**Astalavista Group Security Newsletter**
**Issue 23 - 30 November 2005**
http://www.astalavista.com/
security@astalavista.net

## [01] Introduction

---

Dear readers,

**Welcome to Issue 23 of the Astalavista Security Newsletter!**

In this issue we have interviewed **David Endler**, a director of Security Research at **TippingPoint**, covered events and news worth mentioning during November, and provided you with two articles as usual, namely – **"Breaking through security myths – Part 1"**, and **"Managing the threats posed by stolen laptops - Tips"**.

Perhaps we would be the only ones who wouldn't cover the Sony's rootkit case, given all the publicity it has already received – consider visiting the following site for further info :

http://www.sonysuit.com/

Enjoy **Issue 23**, and stay tuned for our Christmas edition!!

And remember – "**When you know how it works, you can either, improve, abuse, or destroy it**" – let's hope there are still people out there emphasizing on creativity and less destruction!

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

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

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

**Previous issues of Astalavista Security Newsletter can be found at:**

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

Yours truly,

**Editor - Dancho Danchev**
dancho@astalavista.net

**Proofreader – Yordanka Ilieva**
danny@astalavista.net

## [02] Security News

---

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have

decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[ **FBI, PENTAGON, PAY FOR ACCESS TO TROVE OF PUBLIC RECORDS** ]

The **US Federal Bureau of Investigation** (FBI) and the **Defense Department** have been purchasing records on individuals from data aggregator **ChoicePoint** since **2002**, according to documents obtained by **National Journal and Government Executive**. **ChoicePoint** maintains a database of 19 billion records for use in background checks and similar services, and has been selling access to the federal government. According to a contract obtained under the **Freedom of Information Act**, the FBI's **Foreign Terrorist Tracking Task Force** (FTTTF) Apparently signed a deal with ChoicePoint to access records the FBI is forbidden to collect under the 1974 Privacy Act.

**More information can be found at :**

http://govexec.com/dailyfed/1105/111105nj1.htm

**Astalavista's comments :**

*The worst thing, and perhaps the scariest one is that, what intelligence organizations cannot gather or don't want to dedicate resources to, the private sector has vast access to! Sometimes, the sector even holds info that would be otherwise impossible, or impractical to collect by means of assigning intelligence officers to gather it.*

*This fact, perhaps, has to do with prioritizing and exploiting the system itself, but providing web based interface makes me sik! I have always been concerned by what's going on with any kind of information I provide to any kind of organization, mainly because it ends up in a digital format. Even though, if I were to decline cooperation, I wouldn't be actually able to exist in the digital era we all live in. My advice - try to get as much info as possible whenever providing any kind of info you define as sensitive, knowing what's being done with it, will raise your eyebrows next time you decide to give it away under any circumstances.*

*What bothers me? – It's Google when it comes to law enforcement! My point – Google being the homepage of the entire Internet population, and Gmail acting as the sexy provider of n GB space, turns it into the biggest honeypot for detection, collection and tracing of illegal/malicious activities. Check this out, even though the story doesn't get into details how were the keywords restored, I've always envisioned the scenario of restoring deleted "eternal" cookies and associating them with sessions :*

*http://media2.foxnews.com/111305/tech_google_111305_300.wmv*

*It's scary because deleted cookies can be restored under forensic investigation, what follows is restoration of the search activity in terms of physical location (wake up, it's so easy!), search terms and the results follow. It's not just Google to be primarily concerned with, but any commercial entity at all!*

*Data retention seems to be winning acceptance among government officials, and civil liberties concerns are tackled by limiting the timeframe for keeping the data in order to maintain the balance between the public and any government's ambitions.*

*Watch the Watchers!!*

[ **SEC ACCUSES ESTONIAN FIRM ON FINANCIAL NEWS HACK** ]

The **US Securities and Exchange Commission** (SEC) has filed an emergency federal court action against Estonian finance firm **Lohmus Haavel & Viisemann** for **hacking** embargoed press releases on **Business Wire**. The hacks gave the company **insider information**, allowing traders to time stock trades against the time business notices were scheduled for public release. However, the evidence of wrongdoing may be murky, since the company used a **spider program** to **crawl** Business Wire links, and may not have needed to circumvent security features. **Business Wire** assures investors that press releases were not stolen, but that the hackers managed to use screenshot to get the desired information.

**More information can be found at :**

http://news.com.com/SEC+accuses+Estonian+firm+of+financial+news+hack/2100-7348_3-5931168.html

**Astalavista's comments :**

*Knowing what's going to happen in the financial industry, or any other, proves profitable, and of course it would as it gives you advantage over those currently unaware of what's to come.*

*Business Wire's weak statement can be interpreted as – not stolen = but accessed, namely confidentiality is still abused. If the SEC was to prosecute the company, Lohmus Haavel & Viisemann I'm talking about, they should get into knowing, did spidering around the service as a legit customer actually broke any of Business Wire's terms of service. It sure did! A bit unethical, but rather an experiment, I feel the company has successfully done an internal search, thus exposing embargoed press releases resulting, not in a scientific investment strategy :-) , but on purely unethical one. Would the company be still prosecuted given it hasn't taken advantage of the information already collected? Perhaps, this case would then be similar to the Stanford University's one, where students, led by a link on BusinessWeek's forum accessed info on their admission status.*

[ **UNSECURED WI-FI UNDER FIRE IN THE BIG APPLE** ]

Officials in suburban Westchester County, **New York**, would like to make having an open **wireless connection** without a separate server for **security** a crime for everyone. In the proposed law, not only must all public internet access include **a firewall-equipped network gateway server**, but any business or home office that stores personal information must also install such server, even if its wireless connection is encrypted and not open to the public. Within 90 days of the law being passed, all

businesses that provide internet access would be required to register with the county, and violations of any part of the law would be punishable with **fines of $250 or $500**. The law is currently in draft form.

**More information can be found at :**

http://networks.silicon.com/mobile/0,39024665,39153963,00.htm

**Astalavista's comments :**

*That's a piece of news worth mentioning! I cannot name a country, what's left for a state that seeks accountability for insecure systems(anyone?!), and while the modest fine is still in experimental mode, I truly believe seeking accountability might reduce revenues on a large scale, but result in long-term reputation and less unserious security issues resulting in serious threats! In the banking sector, the FTC is seeking customer security through requiring banks to issue two-factor authentication approaches – it's the only thing they could do for the time being, besides issuing a 30/40 pages "brochure" on the actual threats. My opinion is that enforcement of educational approaches, and ensuring customers understand the risks of doing E-banking would prove even more useful!*

[ **SYMANTEC PROTECTS ATMS** ]

**Symantec** in Canada, based in Toronto, has announced a real-time endpoint compliance system to implement fully protected **Internet Protocol automated teller machines**. **Symantec IP-ATM Security** includes antivirus, host intrusion prevention, device control, policy enforcement, remediation, and control over managed and unmanaged endpoints to provide banks a secure and manageable **ATM infrastructure**.

**More info can be found at :**

http://www.globetechnology.com/servlet/story/RTGAM.20051124.gtatm1124/BNStory/einsider/

**Info on the service itself can be found at :**

https://ses.symantec.com/industry/finance/IPATMSecurity.cfm

**Astalavista's comments :**

*Symantec's ambitions can be only compared to Google's, capitalize on what's trendy, and set new trends for decades to come, but my only justification for an initiative like that is availability of IP infrastructure and cutting costs; the thing is, would the costs associated with securing the ATMS outpace the costs for keeping it the way it is right now?! The "IP flexibility" in terms of availability, economies of scale in terms of infrastructure on a large scale seems to be the future, I mean even the U.S government pays for access to commercial satellite providers trying to get the bandwidth necessary to provide forces with the joys of Network-Centric-Warfare.*

*In the future – forget about phishing, just be around by the time the cash starts popping out of the ATM!*

[ **JUDGES REJECT CELL-PHONE TRACKING** ]

In recent months, federal judges in **New York**, **Long Island**, and **Texas**, have declined to allow the Justice Department to follow citizens in real time using cell phone signals without probable cause. The three **cell-tracking** requests accompanied requests to capture the incoming and outgoing dialing information, which only requires that the information likely be relevant to an ongoing investigation. The **Long Island** and **Texas** judges did not buy the argument that cell-phone users **"assume the risk"** of information disclosure to law enforcement because they freely transmit signals to their carriers.

**More information can be found at :**

http://www.wired.com/news/privacy/0,1848,69598,00.html?tw=wn_3polihead

**Astalavista's comments :**

*In my opinion, that's a temporary victory, and the issue will get even more attention in the future, especially when prepaid services are concerned. Let's face it, our carriers aware of their subscribers/sim users given the phones are on, and there's coverage. Information like this could prove extremely valuable to any kind of law enforcement efforts, and "assuming the risks" will soon happen..*

***The Net** (1995) – such a long time ago!! was perhaps one of the few movies, (I tend to favor the retro classics sometimes) that actually showed a Linux interface, and situations where Sandra Bullock was being chased through her mobile phone signal and credit card purchases in real-time, the thing is that the same were used for misleading the ex-KGB folks :-)*

[ **CEO STEPS DOWN OVER EMAIL SCANDAL** ]

**Nick Morris**, chief executive of ACIL Tasman, has resigned over charges of failing to uphold his duties in connection with a series of **hacks** into the **e-mail servers** of Access Economics, a **competitor**. The Australian Securities and Investments Commission (ASIC) has released few details of its charges against Morris, but the incidents appear to be evidence of **corporate espionage**. Former ACIL Tasman director **Jeffrey Rae** also faces charges for the hacks. If convicted, each suspect faces up to five years in prison and a $220,000 AU ($ 164,000 US) fine.

**More information is available at :**

http://www.smh.com.au/news/breaking/ceo-steps-down-over-email-scandal/2005/11/01/1130720537603.html

**Astalavista's comments :**

*Availability stands for temptation, malware on demand, DDoS on demand, in that case, I feel that's been hacking on demand, a rather unsuccessful*

*one. Hacking a competitor's email server can only be compared with using an intellectual property worm specifically crafted for a specific purpose or organization – total ownage!*
*More cases like these are currently happening, and in the future it would be hard to distinguish, a real hacker, a script kiddie, and corporate spy, these lines are already blue enough! This should act as a wake up call, competitive efforts can sometimes be very unethical, clearly illegal sometimes.*

[ **THAILAND TO BLOCK OVER 800,000 SITES** ]

Thailand's Prime Minister **Thaksin Shinawatra** has announced plans to block over **800,000 websites** deemed **violent** or **pornographic**. Internet service providers who refuse to block the websites face having their licenses revoked. The ban will likely go into effect before Children's Day, January 14, 2006.

**More information can be found at :**

http://www.smh.com.au/news/breaking/thailand-to-block-over-800000-sites/2005/11/28/1133026373171.html

**Astalavista's comments :**

*Large number of sites, and the country will indeed gain a short-term advantage, given the majority of these wouldn't that easily modify their Internet presence. It's a great effort, perhaps a coordination with leading content blockers in order to improve the ban would prove even more useful! Two things will happen – a market for pornography, an illegal one of course, will develop and turn such content into a premium one, the country will switch its efforts to detect and prosecute these. The second thing, given web site owners get more of their traffic/revenues from local customers, a game of cat and mouse when it comes to filtering will occur, while I doubt the second, and favor the first.*

**[ HOW LONG DOES IT TAKE TO CRACK A TERRORIST HARD DRIVE? ]**

**Andy Hayman**, assistant commissioner of the United Kingdom's Metropolitan Police, says it is necessary to lengthen to time **terrorist** suspects can be held without charge from 14 to 90 days to give investigators time to examine the contents of their computers. **Forensic examination** of a hard disk comes in two stages, acquisition and analysis. Acquisition is simply a matter of copying the hard drive, but analysis can take from one week to three, depending on the sophistication of **encryption**. A translator may also be necessary to translate any evidence, as well as cooperation with law enforcement in other countries. However, a law extending the time police can hold a suspect is unlikely to pass due to concerns over **civil liberties**.

**More information can be found at :**

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=4727

**Astalavista's comments :**

*Depends on how successful your interrogation practices are some may say, that doesn't work like that these days, of course, depending on the individual! This issue could have huge impact for those though to be terrorists, and as we're witnessing these days, governments are getting paranoid by everyone wearing a hat, a jacket in a hot weather (give me a break!), and a bag, let's not mention look at surveillance cameras, and why not, given they look at you as well?! :-)*

*A clear distinction of what is a terrorist, or a cyberterrorist should be made,*
*While cracking or acquiring a private key could be done in a pre-arrest manner,*
*Namely let the person involved expose these, without having to hold him/her!*
*Two issues are solved – law enforcement are aware of terrorist activities,*
*and cracking of the information would be done in the easiest way possible.*
*The Australian government for instance allows law enforcement to use spyware when necessary, that's flexible :*

*http://news.com.com/Australian+police+get+go-ahead+on+spyware/2100-7348_3-5491671.html*

**[ CHINESE HACKERS BREACH US MILITARY DEFENCES ]**

A group of about 20 **Chinese hackers** called **'Titan Rain'** by US government investigators, "thought to have stolen **US military secrets**, including aviation specifications and flight-planning software", most likely sold the information to the **Chinese government**. Titan Rain was later counter-hacked by a US security expert, **Shawn Carpenter**.

**More information can be found at :**

http://software.silicon.com/security/0,39024655,39154524,00.htm

**Astalavista's comments :**

*A government team of "penetration testers" or hired third-party experts to do the job is what should be taken into consideration. I am a firm believer of government funded teams for industrial, in this case military espionage, but the second requires insiders, or the interception of communication of parties involved. Whatever the case hackers take the blame for being malicious attackers. Don't get me wrong, the U.S military like any other takes advantage of IP based communications and data transfers/ storage, but security through obscurity(if any!) is not the way :*

*http://www.usdoj.gov/usao/vae/ArchivePress/NovemberPDFArchive/02/mckinnonindict111202.pdf*

**[ CYBERCRIME YIELDS MORE CASH THAN DRUGS ]**

According to **Valerie McNiven**, advisor on **cybercrime** to the US Treasury, cybercrime yielded more revenue than the drug trade's $105 billion for the first time in 2004. Speaking at an information security conference in Riyadh, McNiven said **cybercrime** can be a major problem for developing countries which lack **cybercrime** experience. Growing use of the Internet in such countries can also exacerbate other crimes, such as human trafficking, since it allows easy communication. While McNiven finds some links between **cybercrime** and **terrorism**, she argues that it is more important to focus on

protecting **information systems**.

**More information can be found at :**

http://news.com.com/Cybercrime+yields+more+cash+than+drugs/2100-7348_3-5973918.html

**Astalavista's comments :**

*Terrorists are already taking advantage of cyber scams to raise funds for anything but legal, even though the funds raises can and are successfully laundered. Cybercrimes might have surpassed drug trade in terms of gaining more popularity because of the ease and lack of costs it takes to initiate these, but given that cybercrime's financial impact cannot and is not measured until now, I doubt statements like these can be made.*

[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**

" **SIP SEND FUN V0.2** "

A tool to exploit the various weakness in VoIP-Phones. Written in php.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5452

" **GQUILT V0.15**"

quilt is a tool for managing a series of patches by keeping track of the changes each patch makes. Patches can be applied, un-applied, refreshed, etc. gquilt is a PyGTK GUI wrapper for quilt.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5462

" **COARSE KNOCKING – PORT KNOCKER** "

This is a simple implementation of Port Knocking techniques. It sniffs network packets looking for predetermined keys and executes commands to open and close ports on the firewall. In the client mode it injects packets with the key to server.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5482

" **THE DOORMAN** "

The doorman is intended to run on systems which have their firewall rules turned down tightly enough as to be effectively invisible to the outside world. The doorman adds and removes extra rules in a carefully controlled manner.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5489

" **TRUECRYPT – OPEN-SOURCE DISK ENCRYPTION SOFTWARE** "

TrueCrypt is on-the-fly disk encryption software that can create a virtual encrypted disk within a file and mount it as a real disk. It can also encrypt an entire hard disk partition, or a storage device such as USB memory stick. The product also supports plausible deniability.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5509

" **CAMELOID** "

CAMELOID is a composite suite of P2P communication applications used to talk with a high level of security to other people. It consists of secure video, voice, and instant messenger applications.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5522

" **MACSCAN V2.0B3** "

MacScan is designed to detect, isolate and remove spyware, keystroke loggers, Trojans, and bring awareness to remote administration type applications which could have been maliciously or inadvertently installed on your Macintosh. MacScan is available for Mac OS and Mac OS X containing the latest definitions for spyware.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5527

" **PSEUDO RANDOM NUMBER GENERATORS - SOFTWARE LIBRARIES** "

This page contains software libraries for some very good random number generators. The basic random number generators make floating point or integer random numbers with uniform distributions. This code is available in C++ and assembly language.

http://www.astalavista.com/index.php?section=directory&linkid=5546

" **ROOTKIT HOOK ANALYZER** "

RootKit Hook Analyzer is a security tool which will check if there are any rootkits installed on your computer which hook the kernel system services. Kernel RootKit Hooks are installed modules which intercept the principal system services that all programs and the operating system rely on. If any of these system services are intercepted and modified it means that there is a possibility that the safety of your system is at risk.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5554

" **MD5 COLLISION GENERATION** "

Collision generation for MD4 and MD5.

http://www.astalavista.com/index.php?section=directory&linkid=5534

[04] **Astalavista Recommended Papers**

" **A TAXONOMY OF CYBER ATTACKS ON 3G NETWORKS** "

This paper also proposes an abstract model of the 3G network entities. This abstract model has been a vehicle in the development of the attack taxonomy, detection of vulnerable points in the network and validating 3G network vulnerability assessment tools. This paper examines the threats and vulnerabilities in a 3G network with special examination of the security threats and vulnerabilities introduced by the merger of the 3G and the Internet.

http://www.astalavista.com/index.php?section=directory&linkid=5432

" **REPORT OF THE PANEL OF EXPERTS ON SPACE AND SECURITY** "

The ready availability of technology to well financed groups who are willing to use unlimited violence to inflict massive casualties means that the technological edge that gave many developed countries a feeling of security has been significantly eroded. This means that Europe must re-evaluate how it protects its citizens with today's assets and also how it develops both the assets and operating procedures in order to keep pace with the ever changing threat. In this environment no single country is able to tackle such complex problems on its own.

http://www.astalavista.com/index.php?section=directory&linkid=5437

" **22 WAYS TO FOIL CREDIT CARD THIEVES** "

You probably won't end up paying the bill, but a stolen credit card can still cost you big in time and aggravation. Here's how to protect yourself online and off.

http://www.astalavista.com/index.php?section=directory&linkid=5442

" **ON THE RACE OF WORMS, ALERTS AND PATCHES** "

We study the efficacy of patching and filtering countermeasures in protecting a network against scanning worms. Recent work has addressed the question of detect- ing worm scans and generating self-certifying alerts, specif- ically in order to combat zero-day worms.

http://www.astalavista.com/index.php?section=directory&linkid=5449

" **DETECTION OF COVERT CHANNEL ENCODING IN NETWORK PACKET DELAYS** "

This paper investigates the channel capacity of Internet-based timing channels and proposes a methodology for detecting covert timing channels based on how close a source comes to achieving that channel capacity. A statistical approach is then used for the special case of binary codes.

http://www.astalavista.com/index.php?section=directory&linkid=5461

" **SPAM 2005 : TECHNOLOGY, LAW AND POLICY** "

The papers in this compendium attempt to present a snapshot of the current conversation about spam. Some of the papers assess the status of the spam problem and the efforts of law enforcement to use the CAN-SPAM law.

http://www.astalavista.com/index.php?section=directory&linkid=5508

" **CAN DIGITAL PHOTOS BE TRUSTED?** "

The web is crawling with jokes, hoaxes and more insidious fakes. Digital-image experts aim to develop foolproof detection tools, but until then, seeing is not believing.

http://www.astalavista.com/index.php?section=directory&linkid=5497

" **STEGANALYSIS USING HIGHER-ORDER IMAGE STATISTICS** "

Techniques for information hiding (steganography) are becoming increasingly more sophisticated and widespread. With high-resolution digital images as carriers, detecting hidden messages is also becoming considerably more difficult. We describe a universal approach to steganalysis for detecting the presence of hidden messages embedded within digital images.

http://www.astalavista.com/index.php?section=directory&linkid=5529

" **PREVENTING INSIDER SABOTAGE : LESSONS LEARNED FROM ACTUAL ATTACKS** "

Are Insiders a Threat? - informative slides from this year's CSI Conference.

http://www.astalavista.com/index.php?section=directory&linkid=5545

" **ONLINE IDENTITY THEFT : PHISHING, TECHNOLOGY, CHOKEPOINTS, AND COUTERMEASURES** "

This report examines the information flow in phishing attacks of all types. Technologies used by phishers are discussed, in combination with countermeasures that can be applied. The focus is primarily on technology that can be deployed to stop phishing. Both currently available countermeasures and research-stage technologies are discussed.

http://www.astalavista.com/index.php?section=directory&linkid=5553

[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

---

**Anti-DMCA**

http://www.anti-dmca.org/

This site is the result of many people's anger toward the DMCA, Corporations, loss of Constitutional Rights, the WTO and the buying of America and her laws.

## [07] Tool of the month

---

**CAMELOID**

CAMELOID is a composite suite of P2P communication applications used to talk with a high level of security to other people. It consists of secure video, voice, and instant messenger applications.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5522

## [08] Paper of the month

---

**Eavesdropping Vulnerabilities**

Great visual representation of various eavesdropping vectors

http://www.astalavista.com/index.php?section=directory&linkid=5443

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

---

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

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

**More information about the DVD is available at:**

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

[10] **Enterprise Security Issues**

---

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

- **Breaking through security myths – Part 1**

This article aims to point out 10 of the most common misunderstandings I have encountered recently among a various organizations, and what are the real issues to worry about. **Part 1** will cover, **Vulnerability Management and Patching, Insiders**, **Perimeter based defense**, and **Antivirus solutions** Enjoy!

- **Vulnerabilities management/Patching**

  Vulnerability management companies ensure they(and you!) are aware of the latest vulnerabilities discovered, and that adequate measures are taken to ensure your organization's network is protected against these. Mainly using public sources, unless your vendor utilizes an in-house vulnerability research, or has an active program like the **iDefense's** or **ZeroDayInitiative's** one, these companies act as a watch dog you should always take advantage of.

  A common myth is that these vendors tackle the entire vulnerability management issue, while a great deal of attention should be put when choosing your vendor purely based on the comprehensiveness and relevance of their database/approach.

The timeframe between a vulnerability and an exploit is getting shorter, namely Patching is important, but when there are patches! 0day vulnerabilities that aren't in "the wild" often cause a lot of trouble, and buffer-overflow protection shouldn't be taken as the core of all vulnerabilities. When it comes to patching, you will sooner or later have a situation where a patch for important vulnerability wouldn't exist, some of your infrastructure assets will be missed, or a patch supposed to protect you from a major worm outbreak, will result in OS troubles and downtime. Given today's rate of vulnerabilities disclosure, outsourcing the task is highly recommended, but keep in mind that the threats you need to see coming are the threats you wouldn't see coming!

What you should be looking at is – experience of the vendor, proactive, rather than active attitude, flexibility and know-how on 0day threats, company-wide approach, including quarantining and consideration of the mobile workforce, and of course, timeliness, transparency and control of the process.

A great review of vulnerability management suites can be found at :

http://nwc.securitypipeline.com/howto/54200188

- **Insiders**

Insiders have been getting a lot of media attention recently, and that's fully Justified given the overall maturity of malware and perimeter based defence as a security threat. Insiders deserve particular attention mainly because they are authorised users who can sometimes cause even more damage than an unauthorised ones, in terms of easily hiding activity defined as malicious, and making it harder to trace. The biggest issue to consider is – **try not to promote a BigBrother is watching you culture,** that will inevitably influence what's most important to your organization besides it's secrets productivity. Who can become an insider? Anyone, from top management, to bottom end office clerks! **No one is insider unless your corporate culture, work and treatment and dissatisfaction turns them into such!** Pay extreme attention to identification, as it stands for accountability, consider not just relaying on signature based approach like **Vontu's** one, but constantly test the loyalty of employees in one way or another.

- **Perimeter based defence**

Perimeter based defence is perhaps one of most popular security measure, mainly because it mostly comes the form of hardware security appliance, a fully integrated suite, where the firewall as the buzz word plays the most important role. These days, any major security company has invested in the development of these, but simply relaying on perimeter based defence stands for lack of understanding, or wanting to understand the entire security problem. Firewalls cannot protect integrity or confidentiality of information, they can though take measures to ensure its availability. What you should keep in mind is constantly educate yourself on your vendor's strategy, do they aim to build the perfect all-in-one device, or are actually specializing into something, the way anti-virus software takes care of the malicious junk targeting your organization, firewalls protect the organization at a network level, leaving more more aspects such as integrity, identification and employee's education to consider. **@stake's Security Blueprint** is also handy for considering the issues you need to set as priorities, in respect to security management.

- **Anti-virus solutions**

  I often find myself saying that anti-virus solutions are a commodity and more efforts should be put into other, far more urgent ones. A trend to note in respect to anti-virus solutions is the today's domination of network worms, namely, anti-virus solutions did not protect the industry from the Warhol worms we've witnessed in the last 2 years. Signatures are extremely outdated concept these days, and anti-virus vendors find themselves reaching record levels for worm families, that is slightly modified versions of known malware. Do not blindly rely on how promptly a vendor releases updates, or how many signatures its databases detects, the more the better that's for sure, but what to consider are the vendor's steps towards proactive protection, IPSs, policy based security, sandboxing, behaviour blockers. As you will see in the following document, some of the industry's leaders highly differentiate into what they specialise in, consider knowing what truly matters in the long-run, or if cost-effective and lower TCO as far as anti-virus solutions is concerned can be achieved – use multiple ones, given one's weaknesses are the other's strengths.

  http://www.viruslist.com/en/downloads/vlpdfs/wp_nikishin_proactive_en.pdf

## [11] Home Users' Security Issues

---

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

### - Managing the threats posed by stolen laptops - Tips

This brief article will provide you with tips and recommendations on how not to have your laptop stolen, and what to do in case it happens to you. Laptops theft is on the rise, whether corporate espionage, or a dry cleaner with Citibank's customer's database at his disposal, a great deal of efforts should be put in ensuring the information in it is useless, unless the owner possess it.

No stolen laptop would even be returned – that's for sure, the best you can do it, learn more about the types of behavior leading to forgetting or contributing to have it have it stolen, and rendering the information inside useless for anyone but the owner him/herself

1. **Avoid the obvious – laptop bags!**

Completely ignore using laptop bags, first, because you look like an IT retard :-) second, because it increases the chances of getting someone's attention. All the need to do, given they have the time to, is try to have you lose sight of your asset. Once a potential target, you lose your superiority for acting as you don't own one.

2. **Trust no one, and be aware!**

Picture yourself having a drink at the airport's cafeteria, but wanting to go the toilet. It's full with people "going places", and nothing would even make your suspicious on the girl that you've asked to watch out your laptop for a little while. The thing is that it's the same situation when you ask someone to take a photo of you, and trying to catch up with him to get your camera back. Even worse, it's not her laptop, and in situation like this, she wouldn't be as aware as you would, and can be easily socially engineered into pretty much everything. Don't trust anyone in situations like this, it's not their responsibility to pay utmost attention to your laptop anymore!

Looking at the guards, the security cameras around the airport, or any other place, might give you a false sense of comfortability and the feeling that your security is well taken care of, but it isn't. Trust yourself only, don't build

3. **Access control**

Extremely important, the higher the number access control measures, the more hassle for anyone to not only get hold of the information inside, but get even a temporary peek at your current activities. BIOS passwords, no auto-start CD features, password protected screensavers are among the things to consider. Two-factor authentication is always an option, and these days the costs associated with this measure for an end user are getting extremely low. I have seen people peeing up at my laptop, on purposely left just with the idea to see if it happens, yes it does, but if you cannot see it's brand because of l33t stickers, it sure gets even more attention :-)

4. **Alarms & Tracking devices**

Alarms are extremely handy, whenever you want to find out whether someone is moving your device out of a specific range. Latest features includes, on-the-fly file system or files encryption in case of a movement. On the other hand, tracking devices is rather a paranoid option, but it has greatly involved as a concept and the mass introduction of 3G services and commercialization of other approaches. In case you really have something to ensure, have to comply with government guidelines, or want to make sure you know where's your stolen laptop – consider using these.

Some vendors to consider are :

http://www.absolute.com/
http://www.ztrace.com/
http://www.stealthsignal.com/

5. **Encrypt!**

Encrypted file systems are the best option, as using other measures opens up a great deal of OS based vulnerabilities, NTFS is always an option. Whereas it may cause you a little loss of productivity, that's a necessary evil, given the consequences

Check out the following :

http://support.microsoft.com/default.aspx?scid=kb;en-us;223316&sd=tech
http://www.infoanarchy.org/wiki/index.php/Hard_Disk_Encryption

Laptop theft is on the rise, lack of physical maintenance, end users' unaware of how easy they can have it stolen are perhaps the primary reasons for that

## [12] Meet the Security Scene

---

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed **David Endler**, director of security research at **TippingPoint,** a division of **3Com**.

**Your comments are welcome at security@astalavista.net**

---

**Interview with David Endler,** http://www.tippingpoint.com/

**Astalavista :** Hi Dave, would you, please, introduce yourself to our readers and share with us some info about your experience in the industry?

**Dave :** Sure, I'm 6'1", a Leo, I like long walks on the beach, coffee ice cream,^H^H^H^H^H^H^H . . . oh, sorry, wrong window. I'm the Director of Security Research at 3Com's security division, TippingPoint. Some of the functions that fall under me include 3Com's internal product Security testing, 3Com Security Response, and the Digital Vaccine team Responsible for TippingPoint IPS vulnerability filters. Prior to 3Com, I was the director of iDefense Labs overseeing vulnerability and malware research. Before that, I had various security research roles with Xerox Corporation, the National Security Agency, and MIT.

**Astalavista :** What's the goal of your Zero Day Initiative, how successful is your approach so far, and what differentiates it from iDefense's one?

**Dave :** Over the past few years, no one can deny the obvious increase in the number of capable security researchers as well as the advancement of publicly available security researching tools. We wanted to tap into this network of global researchers in such a manner as to benefit the researchers, 3Com customers, and the general public. Our approach was the construction of the Zero Day Initiative (ZDI), http://www.zerodayinitiative.com , launched on August 15, 2005.

The main goals behind the program are:

**a.)** Extend 3Com's existing vulnerability research organization by leveraging the methodologies, expertise, and time of others.

**b.)** Responsibly report 0day vulnerabilities to the affected vendors

**c.)** Protect our customers through the TippingPoint Intrusion

Prevention Systems (IPS) while the product vendor is working on a patch

**d.)** Protect all technology end users by eliminating 0day vulnerabilities through collaboration with the security community, both vendors and researchers.

The ZDI has had an incredibly positive result in only three months of activity, far exceeding our expectations. To date we have had over 200 researchers sign up through the portal, and received over 100 vulnerability submissions. We suspect that part of the early success of the program can be attributed to the wild launch party we threw at Blackhat/Defcon 2005. For pictures, visit http://www.zerodayinitiative.com/party_2005/.

The ZDI is different from iDefense's program in a number of ways. 3Com has invested considerable resources to ensure the success of the ZDI. As a result, ZDI contributors will receive a much higher valuation for their research. We provide 0day protection filters for our clients, without disclosing any details regarding the vulnerability, through our TippingPoint IPS, as opposed to simply selling vulnerability details in advance of public disclosure. Finally, we altruistically attempt to protect the public at large by sharing the acquired 0day data with other security vendors (yes, this includes competitors) in an effort to do the most good with the information we have acquired. We feel we can still maintain a competitive advantage with respect to our customers while facilitating the protection of a customer base larger than our own.

**Astalavista :** 0day vulnerabilities have always been a buzzword in the security community, while in recent years decision makers have started realizing their importance when evaluating possible solutions as well. What's the myth behind 0day vulnerabilities from your point of view, and should it get the highest priority the way I'm seeing it recently?

**Dave :** Certainly not all vulnerabilities should be treated equally, including 0day. A typical vendor-announced vulnerability can be just as devastating as a 0day due to the trend of shrinking windows of time for exploit release. Obviously, for an organization or home user that doesn't stay up-to-date with security patches, a three-year old exploit for a patched vulnerability could be just as devastating as a 0day exploit. I think 0day vulnerability protection has begun to take more shape in security buying decisions simply due to the growing frustration and helplessness felt by users when vendors take a long time to patch these issues when exploits are widely circulating. In the last year alone, we saw several of the 0day browser exploits incorporated into spyware sites within one day of their disclosure.

**Astalavista :** Do you feel the ongoing monetization and actual development of security vulnerabilities market would act as an incentive for a ShadowCrew style underground market, whose "rewards" for 0day vulnerabilities will contribute to its instant monopoly?

**Dave :** I think there will always be an underground market, but I doubt it will ever have a monopoly for a few reasons. We know there is a thriving underground market today for 0days, especially browser vulnerabilities that can be used to inject Trojans and steal financial data. I think the main obstacle

currently curbing the growth of the underground vulnerability-purchase movement is a lack of trust. Since a security researcher doesn't really know the identity of an underground buyer, there's no guarantee he will get paid once he unveils his discovery. Also at the end of the day, many researchers want these vulnerabilities to be fixed and want to receive the appropriate recognition in the mainstream security community.

**Astalavista :** While you are currently acting as the intermediary between a vendor and researcher, do you picture the long-term scenario of actually bidding for someone else's research given the appearance of other competitors, the existence of the underground market I already mentioned, and the transparency of both? How do you think would the market evolve?

**Dave :** Good question. I hope the markets evolve in a way that encourages Vendors to put more skin in the game. It behooves these vendors to help protect their own customers more by rewarding outside researchers for security discoveries that escape internal QA testing. The only vendors I know of who currently do this are Netscape and Mozilla through their bug bounty programs.

I think a "0-bay" auction model could be viable if a neutral party launched it that was trustworthy as a vulnerability "escrow agent" and could guarantee anonymity and payment to researchers. There was some good discussion on the Daily Dave list of some of the issues raised by such an auction model (http://archives.neohapsis.com/archives/dailydave/2005-q2/0308.html).

**Astalavista :** Should a vendor's competencies be judged on how promptly it reacts to a vulnerability notification and actually provides a (working) fix? Moreover, should vendors be held somehow accountable for their practices in situations like these, thus eliminating or opening up windows of opportunity for pretty much anything malicious?

**Dave :** I've worn the hat of a security researcher, vulnerability disclosure intermediary, and most recently, a vendor. I now have a great amount of sympathy for all three groups. In general, vendors need to make a more concerted effort to reach out to security researchers in the vulnerability disclosure process. Many vendors don't seem to understand that most security researchers get no tangible benefit for reporting a security issue. More and more 0day disclosures it seems are also the result of a vendor-researcher relationship breaking down due to a misunderstanding over email or poor follow-up from the vendor. Ideally, vendors should also reward these researchers, if not with money, then other perks or recognition as a sign of appreciation.

It's hard to judge all vendors the same on the amount of time it takes to patch a vulnerability. Some vulnerabilities legitimately take longer to fix and QA than others. Because there are no laws today that govern a vendor's security response, the market is going to have to be the ultimate judge in this arena. If enough potential customers are lost to a competitor because of poor security patch handling or a destructive worm, you can bet that more money will be budgeted into their security development lifecycle.

**Astalavista :** Having conducted security research for the NSA must have been quite an experience. Does the agency's approach on security research somehow differ from the industry's one, in terms of needs for sure, but in what way exactly?

**Dave :** No comment :-)

**Astalavista :** Can money buy creativity and innovation from an R&D's point of view?

**Dave :** Of course no amount of money can buy your way to really innovative research.Some of the most prolific research teams are built through visionary research directors creating a nurturing and non-restrictive environment, insulating the team from most corporate pressures and politics.

**Astalavista :** Thanks for your time!

## [13] IT/Security Sites Review

---

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

-
**Web3d.org**
-

http://www.web3d.org/

Open Standards for Real-Time 3D Communication

**-**
**Fullscreenqtvr**
**-**
http://www.fullscreenqtvr.com/

Fullscreenqtvr.com is a collaborative effort between Hans Nyberg of panoramas.dk, and Marco Trezzini of VRMAG.org, the Virtual Reality photography and travel magazine hosted by VRWAY Communication.

-
**ITconversations.com**
-
http://www.itconversations.com/

IT Conversations is a listener-supported web site. Many listeners contribute to our tip jar, but others contribute in a different way: They're the people behind the scenes who volunteer their time to write and debug the software, write the descriptions, track down the photos, and engineer the audio of IT Conversations programs.

-
**Twatech.org**
-
http://www.twatech.org/

A daily hardcore tech radio show

-
**IdiotToys.com**
-
http://www.idiottoys.com/

Great tech reviews!!

## [14] Final Words

---

Dear readers,

Watch out for our special Christmas edition of the **Astalavista Security Newsletter!** Keep sending us your feedback and ideas – cause at the bottom line it's your opinion that matters!

Till our next issue!

Yours truly,

**Editor - Dancho Danchev**
dancho@astalavista.net

**Proofreader – Yordanka Ilieva**
danny@astalavista.net