Astalavista Group Security Newsletter
Issue 18 - 30 June 2005
http://www.astalavista.com/
security@astalavista.net

[01] Introduction

Dear readers,

Welcome to Issue 18 of the Astalavista Security Newsletter!

In this issue you're about the read a great interview with John Young, the person behind **Cryptome.org**, You will learn more **about insiders** and **proactive anti-spam tips**, as well as browse through enormous and unique **hacking/security oriented resources** – all for everyone eager to know more!

The **Astalavista.com Team Members** wish you a challenging summer, we'll continue our tradition to keep you up-to-date with the latest security trends around the underground and the industry itself during the upcoming months.

Feedback is greatly appreciated at **security@astalavista.net**

Consider submitting your shots to our ever-growing **Geeky Photos** section at **photos@astalavista.net** and get the chance to win a prize from our **Underground eStore**!!

Astalavista Security Newsletter is constantly mirrored at :

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

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

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

Previous issues of Astalavista Security Newsletter can be found at:

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

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

[02] Security News

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

---

[GROUP: SECURE BLUETOOTH WITH LONG PINS]

Bluetooth, the wireless connection used on PDAs and phones, is not safe unless you use an eight-digit PIN to secure devices, an industry group has warned.

The Bluetooth Special Interest Group has told people to set eight-digit PINs when pairing two devices and to take other precautions, after a report described a way for hackers to crack the security codes on Bluetooth devices and seize control of them.

More information can be found at :

http://news.com.com/Group+Secure+Bluetooth+with+long+PINs/2100-1002_3-5764838.html

Astalavista's comments :

Hopefully, you have read our short Bluetooth security article in Issue 17 highlighting various security issues on Bluetooth-enabled devices. The truth is that the majority of people use short and easy to remember PINs and facing the age-old password remembering problems might also reflect on the slow adoption of this advice, which is among the many other threats not revealed in this article.

The Bluetooth Special Interest Group on the other hand is perhaps busy with innovation and adaptability, while it needs to publicly state, even build awareness on various Bluetooth security tips, attacks, both publicly and on its commercially oriented web site.

[I'M INNOCENT SAYS INDIAN IN U.K BANK DATA SCANDAL]

An Indian computer worker accused of selling the bank details of more than 1,000 people to a British newspaper said a friend asked him to give a CD to a Briton to earn extra money but he had no idea of its contents.

Twenty-four-year-old Karan Bahree, still on probation after starting his $230 a month job in April, denied any wrongdoing in a one-and-a-half-page handwritten explanation to his company, Infinity eSearch, local media reported yesterday.

More information can be found at :

http://www.computerworld.com/securitytopics/security/story/0,10801,102798,00.html

Astalavista's comments :

You simply cannot pretend to be innocent when you're acting as a "mule" for "three pounds per information" delivery, but what's to note in this case is the prejudice of The Sun towards the Indian workers easy to bribe .

Not surprisingly, at least for me, India is already experiencing problems with its developing economy citizens attitude and the global trends towards outsourcing there. Actions must be taken to continue these investments in the country.

Hopefully you still remember the Citigroup case too :

http://www.citigroup.com/citigroup/press/2005/050606a.htm

[**6.5m POUNDS DUO JAILED**]

An American who masterminded the UK part of a multi-million pound ID theft scam was yesterday jailed for six years. Douglas Havard, 24, was sentenced on Monday at Leeds Crown Court after pleading guilty to conspiracy to defraud and conspiracy to launder money. His accomplice, Lee Elwood, 25, of Glasgow, was jailed for four years after pleading guilty to the same offences in June 2004.

The court heard the duo were integral to a phishing scam that netted an estimated £6.5m. The duo operated the UK end of an international operation that tricked consumers into handing over their banking credentials to bogus websites. The pair used credit cards obtained under false names, money raided from compromised bank accounts and the illicit purchase and sale of goods online to finance a lavish lifestyle.

More information can be found at :

http://www.theregister.co.uk/2005/06/28/phishing_duo_jailed/

Astalavista's comments :

The facts – you don't need an entire Underground army like the ShadowCrew to coordinate and organize huge scams like these, but just knowledge and the courage to do it, which is naturally backed by the eventual "lavish lifestyle" mentioned. Phishing scams or the actual lack of awareness of these have resulted in phishing being the fastest growing threat to E-commerce ever.

More info can be found at :

http://www.astalavista.com/data/idtheft1.pdf
http://www.astalavista.com/data/identity_theft.pdf
http://www.astalavista.com/data/identity_assurance_on_the_internet.pdf
http://www.astalavista.com/data/ciwp200503.pdf
http://www.astalavista.com/data/report.pdf
http://toolbar.netcraft.com/stats/countries

[**CREDIT CARD BREACH EXPOSES 40 MILLION ACCOUNTS**]

In what could be the largest data security breach to date, MasterCard International

on Friday said information on more than 40 million credit cards may have been stolen.

Of those exposed accounts, about 13.9 million are for MasterCard-branded cards, the company said in a statement. Some 20 million Visa-branded cards may have been affected and the remaining accounts were other brands, including American Express and Discover.

MasterCard and Visa both say they have notified their member banks of the specific accounts involved so the banks can take action to protect cardholders.

More info can be found at :

http://news.zdnet.com/2100-1009_22-5751886.html

Astalavista's comments :

The weakest link always gets exploited, in this case, a third party processor of payment data, but why is it that even this function makes me bother when it comes to CCs?! This is indeed perhaps among the biggest data security breaches in terms of credit card number leakages. Perhaps the best clue for the ongoing investigation might be the fact that they leaked credit cards are known and any fraudulent activities will be detected but would it be helpful if someone starts leaking parts of it with the idea to hide himself and diversify the risk of getting caught?

At the bottom line – wish I had a Discover card with 0% liability ☺

[**ISRAELI POLICE UNCOVER TROJAN INDUSTRIAL SPY RING**]

Israeli police have uncovered an industrial spy ring that allegedly used Trojan software to snoop into some of that country's leading companies.
A report in the English-language newspaper Haaretz details how a wide range of businesses, including TV, mobile phone, car import and utility companies, used a Trojan program believed to have been written by a husband-and-wife team living in London to spy on business rivals.

More information can be found at :

http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,102141,00.html

Astalavista's comments :

What's the easiest way to "catch up" or match your competitors propositions and even exceed them? No, it's not called competitive advantage or business intelligence, but taking advantage of remote access control tools to do industrial espionage. Even though major organizations are, at least believed, to be taking care of malware, the story clearly points out the devastating effects of what happens when you don't take your rivals into consideration.

The Trojan, self-coded might somehow get ignored by the anti-virus scanners in place, but what's to note is a technique using the autostart feature of a CD that I described in ***The Complete Windows Trojans Paper*** *back in 2003 and thought it was outdated or at least enough awareness was build on its possible abusive use.*

Hopefully the case will raise even more awareness on the fact that private investigation

companies are actively using Trojans to spy on individuals, and that companies striving to innovate or catch up are actually interested in these services, ethics, e what?!

[**SPAM HURTS DEVELOPING COUNTRIES**]

Spam may be a global problem but it's hurting Net users in developing countries more than their counterparts in industrialized nations, according to a new report by the Organization for Economic Cooperation and Development (OECD) in Paris.

Numerous underdeveloped countries, especially in Africa and Asia, lack the knowledge, technology and money to effectively combat the growing flow of junk e-mail over their domestic communication networks. As a result, users in these regions suffer from more outages and less reliable service, and are often distrustful of the Internet -- all factors that threaten to widen the global digital divide.

"Spam is a much more serious issue in developing countries than in OECD countries, as it is a heavy drain on resources that are scarcer and costlier in developing countries than elsewhere," the report states.

More information is available at :

http://www.thestandard.com/internetnews/001332.php

Astalavista's comments :

Living in the ADSL world where companies strive to increase the speed of connection to levels reaching those of a personal botnet, less is though of, even said about developing countries whose customers'(primarily companies for sure), suffer whenever huge amounts of network traffic is consumed for what's the biggest con of email – spam.

CSIRTs or CERTs are a must have, while my opinion is that instead of reinventing the wheel of filtering huge amounts of incoming spam, outsourcing, users' awareness on how their emails leak on the Internet, and of course the participation and integration of world known spammers blacklists are a must

[**STANFORD REJECTS 41 APPLICANTS WHO ATTEMPTED TO HACK INTO SITE**]

The Stanford University Graduate School of Business has rejected all 41 applicants who tried to hack into an admissions Web site earlier this year.

The applicants were given the chance to explain why they had attempted to gain unauthorized access to their files, business school Dean Robert Joss said Saturday night.

`At the end of the day, we didn't hear any stories that we thought were compelling enough to counterbalance the act,' Joss said.

In early March, an unidentified hacker used a Business Week online forum to post instructions on hacking into ApplyYourself, an online service that some schools use to notify students of their admissions status.

More information can be found at :

http://www.mercurynews.com/mld/mercurynews/living/education/11773260.htm

Astalavista's comments :

I believe at the bottom line it was about reputation and prejudice, while on the other hand we could take this story from another angle, what if I were to identify myself with a competing fellow student in order to eventually get him/her into trouble?

Check out the following :

http://www.applyyourself.com/
http://blogs.law.harvard.edu/philg/2005/03/08#a7726
http://www.osvdb.org/14655

[**ADWARE MAKERS EXPLOIT BITTORRENT**]

A row has broken out after a marketing firm was caught hiding adware in files distributed on the BitTorrent file sharing network. P2P applications such as Kazaa have been bundled with various adware packages for some time, to say nothing of the increased use of P2P networks as a distribution network by virus writers, but BitTorrent has been a cleaner environment. Recent developments suggests that may be about to change.

More information can be found at :

http://www.theregister.co.uk/2005/06/17/adware_outbreak_bittorrent/

Astalavista's comments :

Perhaps one of the last untouched pilars of the P2P industry started getting Adware's attention and it's all about tracking, and monitoring trends, but what about prosecutions based on copyrights infringement? Don't forget that there's no such thing as free lunch, and has never been both in life and on the Net.

Here's a list of Clean and Infected P2P file-sharing networks :

http://www.spywareinfo.com/articles/p2p/

[**JAPAN NUCLEAR DATA LEAK RAISES SECURITY CONCERNES**]

Japanese officials scrambled on Thursday to contain the public relations fallout from reports that confidential information about Japan's nuclear plants had leaked onto the Internet through a virus on a personal computer.

Japan's top government spokesman pledged to take steps to protect information after data on several nuclear plants appeared online, including photographs of their interiors, details of regular inspections and repair work and names of workers.

"Nuclear plants are important facilities in terms of anti-terrorist measures, security and what not, and therefore we would like to take full steps to ensure information management," Chief Cabinet Secretary Hiroyuki Hosoda told reporters.

More information can be found at :

http://news.yahoo.com/news?tmpl=story&u=/nm/20050623/wl_nm/japan_nuclear_secrets_dc

Astalavista's comments :

Looking for a terrorist break-in scenario roadmap, just stay tuned for possible information leakages like these. As we have already seen in the previous news item, malware is used to conduct competitive intelligence or let's pretty much call it industrial espionage. Even though the "virus" mentioned wasn't especially crafted for this purpose, future "releases" might indeed start contributing to the not so publicly discussed threat of industrial espionage.

[**MOBILE MALWARE WON'T SHOW UNTIL 2007**]

Mobile phone and PDA users have more than two years to get ready for a quick-spreading worm, security research analysts said as they poked holes in anti-virus vendors' hype about the immediate need for defences.

"Anti-virus vendors see huge potential profits in selling security to billions of cell phone and PDA users," said John Pescatore, vice president and research fellow with Gartner. "In particular, the anti-virus industry sees cell phones as the way to grow sales outside of a flat, commoditised PC market."

More information can be found at :

http://www.itnews.com.au/newsstory.aspx?CIaNID=19168

Astalavista's comments :

Rather contradictive statement, mainly because that in my opinion manufacturers will continue to see and of course achieve innovation on the devices where the trade-off is from a security point of view, at the end, as usually the end users are caught in between something they cannot live without, but is insecure.

http://www.f-secure.com/ are currently doing the most to publicly build awareness of mobile malware. and although they're vendor itself, I'd rather they target the carriers and not the end users.

[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**

" **MODGREPER – HIDDEN KERNEL MODULES DETECTOR** "

modGREPER is a hidden module detector for Windows 2000/XP/2003.

http://www.astalavista.com/?section=dir&act=dnd&id=4380

" **TATTLE – AUTOMATIC REPORTING OF SSH BRUTE-FORCE ATTACKS** "

Tattle is a Perl script that crawls through your SSHd logs (usually /var/log/messages) and finds hosts who've connected to your SSH server.

http://www.astalavista.com/?section=dir&act=dnd&id=4459

" **SSSS – SECRET SHARING SCHEME FOR UNIX SYSTEMS** "

ssss is an implementation of Shamir's secret sharing scheme for UNIX systems. Secret sharing can be used to require that several parts of a message be present, or require that several people in a group are present, or split the sending of secret data into several channels, all of which would need to be intercepted to recover the information.

http://www.astalavista.com/?section=dir&act=dnd&id=4428

" **BLUEFISH – POWERFUL WEB EDITOR** "

Bluefish is a powerful editor for experienced web designers and programmers. Bluefish supports many programming and markup languages, but it focuses on editing dynamic and interactive websites.

http://www.astalavista.com/?section=dir&act=dnd&id=4404

" **ACID – ANALYSIS CONSOLE FOR INTRUSION DATABASES** "

The Analysis Console for Intrusion Databases (ACID) is a PHP-based analysis engine to search and process a database of security events generated by various IDSes, firewalls, and network monitoring tools.

http://www.astalavista.com/?section=dir&act=dnd&id=4414

" **MWCOLLECT – WORMS COLLECTOR** "

mwcollect is an easy solution to collect worms and other autonomous spreading malware in a non-native environment like FreeBSD or Linux.

http://www.astalavista.com/?section=dir&act=dnd&id=4478

" **SPAM FEEDER**"

Sick of spam? Want to fight back? A tool for poisoning a spammer’s database through fake emails generation.

http://www.astalavista.com/?section=dir&act=dnd&id=4465

" **MALCODE ANALYST PACK** "

The Malcode Analyst Pack contains the following GUI driven utilities: FakeDNS A minimal DNS server allowing the user to have all DNS queries resolve to a predefined IP. IDCDumpFix This tool can be used to associate API names to IAT addresses for IDA disassemblies of raw memory dumps. Fast, simple technique to get a readable disassembly for arbitrarily packed executables. MailPot A small lab-quality tool for capturing e-mails sent out by trojans and mass mailers.

http://www.astalavista.com/?section=dir&act=dnd&id=4494

" **JSTUN**"

JSTUN is a STUN (Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translation (NAT)) implementation. STUN provides applications a mean to discover the presence and type of firewalls or NATs between them and the public Internet. In the presence of a NAT, STUN can also be used by applications to learn the public Internet Protocol (IP) address assigned to the NAT.

http://www.astalavista.com/?section=dir&act=dnd&id=4535

" **KLOG** "

Klog demonstrates how to use a kernel filter driver to implement a simple key logger.

http://www.astalavista.com/?section=dir&act=dnd&id=4566

[04] **Astalavista Recommended Papers**

" **THE SECURITY RISKS OF DESKTOP SEARCHES** "

Google has recently released a very handy new tool that allows you to perform searches against your own computer in the same way that you would search the Internet. With this tool come some serious security problems though. In this article, I will discuss Google's security issues and talk about what this might mean for other companies developing similar applications.

http://www.astalavista.com/index.php?section=dir&act=dnd&id=4314

" **ANALYSIS OF A SUSPICIOUS PROGRAM** "

An article published in the first English hardcopy issue of Hakin9 magazine - 1/2005.

http://www.astalavista.com/index.php?section=dir&act=dnd&id=4320

" **HACKING IN A FOREIGN LANGUAGE : A NETWORK SECURITY GUIDE TO RUSSIA** "

Brief outline : Russia as a threat, Russia as a resource, Crossing International Borders, The International Political Scene.

http://www.astalavista.com/index.php?section=dir&act=dnd&id=4315

" **GUIDE TO EVALUATING TECHNICAL SOLUTIONS TO COPYRIGHT INFRINGEMENT ON CAMPUS NETWORKS** "

This paper is intended to help institutions of higher education critically evaluate the principal technological tools and policies being used to enforce copyright on campus networks.

http://www.astalavista.com/?section=dir&act=dnd&id=4384

" **WHO OWNS YOUR NETWORK?!** "

A discussion of Bot networks. The more one learns...the more paranoid one becomes.

http://www.astalavista.com/index.php?section=dir&act=dnd&id=4379

" **CRACKING THE BLUETOOTH PIN** "

This paper describes the implementation of an attack on the Bluetooth security mechanism. Specifically, we describe a passive attack, in which an attacker can find the PIN used during the pairing process.

http://www.astalavista.com/index.php?section=dir&act=dnd&id=4356

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

We all have had problems with machines being overrun by malware: taking 20 minutes to startup, constant popups, hijacking of the home and search pages, bookmarks being added, etc. Malware can even turn a machine into a "zombie", and be an unwilling participant in spam sending/relaying, address harvesting, or DDOS attacks against other computers.

http://www.astalavista.com/?section=dir&act=dnd&id=4426

" **IS THE WEPONOZATION OF SPACE INEVITABLE?** "

If war-fighting in or from space is inevitable, it then follows that the United States should have the panoply of military capabilities not just to deter warfare in the heavens, but also to actively defend satellites in orbit that are essential for the conduct of U.S military operations on the ground.

http://www.astalavista.com/?section=dir&act=dnd&id=4467

" **AUTHENTICATION AND SESSION MANAGEMENT ON THE WEB** "

This paper looks at the security concerns specific to websites that have a secure area where users can login. For much of the paper we use the example of Acme Enterprises, a fictitious company that sells generic goods by mail order.

http://www.astalavista.com/?section=dir&act=dnd&id=4455

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

This(160 pages) dissertation provides a detailed overview of basic services that any m-Commerce application should provide to the banking industry. The security of GSM networks has come under attack in the past. This dissertation aims to evaluate the security offered by GSM and assess potential attacks in order to further understand risks associated with m-Commerce applications over GSM.

http://www.astalavista.com/?section=dir&act=dnd&id=4443

[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 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

---

http://www.utm.edu/research/primes/

An outstanding resource on prime numbers!

[07] Tool of the month

Rainbow-tables calculator

Online program to count pre-calculated Rainbow-tables parameters.

http://www.astalavista.com/?section=dir&act=dnd&id=4402

[08] **Paper of the month**

Cyberanarchists, Neuromantics and Virtual Morality

Great cyberpunk related thesis.

http://www.astalavista.com/data/thesis01010.pdf

[09] **Geeky photo of the month – 'RadioShack Operations'**

Every month we receive great submissions to our Geeky Photos gallery. In this issue we've decided to start featuring the best ones in terms of uniqueness and IT spirit.

'RadioShack Operations' can be found at :

http://www.astalavista.com/images/gallery/dscf0099.jpg

[10] **Free Security Consultation**

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

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

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

Question : I represent the marketing department of a middle size enterprise and I wanted to ask you on your opinion as the opinion of a security site I know for many years now, how should I limit the sensitive information that my employees reveal while blogging? I myself am not against blogging, as I blog on a a daily basis, what bothers me is that they sometimes reveal too much sensitive company information?

Answer : If you have the resources and the motivation you can always monitor these blog enties depending on your workforce size, and while a bit unpractical it would perhaps reveal even more leakages of business information. Start by defining sensitive and confidential information, educating your workforce on what is sensitive information and even a certain degree of common sense would do the job, most of all, don't create the negative impression that they cannot blog, of course they can, the thing is that they simply cannot discuss certain things for

the sake of keeping the business alive. Communicate, don't restrict.

A Legal Guide for Bloggers can be found at :

http://www.eff.org/bloggers/lg/

Question : I have a very basic question for you guys, meanwhile congratulations on what you've managed to develop at your web site, I'm a regular visitor!! I believe from a network point of view our company's network is pretty secure, what bothers me are all the physical devices that employees bring and what they do with them, namely, bring malware or upload sensitive information in terms of convenience. What to do with these, a lot of people have complained that it's handy when it comes to work efficiently?

Answer : Even though your administrators can tip you on a large-scale USB devices blockage techniques, you can also consider using a commercial solution, where the goal would be to not only block, but actually monitor what's being uploaded, who's uploading it and coordinate it with eventual insider related investigations. USB sticks or any digital device capable of storing information can be primarily used to leak sensitive information. Either totally restrict these, or use them as honeypots for further investigations. You might also consider doing a usability audit of your intranet and the way your employees work, access and distribute information, doing so would create a perfect and hopefully secure, virtual work environment.

Question : Hi Asta folks, I have recently come across an article pointing out that Google is spreading spyware links on their advertisements and wanted to hear your opinion on that as I've came across about some of your previous comments on many Google privacy related issues and really liked them?

Answer : In this very same fashion we might also consider that spyware vendors are actively working on their search engine optimisation strategies, while they aren't as thankfully Google is taking certain measures to ensure that the most visible results are indeed relevant and spyware free ones. On the other hand this action is in contradiction with the nature of AdSense which might give spyware vendors greater reach, which this is just among the many vectors they try to adopt when looking for more "leads". What you should worry about is not coming across these intermediaries, or even if you do - make sure your system's integrity is exactly the same as it was before you were there.

Benjamin Edelman's article is on the other hand available at :

http://www.benedelman.org/news/060605-1.html

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

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

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

More information about the DVD is available at:

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

[12] 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!

- Insiders at the workplace – trends and practical risk mitigation approaches -

This short article will give you a brief overview of the threats posed by insiders and will highlight various practical approaches for mitigating the threats.

Major companies or emerging ones are constantly confronted with the need to seek and achieve competitive advantage over their rivals, while empower their workforce as much as possible and comply with both internal and external privacy regulations. Where's the line between promotion innovation, open culture and corporate citizenship and turning yourself into a corporate **BigBrother** to preserve what's most secret to you, and what is most secret to you, your assets or your workforce talent and expertise?

Insiders are and have always been there as a threat, and if you cannot achieve what you want to achieve from the outside, look for ways to achieve an inside-outside approach, mainly because of the trust based nature of how they attack.

Who's attacking you? – those you empower to put your company's mission into action, namely your employees, part-time, full-time, interns and in certain cases your partners

Why are they attacking you? – seeking a revenge, financial gains, or expressing their overall dissatisfaction with a company's policies, actions or treatment towards them, while specific industrial or competitive intelligence scenarios should be considered as well

Should you worry about turning yourself into a corporate BigBrother? – no, But going back to basic management practices is your workforce **Theory X** or **Theory Y** centered, and I'm sure that in case you go for the second, you would actually "communicate", not blindly "enforce" these practices

Some approaches to dealing with insiders might be :

- ICT and HR department coordination – namely make sure that there's a real-time coordination between these two departments and that past employees have all their access to the network restricted, what's better, certain organizations even consider monitoring these

- Background checks are a must have, employees from rival companies and interns are to be considered

- Build awareness of the potential damages to both the enterprise and the individual's future in case someone gets caught

- Ensure as much information is gathered for the employees' activities in the corporate environment so that malicious activities can be detected in real-time or at a later stage

- Develop benchmarks for suspicious activity, suspicious activities coordinated monitoring and establish guidelines for early-warning detection of suspicious activities

- Constantly use your electronic resources to efficiently measure, compare and improve your employees satisfaction, and even though early-warning "bad or revenge mood" methodology is pretty abstract as an idea, this should be considered

- Put your system administrator's in "your next security breach attempt might be your ex-colleague's remote connection attempt back to the company's network" mode of thinking

A great and very relevant report is also available at :

http://www.cert.org/archive/pdf/bankfin040820.pdf

[13] 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.

- Spam – proactive security tips -

The purpose of this brief article is to give you general advices and practical solutions for taking proactive rather than active measures against spam

Prevent the disease, don't fight it once developed – is perhaps the best and most user unfriendly approach for dealing with spam, but how come? End users usually start taking active measures by the time they find themselves receiving tons of spam on a daily basis, and by the time they learn how to filter the current spam that's targeting them, a multilanguage spam attack comes next!

Make sure your email hasn't leaked on the Internet

Don't leave your email publicly available on web sites, web forums or ensure

that registration based web sites do not leave it in the worst **mailto:** based way on the web. Consider converting your email to a small gif that cannot be processed by spam crawlers, use letters separation such as **s e c u r i t y@astalavista.net** , or replace @ with AT and . with DOT

The Address Book dilemma

Even though you manage to somehow preserve your email from spam crawlers, Malware has been known to build networks using the victim's address book or hard drive.

The above advices fully apply when leaving your email in a document, presentation etc. make sure even though someone that's in possession of your email gets their PC hacked, your email would hold on for a little while, or you could modify in a perhaps not so convenient for your buddies way address card way, but at least you'll limit the chance of its exposure.

When subscribing to mailing lists

Ensure the mailing list is trusted, Google is your friend here, and the worst thing you could probably do is have all-in-one email account, instead set up a separate account with the idea to verify if there're reselling your address or somehow distributing it to earn $. The worst thing, that perhaps out of your reach is the eventual exploitation of the mailing lists's database, even though on a mass-scale this isn't a practical solution from a spammer's point of view.

When dealing with spam itself

Make sure your email client doesn't load remote images, and make sure you don't interact with the message itself, don't try to remove yourself by following "Remove me" messages, as what you're doing is actually confirming that your email is indeed active.

A good article on how spammers harvest email addresses can be found at :

http://www.private.org.il/harvest.html

As well as the following resources related to spam and fighting it :

http://www.stopspam.org/email/headers.html
http://www.astalavista.com/data/voipspamfinal.pdf
http://www.astalavista.com/data/030319spamreport.pdf
http://www.astalavista.com/data/spampaper.pdf
http://www.astalavista.com/data/spamfaq.html
http://www.astalavista.com/data/ciwp200502.pdf

[14] 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 **John Young**, the person behind **Cryptome.org** and the **Eyeball-Series.org**

Your comments are welcome at security@astalavista.net

Interview with John Young, http://www.cryptome.org/

Astalavista : Hi John, would you, please, introduce yourself to our readers, share some info on your background, and tell us something more about what are Cryptome.org and the Eyeball-Series.org all about?

John : Cryptome was set up in June 1996, an outgrowth of the Cypherpunks mail list. Its original purpose was to publish hard to get documents on encryption and then gradually expanded to include documents on inforamtion security, intelligence, national security, privacy and freedom of expression. Its stated purpose now is:

"Cryptome welcomes documents for publication that are prohibited by governments worldwide, in particular material on freedom of expression, privacy, cryptology, dual-use technologies, national security, intelligence, and secret governance -- open, secret and classified documents -- but not limited to those.

Documents are removed from this site only by order served directly by a US court having jurisdiction. No court order has ever been served; any order served will be published here -- or elsewhere if gagged by order. Bluffs will be published if comical but otherwise ignored."

The Eyeball Series was initiated in 2002 in response to the US government's removal of public documents and increased classification. Its intent is to show what can be obtained despite this clampdown.

Astalavista : What is your opinion about cyberterrorism in terms of platform for education, recrewting, propaganda and eventual real economic or life loses?

John : Cyberterrorism is a threat manufactured by government and business in a futile attempt to continue control of information and deny it to the public. Cyber media threatens authorities and authoritarians so it is demonized as if an enemy of the state, and, not least, corporate profits.

Astalavista : A couple of words - privacy, data aggregation, data mining, terrorism fears and our constantly digitized lifes?

John : Privacy should be a right of citizens worldwide, in particular the right to keep government and business from gaining access to private information and personal data. The argument that government needs to violate privacy in order to assure security is a lie. The business of gathering private information by corporations and then selling that to government and other businesses is a great threat to civil liberties. Much of this technology was developed for intelligence and military uses but has since been expanded to include civil society.

Astalavista : Shouldn't the U.S be actively working on hydrogen power or alternative

power sources instead of increasing its presence in the Middle East or to put the question in another way, what is the U.S doing in Iraq in your opinion? What do you think is the overall attitude of the average American towards these ambitions?

John : No question there should be energy sources as alternatives to the hegemonic fossil fuels. Dependence on fossil fuels is a rigged addiction of that worldwide cartel. Car ads are the most evil form of advertising, right up there with crippling disease of national security.

Astalavista : Is ECHELON still functioning in your opinion and what do you believe is the current state of global communications interception? Who's who and what are the actual capabilities?

John : Echelon continues to operate, and has gotten a giant boost since 9/11. The original 5 national beneficiaries -- US, UK, CA, AU and NZ -- have been supplemented by partial participation of other nations through global treaties to share information allegedly about terrorism. Terrorism is a bloated threat, manufactured to justify huge funding increases in defense, law enforcement and intelligence budgest around the globe. Businesses which supply these agencies have thrived enormously, and some that were withering with the end of the Cold War have resurged in unprecedented profits, exceeding those of the Cold War.

Astalavista : Network-centric warfare and electronic warfare are already an active doctrine for the U.S government. How do you picture the upcoming future, both at land and space and might the Wargames scenario become reality some day?

John : Network wargames are as pointless and wasteful as Cold War wargames were. They churn activity and consume expensive resources. None are reality-based, that is, outside the reality of imaginary warfare.

Astalavista : Do you believe there's currently too much classified or declassified information, namely documents, maps, satellite imagery etc. available on the Net these days? In the post 9/11 world, this digital transparency is obviously very handy for both terrorists and governments, but who do you think is benefiting from it?

John : Far from being too much information available to the public, there is a diminishing amount, especially about exploitation of those who have access to classified and "privileged" information -- government and business -- and those who lack access.

The concocted warning that open information aids terrorism is a canard of great legacy, one that is customarily spread during times of crisis, the very times when secret government expands and becomes less accountable. "National security" is the brand name of this cheat.

Astalavista : In conclusion, I wanted to ask you what is your opinion of the

Astalavista.com's web site, in particular, our security newsletter?

John : Great site, very informative, give yourself a prize and a vacation at G8 with the world class bandits.

Astalavista : Thanks for your time John!

John : Thanks to you!

[15] **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.

-

Prime Numbers

-

http://www.utm.edu/research/primes/

A comprehensive web site deadling with prime numbers research, records and resources

-

Koders.com

-

http://www.koders.com/

The source code search engine, searching **225,816,744** lines of code

-

Spamlinks.net

-

http://www.spamlinks.net

The anti-spam portal

-

Electronic-circuits-diagrams.com

-

http://www.electronic-circuits-diagrams.com

Electronic circuits, kits, do-it-yourself, circuit diagrams, design and electronics hobby schematics

-

AboveTopSecret.com

-

http://www.abovetopsecret.com/

The Internet's most popular conspiracy discussion forum

[16] **Final Words**

Dear readers,

We hope you've enjoyed going through Issue 18 of our security newsletter and that we have either increased or improved your security awareness knowledge in the most recent security trends!

Enjoy the summer, don't forget to keep an eye on **Astalavista.com** on a daily basis and watch out for our **weekly** security resources newsletter coming out at the end of July!

Cheers from the **Astalavista.com** team!!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net