Astalavista Group Security Newsletter
Issue 15 - 30 March 2005
http://www.astalavista.com/
security@astalavista.net

[01] **Introduction**

Dear readers,

Welcome to the 15th issue of Astalavista Security Newsletter!

It has been a year and a half since we started this newsletter with the idea to raise your security awareness and provide you with an entertaining way of learning about the latest security events and trends. Now we have the confidence to claim that our efforts have been more than successful.

Stay tuned, folks, many new events are waiting for you!

In Issue 15 you will read **an interview with Bruce, an organizer of the DallasCon event,** you will go through two articles, namely, **'P2P networks – unaware employees, security threats and your organization in between'** and **'Help, my boss is spying on me! '** and, hopefully, add a couple of more useful sites to your bookmarks.

Something else to note is that the **Top 20 Featured Papers** and the **Top 20 Featured Tools** sections at Astalavista.com have been updated; during April we will pay serious attention to updating this on a weekly basis.

As always, we appreciate your feedback, so, please, feel free to contact us and express your thoughs about the Astalavista.com site and our security newsletter! Your opinion will always be respected – positive or negative.

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

----

[**ANTIVIRUS COMPANIES REPORT FIRST MOBILE MESSAGING WORM**]

The first mobile phone virus that spreads using the popular **Mobile Messaging Service (MMS)** is circulating among mobile phone users with Symbian Series 60 mobile phones, antivirus companies have warned.

Antivirus vendors first spotted the new virus, dubbed **CommWarrior.A**, yesterday. When opened, it places copies of itself on vulnerable mobile phones and uses the phone's address book to send copies of itself to the owner's contacts using MMS. Antivirus experts believe **CommWarrior**, which has been spreading slowly among cell phone users since January, is not a serious threat. However, the virus could herald a new age of malicious and fast-spreading cell phone threats, according to **Mikko Hypponen**, director of antivirus research at **F-Secure Corp**.

More information can be found at :

http://www.computerworld.com/securitytopics/security/story/0,10801,100256,00.html

An analysis of the worm can be found at F-Secure's site :

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

Astalavista's comments :

Yet another breakthough on the developing mobile malware scene. During the month a group of researchers constructed a Building a BlueSniper Rifle and published instructions on how to build it. It has the capacity to operate from distances reaching one mile and it's a sniper :--) What's to note is the absolut silence from the vendors' side. T-Mobile got brutally hacked but reading several reports and articles from various news agencies, it seems that the end users are intrested in becoming customers of providers who are getting hacked so badly. What for? If they're all inspired of becoming famous for having their phones hacked, let me tell you – you're already a "celebrity" in the underground with all the spyware and bots that you have running on your PCs right now!

[**DUO CHARGED OVER DDOS FOR HIRE SCAM**]

The FBI last week arrested a **17 year-old** and a Michigan man over suspected involvement in a denial of service for hire racket. The duo allegedly orchestrated an October 2004 attack against a New Jersey company that sells sporting goods over the internet. Jersey-joe.com suffered the loss of "hundreds of thousands of dollars" of business as the result of the disruption caused by the attack, according to a statement by investigators.

More information can be found at :

http://www.theregister.co.uk/2005/03/22/ddos_for_hire_plot_arrests/
http://nj.gov/lps/newsreleases05/pr20050318c.html

Astalavista's comments :

Wait! Don't get impressed by the wannabe hacker's age, he's just a kid looking how to make a quick buck, but get impressed by the fact that the bucks come from his 18 year old fellow who hired him. "Keep your friends close, your enemies closer". My point is that such a low- profile (I honestly doubt it's making millions per month) E-store should keep an eye on its primary competitors. And if I were to know that among them is an eighteen-year- old person, who's naturally excited about his profits, I would expect or at least think about the worse to come.

[**CYBER COPS FOIL $423m SUMITO BANK RAID**]

A hi-tech bid to **steal $423m** from the London offices of the Japanese bank Sumitomo Mitsui has been foiled by police. A gang of **cyber crooks** compromised Sumitomo's computer systems in October 2004 prior to an unsuccessful attempt to transfer money to a series of 10 accounts overseas, the FT reports..

More information can be found at :

http://www.theregister.co.uk/2005/03/17/sumitomo_cyber-heist_foiled/

Astalavista's comments :

Greed, greed and again greed! That makes it 423/10 = $42.3m per account. I mean even The Plague in "Hackers" was smart enough to "bite" a great deal of accounts and cash out with less, but safe money! I especially enjoyed how the bank took advantage to promote itself as taking good care of its security, where it was the bank's security that was breached in the first place, and since the majority of huge transfers are well monitored, I believe it was a standard practice to look in depth at these transfers.

Smells like an insider or physical security breach, since I doubt they've managed to keylog banking details of such a wealthy account or take advantage of a mass phishing scam targeting especially the Sumitomo Mitsui bank.

[**911 TROJAN AUTHOR JAILED FOR SIX MONTHS**]

A Louisiana man has been jailed for six months after he was convicted of **infecting** WebTV users with a **Trojan horse that made 911 nuisance calls**. David Jeansonne, 44, of Metairie, Louisiana, **pleaded guilty** last month to causing a threat to public safety and causing damage to computers.

More information can be found at :

http://www.theregister.co.uk/2005/03/15/webtv_vxer/

http://www.sophos.com/virusinfo/articles/webtv911.html

Astalavista's comments :

I stll remember the age-old dialers that never got the popularity that RATs started getting years ago. This is a very serious case, and I'm sure that those spotting the "big picture" would know whose eyebrows raised twice when the idea of blocking 911 or flooding it with false messages suddenly became real. Coordination matters, 911 blocked, Google.com hijacked to Al Jazeera's site; wouldn't it undermine an entire nation's ability to protect its citizens?!

[**'DVD JON REOPENS ITUNES BACKDOOR'**]

A group of **underground programmers** has posted code online it says will reopen a **backdoor in Apple Computer's iTunes store**, allowing Linux computer users to purchase music free of copy protection.

More information can be found at :

http://news.com.com/DVD+Jon+reopens+iTunes+backdoor/2100-1027_3-5630703.html
http://news.com.com/iTunes+hack+disabled+by+Apple/2100-1027_3-5628616.html?tag=nl
http://www.theregister.co.uk/2005/03/22/apple_blocks_pymusique/

Astalavista's comments :

'DVD Jon' stikes again, and he has my respect for being the activist he is! If it was anyone else but Apple and Steve Jobs, they would definitely consider this an illegal action against the company, instead they preffered to handle it as silently as possible – a very good strategy given Apple's overal image.

Meanwhile,PyMusique's site has been down for the last couple of days..

Personal opinion – if you have already purchased a song, you're free to do whatever you feel like doing with it, and although it doesn't necessarily mean to share it with the rest of the world, you need to have the ability to chose either to do what's defined as an illegal action or do nothing special with it.

How about developing an "over the counter" C2C market - "I got tired of my Britney Spears, let me taste the real sound and exchange it for some Deftones with you!" - "You gotta be kiddin' me, right?" :--)

[**HUNGARIAN MAN CHARGED WITH HACKING SONY ERICSSON SITE**]

Swedish authorities formally charged a 26-year-old Hungarian man with **industrial espionage** on Tuesday, charging him with **hacking into the Sony Ericsson AB and Ericsson AB intranets**.

Csaba Richter told officials he hacked into the intranets hoping that Sony Ericsson or Ericsson would hire him when they saw his skills, Chief District Prosecutor Tomas Lindstrand said.

More information is available at :

http://www.infoworld.com/article/05/03/08/HNsonyhack_1.html

Astalavista's comments :

Intranets - a company's core asset for distribution and exchanging internal information, consequently its worst nightmare when an unauthorized access occures. In this particular case it was a guy interested in getting a job, there was a well coordinated unethical competitive intelligence. He has been around for 2 years, he's seen a lot, and accessing information of the Swedish national defense in between (your contractors are your weakest link!). On the other hand, 3 years ago an insider did something even worse (how reliable are your contractors, really?!)

Note: each and every respected company has a Career and Job Opportunities section at its site, and even though there might not be security positions currently available, it's worth submiting your CV so that they might eventually get back to you in the future.

[**GROUP PROTESTS CHINA'S WEBSITE CRACKDOWN**]

Shuimu.com is just one of China's thousands of Internet chat rooms.
But when **non-students were barred this month from using the site** at **Tsinghua University in Beijing**, it triggered a rare burst of outrage.

A brief protest erupted at the school. Users posted appeals on other sites for Web surfers to speak up, with some comparing the crackdown to persecution in Nazi Germany.

More information can be found at :

http://abcnews.go.com/Technology/wireStory?id=618018

Astalavista's comments :

A piece of news worth mentioning given the rare case of such a protest in China! I especially liked ABCNews featuring and requesting info from the Ministry of education aka The Thought Police (Orwell, George, 1984) of China. There's a difference between monitoring, content blocking and shutting down sites dating back 10 years ago. A methodology like this works in exactly the opposite direction, by creating undeground communities and negative attitudes among the majority of citizens. From personal experience I know that whenever a Chinese leaves the country for whatever reason, and gets access to a decent Internet connection, it's like seeing ICQ sending IM messages for the first time, and the Internet suddenly becomes the one we all know it as - the free speech one!

[**LIMEWARE SECURITY FLAW FOUND, FIXED**]

Researchers at Cornell University said on Tuesday that they discovered a Potentially **dangerous security flaw in the popular LimeWire file-sharing software**, but that the company has quickly released a fix.

More information can be found at :

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

Astalavista's comments :

Quite a bad scenario for a file-sharing software users, which happen to be millions of us out there. Flaws like these make me think about the ethical side of the issue- would the RIAA peek to verify my 4GB mp3s archive? Even worse, have you noticed how many people are usually connected to your P2P? I bet over 1m or even less - my point is that if you could simulteneously spread any kind of malware bypassing the majority of security measures of your PC (assuming your P2P is defined as trusted application), that would be a disaster and a very serious attack point. Remember the SETI@Home flaw years ago?

[**BUSINESS SCHOOL 'HACK' RAISES ETHICAL QUESTIONS**]

Where do morality and ethics end, and criminality begin? What is the appropriate "punishment" for the crime of curiosity coupled with the act of snooping? These questions have been raised once again in the case of a number of applicants to the **US' most prestigious business schools** who went beyond the normal processes to **sneak a peek at the status of their applications**.

More information can be found at :

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

Astalavista's comments :

Doesn't matter if it's DeepIntoTheWoods University or Harvard, whenever a student Applies he/she is more than impatient to see the results in order, to put it simple – make up his/her mind for the upcoming events as soon as possible. Image yourself as a student in a situation where you've applied at Harvard and Stanford, got a positive reply from Stanford, but Stanford is your second choice(yeah, you must have very high prefferences, but also the genious). Coming across a link like this will make a lot of people think about peeping what's the status of their application, wouldn't it?

Everyone's talking about the universities' reactions and if the students are responsible or not, while ApplyYourself is keeping it safe.

I myself have been aware of ApplyYourself for a long time, and I was impressed indeed that a great deal of prestigious universities use it as a standard. It is entirely centralized and all competing universities pretty much rely on its system. Are these cost savings or a lack of will to build an in-house verification system? It doesn't matter, what matters is ApplyYourself's actions on being responsible for scripting errors and later reporting those who have actually checked their status. What if the person that posted the bug had downloaded each and every university's databases and distributed them in way?

*While Harvard are taking this way too personal, **Standord University** are a bit more tolerant on the issue. That is why I have always had them on the top of my personal favourite and most respected universities! Of course, I respect the opinion of my Astalavista colleagues, too, having strong preferences for the Stern!*

[**IS YOUR MAC REALLY MORE SECURE?**]

Apple Macintosh users are quick to point out the dearth of **malware, viruses,**

And security problems in the OS X world. Compared to the Windows/Intel Win32 platform, Mac OS X looks like an attractive alternative, at least when malware is the deciding factor. Win32 machines have suffered from any number of spectacularly successful malcode attacks over the years, and the problem shows no signs of abating.

More information can be found at :

http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=159900444&classroom=

Astalavista's comments :

It used to be at least less targeted, and although it doesn't count for even 5% of the desktop market, it gives attackers or even phishers a great advantage – Mac users have a very good sense of security, false or true they're very sure they cannot get hacked or have their browsers hijacked - a trend we've seen changing during the last couple of months.

On other hand, I've never seen so many security patches coming out from Apple, and recently a company that offered $25k for the creation of a Mac virus, called off the contest. Even though it claimed it did it for legal reasons, I think they still wanted to do something useful with the $25k instead of loosing them in the next couple of months.

[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**

" BLOOoVER - J2ME PHONE AUDITING TOOL "

Blooover is a tool that is intended to serve as an audit tool people can use to check whether their phones and phones of friends and employees are vulnerable to various attacks

http://www.astalavista.com/?section=dir&act=dnd&id=3738

" HACKERS - AN INTERACTIVE REPORT "

An interactive report on the exploits of hackers and how they have highlighted the Internet's insecurities

http://www.astalavista.com/?section=dir&act=dnd&id=3744

" GSM, BLUETOOTH, WIFI & CDMA MOBILE PHONE SECURITY "

Comprehensive page on the topic

http://www.astalavista.com/index.php?section=dir&act=dnd&id=3755

" **XNMAP 2.2.1** "

XNmap is a free Cocoa user interface to the nmap command line
program, written for Max OS X 10.3

http://www.astalavista.com/?section=dir&act=dnd&id=3775

" **SSDT - SPOOFED SECURE DATA TRANSFER** "

Spoofed Secure Data Transfer exploits ICMP and UDP protocols to
send RSA encrypted files from a spoofed source ip

http://www.astalavista.com/?section=dir&act=dnd&id=3815

" **BUILDING A BLUESNIPER RIFLE** "

The gun, which is called the BlueSniper rifle, can scan and attack
Bluetooth devices from more than a mile away.

http://www.astalavista.com/?section=dir&act=dnd&id=3793

" **GUIDELINES FOR WRITING SECURE SOFTWARE** "

This paper presents a summary of technical considerations and best
practices for programmers and team leaders to review as a part of
their software development process

http://www.astalavista.com/?section=dir&act=dnd&id=3726

" **OPEN SOURCE MICROSOFT EXCHANGE REPLACEMENT** "

The OSER project provides a replacement for Microsoft Exchange.
It provides email, groupware, and instant messaging, all compatible
with Microsoft Outlook

http://www.astalavista.com/?section=dir&act=dnd&id=3769

" **KIOSK** "

Kiosk is a Palm hack/DA combination that can be used to lock
a Palm handheld to a single application

http://www.astalavista.com/?section=dir&act=dnd&id=3767

" **YAHOO! NETROSPECTIVE : 10 YEARS, 100 MOMENTS OF THE WEB** "

To celebrate the first ten years of the Interent, Yahoo! selected the
top 100 moments of the web from 1995 to 2005

http://www.astalavista.com/?section=dir&act=dnd&id=3741

[04] **Astalavista.net Advanced Member Portal - Lifetime memberships still available!**

Get yours and become part of the community, not only for the rest of your life, but also in a cost-effective way. **Join us!**

http://www.astalavista.net/new/join.php

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. **This is a lifetime investment.**

Among the many other features of the portal are :

- Over **3.5 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://cebit.150.dk/

CeBIT 2005 video coverage!

[06] **Tool of the month**

World Wind 1.2

A tool that will let you zoom from satellite altitude into any place on Earth

http://www.astalavista.com/?section=dir&act=dnd&id=3740

[07] **Paper of the month**

Remote physical device fingerprinting

Discusses various innovative approaches for remote physical
device fingerprinting. **Recommended reading!**

http://www.astalavista.com/?section=dir&act=dnd&id=3776

[08] **Geeky photo of the month – 'From Russia with Love'**

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.

'From Russia with Love' can be found at :

http://www.astalavista.com/images/content/p1204001.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 : How's it going, guys, keep up the good work. I wanted to ask you a question related to my OS choice – Mac. It has always been giving me a good sense of security but recently I have started to have the feeling that in the next couple of months I would have to consider the purchase of Mac related security software. What do you think?

Answer : Purchasing more software wouldn't solve your worries, it will make them even worse and make you feel even more tricked in case a possible security scenario happens. Indeed, the Mac OS is getting more and more targeted recently, but you can be sure that it will take a while by the time you need to check Apple's Downloads site. Why? Because the Mac OS isn't as popular as Windows is, thus it's not a very common target for scammers or phishers or at least that's what they want you to think. Educate yourself, don't live behind the firewall that's protecting just one of the many entry points in your PC.

Check out these links :

http://www.apple.com/support/downloads/
http://homepage.mac.com/macbuddy/SecurityGuide.html
http://www.csse.uwa.edu.au/~pd/securing_mac_os_x.pdf
http://macenterprise.andrew.cmu.edu/dmdocuments/20041015-220_swarthmore_osxsecurity.pdf
http://Freaky.staticusers.net/

Question : Oustanding newsletter, I always appreciate the way you present security to me. I have a question, I constantly do E-banking, I have my random number generator…

Answer : Your biggest concert should be the way your bank identifies. That it's indeed you the one trying to access the account and make transfers, as well as making sure that you're indeed at the bank's site and not at another one. Don't check your balance from a netcare or from any untrusted computer and if your bank is offering you a two-factor authentication, take advantage of it even though it wouldn't protect you from Trojans. Certain banks offer you the opportunity to receive an sms whenever there's a change in your balance. Consider setting this permanently as it would act as an early warning system in case something's going on.

You can check out the following paper, it will definitely provide you with more insights on your problem, it's a very well written one :

http://ebankingsecurity.com/ebanking_bad_for_your_bank_balance.pdf

----

Question : I'm a computer programmer interested in security.
I'd like to use internet, but keeping my computer clean without spending a lot of money! I tried and I'm still looking for the best, least expensive and quick solution:
1) Ghostzilla browser... old...
2) using a CD version of windows XP (BartPE), good for a LAN, but not for home users... configuring modems...
3) using a CD linux distro (same problems with modems configuration)
4) using a backup software after (Norton GoBack) or registry tracer and backup software
5) clone the hard disk before surfing (Symantec Ghost)
6) using firewall/antivirus/antispyware, malware, adware, etc. softwares... not 100% security
7) proxy anonymous surfing... you can still received softwares, attacks...
8) a lot of others...
Any suggestion to use all the internet services and be sure to have a 100% cleaned PC after that (I know it's a difficult request, but you are more expert than me!)

Answer : Compared to the majority of questions we get, you're aware of various concepts, but I think you should take into account the fact that you simply cannot achieve 100% security and still have your computer connected to the Internet. This is what we try to promote as an idea at the Astalavista's web site. Consider securely wiping the content of your HDD, you can even do that with

PGP Wipe tools or find an alternative. Get yourself a decent browser and keep yourself aware of its vulnerabilities if any; beside all making backups is a very wise decision. Keep an eye on our Useful Tools and Utilities section and keep up to date, you're definitely not a naïve user.

[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!

- **P2P networks - unaware employees, security threats and your organization in between** -

During the last couple of years, the increased availability of broadband connections, the popularity of downloading free music and movies and the thought to be free of security or privacy threats P2P applications, has resulted in millions of active participants actively exchanging data, exposing themselves and the organizations they represent to malicious code, spyware, and privacy invasion threats. This short article will briefly summarize the most common threats, real-world scenariuos and what a company can do to protect its sensitive assets.
While P2P communications weren't primarily developed with the idea to spread music or movies, the way P2P works made it possible to exchange those files in a completely anonymous environment. The majority of your end users are savvy and use P2P networks. They're well aware of the potential benefits of the company's bandwidth compared to their home one and constantly try to install and take advantage of these on the company's infrastructure. What are the risks?

The legal threats from the possession, distribution and sharing of music could result in lawsuits reaching millions of dollars. You wouldn't enjoy having your servers sharing files like these, would you?

P2P networks should also be considered as yet another spreading point for various malware in the form of renamed files, malware targeting specific vulnerabilities in the clients themselves or exploiting vulnerabilities in third-party software that is closely related to playing multimedia files like Real Player or Windows Media Player that could result in further infections.

The complete exposure of sensitive company info is yet another serious threat to consider. Recently, confidential files belonging to the Dutch government were found on KaZaa. Guess what had happened? An employee had unknowingly shared the entire HDD with the rest of the world. And although such information should always be kept encrypted, you should't risk having a scenario like this as it could entirely ruin months of research or completely destroy it.

When may this happen? Let's assume that the corporate network is blocking the majority of P2P communications, while the mobile warriors are out there right now taking advantage of a high-speed hotel based Internet connection, on a company's laptop. Situations like these prompt for a coordinated integrity checking before the laptop leaves the organization and after it enters it again, before it's connected to the network.

The majority of P2P applications have also built-in chat features, which on the other hand open countless number of social engineering and identity theft on the other side of the communication channel resulting in the possible dissemination and actual execution of malicious code, trust is easily established and maintained. Recent phishing attacks are targeting any IM application, being AOL, MSN, ICQ, or the integrated within P2P software functions. It is all a matter of direct communication.

What you can do is either take advantage of a commercial P2P blocking Solution, or to use squid as a transparent proxy blocking the majority of false P2P http requests. Furthermore, establishing and actually enforcing a policy towards the installation of a third party software on the company's infrastructure should be considered as well.

Further reading on the topic can be found at :

http://www.cc.gatech.edu/~mudhakar/dht-security/p2p-security.pdf
http://cnscenter.future.co.kr/resource/security/application/Blocking_Content_Security_Threats.pdf
http://www.ftc.gov/os/comments/p2pfileshare/OL-100005.pdf
http://documents.iss.net/whitepapers/X-Force_P2P.pdf

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

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects

of Information Security in an easily understandable way, while, on
the other hand, improve their current level of knowledge.

- **"Help, my boss is spying on me!"** -

Is he/she just trying to enforce the company's security policy while you're using its infrastructure? This brief article will give you an overview of various issues related to employees' monitoring or worst BigBrother invasions on the work place.

Each and every time you log on to your company's network, you are monitored- monitored by the the internal access controls trying to verify if it's really you when you try to identify yourself. There's a program whose purpose is to count your keystokes or mouse clicks with the But where's the actual boarder between monitoring users' activities or totally invading their privacy by keeping copies of personal emails (ones not sent via the company's account)?

A difference should be made between content blocking, web filtering, web Monitoring and full PC activities logging. These should be distinguished by both the executives and you as an invidual. Has your organization integrated a system with predefined dangerous categories like hacking/porn sites in order to block and log if you have tried to access there, or is it gathering every event that occurs on its network?

From your executive's point of view, the company has to know how its employees are using the infrastructure and the intellectual property they work with on a daily basis

What to do about it?

- request more info on what is actually watched, are there keylogging activities in place and if yes, why, for how long is the information collected
- are there any laws in your country concerning the monitoring of the workforce
- don't do the obvious – surf porn web sites while @work, although according to the SexTracker.com a huge percentage porn related visits are made around working hours

Further reading on the topic can be found at :

http://www1.cmis.csiro.au/Reports/blocking.pdf
http://www.websense.com/hr/hr_wp.pdf
http://www.privacyrights.org/fs/fs7-work.htm

[13] **Meet the Security Scene**

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed Bruce, one of the organizators of the **DallasCon event**.

Your comments are welcome at security@astalavista.net

Interview with Bruce, http://www.dallascon.com/

Astalavista : Hi Bruce, would you please share with us some more information on your background in the security industry and what is DallasCon 2005 all about?

Bruce : Thanks for this opportunity. I have over 7 years of engineering experience working as a System's Engineer for companies such as Nortel Networks and Fujitsu. Realizing the importance of real information security training experince for everyday people, about 4 years ago a few colleagues and I decided to start truely academic Information Security Conference in Dallas and see what happens. We held the first DallasCon in 2002, just a few months after the tragic events of Septmber 11, 2001 in the U.S. The reponse was overwhelming with academic papers being presented from as far away as Russia and attending coming from countries such as Japan and China.

Astalavista : There are so many active security cons and conferences out there that it is sometimes hard to decide which one is worth visiting. What, in your opinion, makes a con/conference qualified? Do you think that although there's nothing wrong with commercialization, some cons are becoming too commercial so they have lost sight of what their vision used to be in the very beginning of their history?

Bruce : Truly, I must admit the lure of money being thrown at many of similar conferneces such as ours is sometimes overwhelming. When a company such as Microsoft comes knocking on your door with a fist full of cash wanting to by into a Keynote speaker slot, it's hard to resist the temptation to give in. But we have tried to separate the academics from the commercial side. The training courses and the conference itself are designed to present the latest unbiased view of current trends in information security. We have a team of dedicated colleagues that read every paper carefully and look for flagrant promotions of certain technologies or companies. They also work very closely with the speakers who are chosen to present at DallasCon, to make sure that they know what is expected from them. We do offer sponsorship opportunites to companies to help us carry the costs of such an event, but we try very hard to separate the business side from what people come to DallasCon for, which is the latest unbiased view of the trends and research in information security. I think many conferneces lose sight of what made them big and forget their roots.

Astalavista : Like pretty much every organization, ChoicePoint or T-Mobile, keep a great deal of personal, often sensitive information about us, as citizens, students or employees. What actions do you think should be taken by the general public, the companies themselves and the government to ensure that the security within such databases or service providers is well beyond the acceptable level of security for most organizations?

Bruce : I think companies need to stop treating their customers like numbers and really put a face with the information that they are gathering. When someone gives you detailed information about themselves, they have put their trust in your company to protect them. When a breach is made, the cusomter feels betrayed and may never come back to you to do business. I laugh when

I hear that huge muti-billion dollar companies are constantly having their cusotmer data stolen. I wonder how much they are really spending on security? How much are their cusotmers worth to them? These days it is hard to distinguish between legitiamte companies and fake ones online. It's funny, but people have trouble revealing their credit card information or social security number to a physical business down the street, but put the same business online and people throw that information at you without thinking twice. I think consumers need to stop taking security for granted and use some common sense. The first step of security is common sense... You can't put a price on that!

Astalavista : Two words - Symbian and malware - what are your assumptions for the future trends on the mobile malware front?

Bruce : I predict that it will be huge. The future of mobile OS is wide open and as the competition for market share grows, mobile companies want to offer anything they can in a smart-phone. I am always surprised as to what phones can do right now... in a few years, they might even serve us breakfast in bed! The downside is the huge vulnerability of the mobile-OS. First of all, more people own phones than computers around the world. It is the obvious next frontier for virus writers. Secondly, theoretically, it is much easier to infect an entire phone network than PC's. All you need is one infected phone syncking with a base station. Again, I go back to my previous answer, people need to use common sense... Do you really need to put your financial data or your sensitive e-mail on your phone?

Astalavista : What is your opinion about the mass introduction of biometrics on a world wide scale?

Bruce : Good - it will make security more individualized. We will all carry our security inside our DNA. Bad - it might increase the market for organ theft! (just kidding!)

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

Bruce : I have been visiting Astalavista.com for many years now, and I am very impressed with the up to date cutting edge news, articles and really underground topics covered on your site. When we wanted to really reach out to the educated hacker community, Astalavista.com was the obvious choice. Thanks for putting us on your site and thanks for helping us promote our event.

Astalavista : You're welcome, wish you luck with the con!

[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.

-

Kernelnewbies.org

-

http://www.kernelnewbies.org/

Kernelnewbies is a community project meant to help people learn how operating system kernels work

-

Infonomicon.org

-

http://www.Infonomicon.org/

Infonomicon Radio - "Tech news you need, like it or not"

-

Phoronix.com

-

http://www.Phoronix.com/

Definitely worth the visit!

-

Webtechgeek.com

-

http://www.Webtechgeek.com/

Recommended site for tips, reviews and free software

-

Freaky.staticusers.net

-

http://Freaky.staticusers.net/

Macintosh security site, archive, tools and lots of info

[15] **Final Words**

Dear readers,

Thanks for taking your time to go through our security newsletter, till our next issue.

Keep the spirit and ,most importantly, stay tuned!

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net