patch is available, enough details have to be provided to the user to understand the vulnerability. Otherwise, the user can not make an educated decision about how urgent the patch is for a particular environment. I am however against the release of some of the exploits that are labelled as "PoC" exploits. A PoC usually does not need to provide a remote shell to proof the existence of the vulnerability.

Astalavista : In conclusion, I wanted to ask for your viewpoint on the possible future release of a router worm, the motives behind it and its implications for the Internet?

Johannes : Router worms, or at least a router DDOS attack has been a possibility for a while. These days, most routers are attacked using weak passwords. I don't think this is a big infrastructure-wide issue, as core routers are typically well maintained and have contingency plans setup. It would need something like a zero day router worm to make an impact. However, small ISPs and such can still be hit. If it took an ISP a week to find the right command to setup ACLs for slammer, they are probably not able to deal with a widespread router exploit either.

[14] IT/Security Sites Review

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

-

ComputerForensicsWorld.com

-

http://www.computerforensicsworld.com/

ComputerForensicsWorld is a growing community of professionals involved in the forensics industry.

-

Top 50 Sci-Fi, Shows of All Time

-

http://www.boston.com/ae/tv/gallery/topscifishows/

With the resurgence science fiction shows this season, Boston.com's Entertainment staff decided to take a look at some of the sci-fi genre shows from yesteryear. Based on years of sci fi viewing experience and through a variety of online sources, we've come up with our picks for the Top 50 science fiction shows of all time.

-
Xatrix.org
-
http://www.xatrix.org/

Security news, downloads and many other resources.

-
TiVo Techies Forums
-
http://www.tivotechies.com/

TiVo technical information, tips, tricks, guides and secrets

-
FreewareFiles.com
-
http://www.freewarefiles.com

Hundreds of freeware applications.

[15] Final Words

Dear readers,

We are sure you have had great time while going through Issue 21.

Let us know your comments for this issue!

Till next time, but in the meantime – disrupt concepts and develop new ones, keep your spirit, and your eyes open :--)

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net