Astalavista Group Security Newsletter
Issue 19 - 30 July 2005
http://www.astalavista.com/
security@astalavista.net

[01] Introduction

Dear readers,

Issue 19 of the Astalavista Security Newsletter is out!

In the middle of the hot summer, our special edition is full with holiday spirit**, juicy details from the security scene**, the **most valuable security tools** and **security documents** we've featured during July, an article about **the most trendy security threats and how your organization should deal with security researchers looking for vulnerabilities in your software**, as well as an outstanding interview with **Eric Goldman.**

Keep the spirit,folks, and don't forget - **work like you don't care for the money and dance like nobody is watching!**

Note : Due to the numerous questions and concerns we would officially like to acknowledge that **Astalavista.com** is NOT affiliated with **Astalavista.box.sk** and that there are NO cracks/serials/keygens/warez etc. hosted on the **Astalavista.com's server!**

In case you're experiencing obvious problems trying to locate some of the recommended security tools and documents from past issues of out newsletter – try locating them using the associated title through our fully working and improved **Security Search** at :

http://www.astalavista.com/index.php?section=directory&cmd=search

Apologies for the inconvenience!

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

---

[HACKERS UNLEASH INDUSTRIAL SPY TROJAN]

IT security experts have detected a malware-based hack attack that attempts to gain unauthorised access to the networks of specifically targeted domains.

Security firm MessageLabs, which discovered the attack, explained that the Trojan targets only a small number of email addresses - 17 in this case - rather than mass mailing itself to as many recipients as possible.

More information can be found at :

http://www.pcw.co.uk/vnunet/news/2139033/hackers-unleash-industrial-spy

Astalavista's comments :

These are clear signs of active segmentation instead of the usual mass-mailing nature of the malware released. Even though this particular case is more likely to be an early stage experiment, malware authors are getting more aware of the active and Internet-wide anti-software vendors' sensors in place, that is why they try to avoid them as much as they can.

As the industry already has evidence of the clear spammers&malware authors affiliations, we would consequently soon witness the segmentation based nature of worms, given the huge email databases, which would just have to be datamined in order to differentiate and evaluate a potential company/organization/ISP to attack.

Another recent case to note is the Israeli corporate espionage case that finally brought the plain truth to the eyes of the public – namely that a specially developed 0-day malware remains undetected until signature is available to the vendor.

[FIREWALLS A DANGEROUS DISTRACTION SAYS EXPERT]

According to Abe Singer, security researcher for the San Diego Supercomputing Center (SDSC), companies spend 90% of their security effort on firewalls, protecting their perimeters but not the network as a whole. Singer says the SDSC has gone for four years without a root-level intrusion using no firewalls. The focus on firewalls leaves other security concerns unaddressed; Visa's requirements for merchants

mandate a firewall but give no guidance on configuring the device. Administrators need to consider business processes when setting up security instead of simply purchasing the latest technology.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=3992

Astalavista's comments :

Even though the introduction of all-in-one security appliances greatly improved the security of corporate networks, and reduced the obvious mess while relying and integrating solutions from multiple vendors, perimeter based and access control based defense is a convenient solution to say – we're secured, while it's like buying an ice cream for your kid when it wants an EuroDisney trip just to keep it quiet for a little while, but when it eats the ice cream, the EuroDisney trip will again be as desirable as before, perhaps even necessary ☺

Web applications vulnerabilities
Malware
Insiders
Physical security
Data encryption
Secure communications, both internal and external etc. are among the many other threats and vulnerabilities to think about, but before going into the countless aspects of the threats today, know what's most valuable to you, and learn how and why you should protect it.

Don't go forthe products but forthe solution and that usually requires more than just purchasing a security appliance. What you should also take into consideration is that even a perfectly developed firewall is pointless unless configured and maintained properly.

In Issue 12 of our newsletter we've covered the topic of ***"Can our 5k firewall tell us if we're really under attack?"*** *– read it at :*

http://www.astalavista.com/media/archive1/newsletter/issue_12_2004.txt

[**PENGATON UBER-HACKER RAP SHEET SPILLS ATTACK DETAILS**]

A US indictment of an alleged hacker mistakenly reveals the IP addresses of the sensitive defense servers targeted in the attack. Gary McKinnon, 39, of London, England, faces extradition to the US for allegedly hacking into 53 military and NASA (National Aeronautics and Space Administration) servers between February 2001 and March 2002 to find evidence of Unidentified Flying Objects (UFOs). The indictment was made publicly available as a PDF file with the sensitive IP addresses blacked out. However, a reader could copy the data from Acrobat Reader and paste it into a text editor to reveal the IP addresses.

More information can be found at :

http://www.theregister.co.uk/2005/07/11/mckinnon_indictment_snafu/

Astalavista's comments :

As I'm sure both the Pentagon and NASA are pretty aware of the issue, these might have already turned into publicly known honeypots given the attention they have attracted.

The indictment with all Ips involved in the attacks is publicly available at :

http://www.4law.co.il/501.pdf

While, on the other hand, a dangerously comprehensive list of Government and Military IP ranges and actual hosts can also be publicly located at :

http://www.governmentsecurity.org/forum/lofiversion/index.php/t5818.html

A very handy tool, for the purpose of measuring the popularity of network IP classes. GoogleSweep would come useful not only to the U.S military but to the average system administrator as well. Get it at :

http://cse.msstate.edu/~rwm8/googlesweep/

[**ISPs VERSUS THE ZOMBIES**]

Internet service providers (ISPs) find themselves under increasing pressure to protect their customers, as well as the Internet as a whole from malicious attacks. The Federal Trade Commission (FTC) will soon be reporting zombie network information to hosting ISPs. Analysts warn that if ISPs do not clean up their networks, users could lose faith in online activity in general. However, the increased monitoring required for ISPs to increase the security of their networks has privacy advocates worried. Some ISPs are already attacking the problem through port 25 blocking, which only allows email to be sent from the member's server, and rate blocking, which limits the number of emails a single member can send, among others.

More info can be found at :

http://news.com.com/ISPs+versus+the+zombies/2100-7349_3-5793719.html?part=rss&tag=5793719&subj=news

Astalavista's comments :

Several years ago, when me and a local admin were trying to figure out how to detect and eventually block a trojan infected PCs, it was a piece of cake given the fixed nature of the ports during these days. So whenever we noticed any connections on these, we immediately notified and blocked the associated ports – the end user felt secure, no one bothered for privacy violations etc. And even though malware got way too sophisticated to detect and track, a responsible ISP and nerdy and well experienced admin will always be able to detect abusive activity going out of the network.

Hopefully, in the future, an end user or a corporate organization will start preferring an ISP with security experience and security-conscious mode of thinking as a main differentiation factor. Simply providing an Internet connection, and by Internet connection I mean more one that's starting to become a dangerous toy in the hands of the end user, should NOT be enough for an ISP to survive, even make profits.

Taking an outside-inside approach, we would start with listing the major ISPs whose users are unknowingly responsible for a great deal of DdoS attacks and malware/spam dissemination with the help of projects such as the SANS Internet Storm Center – isc.sans.org or Dshield.org. My point is that most security unaware end users of major ISPs are publicly known, while the only incentive ISPs currently hide is the chance to make a buck from strategic partnerships with security vendors. But let's face it – ISPs can detect and block malicious activity going out of their network – it's just a matter of time they're going to do it under future laws or rival propositions.

A great Botnet Tracking research is available at :

http://www.honeynet.org/papers/bots/

[**BUG BOUNTY HUNTERS RECRUITED BY SECURITY FIRM**]

TippingPoint, a subsidiary of 3Com, announced a program to pay for vulnerability information. The amount of the reward will depend upon the severity of the bug discovered. The company plans to inform the flawed product's producer and also update its own security products. The rewards will be offered through TippingPoint's "Zero Day Initiative". The program will be officially launched on July 27, 2005.

More information can be found at :

http://www.silicon.com/0,39024729,39150680,00.htm

Astalavista's comments :

We're witnessing the development and actual investments in the "vulnerabilities market", a market that was originally developed by iDefense(now part of VeriSign), namely $ for a valid vulnerability. The good side for you ,as a programmer or security researcher, is that now there's competition going on, and competition is always good for you as the "customer". The bad side is that whenever a market is developing, it consequently prompts for the development of an underground market, usually with many more deep-pocketed buyers.

These and many other reasons prompted us to write an article entitled "Security Reseachers and your organization caught in between?"

[**ATTACKERS LURK ON PHOTO SITES, FIRM WARNS**]

Cybercriminals are increasingly using blog sites and other free online services to spread malicious code, Websense has warned.
In the first two weeks of July, the security company's labs saw more than 500 incidents of such attacks, Websense said on Monday. The free services are being abused to install software designed to steal personal information or hijack a victim's PC.
"July has seen a major boom--in the first two weeks alone, we found more instances than in May and June combined," Dan Hubbard, the senior director of security and technology research at Websense, said in a statement. For the year until mid-July, the San Diego company found a total of 2,500 incidents.

More information is available at :

http://news.com.com/Attackers+lurk+on+photo+sites,+firm+warns/2100-7349_3-5803863.html

Astalavista's comments :

I must admit – there's a huge deal of social engineering factors when it comes to the success of certain malwares and until the user goes through the naïve => infected => cautious stages, everyone's is in danger simply because you cannot advise users not to visit web links, check their greeting cards confirmations etc. So far, all the benefits of the developing and entertaining Internet go for the malware authors in my opinion and there's an overall change in net users' behaviour in order to bypass the obvious threats.

[**BIGGEST 419 BUST IN HISTORY**]

The US Federal Bureau of Investigation and Spanish police have arrested 310 people in Malaga, Spain, in connection with a €100 million lottery scam run by Nigerian 419 gangs. Authorities raided 166 homes throughout southern Spain, seizing €218,000, 2,000 mobile phones, 327 computers, and 165 fax machines. The gangs are also responsible for the well-known 419 e-mail scams which claim to come from a former dictator soliciting help in laundering money, with 20,00 victims in 45 countries. The arrests, the end result of an investigation begun in 2003, could lead to a drop in spam e-mails.

More information can be found at :

http://www.theregister.co.uk/2005/07/21/scammers_nabbed/

Astalavista's comments :

Why do they succeed – because of the global reach, the personalization of the message, namely not another viagra or cheap rolexes ad, and perhaps of the easy to implement automation of such messages. What bothers me is the magnitude of this growing "business".

Zone-H took the time and effort to initiate correspondence with the scammers which can be found at :

http://www.zone-h.org/files/61/nigerian.pdf

As well as a telephone conversation :

http://www.zone-h.org/files/61/MOL005.mp2

A complete history of over 500 variants of this cam is available at :

http://www.potifos.com/fraud/

[**FLAW RESEARCHER SETTLES DISPUTE WITH CISCO**]

The dispute over a presentation on hacking Cisco Systems' router software at the Black Hat security conference culminated in a legal settlement Thursday. Michael Lynn, a former Internet Security Systems researcher, and the Black Hat organizers agreed to a permanent injunction barring them from further discussing the presentation Lynn gave Wednesday. The presentation showed how attackers could take over Cisco routers, a problem that Lynn said could bring the Internet to its knees. The injunction also requires Lynn to return any materials and disassembled code related to Cisco, according to a copy of the injunction, which was filed in U.S. District Court for the District of Northern California. The injunction was agreed on by attorneys for Lynn, Black Hat, ISS and Cisco.

More information can be found at :

http://news.com.com/Flaw+researcher+settles+dispute+with+Cisco/2100-1002_3-5809390.html?tag=st.rn

Astalavista's comments :

*Impressive! (Ironically of course), Cisco – the company whose routers have an indisputable role in the success and penetration of networks and the Internet the way we know it – are destroying CDs trying to censor a presentation(offline) and filing lawsuits against security researchers. What the ****?! It's these actions that prompted us to feature all possible mirrors of the "questionable" presentation and perhaps it's again these very same actions that motivated hundreds of people out thereto host it. What were they thinking? That denying and keeping it quiet ,for the sake of their business, would do any good for the security of an organization or the Internet at all? I doubt so, and while I have my concerns about full-disclosure and what happens later on, based on networking contacts, responsible full-disclosure improves security, gives incentives to companies to fix the issues *publicly* so that it's all a matter of communication, awareness and patching later on.*

A must-read opinion on the topic "Is finding security holes a good idea?" is available at :

http://www.dtc.umn.edu/weis2004/rescorla.pdf

[**GOOGLE GROWTH YIELDS PRIVACY FEAR**]

Google is at once a powerful search engine and a growing e-mail provider. It runs a blogging service, makes software to speed web traffic and has ambitions to become a digital library. And it is developing a payments service.
Although many internet users eagerly await each new technology from Google, its rapid expansion is also prompting concerns that the company may know too much: what you read, where you surf and travel, whom you write.

"This is a lot of personal information in a single basket," said Chris Hoofnagle, senior counsel with the Electronic Privacy Information Center. "Google is becoming one of the largest privacy risks on the internet." Not that Hoofnagle is suggesting that Google has strayed from its mantra of making money "without doing evil."

More information can be found at :

http://www.wired.com/news/privacy/0,1848,68235,00.html

Astalavista's comments :

It was about time everyone started getting bothered by Google's usefulness and search engines domination – facts that make millions of people pretty much "talk" to the engine. What bothers me is their one-page privacy policy, and their ambitions to make everything Searchable, and their obvious data retention policies – it's a ticking privacy time-bomb.

While too anti-google oriented the http://www.google-watch.org/ *site has a lot to say on the topic.*

[**INTERNET HAS 'GIVEN AL QAEDA WINGS' CLAIMS BBC POTBOILER**]

Al Qaeda is now a "global brand driven by the power of the world wide web", and media-savvy cyberjihadis are manipulating the internet for training, recruitment and propaganda, according to the first of a three part series on *The New al Qaeda* broadcast on Monday 25th July) on BBC2. "The internet," says programme-maker Peter Taylor, "has given it wings." These apparent bombshells, however, appear to be based on a number of unremarkable discoveries, such as that terrorists have computers,

that cheap video cameras allow them to film attacks and executions and distribute the results via the internet, and that there's stuff on the internet you might not like but can't necessarily get much of a lid on.

More information can be found at :

http://www.theregister.co.uk/2005/07/27/bbc_al_qaeda_internet/

Astalavista's comments :

In my opinion Al Qaeda were never into hiring elite hackers to take control over SCADA devices or intercept troops movement communication through IP networks as the plain truth remains, namely that death people have higher social and panic influence than infected people or mobile devices blocking malware on a large scale.

I am a firm believer in the possibilities of cyber terrorism as the Internet represents a huge number of possibilities for intelligence gathering, coordination, propaganda etc. while I have recently come to the conclusion that the number of terrorist roadmaps on how they could use the Internet might have even surpassed their imagination!

An outstanding fact-based research on the topic can be found at :

http://astalavista.com/index.php?section=directory&linkid=4689

[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**

" **DESPOOF – ANTI PACKET SPOOFING** "

Despoof is a free, open source tool that measures the TTL to determine if a packet has been spoofed or not.

http://astalavista.com/index.php?section=directory&linkid=3070

" **MWCHAT** "

MWChat (My Web based Chat) is a Web-based chat system that uses PHP4 and an SQL backend database. It has support for multiple rooms and languages, a large number of IRC-like commands, private messages and rooms, message encryption, buddy lists, logging, registered users, chat profiles, file sharing, and more. It is a very lightweight, full-featured, and secure chat room.

http://www.astalavista.com/index.php?section=directory&linkid=4735

" **FLASH RESCUER** "

FLASH RESCUER is a free command line utility for rescuing JPEG images form the damaged FLASH cards. It searches through all the flash card memory in order to find bytes, which look like JPEG image and writes them to the files in current directory.

http://astalavista.com/index.php?section=directory&linkid=4636

" **SHC – A GENERIC SCRIPT COMPILER** "

Shc is a generic shell script compiler. It takes a script which is specified on the command line and produces C source code. The generated source code is then compiled and linked to produce a stripped binary executable.

http://astalavista.com/index.php?section=directory&linkid=4673

" **GNOME BLUETOOTH CONTROL REMOTO PROYECT** "

GNOME Bluetooth control remoto (AKA GBTcr) It is meant to be a fast and functional remote control for GNOME Desktop working between a phone mobile and computer box using Bluetooth comunication protocol.

http://astalavista.com/index.php?section=directory&linkid=4419

" **KCPENTRIX – PENETRATION TESTING LIVECD** "

KCPentrix is liveCD design to be a standalone Penetration testing toolkit for pentesters and security analysts KCPenTrix based on SLAX, a Slackware live cd and gentoo,auditor and whoppix. The Powerful modularity which KCPenTrix uses, allow us easily customize our version, and include whichever modules we like from any Slax distribution.

http://astalavista.com/index.php?section=directory&linkid=4652

" **ONE-TIME PASSWORD GENERATOR** "

A program for portable devices supporting Java 2 Micro Edition (almost all recent mobile phones) generating one-time access passwords (eg. for s/key or OPIE).

http://astalavista.com/index.php?section=directory&linkid=4734

" **DEVOLUTION SECURITY – VIDEO SURVEILLANCE SYSTEM FOR LINUX** "

Devolution Security is a video surveillance system for Linux based systems. It supports up to 16 cameras and features unicast and multicast broadcasting, a Web interface, an X11 interface, themes, motion detection, record on motion, eight different camera layouts, camera cycling, fullscreen mode, and more. Devolution Security uses its own toolkit (dtk).

http://astalavista.com/index.php?section=directory&linkid=4748

" **DETECTCON – HIDDEN PORTS DETECTOR** "

This little program is able to detect if a rootkit is hiding a certian port from being detected as a port that listens on connection. The program will only work when the rootkit uses a port - based listening backdoor.

http://astalavista.com/index.php?section=directory&linkid=4608

" **ANTIEXPLOIT – ON-ACCESS EXPLOIT SCANNER** "

AntiExploit is the first ON-ACCESS exploit-scanner for Linux and FreeBSD. Aexpl can help you to identify local intruders or users who want to harm your or other systems with well known tools. Aexpl uses the dazuko kernel-module and md5 hashes (signatures are planed) to identify bad files when they are created or used by listenning to the kernel file systemcalls. So you can immediately interact with the file and fileowner.

http://astalavista.com/index.php?section=directory&linkid=4728

[04] **Astalavista Recommended Papers**

" **ATTACKING DDOS AT THE SOURCE** "

We propose D-WARD, a DDoS defense system deployed at source-end networks that autonomously detects and stops attacks originating from these networks.

http://www.astalavista.com/index.php?section=directory&linkid=4511

" **THE RECORDING INDUSTRY 2005 – PIRACY REPORT** "

Overview of piracy trends around the world and various statistics.

http://www.astalavista.com/index.php?section=directory&linkid=4495

" **MALWARE PREVENTION THROUGH BLACK-HOLE DNS** "

One of the more popular techniques for fighting malware among home users is through the use of a host file for DNS redirection. A host can be used to maps hostnames associated with malware to a different IP address (such as a loopback address, 127.0.0.1). This will prevent connections to those malicious sites from ever taking place. (There is an irony here, as some of the more "evil" malware hijacks your host file to prevent their removal or to redirect search queries).

http://www.astalavista.com/index.php?section=directory&linkid=4426

" **MOBILE COMMERCE OVER GSM : A BANKING PERSPECTIVE ON SECURITY** "

This(160 pages) dissertation provides a detailed overview of basic services that any m-Commerce application should provide to the banking industry.

http://www.astalavista.com/index.php?section=directory&linkid=4443

" **COMMERCIAL SATELLITE SERVICES AND NATIONAL SECURITY** "

"Commercial Satellite Services and National Security : We Are Not Alone" gives an overview of the U.S and Russia's satellites dominance myth and provides a great deal of information on the satellite market and its implications to national security.

http://www.astalavista.com/index.php?section=directory&linkid=4666

" **COMPUTER FORENSICS FOR LAWYERS** "

"Computer Forensics for Lawyers Who Can't Set the Clock on their VCR" is a great, beginners' oriented introduction to computer forensics.

http://www.astalavista.com/index.php?section=directory&linkid=4646

" **HACKING PGP** "

Great presentation on the topic of hacking PGP, public key weaknesses, symmetric key weaknesses, hash algorithm weaknesses and the advances in factoring.

http://astalavista.com/index.php?section=directory&linkid=4732

" **WEB ENGINEERING FOR MOBILE DEVICES** "

This thesis discusses concepts for accessing information services via the mobile and gives an overview of the "mobile web".

http://astalavista.com/index.php?section=directory&linkid=4758

" **REAL-TIME AND FORENSIC NETWORK DATA ANALYSIS** "

"Real-Time and Forensic Network Data Analysis Using Animated and Coordinated Visualization" - presents a great concept for visualization of network and honeypot data.

http://astalavista.com/index.php?section=directory&linkid=4640

" **ECONOMIC ESPIONAGE - OVERVIEW** "

Part of the "Intelligence Threat Handbook", this 22 pages documents outlines issues such as : Costs of Economic Espionage The Outsider Threat - Foreign or Domestic Competitors The Outsider Threat - Through Unwitting Accomplices The Outsider Threat - From Foreign Intelligence Services The Insider Threat - Moles The Insider Threat – Espionage Entrepreneurs Developing a Countermeasures Strategy Outsider Threat Indicators Insider Threat Indicators

http://astalavista.com/index.php?section=directory&linkid=4647

[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**

Michael Lynn's Cisco IOS Shellcode And Exploitation Techniques lynn-cisco.pdf Mirrors

http://www.securitylab.ru/_Exploits/2005/07/lynn-cisco.pdf
http://cryptome.org/lynn-cisco.zip
http://snafu.priv.at/download/lynn-cisco.pdf
http://www.milw0rm.com/sploits/lynn-cisco.pdf
http://security-protocols.com/whitepapers/lynn-cisco.pdf
http://attrition.org/misc/ee/lynn-cisco.pdf
http://illmob.org/0day/lynn-cisco.zip
http://www.jwdt.com/~paysan/lynn-cisco.pdf
http://www.dfconsultants.com/lynn-cisco.pdf
http://42.pl/lynn/lynn-cisco.pdf
http://s48.yousendit.com/d.aspx?id=1EOE4MPD1E6U53MYQE6ROJID0R
http://www.megaupload.com/?d=31GTUIFR
http://teknews.net/~radio/lynn-cisco.pdf
http://www.stephencollins.org/library/linn-cisco.pdf
http://www.mininova.org/get/81889
http://www.warbard.ca/temp/lynn-cisco.pdf
http://www-cs.stanford.edu/people/miles/stuff/lynn-cisco/lynn-cisco.pdf
http://www.darkgrid.com/lynn-cisco.zip
http://files.bitchx.ru/index.php?dir=ebooks/&file=lynn-cisco.pdf
http://cryptome.org/lynn-cisco-jpg.htm

http://parrhesia.com.nyud.net:8090/lynn-cisco.pdf
http://lists.grok.org.uk/pipermail/full-disclosure/attachments/20050729/dfc5372b/lynn-cisco-0001.bin
http://thepiratebay.org/details.php?id=3363249
http://barcelona.indymedia.org/usermedia/application/5/lynn-cisco.zip
http://srv10.qfile.de/operator.php?sysm=file_transfer&sysf=center&file_id=125473&file_name=lynn-cisco.zip.html
http://dluz.tzo.com:8080/Devel/000_LINUX/Security/lynn-cisco.zip
http://www.sean-feeney.com/stuff/lynn-cisco.zip
http://www.undercan.com/uploads/lynn-cisco.zip
http://www.nvram.com.ar/adjuntos/lynn-cisco.zip
http://seedler.org/es/fhtml/info/143171
http://snakeshit.nl/files/lynn-cisco.pdf
http://www.parseerror.com/cache/lynn-cisco.pdf
http://linuxmafia.com/pub/linux/security/lynn-cisco.pdf
http://www.grupohg.net.mx/cisco/lynn-cisco.pdf
http://www5.tok2.com/home2/Nabokov/others/lynn-cisco.pdf
http://www.mininova.org/get/81889
http://md.hudora.de/archive/pub/lynn-cisco.pdf
http://www.indianz.ch/tools/txt/lynn-cisco.zip

Lynn's presentation being trashed at BlackHat?! :

http://downloads.oreilly.com/make/cisco.mov

Cisco System's Advisory can be found at :

http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml

[07] **Tool of the month**

Multipot – Emulation based honeypot

Multipot is an emulation based honeypot designed to capture malicious code which spreads through various exploits across the net. Design specifications for this project mandated that the captures be done in such a way so that the host machine would require only minimal supervision and would not itself risk getting infected.
Multipot was designed to emulate exploitable services to safely collect malicious code.

http://astalavista.com/index.php?section=directory&linkid=4649

[08] **Paper of the month**

Examining The Cyber Capabilities of Islamic Terrorist Groups

The purpose of this very well written and illustrated presentation is to detail Islamic terrorist groups' use of cyber technologies, namely the Internet for propaganda, coordination, recruitment and training etc.

http://astalavista.com/index.php?section=directory&linkid=4689

[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, Astalavista, folks! Congratulations on your new layout, even though I miss the old one, I see you're actively working on restoring all the sections, keep up the good work, everyone!! As an average U.K citizen, I pretend I live in a world free of Internet Censorship compared to regimes that control the Internet traffic of their citizens, but terrorism is on the rise, which prompts for a completely different picture when it comes to using the Internet, even my GSM these days. My question is, do you believe the "civilized" and open-minded part of the Internet we're used to would eventually turn into something where "forbidden" or "access to this resource is denied" messages would pop-up whenever I try to browse through resources I'm used to? Keep up the good work, respect to your work!!

Answer : Censorship is a very aggressive approach that is usually used by highly restricted societies like China, Iran etc., which still believe blocking access to certain resources would keep the local culture untouched by foreign propaganda or that history is what you present out of it. I seriously doubt the "civilized" part of the Internet would ever face large-scale censorship the way the Great Chinese Firewall acts, and even though law enforcement agencies are concerned on how users/criminals use the Internet or any sort of communication, monitoring instead of blocking would be the trend. Consider the following, the internet censorship in China may let you view the entire CNN.com but will silently remove sensitive content such as china-taiwan's relations in a news article, thus creating visible and invisible web for the surfers over there.

A recent EU's ambition was to retain a great deal of "traffic data", mobile, Internet etc. in order to investigate crimes and naturally, terrorism, a copy of the draft is available at :

http://www.edri.org/docs/Data-retention-council-draft-29062005.pdf

While activists have already started signing a petition against the draft, which is available at :

http://www.dataretentionisnosolution.com/

Question : Greetings, Astalavista team members!! I am an average IT professional, and by Professional I mean a person with 7 years of IT experience. While I'm not a security expert,

the nature of my work obviously requires me to keep up to date with the latest events, and of course, patch my system. During previous years I have noticed the growth and development of the security industry, while on the other hand the obvious invasion of sales-driven products and services. Not having respect for a company that charges $39.99 to clean your cookies and IE history is nothing compared to my attitude towards the mobile malware hype! My question is – do you think that security threats are overhyped with the idea to develop yet another sector in the security industry?

Answer : Good point on the $39.99 privacy solution, whereas understanding the issue from this point of view would bring back the old discussion of do marketers make us buy things we never actually wanted? The answer is no – they're just good at communicating value to targeted audience. Security and the Internet are evolving concepts, the more usefulness and efficiency you get out of a solution, the higher the risk and the eventual consequences of its abuse – a risk that must be taken seriously. To me security is all about stages, and if you're in the stage where your workforce security threats shouldn't be considered overhyped, the more there's written, said, tested and implemented about security – the higher the –overall- level of security. Let's consider passwords - the most popular and cost-effective authentication method available. However, given today's threats, it's so weak as a concept that considering an organization encrypting its sensitive data through password protected zip files over the Internet is unpractical and ridiculous. Stages pass, concepts evolve, one time passwords in everything appear as consequence, for instance, but make sure you're aware of what you're trying to protect, what the current threats are , safeguard it and start looking in the future.

Question : I wanted to ask you a question concerning the use of social engineering. I did some research even though the topic isn't greatly researched the way I see it. Kevin Mitnick impresses me with how he was able to steal source code just by pretending to be a company's employee. It got me concerned, as you would define me – end user. I want to know who exactly I'm communicating with while online and how I should protect myself from possible social engineering attacks.

Answer : As there was a saying, for locked, unplugged and disconnected from any network "secure" PC, you should consider turning yourself into the most anti-social and paranoid creature; even the less is known about you, the more socially engineering secure you are. Rather aggressive approach, but consider that there're no protection mechanisms for fighting such attacks, and today's electronic environment makes the situation even worse, even caller Ids are spoofed! What's created by humans will eventually be exploited by humans, or as I often like to say, - when you know how it works, you can either improve, abuse or destroy it which pretty much answers your question. Your best friends can turn into your worst enemies, knowing all your weak points, or even a complete stranger can trigger an emotion – make you visit a malicious web site promising free porn, warez etc. Don't be naïve, impulsive, and always question!

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

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

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter

whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

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

[11] Enterprise Security Issues

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

- Security Researchers and your organization caught in between? -

This brief article will introduce you the big picture of security vulnerabilities reseachers, the market for software vulnerabilities. It will cover its usefulness, dark sides and it would provide you with recommendations towards understanding the main issues and their eventual enforcement in your organization's security framework.

No OS is secure, be it Windows or Linux, commercial or open-source. Sooner or later a potentially abusive vulnerability is found that allows the attacker to gain higher privileges on the affected machine, or execute any command/code on the affected device. During the years, there has been a countless number of discussions on which OS is more secure, which "front" on the market takes security more seriously, while to me, the question is which one is more attacked, which one is clearly interested in fast, and reliable vulnerabilities fixing.

The number of reported vulnerabilities, as well as released exploits is steadily growing, perhaps due to the obvious global penetration of the Internet, namely the number of people having in-depth technical and research capabilities is getting bigger, and the obvious huge amounts of free documentation, even commercial books on vulnerabilities research are, too. Several other factors to consider are the introduction of tools such the Metasploit Framework, and the current level of automation when it comes to malware, have created a whole new window for successful development and abuse of working exploits.

Currently, there's a seemingly useful centralization when it comes to releasing security vulnerabilities – and it's all because of the **Bugtraq** Mailing List. When I use useful, I refer to the plain truth that this very particular mailing list (purchased by Symantec for $75m back in 2002, hah), acts as a transparent and publicly known vulnerabilities posting platform, whose biggest incentive is the publicity a researcher gets and the eventual job position, popularity among a very knowledgeable audience, and its reputation. Without such a centralized discussion list, we would have probably witnessed the chaotic ways vulnerabilities are reported and the way their researchers and their buddies take advantage of them. Thankfully, there's a competition arising whereas this new competition promotes new incentives to the participants –

a powerful but dangerous one – money! **iDefense.com** has always been gathering freshly discovered vulnerabilities intelligence because they have a sense for a researcher's quick needs, and the recent **Zero Day Initiative** will actively be competing with **iDefense's** proposition. Where's the problem? It's called moral and ethics, given $ incentives people tend to ignore both of these and once involved in these activities $ becomes an inspiration that where at the bottom line the one with the best proposition usually wins. Activities like these eventually develop deep-pocketed underground markets, me as a hypothetical spyware vendor would be willing to invest a great deal of $ given that I would be able to take advantage of 0-day vulnerability in IE. And as there're people with ethics and moral, so there're people without these, who might tend to anonymously ignore them for a temporary situation, while in the long run, we might end up having a security vulnerabilities' bidding system, where a newly established security threats monitoring company(yet another one!), would be posing to be such, when it's actually one of the many vendors or interested parties I mentioned above. At the bottom line researchers, blackhats, whitehats, unemployed or employed ones would favour such a bidding concept – to me companies looking to capitalize on someone else's research in the cheapest, yet profitable for them way, is playing with dangerous fire, and once intermediaries like these are being replaced with one-to-one contacts and propositions, security companies, threat monitoring ones, or primary security vendors will find themselves adding yet another table in their SEC fillings whose budget would have to keep on growing as will the demands of the researchers involved, who will finally be driven to seek a different kind ofacknowledgement..

A couple of things are of great importance whenever a researcher finds a vulnerability in your software products or software products your organization uses :

- Your response time to the first notification, standard auto-replies piss off pretty much everyone, make sure you have a security@yourorganization.com email that's being monitored and responses are provided within 24 hours. Even though you wouldn't be able to provide a fix within such a short period of time, make sure you keep them updated and keep in touch for each and every aspect of your verification, too much attention you might say? The thing is that you risk having the vulnerability released in the wild, which would definitely result in long nights and short deadlines for the testing and the release of a working patch. The way you threat them, the same way you would be treated!

- Whether credit would eventually be given to them or their group for the discovery of the vulnerability, should definitely be judged on how responsibly it was reported, namely that it wasn't released in the wild, without giving you response-time. Barely sticking to the researchers' very own schedule is egocentric and the consequences of publicly announcing several weeks of hard work should be discussed taking into consideration both sides.

- What kind of treatment is he getting, namely would you rather go for the "we were already aware of the issue and about to fix it prior to your email" would piss off pretty much everyone. If you don't like a company in the real world, bad word of mouth will go to around 5/10 people, but if you don't like a company on the Internet, it may reach 50,000 or more people, and considering the recent Cisco/ISS vs Michael Lynn case, I'm sure the majority of security researchers would love to "irresponsibly" release a vulnerability just because of the actions they have taken to cover up the entire story!

What do you do about possible security vulnerabilities' fiascos?

1. Keep in touch and don't ignore/delay the communication – for no reasons whatsoever!
2. Forget about censoring an eventual problem, it would ruin your reputation a LOT.
3. Take into account the obvious publicity-based pressure to announce and verify the vulnerability, make sure credit is given in case of a responsible disclosure and make them sure that you're aware

that it was them that originally found the vulnerability(if they did of course)
4. Perhaps among the most important aspects of the problem to consider is the establishment of an in-house security research department, actively doing code auditing and vulnerabilities research, but make sure it's not the $ that motivates them, but the overall responsibility and corporate citizenship of your company!
5. Constantly work on the successful establishment and improvement of a worldwide security alert notification and fast and reliable patching mechanisms for any of your customers, departments.
6. Give incentives, (and incentives doesn't necessarily have to be in the form of $, remember, it's a geek you're dealing with), so that security researchers will see the benefits of reporting eventual vulnerabilities, coordinating and respecting your schedule as well.
7. Attending security/hacking conferences and keeping an eye on who's who, and the current practices in place on the "other front" ,would prove highly valuable for the improvement of any future communication or in case a problem arises.

Security researchers are not enemies of yours, and even though both virtual and corporate barriers may exist, breaking them and taking the maximum out of sharing/accepting someone else's point of view is the first factor for successful communication and creativity!

ShadowCrew did the unthinkable (and ended up in jail) – developed an underground black market like the one I mentoned.

Find more about them or what they used to be at :

http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm

A well writen – Windows vs. Linux security comparison report can be found at :

http://www.securityinnovation.com/pdf/windows_linux_final_study.pdf

As well as "OIS Guidelines for Security Vulnerability Reporting and Response"

http://www.oisafety.org/guidelines/Guidelines%20for%20Security%20Vulnerability%20Reporting%20and%20Response%20V2.0.pdf

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

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

- **Today's security trends – practical tips for your security – Part 1** -

This article will deal with today's major security issues from an end users"point of view and would not only reveal their importance, but also provide the reader with recommendations on how to deal with them. In the next issue of the **Astalavista Security Newsletter**, we will continue the article with many more threats to be discussed and understood.

1. Lack of encryption

Once breached, it's better to have your most important files encrypted and obviously, useless to a potential attacker, both physical or remote. While I myself am a big fan or symmetric encryption and usually use an USB stick for the purpose, as any other concept it has its risks. Taking advantage of the highest possible encryption standards is useless in case your private key and passphrase get lost/stolen. Realize the potential of having your sensitive data in an encrypted form and show some creativity or even common sense when it comes to guarding these, a little inconvenience for the sake of your data's privacy is worth the trade-off.

2. Plain-text communications

Communicating in plain-text over the Internet, while transmitting, sensitive, company or any kind of informationm you wouldn't want to have in someone else's hands is a very bad, but naturally common practice. The biggest disadvantage of encrypted communications so far is the overall acceptance by your friends, probably defining you as a paranoid, ignore these and insist that certain information is send in an encrypted form, perhaps taking advantage of at least the slight publicity PGP already has. Even though SSL traffic can be intercepted and analyzed, ensure you're using SSL login mode and carefully examine the integrity of the security certificate provided, namely, whether it is relevant to the site you're trying to log in. Whereas, here we could open yet another discussion on the possible DNS abuses, this topic will be covered in Issue 20.

3. Passwords

Passwords are still de-facto the standard for authentication, but what you should take into consideration when using them is the plain-text communications I mentioned above. Namely try taking advantage of SSL as much as possible, protect yourself from obvious brute forcing attacks and add certain sophistication to your passwords. As I'm sure, you and everyone else keeps a great deal of passwords, but make sure that you don't use the same passwords on different services. While remembering so many passwords might pose a challenge, you might also consider using a password manager. The biggest disadvantage of this "convenience" is that once breached, the master password reveals ALL your passwords. Writing down passwords without of course associating them like hEi3@1NAz – email etc. is an alternative you could easily take advantage of.

4. Phishing

Perhaps the biggest advice as far as phishing is concerned is – don't be naïve, and make sure you tell it to all of your friends. No organization will want you to confirm your financial/login information UNLESS you insisted it does so. Don't trust your browser, unless you're sure you're running the latest version. What I'm trying to say is this could be dangerously misleading and let you think it's paypal.com you're at, while it's sending all the information gathered at a remote and naturally compromised host. Don't fall a victim! Consider looking at the following papers as well :

http://astalavista.com/media/directory/uploads/ciwp200503.pdf – a brief intro to the topic

Check out how a phishing email looks like at :

http://www.trendmicro.com/en/security/phishing/overview.htm

Received a phishing email? Consider forwarding it to the Anti-Phishing-Working-Group

so that other naïve users would eventually be protected :

http://www.antiphishing.org/report_phishing.html

In part two, we'll cover ten more security theats that are relevant for today's environment from our point of view.

Stay safe and be aware!

[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 **Eric Goldman**, a professor at the University of Marquette, Law Faculty.

Your comments are welcome at security@astalavista.net

Interview with Eric Goldman, http://www.ericgoldman.org

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

Eric : I am an Assistant Professor of Law at Marquette University Law School [http://law.marquette.edu/cgi-bin/site.pl] in Milwaukee, Wisconsin. I have been a full-time professor for 3 years. Before becoming an academic, I was an Internet lawyer for 8 years in the Silicon Valley. I worked first at a private law firm, where most of my clients were Internet companies that allowed users to interact with other users (eBay was a leading example of that). Then, from 2000-2002, I worked at Epinions.com [http://www.epinions.com] (soon to be part of eBay) as its general counsel.

As an academic, I principally spend my time thinking and writing about Internet law topics. Some of my recent papers [http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=332758] have addressed warez trading, spam, search engine liability and adware. I run two blogs: Technology & Marketing Law Blog [URL: http://blog.ericgoldman.org], where we discuss many Internet law, IP law and marketing law topics, and Goldman's Observations [http://blog.ericgoldman.org/personal], a personal blog where I comment on other topics of interest.

Astalavista : Teaching tech and Internet-savvy students on CyberLaw and Copyrights infringement is definitely a challenge when it comes to influencing attitudes, while perhaps creative when it comes to discussions. What's the overall attitude of your students towards online music and movies sharing?

Eric : Students have a variety of perspectives about file sharing. Some students come from a content owner background; for example, they may have been a freelance author in the past. These students tend to strongly support the enforcement efforts of content owners, and they view unpermitted file sharing as stealing/theft, etc.

Other students come from a technology background and subscribe to the "information wants to be free" philosophy. These students come into the classroom pretty hostile to content owners' efforts and tend to be fatalistic about the long-term success of enforcement efforts.

However, I think both of these groups are the minority. I think the significant majority of students do not really understand how copyright law applies to file sharing. They learned how to share files in school and do so regularly without fully understanding the legal ramifications. Usually, their thinking is: "if everyone is doing it, it must be OK." These students tend to be surprised by the incongruity between their behavior and the law.

Even when we discuss the rather restrictive nature of copyright law, these students are not always convinced to change their behavior. Deep down, they still want the files they want, and file sharing is how they get those files. As a result, I'll be interested to see how attitudes evolve with the emergence of legal download sites like iTunes. I suspect these sites may be retraining students that there is a cost-affordable (but not free) way to get the files they want. We'll see how this changes the classroom discussions!

Astalavista : Where do you think is the weakest link when it comes to copyright infringement of content online, the distribution process of the content or its development practices?

Eric : With respect to activities like warez trading, consistently the weakest link has been insiders at content companies. Not surprisingly (at least to security professionals), employees are the biggest security risk. I do think content owners are aware of these risks and have taken a number of steps to improve in-house security, but the content owners will never be able to eliminate this risk.

I'd like to note a second-order issue here. Content owners have historically staggered the release of their content across different geographical markets. We've recently seen a trend towards content owners releasing their content on the same day worldwide (the most recent Harry Potter book is a good example of that). I think the content owners' global release of content will reduce some of the damage from warez traders distributing content before it's been released in other geographic markets. So as the content owners evolve their distribution practices, they will help limit the impact of other weak links in the distribution process.

Astalavista : Do you envision the commercialization of P2P networks given the amount of multimedia traded there, and the obvious fact that Internet users are willing to spend money on online content purchases (given Apple's Itune store success, even Shawn Fanning's Snocap for instance) given the potential of this technology?

Eric : Personally, I'm not optimistic about the commercialization of the P2P networks. The content owners continue to show little interest in embracing the current forms of technology. I think if the content owners wanted to go in this direction, they would have done so before spending years and lots of money litigating against Napster, Aimster, Grokster and Streamcast.

In my opinion, without the buy-in of the content owners, P2P networks have little chance of becoming the dominant form of commercialized content downloads. So I think, for now, we'll see much more content owners' efforts directed towards proprietary download sites than cooperation with the P2P networks.

Astalavista : Were spyware/adware as well as malware the main influence factors for users to start legally purchasing entertainment content online?

Eric : We have some evidence to suggest otherwise. A recent study conducted at UC Berkeley [http://www.sims.berkeley.edu/~jensg/research/paper/grossklags-spyware_study.pdf] watched the behavior of users downloading file-sharing software. The users didn't understand the EULAs they were presented with, so they were not very careful about downloading. But, more importantly, the users persisted in downloading file-sharing software even when they were told and clearly understood that the software was bundled with adware. If this result is believable, users will tolerate software bundles—even if those bundles are risky from a security standpoint—so long as the software will help them get where they want.

Instead, I would attribute the comparative success of the music download sites to their responsiveness to consumer needs. Consumers have made it clear what they want—they want music when they want it, they want to listen to it in the order of their choosing, they want to pay a low amount for just the music they want (not the music they don't), they want the interface to be user-friendly and they want to deal with trustworthy sources. Also, consumers have surprisingly eclectic tastes, so any music download site must have a large database that's diverse enough to satisfy idiosyncratic tastes. The most recent generation of music download sites have finally provided an offering that satisfies most of these key attributes. They aren't perfect yet, but the modern sites are so much better than prior offering where the pricing was off, the databases were incomplete, or the sites were still trying to tell consumers how they should enjoy the music (rather than letting the consumers decide for themselves).

P2P file-sharing networks still serve a consumer need, but the content owners have succeeded some in increasing the search costs that consumers have to receive (such as by using spoof files). As consumer search costs using file-sharing increase, legal downloading sites with efficient search/navigation interfaces become more attractive.

Astalavista : How would you explain the major investments of known companies into spyware/adware? Is it legal but unethical from a moral point of view?

Eric : I'm a little contrarian on this topic, so I may be unintentionally controversial here. From my perspective, we should start with a basic proposition: adware and spyware are not inherently evil. Like many other technologies, adware and spyware are good technology capable of being misused. Indeed, I think adware and spyware are an essential part of our future technological toolkit—perhaps not in the existing form, but in some form. We should not dismiss the technology any more than we should dismiss P2P file sharing technology simply because many users choose to engage in illegal file sharing using it.

Once we realize that adware and spyware are not necessarily bad and could even be useful, then it makes sense that major brand-name companies are working with adware/spyware. Adware and spyware offer new—and potentially better—ways to solve consumers' needs, so we should expect and want companies to continue innovating.

Let me give an example. I use Microsoft XP and it constantly watches my activities. Indeed, in response to my actions/inactions, I get lots of pop-up alerts/notifications…."updates

are available," "you are now connected online," "we have detected a virus," etc. I want my operating system to be monitoring my behavior and alerting me to problems that need my attention. In fact, I'd be happy if Microsoft fixed problems that don't need my attention without even disturbing me. Microsoft is aware of this and is working on technological innovations to be smarter about when it delivers alerts. [http://research.microsoft.com/~horvitz/attend.htm]

So from my perspective, Microsoft is in the spyware business. They have huge investments in spyware. I'm glad they are making these investments and I hope they find even better ways to implement their software.

I think adware and spyware have been maligned because a number of otherwise-legitimate marketers have engaged in (and may continue to engage in) some questionable practices. These practices can range from deceptive/ambiguous disclosures to exploiting security holes. I remain optimistic that legitimate businesses will evolve their practices. We've seen movement by companies like Claria (eliminating pop-up ads), WhenU (deliberately scaling back installations by taking more efforts to confirm that users want the software) and 180solutions (cleaning up its distribution channels). This is not to say that we've reached the right place yet, but I like to think that the major adware companies will continue to improve their practices over time.

However, there will also be people who will disseminate software that is intended to harm consumers, such as by destroying or stealing data. We have to remain constantly vigilant against these threats. But they are far from new; we've had to deal with malicious virus writers for a couple of decades. In thinking about the policy implications, we should not lump the purveyors of intentionally harmful software together with legitimate businesses that are evolving their business practices.

Astalavista : Do you think the distributed and globalized nature of the Internet is actually the double edged sword when it comes to fighting/tracing cyber criminals and limiting the impact of an already distributed/hosted copyrighted information?

Eric : There's no question that the global nature of the Internet poses significant challenges to enforcement against infringement and criminals. While this is mostly a problem, the need for cross-border coordination creates an opportunity for governments to develop compatible laws and legal systems, and there could be real long-term benefits from that.

Astalavista : What's your opinion on the current state of DRM (Digital Rights Management) when it comes to usefulness and global acceptance?

Eric : I know DRM is pretty unpopular in a lot of circles, especially academic circles. Personally, I don't have a problem with DRM. I look at DRM as a way of determining the attributes of the product I'm buying. Consider the analogy to physical space. When I buy a car, most manufacturers give me some options to purchase. For example, I can upgrade the seat covers to the leather package if I'm willing to pay for that. The manufacturer could make that choice for me (and sometimes they do), but when it's my choice, I can pay for what I value.

DRM is a way of creating different product attributes in digital bits. In theory, with DRM, I can buy 24 hour viewing rights, 1 year viewing rights or perpetual viewing rights. Depending on my needs, I may prefer to pay less and get less, or I may want the perpetual rights and will

happily pay more for that. Without DRM, we've relied on physical nature of the content storage medium, plus post-hoc copyright infringement enforcement, to establish those different attributes. DRM does a much more effective job of defining the product. Therefore, DRM gives the content owners new ways to create products that respond to consumer needs. Of course, consumers need to understand what they are buying when it's controlled by DRM, but that's a consumer disclosure issue that we've encountered in lots of contexts before.

As far as I can tell, consumers have no problem with DRM. Indeed, the comparative success of download sites like iTunes indicates that consumers don't really care about DRM so long as they can get what they want.

Astalavista : In conclusion, I would really appreciate if you share your comments about the Astalavista.com site and, particularly, about our security newsletter?

Eric : My first introduction to your site was when one of my articles was linked on the site. My traffic immediately took off like a rocket ship. I was very impressed with the quantity and sophistication of your readers. Thanks for giving me an opportunity to speak with them.

[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.

-

OpenBRR.org

-

http://www.openbrr.org

Business Readiness Rating (BRR) is being proposed as a new standard model for rating open source software. It is intended to enable the entire community (enterprise adopters and developers) to rate software in an open and standardized way.

-

LeadSalad.com

-

http://www.leadsalad.com

LeadSalad is a worth visiting technoculture online comic

-

DRMWatch.com

-

http://www.drmwatch.com

DRMWatch.com is the leading resource for Digital Rights Management, Technologies, Research, Resources etc. are available at your disposal

-

Bluetooth Device Security Database

-
http://www.betaversion.net/btdsd/

This site is dedicated to change this in that form that it trys to provide a database with all needed information like manufacturer/device/revision/services/security_measures

-
Machine Perception and Learning of Complex Social Systems
-
http://www.reality.media.mit.edu/

Our research agenda takes advantage of the increasingly widespread use of mobile phones to provide insight into the dynamics of both individual and group behavior. We have captured communication, proximity, location, and activity information from 100 subjects at MIT over the course of the 2004-2005 academic year. This data represents over 350,000 hours (~40 years) of continuous data on human behavior.

[15] **Final Words**

Dear readers,

We hope we've provided you with yet another qualified viewpoint on this month's security events, helping you deepen your knowledge on various aspects from the security world, previously unknown to you.

Enjoy the rest of the summer, keep your comments coming and stay updated with **Astalavista.com**!

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net