Astalavista Group Security Newsletter
Issue 25 – 31 January 2005
http://www.astalavista.com/
security@astalavista.net

[01] **Introduction**

Dear readers,

Welcome to the first issue of the Astalavista's Security Newsletter for 2006!

In case you haven't had the chance to go through our New Year Greeting you can do so at :

http://www.astalavista.com/index.php?page=157

Meanwhile, in Issue 25, you'll find :

- significant security events during the month, and associated commentaries
- "**Organizational Training and Today's Threatscape**" article whose purpose is to emphasize on the pros and cons of organizational training
- "**Fortifying your Browser – even more**" tips for securing your browser and introduction the Browser Appliance, a virtual machine for your Mozilla
- and an interview with **Johnny Long**, the person behind the Google Dorks database

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

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

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

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

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

Previous issues of Astalavista Security Newsletter can be found at:

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

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

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

---

[**SHOULD ALL YOUR STAFF HAVE A SECURITY QUALIFICATION?**]

Rob Chapman, founder of the Training Camp, argues that companies should give all their employees basic training in cybersecurity to better protect their business. Many companies have IT security policies that their employees must follow, but most do not assure that employees know how to follow policy. Companies may object to the cost of training every employee, but the costs of an innocent mistake could have disastrous effects on a company. Staff are often considered the primary weakness in any company's security; in certain industries, such as finance, companies could see insurance benefits from employee security training. Stuart Okin, a partner in Accenture's security practice, calls security training a necessity, not only for its potential to mitigate risk, but also to give a company a competitive edge.

More information can be found at :

http://www.zdnet.com.au/jobs/news_trends/soa/Should_all_your_staff_have_a_security_qualification_/0,2000056653,39231874,00.htm

Astalavista's comments :

I used to actively argue and believe in end users' education on security, that's three years ago when I conducted a publication entitled "Building and Implementing a Successful Information Security Policy", where I also outlined some of my modest back then security awareness programs experience. Things have greatly changed ever since, and while "communicating" a security policy is highly recommended, periodically training all your employees on the "latest" threats is questionable, as if you were to define the "latest" would you educate your end users not to open multimedia files because they are dangerous or "may have malicious content within"?

Enforce as much security policies and by default preferences as possible, try to spot the "naughty" users, and actually prioritize who needs training and who doesn't. Everyone does for sure, and the more people know about security the more secure your infrastructure at least logically, but at the bottom line, the folks at the IT or ITSecurity department have their roles, and so does Finance, and Marketing, while the second ones aren't interested in becoming security experts and they shouldn't. Security training is necessary, I agree, but make sure you maintain the balance between actual position productivity and the security training progress. At the bottom line, the external factors, namely, the threats I've mentioned so change so fast, that in case you haven't build a working training evaluation and see any effects, it's lost money, but

which part exactly?

[**DAVIS TAKES ISSUE WITH GOOGLE OVER RECORDS REQUEST**]

House Government Reform Committee Chairman Tom Davis (R-VA) has criticized Google for refusing to hand search records over to the US Justice Department while cooperating with China in censoring certain topics. Justice sought the records to bolster its case against a challenge to online anti-pornography laws, but Google refuses to submit the records on privacy grounds. Davis does not expect a standoff between Google and the government, but hopes an agreement can be reached, allowing Google to supply the records without frightening users that their searches may be examined.

More information can be found at :

http://www.gcn.com/vol1_no1/daily-updates/38097-1.html?CMP=OTC-RSS

Astalavista's comments :

Is it just me or that must be sort of a black humor political blackmail given the situation?! First, and most of all, the idea of using search engines to bolster the online anti-pornography laws created enough debate for years of commentaries and news stories, and was wrong from the very beginning. Even if Google provide the data requested it doesn't necessarily solve the problem, so instead of blowing the whistle without any point, sample the top 100 portals and see how they enforce these policies, if they do. As far as China is concerned, or actually used as a point of discussion, remember the different between modern communism, and democracy as a concept, the first is an excuse for the second, still, I feel it's one thing to censor, another to report actual activity to law enforcement. I feel alternative methods should be used, and porn "to go" is a more realistic threat to minors than the Net is to a certain extend, yet the Net remains the king of content as always.

[**PRIVACY GUARDIAN TO EXAMINE SHOREDITCH CCTV SCHEME**]

The United Kingdom's Information Commissioner plans to investigate whether the plans of Shoreditch to open its CCTV (closed-circuit television) surveillance system to the public complies with the CCTV Code of Practice. Under the proposal, the 20,000 residents of Shoreditch would be able to view footage from 500 CCTV cameras located in a poorer neighborhood. This gives neighbors the ability to spy on each other; the Information Commissioner wants to be certain people cannot record CCTV footage for their own amusement and to whether it violates privacy rights to broadcast residents going about their daily lives.

More information can be found at :

http://www.theregister.co.uk/2006/01/17/ic_eyes_shoreditch_cctv/

Astalavista's comments :

Is this the revenge of the middle class or a bad joke?! :) I don't think

exposing a poor neighborhood to the entire population of the small town would do any good in respect to limiting crime, or improving security. Perhaps I have somehow underestimated the possibility or Reality CCTV, but I bet if the public ever gets the chance to see itself through a CCTVs point of view, it might again open up a debate on their actual usability.

*CCTV cameras are *everywhere*, whether providing a false sense of security to a society as a whole, enforcing accountability for events or whatsoever, their use have always been actively questioned.*

[**BRITISH PARLIAMENT ATTACKED USING WMF EXPLOIT**]

MessageLabs, e-mail filtering provider for British Parliament, has confirmed that targeted e-mails exploiting the Microsoft WMF (Windows Metafile) flaw were sent to various Members of Parliament and other government personnel. The attack appears to have originated in China, and occurred on January 2, 2006. The first exploit code was published December 29, and Microsoft released its patch on January 5. If users downloaded the malware from the e-mails, the attackers would have been able to access government computers and possibly install keyloggers. The attack was tailored to 70 people and posed as a message from a government security agency. Though the attack traces back to China, it is unknown whether it was conducted or sponsored by the Chinese government.

More info can be found at :

http://news.com.com/British+parliament+attacked+using+WMF+exploit/2100-7349_3-6029691.html

Astalavista's comments :

That's a very good example of a targeted attack, namely attacking a specific entity only, in this case the British Parliament. Whenever I read on attacks coming from China I always consider the use of zombie PCs as a stepping stone for the attack itself(China has a very large population of zombie PCs and is the second largest source of spam in the world). There's so much speculation and insights on the WMF bug that the majority of news agencies missed the fact that the market for 0day vulnerabilities is developing right in front of our noses. I believe the first to develop such a market, without outsourcing it of course, was the military, just think for a while on how competitive a military's asymmetric power could be given it holds a great deal of 0day vulnerabilities?

Going back to this particular attack, it a very well segmented one, And the impersonation of a government security agency could have caused further damage given MessageLabs didn't block the threat. The clear consolidation of the underground, that is malware authors, spammers and phishers makes it possible

to execute such attacks very easily, namely I bet a spammer has somehow managed to get hold of active government emails, and these were later on used. That's not a script kiddie for sure!

Scary though, but you no longer need to be a Fortune 500 company to get attacked – everyone is a target.

[**THE BACKHOE : A REAL CYBERTHREAT**]

Experts remind that despite "all the attention paid to computer viruses and the latest Windows security holes, the most vulnerable threads in America's critical infrastructures lie literally beneath our feet". The actually physical infrastructure, such as buried fiber optic cables, are vulnerable to "backhoe attacks" - accidental or purposeful, and a report by the Common Ground Alliance estimates "that there were more than 675,000 excavation accidents in 2004 in which underground cables or pipelines were damaged."

More information can be found at :

http://www.wired.com/news/technology/0,70040-0.html

Astalavista's comments :

Satellites and wireless networks anyone? Even though these wouldn't be able to hold up the load in case underground fiber optic cables or stations get destroyed, in case of a terrorist attack or war conflict, key military and government communications will remain active with, or without ground based communications. That's the way it goes, and while some are speculating on the possible use of EMP weapons by terrorists, to me that's an indirect way of fueling the growth of the space arms race – totally wrong and scary scenario.

I feel this threat isn't as realistic as it was to be years ago, mainly because of the way the Internet turned into a facilitator for communication and coordination of terrorist activities from my point of view. Therefore, no one would want to damage and destroy, but taken advantage of it.

[**IPSEC DEAD BY 2008, SAYS GARTNER**]

Gartner issued a report predicting that by 2008 the IPsec protocol will have been virtually replaced by SSL. Increased adoption of SSL will allow more telecommuting, but "end-point security will require more attention, both in terms of client security and the management of increasingly complex SSL access policies".

More information is available at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=5173

Astalavista's comments :

Anyone else in love with SSL? I wouldn't pay a couple of hundred bucks to find out what their justification for such

a statement is, but I find it totally wrong mainly because of the fact that IPSec is an inseparable part of IPv6, or Internet2, that is less spoofing, more accountability on a network level, and increase of encrypted and authenticated communications. SSL is so vulnerable and easy to hijack that having SSL by default the way Yahoo! recently started doing would be among the many layers of defense in a possible defense in-depth solution.

Moreover, I feel that the public attention is greatly distracted to the technological side of the problem, encryption techniques etc. whereas client side attacks and vulnerabilities are totally ignored. It wouldn't make hell of a different even if you have the entire lyrics of your favorite song set as a passphrase if someone has managed to installed a KeyGhosts on the PC in question, would it?

To me IPSec is the v2.0 of the current plain-text communications based Internet, still, encrypted communications have one downsize besides key and passphrase management – that is inevitable slowdowns depending on the infrastructure and the type of information exchanged.

[**MICROSOFT ISSUES PATCH FOR UNRELEASED VISTA**]

A patch to fix graphics-rendering problems in the Community Technology Preview of Microsoft's operating system Vista has been released. The general release of Vista, now only available to developers, will occur later in 2006.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=5165

Astalavista's comments :

That's a news item worth mentioning, and puts Microsoft in a very favorable position given the proactive release of such a patch, wish they were so committed towards securing what they already have running on 95% of PCs across the world before jumping on the "next big thing". What's worth mentioning is how obsessed with revenue generation MS is, which is perhaps because of the fact that it's market value is so high compared to rival tech companies. My point is that, this obsession leads to insecure Internet given all Windows boxes are connected to the Internet, and while the information security industry picks it from there, I feel that there are far more serious threats to fight compared to those posed by lack of commitment towards improving your products.

[MCAFEE FINED FOR ACCOUNTING SCAM]

The US Securities and Exchange Commission (SEC) has fined McAfee for "inflating its revenues during the dot.com era" and the company had agreed to the "unusually heavy" fine of $50 million, without formally

admitting to wrongdoing. The money will go to McAfee shareholders that the SEC determines have "suffered as a result of the drop in the company's market capitalization when it announced its need to re-state revenue in December 2000". Criminal charges may still be pressed against some of the company's previous management team.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=5098

Astalavista's comments :

There's a relevant joke that during the dotcom era every entrepreneur used to present with the same powerpoint slide, namely showing the growth of online advertising from nothing, to several billions. Well, wrong timing, lack of Internet penetration, users' conformability of purchasing online and many other factors besides the flawed business logic contributed to the Bubble. Did the company build itself on this event, I mean paying $50 million wouldn't be a problem given the kind of revenues any AV vendor can generate these days – they are simply too busy, and their customers' base is constantly growing.

Back in those days experts and average users used to joke on AV vendors distributing malware to fuel growth in the sector, the thing is it has never been necessary, there so much malware and people capable of coding and distributing it that you can actually pay up your fine, and keep it clean. Everything's possible!

[BANGLADESH CONCERNED ABOUT 'OBSCENE CHATTING']

The Bangladesh Telecom Regulatory Commission has asked mobile phone companies to stop free late-night services because they degraded the moral values of young people". Claiming that young people are engaging in obscene chatting", the commission, a watchdog group, blames free late night calling plans that encourage students to disregard sleep and studying.

More information can be found at :

http://www.smh.com.au/news/breaking/bangladesh-concerned-about-obscene-chatting/2006/01/16/1137259973701.html

Astalavista's comments :

What a weak statement from a developing economy! Any service out of the business hours can be offered at a much lower price and that's a competitive advantage of many providers these days. Even though I doubt someone can block obscene chatting, it can also happen during the day, therefore such requests are totally unrealistic from my point of view. Now, whatever a person does with the ability to send and receive SMS is entirely up to them given they don't harass, disseminate racists or religious hatred, wasn't

it like that?

And if you stop the free late night services(there's no such thing as free lunch!) there's this thing called instant messaging, and email that could be used pretty much 24/7 – again for free, block this!

[GOOGLE ADSENSE HIJACKED BY PORN TROJAN]

Google's AdSense advertisements are being covered up with promotions of pornography and gambling websites. The Trojan malware responsible was discovered in the wild by Raoul Bangera. Google is investigating.

More information can be found at :

http://www.techworld.com/security/news/index.cfm?RSS&NewsID=5080

Astalavista's comments :

Welcome in Web 2.0! During the last year I have come to hundreds of networks mimicking Google's AdSense and it's "keep it simple, not annoying" appearance. If a malware is able to appear on the top of every AdSense syndicated ads on any page visited by an infected PC, than Google whose revenues come primarily from AdSense would definitely suffer even more compared to today's pay-per-click hijacking tactics malicious users tend to use. In my research entitled "Malware – future trends" that I released prior to this event happening, I indicated the idea of the "Web as a platform" in respect to future malware developments, and I greatly feel it's actually happening.

Find more info about the trojan by the person who first reported this at :

http://www.techshout.com/internet/2005/27/a-trojan-horse-program-that-targets-google-ads-has-been-detected-by-an-indian-web-publisher/

[03] **Astalavista Recommended Tools**

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

" **LSM-PKCS1** "

A daemon to handle Secure Boxes (cryptographic keys, X509 certificates and data objects), accessible through a PKCS#11 library, supporting non-certified (lite) Hardware or Software Security Modules.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6067

" **SANDBOX FOR GRIDS** "

Sandbox for Grids (s4g) is a Linux user-mode sandbox. It offers
a secure execution environment for suspicious applications. Written
in C, it tries to solve some typical problems of quarantine applications:
efficiency and security.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6048

" **ISO-9660 CD IMAGE FILES OF MS SECURITY AND CRITICAL UPDATES** "

This article describes the ISO-9660 CD image files that contain security and
critical updates for Microsoft Windows and for other Microsoft products.
This article contains a link to the current ISO image file that is available
on the Microsoft Download Center.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=6031

" **TOGGLEBTH**"

This will only work on PocketPCs and Smartphones that use the Microsoft
BlueTooth software. Unfortunately, many PocketPC vendors and one
Smartphone one have decided to use different Bluetooth software that
doesn't let developers write programs for it. If you have a device with
that software, this program isn't going to work.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5990

" **DNSGREP – DNS ENUMERATION TOOL** "

dnsgrep is a Linux based DNS enumeration tool that uses a dictionary in
order to find active addresses and their IP addresses based on a given DNS.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5984

" **STRONGSWAN – IPSEC AND IKEV1 IMPLEMENTATION** "

strongSwan is a complete IPsec and IKEv1 implementation for Linux
2.4 and 2.6 kernels. It interoperates with most other IPsec-based
VPN products. It is a descendant of the discontinued FreeS/WAN project.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5956

" **CENSUS** "

A common trend in communicative devices ensures that, those once
wired will eventually become wireless. With the proper set of hardware
and software, it becomes possible for anyone to monitor a wireless
station using a personal computer. Census was built to perform several
wireless functions which simplify the processes of auditing, monitoring,
and canvasing of wireless Access Points within range of your equipment.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5955

" **REMOTEJ 0.1.1** "

RemoteJ is an application for adding Bluetooth remote control capability to Sony Ericsson's mobile phones such as the K750, W800, Z520, W600, W550, and W900 series. It offers an extendable, configurable interface system that uses XML configuration files. It can be used to control your music player, video player, or PC-TV using a menu appearing in your mobile phone's menu.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5930

" **LEAF – LINUX EMBEDDED APPLIANCE FIREWALL** "

LEAF (Linux Embedded Appliance Firewall) is an easy-to-use embedded Linux system that is meant for creating network appliances for use in small office, home office, and home automation environments. Although it can be used in other ways, it is primarily used as a gateway/router/firewall for Internet leaf sites.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5874

" **STEALFLY – PORT KNOCKER**"

Stealfly is proof of concept perl code that illustrates the usage of port knocking.

http://www.astalavista.com/index.php?section=directory&cmd=detail&id=5860

[04] **Astalavista Recommended Papers**

" **COVERT CHANNELS THROUGH THE LOOKING GLASS** "

We started co-writing a short paper about network covert channels and finally you read that one. Parts 1 to 4 are concepts, ideas, food for the mind and next parts describe toys we published because mind has to play sometimes. Enjoy.

http://www.astalavista.com/index.php?section=directory&linkid=5856

" **THE PERIMETER PROBLEM** "

The old network security model—perimeter defense—was a lot like the old physical security model: Put your assets in a secure location, build a wall and use a gate to control who goes in and out.

http://www.astalavista.com/index.php?section=directory&linkid=5861

" **SOCIAL ENGINEERING – THE HUMANE ELEMENT OF INFORMATION WARFARE** "

Social engineering is one of the most dangerous and easiest to exploit

threats to information security today. The "human element" introduces an unpredictable variation into security that cannot be prevented with a simple technical control.

http://www.astalavista.com/index.php?section=directory&linkid=5882

" **0BAY – HOW REALISTIC IS THE MARKET FOR SOFTWARE VULNERABILITIES? "**

Pros and cons of purchasing vulnerabilities, and the potential for vulnerabilities market discussed.

http://www.astalavista.com/index.php?section=directory&linkid=5890

" **OPEN LETTER ON THE INTERPRETATION OF "VULNERABILITY STATISTICS "**

Steve Christey (CVE Editor) wrote an open letter to several mailing lists regarding the nature of vulnerability statistics. What he said is spot on, and most of what I would have pointed out had my previous rant been more broad, and not a direct attack on a specific group.

http://www.astalavista.com/index.php?section=directory&linkid=5905

" **COLLABORATIVE INTERNET WORM CONTAINMENT** "

Large-scale worm outbreaks that lead to distributed denialof- service (DDoS) attacks pose a major threat to Internet infrastructure security. Fast worm containment is crucial for minimizing damage and preventing flooding attacks against network hosts.

http://www.astalavista.com/index.php?section=directory&linkid=5919

" **THE THREATS AND COUNTERMEASURES GUIDE V2.0** "

The updated Threats and Countermeasures guide provides you with a reference to all security settings that provide countermeasures for specific threats against current versions of the Microsoft Windows operating systems.

http://www.astalavista.com/index.php?section=directory&linkid=5950

" **IDA PLUGIN WRITING TUTORIAL** "

This tutorial will get you started with writing IDA plug-ins, beginning with an introduction to the SDK, followed by setting up a development/build environment on various platforms. You'll then gain a good understanding of how various classes and structures are used, followed by usage of some of the more widely used functions exported.

http://www.astalavista.com/index.php?section=directory&linkid=5997

" **RECOMMENDED PRACTICES ON NOTIFICATION OF SECURITY BREACH INVOLVING PERSONAL INFORMATION** "

The Office of Privacy Protection in the California Department of

Consumer Affairs has the statutorily mandated purpose of "protecting the privacy of individuals' personal information in a manner consistent with the California Constitution by identifying consumer problems in the privacy area and facilitating development of fair information practices."

http://www.astalavista.com/index.php?section=directory&linkid=5995

" **40 WEB SITES OFFERING TELEPHONE CALLING RECORDS AND OTHER CONFIDENTIAL INFORMATION** "

This research is courtesy of the EPIC.

http://www.astalavista.com/index.php?section=directory&linkid=6035

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

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

Wonder why? Check it out :

The Top 10 Reasons Why You Should Join Astalavista.net

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

check out the special discounts!!

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

What is Astalavista.net all about?

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

Among the many other features of the portal are :

- Over **7.22 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing

info on previous hacks of these servers is available as well.

[06] **Site of the month**

VTE – The Virtual Training Environment

http://vte.cert.org/

CERT's Virtual Training Environment (VTE), with more than 160 hours of multimedia-based instruction in information assurance and computer forensics, is now available to the public

[07] **Tool of the month**

Browser Appliance Virtual Machine

The Browser Appliance is a free virtual machine that allows users to securely browse the Internet using Mozilla Firefox

http://www.vmware.com/vmtn/vm/browserapp.html

[08] **Paper of the month**

All Possible Wars? View of the Future Security Environment, 2001-2025

One of the group's initial tasks was to assess the future security environment to the year 2025. This was pursued by surveying the available literature to identify areas of consensus and debate. The goal was to conduct an assessment that would be far more comprehensive than any single research project or group effort could possibly produce. This survey documents major areas of agreement and disagreement across a range of studies completed since the last QDR in 1997. Because it distills a variety of sources and organizes and compares divergent views, this volume makes a unique contribution to the literature. It also provides a particularly strong set of insights and assumptions on which both strategists and force planners can draw in the next Quadrennial Defense Review.

http://www.astalavista.com/index.php?section=directory&linkid=6111

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

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

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

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

More information about the DVD is available at:

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

[10] Enterprise Security Issues

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

- Organizational Training and Today's Threatscape -

In this brief article I am going to discuss the importance and significance of organizational employees' training, yet try to emphasize on its pros and cons given today's constantly evolving threatscape and how hard it is to keep up with all of them.

Back in 2003 I used to argue on the usefulness of training your organization's workforce, and while I still believe the more they know the less troubles you'll have, I have recently came to the conclusion that educating a workforce given today's threatscape, and the slowdown of corporate citizenship, asks for more enforcement than ever.

Educating, Monitoring and Evaluating the progress are the key steps of any program, that is teach them, monitor activity for a certain period of time and then evaluate if there's any progress, for instance, you might do a real-life simulation of a security scenario and see how they react. Another important fact worth mentioning is your company's financial commitment towards educating your workforce, a workforce whose retention is getting even harder. General Motors recently reported their biggest loss ever, mainly because of too much commitment towards insurance issues related to their workforce, my point is that to a certain extend you might be sort of training your future competitors' employees. Something else that should be kept in mind, is that you cannot and should not educate everyone having access to the corporate's network, instead try to prioritize, cut the privileges to the minimum and give them where necessary only. Today's threats evolve faster then we can keep up with them, anything is exploitable and futuristic scenarios of having images spreading malware are fully realistic these days. Once starting to educate them, you wouldn't be able to keep up with it unless your solutions is a extremely low cost, yet very relevant one.

And while outsourcing is always an option, make sure evaluation of the results from time to time in order to justify the investment is among your top priorities. At the bottom line :

What you can train them to do?

- establish both, conscious and subconscious security mode of thinking when using the company's infrastructure. That is, a behavior slightly different to the one when using their home PCs

- securely maintain their mobile workplace while on the road(hopefully!)

- be suspicious or actually "on alert" while online, namely erase any signs of naivety

- never assume there's 100% and that it's a fact they should live with

- keep themselves up-to-date with the latest security threats through a internally distributed analyses, or public sources

What you cannot teach them to do is ?

- not to listen to online streams and open image files!

- verify the SSL certificates of every site they visit

- to define a suspicious web site, you see, "surfing the Web" is still rather popular

- that technology isn't the panacea of dealing with security, but humans at the bottom line

- convince them in the concept of 0day attacks(it would ruin their entire confidence in security as a whole, still, it's a good point to explain that it's not 100% security you're aiming at, but 98%, where 2% are left for technology or human error, but I feel you should not use 0days, the way a CSO shouldn't use cyberterrorism while seeking further investments)

Educate, but don't forget that if you don't take care of your company's destiny (enforcement), someone else will (unaware end user). To sum up, as much enforcement of security policies as possible and secure by default installations without the opportunity to modify them.

[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.

- Fortifying your browser – even more! -

Is secure surfing even possible? What is the consequence of the growth of client side attacks during the last couple of years, and why did the browser application became so easily targeted. What's more, is a secure browser that's actually still useful for surfing the web an option and how can this be achieved, are among the questions this article aims to answer. Moreover, I will briefly discuss the Browser Appliance, among the most handy utilities I've come across recently for all the Mozilla fans out there, wish we would soon see a Windows based release though!

Excluding email(and P2P perhaps :-), the browser is the second most popular Internet tool used by the entire workforce, that includes top management as well. This common sense fact has always been resulting in the development ot client side attacks, that greatly contribute to having your PC infected with malicious software(virus, trojan, worm), or get tricked by a phishing email.

What to keep in mind when it comes to threats posed by browsers?

- **vulnerabilities**

Even Firefox, or any other browser you name can suffer from vulnerabilities, and while the idea of Firefox is to be OS independent with the idea to improve the level of security, 100% security is futile. And now malicious attackers have the incentive of knowing that hundreds of thousands of security minded people have switched to it, it's as targeted as IE is.

- **insecure settings**

Even the most secure by design browser is useless if it's configured properly, that is, to achieve the balance between usability and security.

- **the trade off between usability, interactivity and security**

Having a secured browser might prevent you from accessing embedded content, And not take full advantage of the interactivity certain sites offer. Given they are trusted (is there such a thing anymore?!),

We can definitely talk about a browser monoculture and the habit/dependence/ of using of Internet Explorer as the most popular one. It is impressive how many people use it, and while Firefox is accepted as secure by default, Microsoft themselves have a point you can check out too :

http://blogs.msdn.com/ptorr/archive/2004/12/20/327511.aspx

One of the most useful, handy, and what I can call truly secured alternatives Is the use of the **Browser Appliance Virtual Machine** :

http://www.vmware.com/vmtn/vm/browserapp.html

The concept is pure beauty, and the only downsize of the idea is that it runs on Mozilla Firefox 1.0.7 and 1.5 running on Ubuntu Linux 5.10. Basically, the idea is that whatever hijackers or abuses your browser, it's all gone by the time you restart it without any modifications done to your system. And while I wouldn't like to advocate switching to Ubuntu for ensuring maximum security, I bet a Windows release is on its way. You can also check out some handy tips of tweaking it :

http://www.spywareinfo.com/articles/vmware/batweaks.php

In conclusion, consider going through CERT's recently released practical HOWTO on how to secure the most popular browsers, and the other resources :

http://www.cert.org/tech_tips/securing_browser/
http://www.windowsecurity.com/articles/Web-Browser-Vulnerabilities.html
http://bcheck.scanit.be/bcheck/
http://www.securityfocus.com/infocus/1848
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/luawinxp.mspx

[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 **Johnny Long,** from http://johnny.ihackstuff.com

Your comments are welcome at security@astalavista.net

Interview with Johnny Long, http://johnny.ihackstuff.com

Astalavista : Hi Johny, would you please introduce yourself, and share with us some info on your background?

Johnny : My name is Johnny Long, and I'm currently a researcher for Computer Sciences Corporation. I've been into security since I was a kid, but my professional security career is going on about 14 years now, the large majority of that has been as a professional hacker / pen tester. These days, I'm doing quite a bit of writing and enjoying the conference tour. I really enjoy getting a chance to hang out with everyone, and for me the community is one of the coolest parts of this field.

Astalavista : When did you first start doing Google Hacking, and what inspired you to deepen your research in this field?

Johnny : We (CSC's Strikeforce team) used to troll Google prior to a vulnerability assessment. When we started doing it we were primarily looking for information about targets we were breaking into physically. For example, it was pretty common to locate a snapshot of an employee wearing a badge. Those photos are real handy for recreating fake photo ID's which we could use to bypass a casual security guard's

gaze. After a while we started realizing that Google scans could reveal a great deal of information about the target network as well. I started posting some of these searches to my website along with a bit of text about why the search was interesting. After a while, folks started sending me their searches, and the rest is history. It's worth noting that I was certainly not the first person to do this stuff. The technique's been around for many years. I like to think I gave the technique new "legs" and raised the awareness that even the simplest (and oldest) of tricks can come in quite handy when used properly.

Astalavista : The concept and perhaps its usefulness given Google's snapshot of the *known* web turned it into an important penetration testing tool, let's not mention its popularity due to ease of use. My question is, to what extend is Google hacking illegal, would it ever be, or is it just Google doing a favour both, to the good and the bad guys at the bottom line?

Johnny : Google Hacking is not any less legal than straight-up Google queries. Period. It's what you do with the results that make it illegal.

Astalavista : Is the use of robots.txt enough to tackle the problem, and what are your comments on initiatives such as Google honeypots? To me, the results are an invaluable indication of the interest in this field, but what is your recommendation as a practical approach to protect against such attacks?

Johnny : Certainly honeypots are not preventative (I know you know that, just clarifying) and while I think the idea of a Google honeypot is way cool, there's just too many amateur webmasters out there, and way too many targets for honeypots to do much good. Robots.txt is a gentleman's agreement, and even worse, it's a roadmap for even the most amateur hacker. The solution is to crawl your own stuff, get an idea of what's out there and set strict policies for monitoring your web presence and preventing employees / users from posting inappropriate content. In addition, all web apps should be thoroughly tested by a professional, source code audits performed and policies established and enforced about secure coding processes.

Astalavista : How would you describe your best, and most sensitive discoveries through Google Hacking?

Johnny : Some of my discoveries are unmentionable, especially if I intend to keep my current job. I will say, however, that there's NOTHING I haven't seen. Everything from medical records to social security info, credit card numbers and reports, internal corporate memos, and even "sensitive" *Ahem* non-commercial *ahem* documents. Some things are just plain hilarious. For

example, we have several searches that reveal home control interfaces including power, security, cameras, VOIP control, the whole nine. Google someone's light's off? Sure thing.

Astalavista : The recent DoJ's request over Google's databases and even aggregate searches sparkled a lot of debate, and to be honest I am surprised by the lack of creativity by law enforcement while obtaining that type of data. What is your opinion on Google's reaction, what are your comments on the rest of the search engines(Yahoo!, MSN) compliance with the subpoena as well? Moreover, Google, like pretty much every company trying to capitalize on the emerging opportunities in China, is actively involved in censorship. Differentiating Google from the rest of the search engines, as the most popular one, how would you comment on their strategy not to introduce email and blogs in China due to fear of having to actually put people in jail for expressing their right of free speech? Is this marginal thinking better than nothing, and how you do think they should respond at the bottom line?

Johnny : First of all, Google is a business. Pure and simple. Some make pie-in-the-sky remarks about Google as a cultural barometer, an icon, the best thing since sliced bread, etc but without capital, they're outta luck. Google's got to keep the funding coming. Certain decisions should be seen as simply business decisions, and I think the (public) decisions on China are a reflection of that fact. There are great opportunities in China, and it certainly makes no sense for them to shoot themselves in the foot as they're walking through the door. I know I should be taking the "information should be free" stance and be a "true hacker", but that's how I see it.

Astalavista : While I am certain you have came across Koders.com, which as a matter of fact is great initiative, what do you think is the potential of utilizing their search feature for spotting trivial coding mistakes that quite some times could lead to a common sense vulnerability? Can patterns be used or put into practice the way you achieved it at Google Dorks database?

Johnny : The key word here is trivial. I think it is certainly possible to use Koders.com (great resource, I agree) as a launching pad for vulnerable code search. While you could certainly search for every instance of a traditionally insecure strcpy function, the function itself is not necessarily the problem. The context and placement of the function call is

significant, and without being able to easily cross-reference the rest of the code through that interface, the job gets... complex. This is still a worthy exercise, however, and certainly the door is open for a couple of Koders searches to get the ball rolling. That's all it takes.

Astalavista : Where is the future of search going? Vertical search engines, or personally tailored results based on search history? What would Google 2.0 look like as a concept and how you do envision any future developments in web search?

Johnny : Personally, I'm very interested in "desktop" search stuff. I don't mean the pithy Google product, but the Spotlight feature in Mac OS X, for example. A really well-thought-out feature like that can literally change the way you use a machine. For example, I've stopped using my dock (err... OS X launch bar) since I can hit MAC-SPACE, type the first few letters of the app I want to run, hit down arrow and enter and it launches. The search function digs into metadata inside files as well, and is extensible and scriptable. Truly well done. Now, this is all well and good, but beyond the gee-whiz factor, there's some interesting stuff lodged deep in the usage statistics of this widget, and in the way I work. Statistically speaking, my machine knows a great deal about me, and what makes me tick. What my habits are (both short and long term), my preferences, my hobbies, just about everything. Now, tie this to an online search engine, and the engine has a great chance of knowing what I want before I do. Sounds spooky and odd, but it could work. Online search history/prefs are one thing, but only a fraction of my activity is "online". That other computer activity is where a great deal of my passion lies. Tapping that would revolutionize searching, but it should be transparent to the user. Oh, and the security ramifications of "owning the man" are significant as well, so early adopters of such a technology should be ready for quite a battle...

Astalavista : What might happen if Google gets evil, and isn't evil just a twisted word anyway?

Johnny : See above. In that scenario, evil Google 0wnz0rz you. Evil Google is a talk for another interview. ;)

Astalavista : In conclusion, I wanted to ask you what are your future development plans for the Google Dorks database, and are there any other projects you're actively working on?

Johnny : Right now, we're getting ready to roll out a

snort rule list based on the GHDB. This would help admins see a malicious search coming in through a referrer. This could certainly be handy, and it's a relatively easy way of repackaging our content to help protect from the bad guys. Other than that' we're getting ready to undergo a major hardware and software overhaul to compensate for all our recent popularity. I'd like to thank everyone at ihackstuff.com for the continued support. Our admins put in quite a bit of work to keep things running, and without them, Johnny would be too busy maintaining stuff instead of hacking stuff!

Astalavista : Thanks for your time Johnny!

Johnny : Thank you!

[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.

-

Channel 9's Security Content

-

http://channel9.msdn.com/tags/Security

Videos, Podcasts, Screencasts, etc.

-

ANA Spoofer Project

-

http://spoofer.csail.mit.edu/

Our methodology is simple. We make software to test spoofing publicly available and ask the community to run it from as many sites as possible. The spoofer program attempts to send a series of spoofed UDP packets to a server on our campus.

-

The EULA Library

-

http://www.gripewiki.com/index.php/EULA_Library

The GripeWiki's EULA library is a place to find, read, post, and discuss the terms of all manner of end user license agreements.

-

Cryptokids

-

http://www.nsa.gov/kids/

America's Future Codemakers & Codebreakers

-

The XSS security challenge

-

http://community.livejournal.com/lj_dev/708313.html

Give it a try if you're up to it!

[14] Final Words

Dear readers,

Thank you for staying with us and for your invaluable feedback. Did you enjoy Issue 25? Drop us a line and let us know.

Meanwhile, feel free to participate in Astalavista's Geeky Photo contest, and get the chance to win a .NET membership, find out more at :

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

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader – Yordanka Ilieva
danny@astalavista.net