Astalavista Group Security Newsletter
Issue 16 - 30 April 2005
http://www.astalavista.com/
security@astalavista.net

[01] **Introduction**

Dear readers,

Welcome to the 16th issue of Astalavista Security Newsletter!

As usual, a lot's been going around in April, RaFa got busted, Hushmail faced a DNS attack, more Symbian malware in the wild and many other events.

In this issue you will read **an interview with Nicolay Nedyalkov from ISECA,** you will go through two articles, namely, **'DNS Security, common threats, defenses and the introduction of DNSSEC'** and **'Phishing attacks – put yourself in "learning-mode"** and much more!

In **Issue 17** we're about to integrate several more sections, some providing content from other respected resources, others representing our point of view on the topic, watch out!

Keep yourselves busy, and be good at anything you do beside wasting your time!

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

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

---

[**LEXISNEXIS UNCOVERS MORE CONSUMER DATA BREACHES**]

Data broker **LexisNexis** said on Tuesday that personal information on **310,000 U.S. citizens** may have been stolen from its computer systems, 10 times more than its initial estimate last month.

An investigation by **LexisNexis**—owned by Anglo-Dutch publisher Reed Elsevier – Determined that its **databases had been fraudulently breached 59 times using stolen passwords**, leading to the possible theft of personal information such as addresses and **Social Security numbers**. LexisNexis, which said in March that 32,000 people had been potentially affected by the breaches, will notify an additional 278,000 individuals whose data may have been stolen.

More information can be found at :

http://www.eweek.com/article2/0,1759,1784991,00.asp

Astalavista's comments :

"Dear "customer", we would like to express our deepest apologies for the recent leakage of your sensititive information to an unknown individual/individuals. You have to realize that the only reason for which we're notifying you right now is because of California's SB 1386 state law, therefore we would still appreciate some trust to our ability to safeguard and notify you of your private data exposure – protected through passwords of course, we all use passwords, don't we? What to do about it? – nothing, stay tuned for possible identity theft."

Obviously the security policies at LexisNexis have to address that passwords are on the verge of extinction and have decent access controls in place, but that's like stage 1 in the security process.

If anyone(hacker, identity thief, spy) can get to data aggregation companies, they can get to anyone and although there's a great deal of other tactics to do that, these companies have it all stored for you.

As the US Congress, followed by a large number of states are considering the adoption of the SB 1386 law, the industry will finally have the opportunity to put new meaning in the process of probability evaluation while justifying ROSI models or reporting security trends – it's worse than anyone has ever imagined, that's for sure.

More resources on **Identity Theft** can be found at :

http://www.astalavista.com/?section=dir&cmd=file&id=3436
http://www.astalavista.com/?section=dir&cmd=file&id=3983
http://www.astalavista.com/?section=dir&cmd=file&id=1359

[**ARREST MADE IN BREACH OF MILITARY WEBSITE**]

A self-described male model and member of the notorious **computer hacker Group World of Hell** was arrested last weekend and accused of **breaking into U.S. Air Force computer servers** in Denver, authorities said. **Rafael**

Nuñez-Aponte, 25, of Venezuela bragged **about bringing down a Web-based server network** in 2001 that provided training for thousands of Air Force personnel, according to a federal arrest warrant unsealed Tuesday. Investigators said the telecom-security expert replaced the Air Force's Web page with his own and left the **World of Hell** website address.

More information can be found at :

http://www.denverpost.com/Stories/0,1413,36~53~2800528,00.html
http://securityfocus.com/news/10868

A previous article from 2002 "**NASA investigating hacker theft of sensitive documents**" gives more insight on the public leakage of "competitor sensitive" documents on the Internet.

http://computerworld.com/securitytopics/security/hacking/story/0,10801,73305,00.html

Rafael Nuñez-Aponte is also a member of the **Counter Pedophilia Investigation Unit** http://www.cpiu.us/ for quite some time now.

Astalavista's comments :

That's news worth mentioning given WoH's popularity as .gov and .mil defacers, and it got even more interesting back in 2002 when they downloaded and distributed sensitive NASA documents.

The Feds cheered about this one for sure as it acts as a public statement to everyone ever compromised a government system and coming to the U.S.

Although I personally doubt WoH were involved in child pornography trading, and the way you cannot judge an entire nation based on a single citizen, the same way you cannot judge a member of a group based on another members' actions – they use to call it stereotyping. More news will follow, a recent defacement of a military site prompts for "free RaFa", he definitely has a lot of friends, that's for sure.

[**HUSHMAIL HIT BY DNS ATTACK**]

Surfers trying to visit the web site of popular secure email service **Hushmail** were redirected to a false site early Sunday following a **hacking attack**. Hush Communications said hackers changed Hushmail's DNS records after **"compromising the security" of its domain registrar (Network Solutions)**. These changes were undone after a few hours on Sunday and normal Hushmail services have now been restored. During the period of the attack users visiting Hushmail.com were confronted by a **defaced page** containing a jokey reference that **The Secret Service is watching. Agent Leth and Clown Jeet 3k Inc.** Things might have been far worse if hackers had used the ruse to set up a doppelganger site under their control for the purposes of obtaining the pass phrases needed to access the encrypted email service (a trick known as a **pharming attack**). As it was the impact of the attack was limited to **lost email**.

More information can be found at :

http://www.theregister.co.uk/2005/04/25/hushmail_dns_attack/

A defecement mirror can be found at :

http://www.zone-h.org/defacements/mirror/id=2309823/

Astalavista's comments :

Just a thought – wasn't Hushmail used by a large number of web site defacement groups as means of communication with the outside world? ..

You see you definitely cannot crack Hushmail's encryption in place, or guess someone's passphrase, but what you can do is make them "talk" first to you and then to Hushmail.com, there you got it.

Sometimes employees, unaware of social engineering attacks, indeed "make the impact".

Picture your organization in a situation where mail cannot be delivered for hours even though servers are running, administrators and experts are still on their job place, only because of a third-party's(but a vital one) lack of understanding of basic security concepts. I mean a couple of years ago you could change someone's records faking the FROM field, these days all you need is a phone, courage and an unaware employee with authority.

It's so nice that Agent Leth and Clown Jeet 3k Inc. simply wanted to point out the social engineering vulnerability at Network Solutions, ones we've seen before too. The question to me right now is what would Network Solutions do about this second case of soc. egineering problems at the company?

[**INDIAN CALL CENTER WORKERS CHARGED WITH CITIBANK FRAUD**]

Former employees of a call center in Pune, India, **were arrested this week on charges of defrauding four account holders in New York of Citibank**, a subsidiary of Citigroup, to the tune of $300,000, according to a police official in Pune.

The three former employees of Mphasis BPO, the business process outsourcing (BPO) operation of Bangalore software and services company Mphasis BFL Group, **are charged with collecting and misusing account information from customers they dealt with as part of their work at the call center**, according to Sanjay Jadhav, chief of the cybercrime cell of the Pune police.

More information can be found at :

http://www.infoworld.com/article/05/04/07/HNcitibankfraud_1.html

Astalavista's comments :

Operational outsourcing and cutting down costs have been the latest trend in Corporate America, and this case may have an unprecedented decline in the future use of these.

Employees sometimes get tired of acting as an intermediary of financial transactions, they think their organization doesn't pay serious attention to security in order to track them and consequently they feel more secure while commiting the crime.

If Mphasis want to keep its customers and maintain the loyalty to India's outsourcing industry, it has to ensure that the necessary insider related precautions are in place.

[**MOBILE TROJAN KILLS SMART PHONES**]

Virus writers have created a mobile Trojan capable of **rendering an infected Symbian Series 60 unusable**. Fontal-A is a SIS file Trojan that installs a corrupted font file on the device, causing it to fail when the mobile phone is next rebooted.

Fontal-A is a **Trojan**, incapable of spreading by itself or via Bluetooth. The small risk of infection applies **only to people in the habit of installing warez mobile games files or the like** onto their mobile phone.

More information can be found at :

http://www.channelregister.co.uk/2005/04/06/mobile_killer_trojan/

F-secure's description of the trojan can be found at :

http://www.f-secure.com/v-descs/fontal_a.shtml

Astalavista's comments :

Symbian malware authors are still in experimental mode, anti-virus vendors should consider all the stages they've seen on the virus scene to be reestablished on the malware one – destruction, droppers etc.

Later on, we might see coordinated voting scams using a phone's SMS and call abilities and suddenly your mobile phone next to your ADSL connection will turn into the currency of the Underground. Be aware of mobile malware, don't be naïve about download mobile warez, don't get too excited about mobile virus scanner on your phone yet, it's not as bad as they make it sound, but just give it some time.

[**WIDESPREAD INTERNET ATTACK CRIPPLES COMPUTERS WITH SPYWARE**]

Widespread Internet Attack Cripples Computers with Spyware
Experts say at least 20,000 PCs already have been affected. Is your company next? An insidious new **Internet attack** that hijacks a victim's Internet connection and stealthily installs a barrage of **adware and spyware** is targeting businesses and organizations across the United States.

More information is available at :

http://www.pcworld.com/news/article/0,aid,120448,00.asp

Astalavista's comments :

My personal opinion is that what misconfigured Sendmail servers used to be as a threat

a couple of years ago, the same thing goes for DNS spoofing and Cache poisoning attacks, old, easily conducted with great impact for the online scamming rings, spammers, phishers and recently malware authors.

Need freshly acquired victims for your spyware expenditures? Just redirect their Google request to your CoolWWWSearch web site.

Organizations and individuals should be aware that it doesn't take visiting an unknown and untrusted site to get infected, but the ones from your usual daily traffic could also do the job and renovate or implement fresh approaches to deal with the possibility of such a problem.

[**DATING SITE HACK SUSPECT ARRESTED**]

Police last week **arrested a 37-year-old man** from Sheffield on **suspicion of hacking into the website of London dating agency** loveandfriends.com. The unnamed suspect allegedly hacked into the site, took control of a small number of member's profiles (which were defaced), and **made demands for payment in exchange for holding off on threats to delete the firm's database.**

Working with loveandfriends.com, officers from the **Computer Crime Unit at Scotland Yard** traced the suspect to his home in Sheffield, where they executed a search warrant on Friday, 1 April. Met police officers seized the suspect's computers and **recovered evidence** that **he was responsible for writing the Mirsa-A and Mirsa-B mass mailing worms**, which posed as messages from campaign group *Fathers 4 Justice*.

More information can be found at :

http://www.channelregister.co.uk/2005/04/07/dating_site_hack_arrest/

Astalavista's comments :

As I once said to a friend – by the time you get spam or a phishing attack email – expect to get probed from the very same computer later on, it's just a matter of time. To me this is a 37-yea- old l33t wannabe, desperately looking for financial rewards.

[**UNPATCHED FLAW FOUND IN MICROSOFT SOFTWARE**]

Microsoft is investigating the report of a flaw that could open systems using its Access or Office software up to attack.

The vulnerability, which **was not one of eight patched by Microsoft on Tuesday**, is in the Jet database engine component, according to an advisory posted the same day by security company Secunia**. It could enable an intruder to remotely execute malicious code on a vulnerable PC**, Secunia said.

A Microsoft representative said on Tuesday that the company **has not heard of any attacks on customers' systems using the unpatched security hole**.

"We are aware of the exploit code that has been released," the Microsoft representative said, adding that the software maker would take appropriate action once it has completed its investigation of the problem.

"It is unfortunate that this researcher decided to post publicly," the Microsoft representative said.

HexView said in its own advisory that **it notified Microsoft of the flaw on March 30, but had received no response.**

A Microsoft representative said the company had no record of any contact from HexView before the flaw was publicized.

More information can be found at :

http://news.com.com/LimeWire+security+flaw+found,+fixed/2100-1002_3-5618949.html

Original posting at Bugtraq :

http://www.securityfocus.com/archive/1/394758

Astalavista's comments :

A scenario – right now, a 15-year-old script kiddie is waiting for the next phpBB vulnerability to appear, not at some underground chat room, or through personal contacts, but through a public mailing list posting!

Isn't it about time that a company with the size and revenue of Microsoft start getting liable for not releasing a patch in a timely-fashion? You can always miss your patch days as they can be defined as goodwill. In case you didn't come up with a patch for a vulnerability, you can simply state that you didn't get in touch with the author. who suffers - the entire Internet, who benefits - malware authors.

[**U.S MILITARY'S ELITE HACKING CREW**]

The **US military** has created a formidable, secret, multimillion-dollar hacking group for possible **cyber wars against enemy networks**. The group's existence was revealed during a March 2005 Senate Armed Services Committee hearing, where officials from US Strategic Command (Stratcom) disclosed the existence of the **Joint Functional Component Command for Network Warfare (JFCCNW**). JFCCNW's purpose is to defend **Department of Defense networks** and **execute classified Computer Network Attacks**. Little else is known about the group, but Dan Verton, former Marine Intelligence officer, says the group likely includes personnel from the Central Intelligence Agency (CIA), National Security Agency, Federal Bureau of Investigation (FBI), and the four military branches.

More information can be found at :

http://www.theregister.co.uk/2005/03/22/business_school_hack/

Cyber and Information Warfare resources can be found at :

http://www.astalavista.com/?section=dir&cmd=file&id=2753
http://www.astalavista.com/?section=dir&cmd=file&id=3915
http://www.astalavista.com/?section=dir&cmd=file&id=2725

http://www.astalavista.com/?section=dir&cmd=file&id=4018
http://www.astalavista.com/?section=dir&cmd=file&id=4016

Astalavista's comments :

Hint - you don't need a multimillion team to launch a "classified computer attack".
Hint 2 - the article forgot to mention the surveillance capabiities of such teams and the Internet wiretapping engagements of the group on foreign countries, industrial espionage etc.

You think the latest 0-day exploits are at Bugtraq, think twice!

Otherwise that's a public propaganda that "we"(NSA,CIA,FBI in that very particular order) know what cyberwarfare stands for publicly state it perhaps for the first time.

More resources on the topic can be found at :

http://www.astalavista.com/?section=dir&act=search&term=warfare

[**UK COURT ORDERS ISPS TO REVEAL IDS OF 33 FILESHARERS**]

A British judge today ordered five ISPs **to name another 33 music file sharers**.
The individuals concerned **had uploaded more than 72,000 music files to the internet**, according to a statement by the BPI (British Phonographic Industry), which sought the court order as part of its broader legal offensive **against illegal downloading on P2P networks**.
The ISPs concerned have two weeks to give the UK record companies' trade association the names and addresses of the file sharers. The case brings the number of people in the UK to face legal action for illegal file sharing up to 90. These people will face claims for compensation and the legal costs in pursuing them, the BPI warns.

More information can be found at :

http://www.theregister.co.uk/2005/04/19/bpi_p2p_lawsuits/

Astalavista's comments :

Things you're never told while purchasing "our fine 2Mbps ADSL service" – we're always out there to report you under current laws. Although a bit unclear, the users have uploaded, not downloaded, even though both can be easily figured out. Educate yourself on P2P anonymous usage, but before that, try to find what's your country's policy towards P2P networks file sharing.

Further resources on the topic can be found at :

http://www.astalavista.com/?section=dir&cmd=file&id=3820
http://www.astalavista.com/?section=dir&cmd=file&id=3871
http://www.astalavista.com/?section=dir&cmd=file&id=3785
http://www.astalavista.com/?section=dir&cmd=file&id=3970

[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 white papers are defined as a **"must read"** 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**

" **TIVO HACKING FAQ** "

This site contains information and utilities to use to **hack your TiVo**

http://www.astalavista.com/?section=dir&act=dnd&id=3899

" **GOOGLE HACKING FOR PENETRATION TESTERS** "

Excerpt from Chapter 8: Tracking Down Web Servers, Login Portals, and Network Hardware

http://www.astalavista.com/index.php?section=dir&act=dnd&id=3904

" **MULTIMEDIA DATA HIDING** "

This thesis discusses the issues regarding **multimedia data hiding** and its application to multimedia security and communication, addressing both theoretical and practical aspects, and tackling both design and attack problems. Recommended reading! (comprehensive 282 pages thesis)

http://www.astalavista.com/?section=dir&act=dnd&id=3913

" **FORENSICS AND THE GSM MOBILE TELEPHONE SYSTEM** "

The **GSM system** has become the most popular system for mobile communications in the world. This paper briefly explains the basics of the GSM system. **Evidence items** that can be obtained from the **Mobile Equipment**, **the SIM** and **the core network** are explored

http://www.astalavista.com/?section=dir&act=dnd&id=3928

" **WIN-RES-Q** "

Displays "**hidden**" windows, recommended tool!

http://www.astalavista.com/?section=dir&act=dnd&id=3963

" **BLUETOOTH TOOLS** "

This document gives a very short overview of the different tools related to **Bluetooth security**

http://www.astalavista.com/?section=dir&act=dnd&id=3952

" **THE ART OF ASSEMBLY LANGUAGE PROGRAMMING** "

The Art of Assembly Language Programming is the World's #1 book on x86 **assembly language programming**

http://www.astalavista.com/?section=dir&act=dnd&id=3946

" **PASCO V1.0** "

Many **computer crime investigations** require the reconstruction of a subject's internet activity. Since this analysis technique is executed regularly, we researched the structure of the data found in Internet Explorer activity files (index.dat files). Pasco, the latin word meaning "browse", was developed to examine the contents of Internet Explorer's cache files

http://astalavista.com/index.php?section=dir&act=dnd&id=4047

" **CAIN & ABEL V2.68 RELEASE** "

Cain & Abel is a **password recovery tool** for the Microsoft Operating Systems

http://www.astalavista.com/index.php?section=dir&act=dnd&id=4014

" **HARDENING YOUR MACINTOSH** "

Os X security, auditing, hardening, pen-testing, privacy & more

http://www.astalavista.com/?section=dir&act=dnd&id=4010

[04] **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

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.

[05] **Site of the month**

---

http://project.cyberpunk.ru/

The **Cyberpunk Project** is an online, non-profit organization, whose purpose is to promote, support, research, study, and create **cyberpunk** subculture.

[06] **Tool of the month**

Orbitron 3.51

Orbitron is a **satellite tracking system** for **radio amateur** and observing purposes. It's also used by **weather professionals**, **satellite communication users**, **astronomers**, **UFO hobbyist** and even **astrologers**.

http://www.astalavista.com/?section=dir&act=dnd&id=3969

[07] **Paper of the month**

Cyberpunk - Ebook

This, in somewhat cleaned-up format, is the original manuscript of the novel(226 pages) the autor wrote between 1984 and 1989..

http://www.astalavista.com/?section=dir&act=dnd&id=4068

[08] **Geeky photo of the month – 'Dark Matrix'**

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.

'Dark Matrix' can be found at :

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

[09] **Free Security Consultation**

Have you ever had a Security related question but you weren't sure where to direct it to? This is what the "Free Security Consultation" section

was created for. Due to the high number of Security-related e-mails we keep getting on a daily basis, we have decided to initiate a service, free of charge. Whenever you have a Security related question, you are advised to direct it to us, and within 48 hours you will receive a qualified response from one of our security experts. The questions we consider most interesting and useful will be published at the section. Neither your e-mail, nor your name will be disclosed.

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

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

Question : Hi,folks, at Astalavista, I've been with your site for many years and I've recently come across your fine newsletter. I'm an EU citizen that's getting more and more privacy conscious with time. I keep myself up-to-date with various security news and during the last couple of months I've learned more about identity theft, phishing and online privacy than I've ever imagined. I'm aware of A9.com's existence, but I've never imagined Google will have the courage to introduce their Search History feature. What's with that, I mean is this some kind of world domination conspiracy or I've been reading too much literature recently?

Answer : What bothers me is the impact Google has on our lives - we've become so Google-obsessed and Google-dependent that I would love to see what's your second choice of search engine if Google goes down for a day, where's your alternative? Millions of people from all over the world breathe, eat and actually live at Google, and it's all based on trust, trust that searching is private, that their data wouldn't be misused and that there's no way of physically locating the one who searched for sensitive NORAD data, but it isn't so simple. The more you know about databases, networking, government wiretapping policies and "corporate america" where LexisNexis and ChoicePoint, as well as the majority of respected universities suffer database breaches, the more aware and conscious you become. A huge percentage of the aforementioned millions of Google account holders would take advantage of this feature, and even though it would indeed provide more accurate results given everyone's past history, this is privacy related where the trade-off is between convinience and privacy awareness.

As to alternatives to Google, check out **Clusty.com**

Consider the following as more useful reading on the topic :

http://www.astalavista.com/?section=dir&act=search&term=privacy
http://www.astalavista.com/?section=dir&cmd=file&id=4007
http://www.astalavista.com/?section=dir&cmd=file&id=2706
http://www.astalavista.com/?section=dir&cmd=file&id=1997

Question : Hi guys, I'm doing a research on mobile malware, and although I've spoken with quite a lot of knowledgeable folks so far, I keep having thoughts about the recent mobile viruse outbreak and the bluetooth insecurities hype

everyone's talking about. I also wanted to ask you do you think anti-virus vendors might *sometimes* release malware to increase their sales? My point is that although I'm sure in the next few years I'll be attacked by viruses on my mobile, I think I'm pretty safe right now.

Answer : Picture yourself two scenarious, one with a company that's trying to catch up with the latest threats and is still having hard times doing it. The number, diversity and sophistication of the malware released is getting worse forthem. Two, a company that believes spreading mobile malware from time to time is a necessary evil and that it would eventually improve our mobile security over time. A company that's so obssessed with the idea to act as a socially oriented one might release some, probably once only.

Now, let's come back to reality. I really doubt any anti-virus vendor is doing so, they might have done it, but as many other things, we would never know. Right now everyone's trying to catch up with the latest flood of malware and the growing numbers or writers and wanna be writers.

Question : I was wondering whether you could provide me with some inforsec job tips. I have a lot of experience as a system administrator and have a lot of general IT knowledge. I have been seriously thinking on getting into the infosec industry and any recommendations are more than welcome.

Answer : The best thing to keep in mind is that it's a growing industry and it would continue to grow. I would advise you to do the following, go through the links you'll find below and do some research about what is required for each position, most of all try to match your capabilities with the ones mentioned. You would definitely need to consider certifying yourself, but bear in mind that it might take a while before someone considers your application, hands-on experience and various research would be very beneficial.

http://www.gocertify.com/ - Follow the Cerificates -> Security link
http://securityfocus.com/jobs
http://ukjobs.ostg.com/ - Europe mainly

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

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

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

More information about the DVD is available at:

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

[11] **Enterprise Security Issues**

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

- **DNS Security and the introduction of DNSSEC Part 1** -

This short article will give you a brief overview of DNS, DNS security, various attacks and defensive measures. In part 1 we'll go though DNS's basics and security issues, in part 2, we'll discuss DNSSEC, its implications and world wide adoption as the next generation DNS infrastructure.

DNS plays a vital role in the proper functionality of the Internet, and it can be defined as one of its core assets taking care of the mechanism that resolve host names into IP addresses. Originally written many years ago, the DNS protocol as well as the TCP/IP one weren't developed with security in mind, as the idea of a scientist causing denial of service attacks to the system wasn't that realistic at the time.

During 2004 and in the beginning of 2005 there have been numerous (at least reported) abuses related to the misuse of DNS and the actual exploitaition of spoofing or hijacking vulnerabilities. We're also witnessing an increased use of DNS attacks by phishers and online scammers. Panix.com got their domain redirected, thus losing customers' emails and blocking traffic, as well as Hushmail.com, who suffered from Network Solution's lack of security responsibility. What's worse, a large scale DNS poisoning attack was responsible for infecting organizations and average users with spyware. Although there're alternatives, the majority of Internet servers rely on BIND (Berkeley Internet Domain Name), which makes it highly likely for a single vulnerability to cause a lot of damage.

When it comes to security, a DNS breach or a DNS related attack could bypass the majority of security measures your organization has in place, namely because servers or end users trust that when they access Google.com they're indeed at Google.com by default, or that intranet.yourcompany.com is your company's intranet.

Some DNS attacks to consider, beside perhaps the worst man-in-the-middle and the fact that DNS is an UDP based service, are :

Cache poisoning – When a DNS server checks its cache to see if it's in possession of the client's request,;if it doesn't, it passes the request to another DNS server, and in case it has incorrect information (error, hacked) a cache poisoning occures

Breached servers – already breached servers represent a threat to the entire Internet given that they might already be sending untrustworthy information while being part of the chain

and have certain authorities.

Rerouting of communications – email, IM, you name it, the idea is that the attacker is posing as a trusted entity with the idea to intercept certain traffic.

Pharming attacks – although we've already mentioned the possibility, we didn't mention the scenarious that could occur. Imagine a situation where major ISP's DNS records are poisoned with the idea to redirrect their customers to a malicious web site exploiting a 0-day IE vulnerability and dropping malware. We've already seen it happen, the thing is - can we prevent it in the future? These use DNS hijacking or poisoning to redirect users to a fraudulent site, these are often not so easily detected by the average Internet user and beside some obvious web design misplacements, we assume that they're at the right site by default

Social engineering attacks – are to be considered as wel - fake login pages and fake home pages of major high traffic sites where the visitors think they're at the real site, thus immediately trusting its content, propositions etc.

What's the future? – it's called DNSSEC at least for now. In part 2 we'll review DNSSEC And we'll also discuss methods of securing BIND, at least at an acceptable level.

Further resources on the topic can be found at :

http://www.rfc-archive.org/getrfc.php?rfc=3833
http://www.oreilly.com/catalog/dns4/chapter/ch11.html
http://www.linuxsecurity.com/resource_files/server_security/securing_an_internet_name_server.pdf
http://www.astalavista.com/?section=dir&cmd=file&id=3622
http://www.astalavista.com/?section=dir&cmd=file&id=3233

[12] Home Users' Security Issues

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

- Phishing attacks - put yourself in "learning mode" -

This article will provide with a short summary of what phishing is, how big the problem is, and it will give you info on how to protect yourself from phishing – by putting yourself in "learning-mode", namely taking proactive steps to tackle the problem.

What is phishing?

Phishing attacks use the Internet as a means of medium to steal sensitive information, even Financial records from unsuspicious and naïve Internet users, through fake banking sites, and spoofed emails. Phishing of course have broad definitions :

http://www.google.com/search?hl=en&lr=&oi=defmore&q=define:Phishing
http://www.webopedia.com/TERM/p/phishing.html

How big is the problem?

Some define it as the E-crime of the 21st century; and indeed, beside spyware, phishing is everyone's greed to take a piece of the pie using the old spamming method, when millions of fake emails are sent with the idea to steal financial or any other type of sensitive information - a method with a very high return with no initial investment costs in running that kind of fraud.

Phishing is primarily based on social engineering attacks. Namely it impersonates another person or organization in an electronic way, or offers something desirable with the idea to initiate and retain the contact party. Everyone's targeted and although there's almost no sign of segmentation, recently we've seen localization starting to take place, namely, multilanguage phishing attacks targeting local banks, beside the most usual phishing emails impersonalizing Citibank or PayPal. Taking a look at NetCraft's recent "Phishiest Countries" report (http://toolbar.netcraft.com/stats/countries) gives the impression that the majority of phishing hosting sites are Asian based but how come? There's been a boom in Internet subscribers in every part of Asia, and the way a novice Internet user usually replies to "personal" spam messages, you can image the level or awareness of security of these subscribers have. Consequently, the majority of phishing sites are hosted at exactly these very insecure, but many, new Internet users.

What factors will assist phishing in the future?

We've already heard of automated phishing toolkits. All you need is a "marketer" and a lot of zombie computers to do the "trick". The authors of these are simply trying to make as much $ as possible in the most convinient way, which is bad if they manage to identify and target unaware or naïve users.

The majority of financial institutions or active participants in most of the phishing attacks are a bit irresponsible and they don't realize the social responsibility they must undertake to fight the problem - to increase their customers' loyalty and even prevent Internet bade fraud by educating them. Another issue to note is the organization's lack of understanding of web applications security. In certain situations it doesn't require you to have an outdated software to get fooled - the attack is within the real site of the organization.

Another important factor that assists in the success of phishing and spamming attacks are the new users joining the Internet, still unaware, naïve, "surfing oriented". These are among the best targest for scammers. Let's start from the basics - should ISP's provide security packages for their customers' education, or should the user go through the cycle of having a HDD erased, then undergoing a worm infection, ending up participating in a DdoS attack?

Tips for protection against phishing attacks :

1. Put yourself in "learning-mode" – you definitely receive a lot of phishing emails. Try to look for some patterns! Don't be naïve to follow an occasional message like "We've been breached", "We've recently experienced problems". Try visiting the site itself and check if there's anything you should be worried about. An example of a phishing email can be found at http://purl.org/net/tbc/misc/phish001.htm

2. Don't follow any URLs in an email message, especially when it comes to login sits or any other type of services that reveales personal or sensitive information, try visiting the site on your own.

3. Although trivial when it comes to security – keep your email client and browser regularly patched.

IE is naturally a great threat when it comes to phishing attacks, it makes the link look as if it was the original site you're about to visit.

4. Use any kind of Anti-Spam filter or software – a great deal of phishing attacks might get detected due to the fact that they operate in pretty much the same fashion as spam does.

5. Check a web site's certificates to make sure you're at the right place – an article to look at can be found at :

http://www.infosecwriters.com/text_resources/pdf/encryption-Phishing.pdf

Further resources on the topic can also be found at :

http://www.antiphishing.org/
http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf
http://ebankingsecurity.com/ebanking_bad_for_your_bank_balance.pdf

[13] Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful things through this section. In this issue we have interviewed Nicolay Nedyalkov, one of the people behind **ISECA**, and an active participant in the Bulgarian IT/Security scene.

Your comments are welcome at security@astalavista.net

Interview with Nicolay Nedyalkov, http://www.iseca.org/

Astalavista : Hi Nicolay, would you, please, introduce yourself to our readers and share some info about your experience in the information security industry? Also what is ISECA all about?

Nicolay : My interest in information security dates back from 1996. At that time, respected Bulgarian experts from all over the country used to meet periodically at closed seminars where we exchanged our ideas and experience. At a later stage we developed the phreedom.org E-zine. I have also participated in numerous national and international mathematics and IT contests.

Currently I am a managing director for the R&D department of one of Bulgaria's most Prominent IT companies – Information Service. In 2002 I decided to initiate an InfoSec course at the **University of Sofia**. Once the course "Network Security" became part of the university's curriculum, we immediately got the interest of over 500 students. During 2003, with the help of several experienced security colleagues of mine we developed another fresh and very useful course in "Secure programming". Both of the courses fitted perfectly into the program curriculum and actually they attracted more students than we had expected. I am also teaching four other courses in Software technologies.

As a whole, we contributed for the development of IT education in Bulgaria establishing the **ISECA** (**Information Security Association**), whose main purpose is to connect our members and inspire them to innovate, create, and enrich their personal knowledge, while being part of a unique community.

Astalavista : Correct me if I'm wrong but I believe not many Eastern European universities emphasize on the practicality of their computer and network security courses? What are your future plans for enriching the course selection further, and also integrating a more practical approach into your curriculum ?

Nicolay : During the last couple of years we have seen a definite slowdown in Europe regarding information security courses and programmes.

Until now we have already developed over eight courses, including the course **Information Systems Security Audits**, which is widely applicable. Furter, there is intensive work on the development of a new **Network & Software Security Lab**. We are also negotiating with ABA representatives for the introduction of a professional certification program – "**Risk Management in the Financial and Banking Sector**"

In fall 2005, University of Sofia will start a specialized master Information Security Program, coordinated by ISECA.

Astalavista : Who are the people behind ISECA, and what are the current local/global projects you're working on, or intend to develop in the upcoming future?

Nicolay : Our core members include certified security consultants and auditors, researchers, IS managers and class teaching professors.

Among the key projects we've already developed or we are working on at the moment are:

- **A National Laboratory for Network and Software Audits**, being developed in close cooperation with The University of Sofia. The lab will be used for audits and R&D in the industry.

- **An Information Security Portal** – ISECA

- **A National anti-spam system** and its integration within international ones like SpamHouse

- Safeguarding the local business interests of information security and promoting its development on a government level

- Active participation in the development of the Bulgarian **Law for E-trade and E-signature**

- Subscription based "Vulnerability Notification" service

- Centralized log analysis and security monitoring

Astalavista : What is the current situation of the Bulgarian IT and Security market? What was it like 5 years ago, and is there an active security scene in the country?

Nicolay : We are currently witnessing a boom in the Bulgarian demand for information security services as a great number of businesses are realizing the importance of information security. On the other hand we are in a process of building strategical relationships with Bulgarian and multinational companies providing security related products and services. In the last couple of years official government bodies also have emphasized on sustaining secure communications. In response, our main goal in the upcoming future would be to build a collaborative working atmosphere with stable relationships between key partners and experts

Astalavista : Bulgaria and Eastern Europe have always been famous as a place where the first computer viruses actually originated, to name the Dark Avenger as the most famous author. What do you think caused this - plain curiosity, outstanding programming skills, or you might have something else in mind?

Nicolay: It is a fact that Bulgaria is popular with its potential in the creation of viruses, trojans and malware at all. The thing is that there are a great number of highly skilled experts, who cannot apply their talent in the still growing local market; consequently they sometimes switch to the dark side. One of our main aims is namely to attract people with great potential and provide them with a professional and stable basis, on which they could develop themselves on the right track**.**

The Bulgarian – Dark Avenger, well, he used to be an idol for the virus writers and the name still brings respect.

Astalavista : Is there an open-source scene in Bulgaria, how mature is it, and do you believe the country would be among the many other actively adopting open-source solutions in the future, for various government or nation's purposes?

Nicolay: Yes, there is a Free Software Society (**www.fsa-bg.org**). Several municipalities have already turned into E-municipalities with the help of open source software. There was a proposition for the introduction of a law for integrating open source software within the government's administration, which was unfortunately rejected later on. Free Software Society is in close contact with various political movements, which reflects the overall support and understanding of open source from the society.

The use of open source is also within the objectives of one of the main political parties in the country, a goal that resulted from the many initiatives undertaken by the Free Software Society. ISECA's members are also active participants in the core direction of the FSS. We are currently developing a new open-source research team, part of Information Service – OSRT (**Open-Source Research Team**).

Astalavista : How skilled is the Bulgarian IT labor market and do you think there's a shortage of well - trained specialists in both IT and Information Security? How can this be tackled?

Nicolay : There are a great number of highly qualified software developers in Bulgaria, who created the Bulgarian Association for Software Developers (**http://devbg.org/en/**). We have had numerous seminars and lectures between ISECA and the Association. One of our main objectives is namely to locate and unite the highly qualified IT and Security experts within Bulgaria. Both organizations are constantly seeking to establish stable relations with international organizations with the idea to exchange experience and promote mutually beneficial partnerships.

Astalavista : India is among the well-known outsourcing countries for various IT skills, while on the other hand the Bulgarian programmers are well- respected all over the world, winning international math and programming contests. Do you think an intangible asset like this should be taken more seriously by the Bulgarian Government, and what do you think would be the future trends?

Nicolay : Every year there is a leakage of highly qualitfied young professionals with great potential for growth, looking for further career development . The core reason for this "brainwave", so painful for the Bulgharian econmy and society, is the lack of a relevant government policy, ensuring stable and beneficial career opportunities for the young generation. I honestly hope that further government policies, not only those related to the IT industry, would be successful in providing what a nation needs – a bright future for its brightest minds.

Astalavista : In conclusion, I wanted to ask you what is your opinion of the Astalavista.com's web site and, in particular, our security newsletter?

Nicolay : I have been visiting **Astalavista.com** since its early days and it is great to see that recently the portal has successfully established among the few serious and comprehensive sites. Furthermore, you can always find whatever you are looking for - software, as well as recommendations and shared experience in information security. I believe Bulgaria needs the same high quality portal, one of our main ideas behind **ISECA**.

Astalavista : Thanks for your time!

[14] IT/Security Sites Review

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

-
Reteam.org
-
http://www.reteam.org/

A site dedicated towards reverse engineering

-
Viruslist.com
-
http://www.viruslist.com/

Regularly updated malware related web site

-
Infosyssec.com
-
http://www.infosyssec.com/

Extremely comprehensive security portal

-
Dougknox.com
-
http://www.dougknox.com/

Doug's Windows tweaks and tips site
-
Vx.netlux.org
-
http://vx.netlux.org/

Features virii related papers, links, magazines, and downloads

[15] **Final Words**

Dear readers,

Thank you for going through Issue 16, enjoy yourselves and stay secure.

Watch out for more quality stuff at Astalavista.com, meanwhile, keep your feedback coming!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net