MEDIABUZZ PTE LTD

Empowering AsianeMarketing
Asia's Electronic Marketers

4TH QUARTER 2005

OCTOBER 2005

BE PROTECTED: INCLUDE ANTI-SPYWARE SOLUTIONS IN YOUR SECURITY MEASURES

INSIDE THIS ISSUE:

HIGHLIGHTS

Do you feel your computer is getting slower or do you see more pop-up ads while surfing the internet? If there is so, your PC is most probable infected by spyware! Spyware sneaks into your computers without your knowledge or consent in many different ways and it can be very tedious to get rid of it.

It's shocking to read recent statistics claiming that approximately 95% of all PCs worldwide are infected with spyware and that around 80 new spyware programs emerge every week, which is double the number of new virus threats. These new released types of spyware are more advanced than most computer viruses and can harm computers enormously.

Spyware is often unknowingly installed by Internet surfers, as these malicious applications are often bundled with software that is willingly download in bona fide to fix a computer problem or to speed up the system or simply together with desired music or games. There are even some programs that claim to remove spyware from the computer, when, in fact, it installs only more.

continues on Page 2

ATTACK OF THE ZOMBIES

Creating zombies out of computers used by average people around the world has become one of the latest tools used by computer hackers, unscrupulous marketers, and other malicious evil-doers. Zombie computers have become a serious and widespread problem. It is estimated that between 50% and 80% of today's spam is being sent by zombie computers.

A zombie computer is a computer attached to the Internet that has been compromised by a hacker, a computer virus, or a Trojan horse, and performs malicious tasks of one sort of another, under the direction of the hacker.

Infected zombie computers, predominantly Windows PCs, are

continues on Page 4

CONTENTS

Spyware can be disguised as software updates or use a similar trick to convince clicking on pop-up ads to start the spyware installation. Another common way to slip onto computers is through peer-to-peer file sharing programs or browser toolbars, such as the formidable Hotbar. Offering, for instance, to enhance browsing experience or allow internet search directly in the toolbar, spyware is secretly installed through "drive-by downloads" (see BUZZwords) or by piggybacking on other applications. Once installed, these mean programs can actually capture keystrokes and send sensitive data to a third party or outside the company. It is able to track web surfing behaviours, take advantage of Internet connections, and slows down computers systems and eve causes complete system failures.

If you accidentally only visit one infected webpage your PC can get infected with the spyware. Such a page typically makes use of ActiveX controls and exploits weaknesses in Internet Explorer. Spyware can be spread through email programs as well, such as Microsoft Outlook and Outlook Express. If a message is encoded in HTML (instead of plain or rich text) the HTML document's head can call a malicious script. The email doesn't even have to be read to infect the system, sometimes just having the message displayed through Outlook's preview pane is enough to cause the malicious script to execute. Fortunately, newer versions of Outlook allow the blocking of external HTML code.

No wonder that Microsoft blames spyware for up to one-third of application crashes on Windows XP computers and estimates that more than half of all Windows operating system failures are caused by it. Fact is, spyware is a major threat for individuals and enterprises and the longer a network is unprotected, the more damage spyware can cause. In all intents and purposes it's getting worse every day. So let me give you some insights into the spyware problem and some advices on how to fight it.

The mentioned methods in which spyware is spread are only one part of the problem, the other is the lack of reliable methods for detecting and removing this unwanted application. At least since last year more spyware detection and removal capabilities have been built into anti virus programs and this is really good news, Although most people know that running any computer these days without a good anti-virus program would be cyber-suicide, only a few have realized that these programs paid no attention to all the spyware that's going around. In general, preventing a computer from spyware is a lot the same like protecting it from viruses or any other security risk. It includes regularly security updates, being careful with visiting web pages or clicking a link, being cautious with opening emails from people you don't know or attachments you don't trust, and being alert of any site offering to speed up your computer or improve your internet connection, especially when it's for free. As an additional safety measure it's also good to build layers of security into your network with firewalls and web proxies to block access to Web sites known to install spyware.

Anti-spyware programs can combat spyware in two ways: **Real-time protection**, which prevents spyware from being installed and **scanning and removal of spyware**. Scanning and removal is usually simple. The program inspects the contents of the Windows registry, the operating system files, and installed programs,

continues on Page 3

and removes files and entries which match a list of known spyware components. Real-time protection from spyware works identically to real-time anti-virus protection: the software scans incoming network data and disk files at download time, and blocks the activity of components known to represent spyware. In some cases, it may also intercept attempts to install start-up items or to modify browser settings. Early versions of anti-spyware programs have been mainly focused on scanning and removal. But as you will see, many programmers and commercial firms have released products designed to remove or block spyware. All claim to be the best, and the choice is yours. Fact is that cleaning an infected PC can be relatively tricky and a number of anti-spyware applications have emerged to counteract the problem. Be cautious as some of the just install more spyware than removing it. But fortunately a few good and effective programs exist and two of the best anti-spyware programs are even free, which I will present you in more details besides some commercial ones. From the point of experts there is unfortunately still no product that provides comprehensive protection against these malicious threats.

The first very useful program I want to present you is **Spybot Search & Destroy**. Many experts consider is as the most effective anti-spyware program, provided by a small group of programmers on their web site for free. Their programmers will ask you to donate something for the service – and I think you should support them if you like the program - but it isn't required. The program aims to remove all spyware it can find on your computer without any false positives. A false positive is when an anti-spyware program identifies a legitimate file as spyware when it shouldn't. Spybot Search & Destroy is easy to install, easy to use, easy to update, and most importantly, very effective. It eliminates spyware on your system and blocks it from coming back. The newest version also offers real-time protection by blocking spyware programs as they try to install themselves and is warning you if anything acts out of turn. The installation is straight forward and you can download Spybot Search & Destroy here. Every time you run it, make sure to get all available updates first (through the "search for updates" feature inside the program.) Then, use the immunize feature, which blocks known bad programs and finally, run a scan.

But as good as this program is, experts recommend to install always at least one other anti-spyware program to be on the safe side. As there is still no anti-spyware software on the market that can clean everything a second program can mop up the rest of spyware from your PC which hasn't been covered before. Therefore, I recommend you a second free anti-spyware software that received very good critics for their good scanning results. Lavasoft's Ad Aware SE Personal Edition is one of the few reliable anti-spyware programs. The program is focused on completeness and is doing a very through scan of your computer to remove all spyware. It risks having a few false positives to guarantee privacy, so make sure you check the list of files it identifies for false positives before deleting. Be assured that Ad Aware usually catches what was missed out by Spybot's Search & Destroy. And to whom this is still not enough, or if you have to treat a very badly infected machine there are still many opportunity to use commercial anti spyware programs like for instance SpySweeper from Webroot, or Computer Associates' Pest Patrol.

Other well-known anti-spyware programs are:

- HijackThis, which is not a scanner like the others, but more like a registry editor.
- Javacool Software's SpywareBlaster, which was one of the first to offer real-time protection, blocking the installation of ActiveX-based and other spyware programs. Spyware Blaster is more designed to prevent spyware than to remove it, which means that its program mainly changes Internet Explorer's security settings to protect PC users from infecting themselves. Programs such as Ad-Aware and Windows AntiSpyware already combine the two approaches.
- Microsoft Anti-spyware works only on Windows 2000 and XP and provides real-time protection, auto-updating and automatic scheduling of scans. Currently only a Beta version exists which occasionally causes some connectivity issues, so back up your system before installing it.
- Blue Coat offers a real-time spyware prevention by tracking sites known or highly likely to push spyware, and then removing the potential spyware code in downloads from those sites.

continues on Page 4

Major anti-virus firms such as Symantec, Sophos and McAfee have come later to the table, adding anti-spyware features to their existing anti-virus products.

Early on, anti-virus firms expressed reluctance to add anti-spyware functions, citing lawsuits brought by spyware authors against the authors of web sites and programs which described their products as "spyware". However, their recent anti-virus product versions include anti-spyware functions, although treated differently from viruses. Symantec Anti-Virus, for instance, categorizes spyware programs as "extended threats" and does not offer real-time protection from them as it does for viruses.

If a computer is so badly infected that the infection don't seem to be removable by any anti-spyware program you can try to solve the problem while working in Safe Mode. The idea is that when you boot Windows into Safe Mode, Windows is running under a minimum set of drivers and services, and you are also isolated from the Internet. The advantage of this method is that most of the time when anti spyware applications are able to detect an infection, but can't clean it (or when the infection comes back immediately after cleaning it), it is usually because some spyware component is currently in the system's memory. Most anti spyware programs focus primarily on the contents of the hard disk rather than the memory and spyware modules in memory consequently often go undetected. However, by booting the machine into Safe Mode, you can usually prevent spyware modules from loading while you try to clean the system. Keep in mind though that you must initially boot Windows normally so that you can download the latest updates to your anti spyware programs. Only then can you effectively boot into safe mode and begin the removal process. Hopefully, booting the machine into Safe Mode and running an anti spyware program will take care of the problem for you. Sometimes even this method fails though. There are some types of spyware that are so hard to get rid of that you will have to remove them manually, like browser hijackers.

Safeguard your privacy, data and know-how and start fighting all types of spyware!

I hope I could be supportive to do it faster and more effectively.♦

By Daniela La Marca

From Page 1 — Attack of the Zombies

now the major delivery method of spam.

Besides relaying spam and launching DOS attacks, a zombie machine can be used to send phisher scams, spread viruses, download pornography, and steal personal information. Some of this data can also be sent to other computers as a massive attack that is meant to overwhelm another computer and shut it down. Attacks of this nature have been mounted against corporations like Microsoft as well as other corporate and governmental entities. Since the attackers can control thousands of computers, these attacks can be devastating.

How zombies work

Viruses are used to penetrate the computer of an unsuspecting victim. The virus can be from an email attachment or it can be downloaded from the Internet with another program.

Zombies are often created from a type of virus called a Trojan horse, a type of virus that invisibly piggybacks on another program or virus. Once the Trojan is in your computer, it gives your computer instructions to perform a malicious task. Your computer, like a zombie, follows the instructions it is given.

Signs that your computer may be a zombie

- The computer seems sluggish.
- The computer seems to be accessing the hard drive constantly.
- The mouse or keyboard becomes unresponsive.

You get excessive bounce notification from people you never tried to email.

There are several steps that you can take to prevent your computer from being turned into a zombie:

- Install a good antivirus program and make sure you update it regularly.
- Install a good two-way firewall. It will notify you when information is being sent from your computer. Unfortunately the Windows XP firewall is not adequate for this purpose.
- Update your operating system and other software regularly.
- Use an anti-spyware program to eliminate spyware on your system.
- Often one of the first instructions given to a zombie computer is to disable the antivirus and firewall software. So check your antivirus and firewall software occasionally to make sure they are running properly.
- Be careful not to open unexpected email attachments.

Be careful when downloading software. Use only reputable companies and be sure to read every screen as you download and install any software.♦

By Shanti Anne Morais

THE EVER-CHANGING FACE OF SPYWARE

Don't let your guard down, spyware, this year's top security concern is even more insidious then previously thought. So banish your thoughts about it simply being a minor annoyance. The statistics alone are horrifying and worldwide, the problem of spyware is growing.

According to Web@Work, in 2004, 92% of enterprise IT managers cite organizational spyware infections and 29% of enterprise desktops are infected at any given time. Computer Economics, 2004 reveals that security threats – such as web attacks, spyware, malicious mobile code, and phishing – cost organizations worldwide an estimated US$16.7 billion in 2004.

A report from security firm Webroot based on spyware activity for the second quarter of 2005 shows that spyware pushers are shifting their focus from pay-per-click advertising to identity theft, and expanding their network of infected machines in the process. Charles Cousins, managing director, Sophos Asia Pte Ltd points out that spyware has been a problem for more than 10 years now, and that money and espionage are its key drivers. "The difference now is that there is a financial incentive associated with capturing transaction activity and/or relaying spam. Spam writers have to hide their identity. It is easy to cut off a source of spam if it all comes from one or two machines as the high volume of email messages is a dead giveaway. But this has led to spam writers especially to write more Trojans to create zombie PCs."

Commenting on the boom in spyware, Tom Clare, director, product marketing, BlueCoat Systems says, "Spyware is enormously successful because companies are paying individuals to install spyware on innocent users' machines. This means the culprits infecting systems with spyware are gaining financial rewards. When people get paid to infect other people's computers, they are motivated, which perpetuates the spyware economy."

"Spyware producers make money on the information they collect, such as market research and personal information, as well as advertisements distributed. Web property owners are paid by spyware distributors to distribute spyware. Both producers and distributors change dissemination and installation methods frequently to avoid detection and to ensure high distribution costs."

According to Clare, spyware is escalating in Asia since the overseas markets, especially the US, are now saturated. "Spyware vendors are now looking for new markets and with the advent of language development kits, spyware now works in Chinese, Korean, Japanese and Bahasa, Korea has been especially hard hit, with Korean companies creating spyware and distributing it through Korean websites. Spyware is now becoming more country-specific, with the same phenomenon happening in Singapore, Japan and Hong Kong. Clearly, spyware will continue to rise in Asia."

Cousins adds that spyware is a very big problem in especially China and Korea because, "many millions of computers in these two countries are connected to broadband, always-on, usually without a personal firewall and usually without good, or up-to-date anti-virus software."

He thinks that awareness of spyware now is quite high, but adds that end-users in particular are not doing enough. "They need to install and activate personal firewalls, they need good world-class anti-virus software with recognized global approvals for catching spyware, and they need to keep it up-to-date. We also suggest that they switch off their computers when not in use."

Clare cautions, "Don't be mistaken to think that spyware removal applications are enough. When such programs run on computers, the Trojans installed by the hackers can easily download a new copy of the spyware and install it again, allowing hackers to get paid twice for infecting the same system. Each time people uninstall it, spyware is re-launched. It's a vicious business."

Since spyware has been around for so long, just how has it evolved? Cousins' says that spyware has moved from simply stealing logging keystrokes, mouse movements and screenviews to harvesting email addresses, looking for web activity associated with transactions, acting as a "relay" for spam and industrial espionage (country-to-country and company-to-company).

Laurent Dedenis, managing director, Acronis Asia adds, "Spying functionality now is only an optional behavior of more complex malicious software that can be installed and then act without your permission in background. We dropped using spyware as a term of software classification because often such software is not only for spying but for opening backdoors to your operating systems, downloading unauthorized advertisements, utilizing computer resources and so on. Now spyware programs can use stealth technologies cloaking your activity, dynamically choose

continues on Page 6

different types of redistribution to another computer and polymorph viral code."

He says that the main trend in spyware now is "building more multifunctional malicious software that are using rootkits, stealth technologies, operating systems security holes to utilize any processor resources via the internet."

Paul Kurtz, executive director of the Cyber Security Industry Alliance, says the Anti-Spyware Coalition's (formed earlier this year when the nonprofit Center for Democracy and Technology teamed up with several tech firms and security organizations) work is vitally important given the damage spyware can do.

"Spyware can be so broad," he says. "We allow forms of it on our computers every day. That's the big issue we need to think about today. There must be common rules and procedures for defining and removing it. If we can establish a common template to determine what should be removed as spyware, we'd at least be putting everyone on the same sheet."

Despite awareness, infection rate stays high Webroots report agrees with Cousins – awareness of spyware is up. Moreover, the security market is flush with new tools to scan and clean systems. Yet the spyware infection rate for enterprise desktops remains above 80%, the report said.

The firm's research team also saw evidence that spyware pushers are aggressively growing their distribution channels. The report said the number of Web sites distributing spyware has quadrupled since the start of the year to 300,000 unique URLs. Meanwhile, the company has seen the number of spyware traces in its spyware definition database double in the same period to over 100,000. In addition, the study shows that spyware pushers are also working hard to test their wares against a range of antispyware software and are successfully using rootkits to avoid detection.

The report also offers a list of programs Webroot has fingered as spyware, including a new one called Look2Me. This spyware may monitor Web surfing activity and report back usage statistics to a centralized server. It may also display pop-up ads and install several other pieces of spyware.

"Once installed, Look2Me may update itself and install other applications," the report said. "These applications are usually other pieces of spyware. Look2Me may download and execute third-party programs on your computer without your knowledge or consent."

Look2Me is usually installed using ActiveX drive-by download sites or flaws in common Web applications, the report said, adding, "Look2Me is very difficult to remove due to its injection into system-level processes. It may also install other pieces of spyware and adware, which decrease your computer's performance, and may display pop-up advertisements."

Bearing all this in mind, it doesn't look like the spyware war will be over very soon. The big question is – will anti-legislation help in alleviating the problem in any way? "No," says Cousins. "It will help the prosecution process, and may deter a few amateurs, but the professionals are well beyond the law.

continues on Page 7

For a start, they will write their spyware in one country, says USA, and then deploy it in another country, say Korea or China.

It is difficult enough to get governments to agree on extradition treaties for murderers, so doing the same for spyware authors is many years away."

Clare adds, " While legislative efforts may have some impact, the Internet is borderless and difficult to control through legislation. The common reaction for spyware purveyors will be to simply move their operations offshore. Commercial spyware vendors will most likely seek to comply with regulations by making license agreements more clear when asking end-users for permission to install spyware. Unfortunately, spyware licensing agreements never go beyond the end user, and the enterprise – who owns the infrastructure – is left out of the decision."

He notes that spyware is difficult to stop technically for a variety of reasons. First, spyware is a new and evolving technology that quickly adopts all of the latest techniques from viruses, worms, and Trojans. Perhaps more importantly, spyware attracts the best and brightest hackers – who are finally being compensated for their efforts by either commercial spyware companies or organized crime.

Second, spyware is an application-level threat , and most existing enterprise defenses focus on the infrastructure layer – i.e., they defend file systems, general network traffic (at the port and protocol level), and known threats on application services (e.g. email servers, database servers, and web servers). Unfortunately, many of the existing defenses such as firewalls and intrusion detection/prevention systems lack the application-level visibility and granularity necessary to block spyware without shutting down Web traffic associated with legitimate business functions. Clare stresses the importance of attacking spyware before it becomes a problem and not after – i.e. at the gateway itself.

On a positive note, Cousins says that spyware does not have a negative impact on genuine e-marketers. However, "it makes them think more carefully about how they craft their EDMs. Some companies are naïve enough to think that writing an EDM is a simple case of writing an email and broadcasting it. EDMs nee as much care and attention and creativity as any other type of marketing collateral, if not more so, as the medium is more restricted." ♦

By Shanti Anne Morais

THE 3 TOP QUALITIES NEEDED IN CREATING EFFECTIVE MAILING LISTS

For building up a mailing you have to be very thoughtful, diligent and patient. It requires a lot of time and care to create a qualitative and extensive mailing list.

Let me give you some advice for supporting your data collection:

1. Guarantee Privacy

Losing "privacy" is what online users fear most. Therefore, guarantee your clients that you are not spying on their online behavior or collecting email addresses for wicked purposes. Your announcement to respect their privacy and your clear refusal to sell information will establish a level of trust. This results in more registrations and a growing database.

2. Deliver what is promised

Whatever value offered - your clients have to get what you promise. Be it information, special offers, privacy etc. deliver it and make sure that your clients come again and that you are not losing them.

3. Manage your Website

Don't forget to place a registration form prominently on your website and promote your values/offers. It's not a big effort and your mailing list will grow continuously. Once your values are highlighted on your Website, identify other Websites where you could advertise your service (e.g. partners), or use search engines, newsletters etc. to promote your mailing list.

4. Don't Ask for Unnecessary Information

Be careful with collecting information. Don't ask too much and only for information necessary for the registration or basic analysis. Offer an easy and transparent registration form so that you don't scare away potential clients already at the beginning. Be assured that you will receive more information once a relationship is developed. Requesting sensitive information such as date of birth or mobile numbers can deter people from completing the sign up process. ♦

By Daniela La Marca

63 WIDESPREAD MISTAKES IN NEWSLETTERS

There are certain rules for good newsletters. But not everybody seems to know them or follow them.

Log-in and log-out

- Dispatch of e-mails without consent
- Web: Registration form is hidden
- Intricate registration
- No attention given to data thrift
- Unnecessary data request
- No indicator or anonymous reference
- No index of the expected contents
- No reference to the frequency of publication
- No information about data protection
- No note on data processing
- No special consent for analysis of personally identifiable information
- No acknowledgement message on the Web
- Bad confirmation (for example " System OK, ")
- No logging of the approval (confirmation mail)
- No welcome e-mail
- Complicated log-in process
- No right of objection indicator (i.e. “cancel")
- Intricate change of e-mail address process
- Belated change of registration data not possible
- Absence of marking duty (imprint)

Sender

- As sender there is only "newsletter"
- As sender there is only "John Smith"
- As sender there is only info@company.com
- Ensure everything is personalized.

Reference

- Subject is meaningless or always the same ("newsletter ")
- Dull subject matter without reference to actuality or value

Introduction

- No individual address
- Unclear subject
- Not clear what advantage/benefits the reader / buyer gets
- Oversized logo at the beginning
- A lot of empty space at the beginning
- Long text blocks at the beginning
- No incentive to read on
- The first message of the newsletter is immediately advertisement
- The editorial at the beginning is signed by "your newsletter team " instead of " Yours, Peter Miller” "
- First announcement is the imprint
- Introduction too long and/or without structure
- Opportunity to countermand is too striking immediately at the beginning

Arrangement

- No clear structure
- Single announcements are inadequately separated from each other
- Unstructured and overloaded text page
- Waste of free space
- Weird subject mix
- Too much continuous text
- No table of contents or it appears at the end
- Single announcements have no link back to the above table of contents

Hyperlinks

- Blue writing is used which is usually associated with hyperlinks
- No hyperlinks on detailed information
- Hyperlinks are not recognizable as those
- Hyperlinks only on homepage instead of leading to special sites
- Not all is "linked": heading, picture and keyword at the end of text

Pictures

- There are no explaining pictures
- Unnecessary pictures
- Order button too small
- Pictures don’t support quicker grasping of subject-matter
- Weighting: too much picture not enough text

Presentation

- Dispatch of the virtual newsletter as appendix of an e-mail
- Writing in capitals which make it indistinct
- Content does not fit to the reference line
- Contents too ornate
- Reader / buyer advantage not or only hardly identifiable
- Long winded wording
- Misspelling♦

By Dr. Torsten Schwarz
ABSOLIT Dr. Schwarz Consulting

ABSOLIT Dr. Schwarz Consulting offers independent strategy consultation on e-mail marketing and integration of electronic media

DR. SCHWARZ CONSULTING
ABSOLIT®

THE TWELVE FACES OF MALWARE

The word “malware’ seems to be cropping about everywhere, but what exactly is it? It is the acronym of malicious software and basically refers to software that does not benefit the computer’s owner, and may even harm it – in other words, it is parasitic in nature.

According to Wikipedia, there are in fact eleven distinct types of malware, and even more sub-types of each.

1. Viruses. The malware that's in the news so much. Viruses have used many sorts of hosts. When computer viruses first originated, common targets were executable files that are part of application programs and the boot sectors of floppy disks. More recently, most viruses have embedded themselves in e-mail as Email attachments, depending on a curious user opening the viral attachment. In the case of executable files, the infection routine of the virus arranges that when the host code is executed, the viral code gets executed as well. Normally, the host program keeps functioning after it is infected by the virus. Some viruses overwrite other programs with copies of themselves which destroys them altogether. Viruses can spread across computers when the software or document they've attached themselves to is transferred from one computer to the other.

2. Worms. These are slight variations of viruses. The main difference between viruses and worms is that viruses hide inside the files of real computer programs (for instance, the macros in Word or the VBScript in many other Microsoft applications), while worms do not infect a file or program, but rather stand on their own. They do modify their host operating system, at least to the extent that they are started as part of the boot process. To spread, worms either exploit some vulnerability of the target system or use some kind of social engineering to trick users into executing them.

3. Wabbits. According to Wikipedia, wabbits are in fact rare, and it's not hard to see why: they don't do anything to spread to other machines. A wabbit, like a virus, replicates itself, but it does not have any instructions to email itself or pass itself through a computer network in order to infect other machines. The least ambitious of all malware, it is content simply to focus on utterly devastating a single machine.

4. Trojans. Arguably the most dangerous kind of malware, at least from a social standpoint., a Trojan is a harmful piece of software that is disguised as legitimate software. Trojan horses cannot replicate themselves, in contrast to viruses or worms. A trojan horse can be deliberately attached to otherwise useful software by a programmer, or it can be spread by tricking users into believing that it is useful. To complicate matters, some trojan horses can spread or activate other malware, such as viruses. These programs are called ‘droppers’.. A common aftermath is the Trojan attracting a large amount of adware/ spyware, causing lots of popups and web browser instability. Trojans rarely destroy computers or even files but don’t relax, this is only because they have bigger targets: your financial information, your computer's system resources, and sometimes even massive denial-of-service attack launched by having thousands of computers all try to connect to a web server at the same time.

5. Spyware. This is software that spies on you, often tracking your internet activities in order to serve you advertising. They usually work and spread like Trojan horses. The category of spyware is sometimes taken to include adware of the less-forthcoming sort.

6. Backdoors. Again, these are similar to Trojans or worms, except that they do something different: they open a "backdoor" onto a computer, providing a network connection for hackers or other malware to enter or for viruses or spam to be sent out through.

Based on how they work and spread, there are two groups of backdoors. The first group works much like a Trojan, that is, they are manually inserted into another piece of software, executed via their host software and spread by their host software being installed. The second group works more like a worm in that they get executed as part of the boot process and are usually spread by worms carrying them as their payload. The term Ratware has arisen to describe backdoor malware that turns computers into zombies for sending spam. The installed software can also be used for anonymizing traffic, brute force cracking of passwords and encryptions, and distributed denial of service attacks (DDOS).

7. Exploits. Exploits attack specific security vulnerabilities. Exploits are not necessarily malicious in intent — they are often devised by security researchers as a way of demonstrating that a vulnerability exists. However, they are a common component of malicious programs such as network worms.

continues on Page 10

8. Rootkit. The malware most likely to have a human touch, rootkits are installed by crackers (bad hackers) on other people's computers. The rootkit is designed to camouflage itself in a system's core processes so as to go undetected (for example by deleting log entries or cloaking the attacker's processes).

It is the hardest of all malware to detect and therefore to remove. Hence, many experts recommend completely wiping your hard drive and reinstalling everything fresh.

9. Keyloggers. Yes, this is the one that logs your keystrokes - what you type. Typically, the malware kind of keyloggers (as opposed to keyloggers deliberately installed by their owners to use in diagnosing computer problems) are out to log sensitive information such as passwords, PIN numbers and financial details.

10. Dialers. Dialers dial telephone numbers via your computer's modem. Dialers either dial expensive premium-rate telephone numbers, often located in small countries far from the host computer; or, they dial a hacker's machine to transmit stolen data.

11. URL injectors. This software modifies the browser's behavior with respect to some- or all domains. It "injects" a given URL in place of certain URLs when you try to visit them in your browser. Usually, the injected URL is an affiliate link to the target URL. An affiliate link is a special link used to track the traffic an affiliate (advertiser) has sent to the original website, so that the original website can pay commissions on any sales from that traffic.

12. Adware. The least dangerous of malware. As its name implies, adware displays ads on your computer. As Wikipedia notes, adware is often a subset of spyware. The implication is that if the user chooses to allow adware on his or her machine, it's not really malware, which is the defense that most adware companies take. In reality, however, the choice to install adware is usually a legal farce involving placing a mention of the adware somewhere in the installation materials, and often only in the licensing agreement, which hardly anyone reads.

Symptoms of Malware

Some of the symptoms users' experience that are caused by the existence of malware programs are:

- Poor system performance, especially while connected to the Internet.
- Computer stops responding more frequently.
- Computer takes longer to start up.
- Browser closes unexpectedly or stops responding.
- Performing a search from a search page provides results on a different site.
- Clicking a link does nothing or goes to an unrelated Web site.
- Browser home page changes to a different site and may not be able to be reset.
- Pop-up advertising windows appear when the browser is not open or over Web pages that do not normally have pop-ups.
- Additional toolbars are added to the browser.
- Web pages are automatically added to list of favorites.
- Desktop icons are automatically added to the desktop.
- When you start your computer, or when your computer has been idle for many minutes, your Internet browser opens to display Web site advertisements.
- When you use your browser to view Web sites, other instances of your browser open to display Web site advertisements.
- You cannot start a program.
- When you click a link in a program, the link does not work.
- Components of Windows or other programs no longer work.

Some of the more well-known malware programs are:

- GAIN
- Hotbar
- GameSpy Arcade
- Ezula
- WeatherCast
- BonziBuddy
- Cydoor
- TOPicks
- BargainBuddy
- CasinoOnNet
- WebSearch ♦

TIP: INFLUENCE PURCHASE DECISIONS

It is a commonly known weakness of human beings to want exactly what's hardly available. If a product seems to be apparently scarce, it wins decisively in attraction. Especially on the Internet this human weakness can straight be used if only the right virtual temptations are created. Use the shortage phenomenon purposeful for your advantage. Inform your clients about the fact that a certain product is only available3.7in a restricted number and presumably not very long. Many companies already use this "tactic of limited amounts", like for instance Amazon. The online bookseller lists the number of titles it has still on stock and requests straight to the purchase.

Another way to use the shortage phenomenon is to limit an offer in its validity (time limit tactics). Besides, the ideal time limit depends on the product, though the pressure on the consumer increases exceptionally shortly before the expiry of the term. In this way, many vendors of Internet services offer their deals only for a short time to a special price. This tactic lends itself particularly for your e-mail marketing campaign: If your customer receives a newsworthy offer by e-mail, you shouldn't give him a lot of time to think about it. Because, if the customer believes that he can still revert back to the offer in a week, he will most likely simply delete the e-mail. It would be different, if you write that the present special offer is valid only for the next three days and that only a small number of items are available. And even better, if you include into the message a code number so that the client receives the special price only with it. So, whoever would like to buy the product has to act fast.♦

By Daniela La Marca

SPYWARE AND BLOGS

There is no doubt that blogs are becoming increasingly popular, including here in Asia. However, many bloggers are unaware that hackers are using blogs to infect computers with spyware, exposing serious security flaws in self-publishing tools used by millions of people on the Web, especially the two most common methods used to launch programs on a Web page – JavaScript and ActiveX.

JavaScript and ActiveX are being used by malicious programmers to automatically deliver spyware from a blog to people who visit the site with a vulnerable Web browser. In addition, spyware tools also have been hidden inside JavaScript programs that are offered freely on the Web for bloggers to enhance their sites with features such as music. As a result, bloggers who use infected tools could unwittingly turn their sites into a delivery platform for spyware.

Spyware has become a thorn of Web surfers and companies in recent years and unsurprisingly, is listed as a top security concern of 2005 by IDC. Creators of malicious code take advantage of security vulnerabilities in e-mail software, Web browsers and desktop applications to spread code used to steal personal information or bombard a PC with advertisements. These same people have now turned their eyes to blogs, using them as a tool to increase their number of installations.

At the moment, the problem tends to affect Web surfers using Microsoft's Internet Explorer who fail to choose the highest IE browser security settings. According to security experts, the blog vulnerability has cropped up most visibly in Google's Blogger, the most widely used blog-publishing too, but it could affect other services as well.

Users of Google's Blogger have complained that they were exposed to infected sites when they used the "Next Blog" link. The feature was designed to help people discover new journals and takes Web surfers to a random Blogspot site. However, visitors were instead targeted with pop-up ads seeking to deliver malicious code to their computers. Other instances included ads erroneously warning people that their computers are vulnerable to spyware, prompting them to click the ad to protect themselves, but which instead, launches a download that infects a machine with spyware.

Google is aware of these issues and has been actively trying to solve them.

However, while it is easy to put the blame on others like Google, or Microsoft, both bloggers and users have to be responsible for their actions too. Bloggers should be more careful about what they offer/ embed on their sites, while users should be more aware of what they click on. A good best practice for users - change IE security settings to deactivate ActiveX or JavaScript in the Web browser,

Once again, it all boils down to what needs to be done to improve security and web browsing. Everyone concerned needs to be actively involved in this fight – from the developers, to the distributors, to the users. Only by uniting and standing together can escalating threats like spyware be overcome. The multiple courses of action include:

- Software developers need to take responsibility for their products and end users should be advised of potential security and privacy risk associated with use of software.
- Governments at the national and international level need to establish laws protecting the privacy and security of internet community.
- End users need to take personal responsibility. They should at least ensure they have a basic understanding of the ramifications of security and privacy risks. They need to understand the ramifications of what they do could affect not just their machine but undermine the protection of an entire network.

IT professionals need to be educated and secure network resources always updated/fine-tuned. Very often, one solution alone will not address all the issues related to needs of the organization and the security of the network.

Standards and independent certification testing, and protocols need to be established to assist with stemming the tide of Internet threats like spyware. This will allow software developers to be able to use their creativity to expand the internet environment while providing a means to safeguard that development and provide some measure of security.♦

By Shanti Anne Morais

SPAM'S DIRY DOZEN

Sophos has released its latest report on the top twelve spam relaying countries over the last six months. According to its research, the impact of zombie computers is steadily rising - over 60% of spam is now generated from zombie computers - hijacked PCs infected by malware. This technique means that the culprits do not have to be in the same country as the innocent computers they are using to send their spam.

The United States remains the worst offender, but is relaying substantially less of the world's spam than it did a year ago. The top twelve spam relaying countries are as follows, with the figures in brackets denoting the spam relayed by each country in the same period in 2004:

April - September, 2005

1. United States	26.35%	(41.50%)
2. South Korea	19.73%	(11.63%)
3. China (incl Hong Kong)	15.70%	(8.90%)
4. France	3.46%	(1.27%)
5. Brazil	2.67%	(3.91%)
6. Canada	2.53%	(7.06%)
7. Taiwan	2.22%	(0.86%)
8. Spain	2.21%	(1.04%)
9. Japan	2.02%	(2.66%)
10. United Kingdom	1.55%	(1.07%)
11. Pakistan	1.42%	New entry
12. Germany	1.26%	(1.02%)
Others	18.88%	(18.10%)

The United States, South Korea and China still account for over 50% of all spam. However, Sophos researchers says that they have seen a sharp drop in spam sent from North American computers due to a number of factors, including jail sentences for spammers, tighter legislation and better system security.

"Efforts such as ISPs sharing knowledge on how to crack down on spammers, and authorities enforcing the CAN-SPAM legislation, have helped North America tackle the spammers based on their doorsteps. Some of the most prolific spammers have been forced to either quit the business or relocate overseas as a result," says Graham Cluley, senior technology consultant for Sophos. "The introduction of Windows XP SP2 a year ago, with its improved security, has also helped better defend home users from computer hijacking. The worry now is that devious spammers will turn to other net-based money-making schemes, such as spyware and identity theft malware to make their dirty money."

Feeling the impact of international awareness and country-specific legislation, spammers are increasingly turning to illegitimate providers to fuel their success and their key partners in crime are virus writers and hackers. By taking control of unprotected PCs, hackers can relay spam, launch denial-of-service attacks or steal user information, without the computer owners being any-the-wiser.

"There are fortunes to be made from the dark side of the internet, and spammers who are finding it harder to sell goods via bulk email are likely to turn to other criminal activities," adds Cluley. "What the chart reveals is that spammers and virus writers can exploit unprotected computers anywhere in the world to send out their unwanted messages - everyone has a part to play in the fight against spam."♦

WEB SERVICES ADOPTION ON THE RISE IN SINGAPORE

Web Services is gaining momentum in Singapore, as the collaborative technology stimulated some S$70 million investment spend, created more than 290 jobs and generated S$450 million in infocomm revenue over the past one year. With this, adoption of Web Services amongst businesses now stands at 14 per cent, up from 8 per cent in 2003.

Web Services has been identified as a key engine of growth for Singapore. IDC estimates that US$2.3 billion was spent worldwide on total Web Services Software in 2004, more than double the amount from the previous year. IDC expects spending to continue to increase dramatically over the next five years, to reach US$14.9 billion by 2009.

An instrumental driver of the adoption of the technology is WEAVE or Web Services Add Value to Enterprises, a three-year industry development program (2003 to 2006) driven by the Infocomm Development Authority (iDA) in partnership with the industry, to fuel Web Services developments in Singapore through seeding intellectual capital, research and development and infrastructure-building.

continues on Page 14

Chan Yeng Kit

iDA CEO, Chan Yeng Kit, said, "Web Services adoption has grown not just in numbers, but deeper and more extensively into key growth industries, transforming key growth sectors. We believe this trend will continue. From a little known technology less than five years ago, the technology has today evolved into a powerful business transformation tool embraced by forward-looking businesses that effectively deploy Web Services to help maintain their leadership positions in their respective industries."

Wider Sectoral Adoption

Today, leading industry players in the transport sector, such as Singapore Airlines (SIA), PSA Corporation Ltd (PSA) and the motor insurance industry (for example: AXA, NTUC Income, Asia Insurance, Mitsui Sumitomo, and Royal and SunAlliance) join others in the financial (like NETS, ABN Amro, Hong Leong); and lifestyle and entertainment (e.g.; SISTIC, NTUC Big Trumpet) sectors in embracing Web Services to raise the bar in customer service and business process re-engineering. Since its inception in 2003, the WEAVE program has helped 52 companies in these sectors.

To give Web Services a further boost in Singapore, IDA and the industry are working together to build higher skilled Web Services manpower, and address interoperability issues.

Under the WEAVE program, there are now more than 2,800 Infocomm professionals with Web Services skills and knowledge. Of this, some 633 have received professional certification. At the WEAVE seminar earlier this month, the first batch of graduates from the NICC Certified Web Services Professional (CWSP) program received their certification. Supported by IDA, the CWSP was launched in 2003, and aims to develop Infocomm professionals and re-skill them by meeting their career and skills-progression needs at all levels, ranging from Web Services developers to professionals, architects and consultants. NICC expects to certify 400 - 500 Infocomm Professionals under the CWSP over the next three years.

SOA (Service-Oriented Architecture) Centre to address interoperability issues

A multi-party collaboration involving IDA, Nanyang Polytechnic (NYP), Singapore infocomm Technology Federation (SiTF) and leading technology vendors, has come up with the region's first-ever Service Oriented Architecture (SOA) Centre, with the aim of encouraging wider adoption of web services technology in Singapore. The S$2.5 million centre, when ready over the next three months at NYP, will allow Web Services solutions providers to use the centre to test cross-platform interoperability applications. The technology vendors involved are Accenture, BEA Systems, Cisco Systems, Crannog Software, Ecquaria, Hewlett-Packard, IBM Singapore, iLOG, Mercury, Microsoft, NCS, Novell, Oracle, Parasoft, SAP, Singapore Computer Systems, SQL View and Sun Microsystems.

Edward Ho, Deputy Principal for Technology, NYP said, "With this partnership comes many great opportunities to promote and embrace SOA technology and to accelerate the adoption of Web Services-based SOA to the local industry. It will also serve as a platform to nurture staff, students and professionals with SOA technology skill-sets, through training and project development. We hope that through this Centre, there will be a more pervasive deployment of SOA technology and innovation in the industry."

Stephen Lim

Stephen Lim, Chairman, SiTF added, "In the SOA Centre, we have leading companies from our Web Services Chapter coming together to address the common challenge of interoperability. In the process, we are also helping to spur the development of the Web Services industry in Singapore, and promote its wider adoption. The SOA Centre will generate significant value, both to our participating members, but also to the industry at large, as it becomes a strategic resource to Web Services development, and to reinforcing the 'Made in Singapore' branding."

As a testing platform, the SOA Center will standardize quality procedures for enterprises to achieve overall improvements to their software quality. Furthermore, the knowledge base developed from testing these projects will be shared with all participating parties, thus raising the competency and expertise of web services developers in Singapore. The SOA Centre aims to test 60 projects over the next two years.

The NYP will manage the operations of the Center and provide the necessary lab facilities, as well as the necessary manpower required to enable the SOA Center to undertake verification and testing services. In addition, it will act as an incubator for innovations to be generated and conceptualized, leveraging the benefits of web services.©

By Shanti Anne Morais

NEW TECHNOLOGIES MAKE SPAM FILTER BETTER

Finally, Spam filters are adaptive. Spam free living is possible.

91 percent of all spam filter manufacturers use artificial intelligence (AI) based filters. This has been established by a market survey of "spam filters" by Absolit Dr. Schwarz Consulting. The study examines 47 products on their filter methods. "Today, who has spam mail in his inbox only has himself to blame. Modern filter methods block more than 99 percent of incoming spam mails, without loosing one single important e-mail ", says the e-mail expert Dr. Torsten Schwarz.

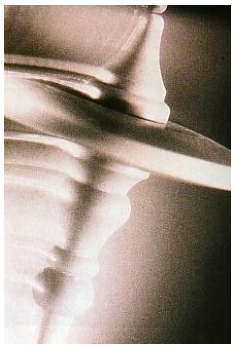
The approach of the artificial intelligence uses heuristic filters to arrange e-mails in mostly predefined classes (spam, no spam). In doing so, the self-learning filters compare new messages to already learned facts and as a result determine whether an e-mail is spam or not.

An excessive use of special characters and capital letters, hidden HTML texts, unsubscribe lines (supposed possibility to opt-out from the list) and a high frequency of certain catchwords can be indicators of spam. These attributes are weighted with a score, which classifies an e-mail as spam if it crosses a specific number.

" Once the filters are trained, they adapt further on their own and even fit themselves to new techniques of spammers", says Janine Bonk, the author of the study. The filters orientate themselves by monitoring the typical e-mail behavior of the user. If, for instance, the user works in a bank, e-mails which contain repeatedly the word loan or the dollar-sign are not defined as spam. The quality of the filter depends highly on the quality of the training. If a filter is not well coached, it can generate a high interest in false positives. Most filters are already pre-trained when purchased, but matching with one's own e-mail behavior must still be adapted. That's why it takes a little bit time until heuristic filters work perfectly. ♦

By Dr. Torsten Schwarz
ABSOLIT Dr. Schwarz Consulting

THE DEATH OF PRINT – A PROPHECY



The disappearance of print will come sooner than you think! Electronic media will be continuously on the rise! Believe it or not – the statistics speak for themselves.

According to IDC, online advertising revenue in Asia is projected to grow more than 400 percent to 1.62 billion US dollars by 2007 from 304.3 million dollars in 2002.

And it's predicted that the trend to search online for information will increase enormously—turning the pages of newspapers, magazines or the Yellow Pages will be a thing of the past.

Savvy Asian media organizations are already investing in Internet technologies to integrate Internet advertising with their business operations as there are projections going around that online advertising revenue will reach 789.6 million dollars in 2007, and search advertisements, classified ads and e-mail marketing will grow to 832.4 million dollars.

In an industry where digital revenues are overtaking print, publishers are confused and are struggling to find the most promising direction for their business. Although many traditional companies in Asia are still skeptical about the Internet economy and are avoiding online advertising, the change cannot be stopped. It started last year, when the use of rich media in digital publications grew by more than 180%. No wonder, as the advantages of online advertising can be quickly summarized: Online ads are efficient, accountable, targeted, offer a superior return on investment, save the environment and costs as its paperless, and help to build brand awareness.

The widespread acceptance of digital media by the new generations, who prefer to self select their content in an increasingly fragmented digital environment, will mean the death of print. If there's a future for print at all, it's in decline as an advertising supported medium. The trend to more online publishing and less print publications simply cannot be stopped. In the mid-to-longer term, publishers will solely take advantage of the capabilities inherent in digital publications and print will completely disappear. ♦

By Daniela La Marca

INTERNET EXPLORER: THE REASON FOR MICROSOFT'S SPYWARE VULNERABILITY

Spyware gets access to computer systems through the deception or exploitation of software vulnerabilities. PC users are tricked as spyware often comes bundled with shareware or other downloadable software, which spyware producers tend to package with desirable software (e.g. music programs).

Spyware attacks frequently target security vulnerabilities in Internet Explorer and in the Microsoft Java runtime, simply because Internet Explorer is still the most widely used browser. Due to the fact that many computer systems are not up-dated, it creates an attractive entry point for spyware.

Windows-based computers can rapidly accumulate a great number of spyware components with fatal consequences. Besides privacy concerns it means loss of system performance, system instability, problematic Internet connection, and a lot of disturbing targeted advertisements. The interactions between spyware components cause the stereotypical symptoms reported by users—computers that slow to a crawl, overwhelmed by the loads of parasitic processes running on it. Moreover, some types of spyware disable software firewalls and anti-virus software, and reduce browser security settings.

Some PC users have become so frustrated with all this that they have switched from Internet Explorer to another web browser (such as Opera or Mozilla Fox) because of security concerns and spyware respectively. Although alternative web browsers are vulnerable as well, Internet Explorer has contributed to the spyware problem specifically in two ways:

1. Many spyware programs hook themselves into IE's functionality (as a Browser Helper Object or a toolbar);
2. Malicious Web advertisers have frequently used security holes in Internet Explorer to force the browser to download spyware.

Internet Explorer users can improve security by keeping security patches updated, and by altering settings in the browser — particularly those disabling scripting technologies such as ActiveX.

The newer version of IE comes with the Windows XP Service Pack 2 and has substantially-improved security defaults, although spyware infections can still occur. Spyware, along with other threats, has led some former Windows users to move to other platforms such as Linux or Apple Macintosh.♦

By Daniela La Marca

BUZZword: Key Logger

A keylogger is software that copies a computer user's keystrokes to a file, which it may send to a hacker at a later time. Often the keylogger will only "awaken" when a computer user connects to a secure website, such as a bank. It then logs the keystrokes, which may include account numbers, PINs and passwords, before they are encrypted by the secure website.♦

Buzzword: Ratware

It's a fairly new term that is used to represent the underlying software used by spammers to achieve their objective of delivering large amounts of email in a short span of time.

Ratware (spammer's software) is capable of providing false or inaccurate information in SMTP dialogues with a view to impersonate, evade detection and spoofing.

Ratware is most often installed on Zombie computers through means of malware such as viruses, worms and Trojan horses. ♦

Buzzword: Drive-by download

A Drive-by download is a process used to install malware on the computer of an unsuspecting visitor. Some installers masquerade as a dialog box: the user clicks on it in the mistaken belief that it is an error report from its own PC. The "supplier" claims that the user "consented" to the download, though often the user is completely unaware that a download and installation has taken place. In some cases, spyware can be installed even if the user chooses any button, not just the "yes" or "accept" button. Users must be careful to ensure that they use the real "close window" button (better still, kill at root level - Ctrl/Alt/Del on PCs). In exceptional cases, the "maliciously crafted website" can exploit a bug in the browser to install the malware payload, without any user intervention whatsoever. To purists, this is the only case that genuinely deserves the term "drive-by download".♦

ROUND 2 OF SINGAPORE'S PROPOSED SPAM BILL AND DMAS VIEWS

Last month, the Infocomm Development Authority of Singapore (IDA), in collaboration with the Attorney-General's Chambers of Singapore (AGC) released it's much anticipated second public consultation paper on the proposed Spam Control Bill in Singapore. This second round exercise sought to gather feedback on the draft Spam Control Bill for Singapore and provides increased clarity on what constitutes spam. In addition, the draft Bill includes mobile spam and proposes that civil rights and remedies be granted to anyone who suffers loss or damage from non-compliant spam.

Key Features of the Proposed Spam Bill

The Inclusion of Mobile Spam

In addition to email spam, legal measures to manage mobile spam in Singapore have also been included. Given Singapore's high mobile penetration rate and the prevalent usage of mobile messaging, IDA consulted both the mobile telephone operators and mobile telephone marketers and examined the economics involved in mobile spamming. While IDA recognizes that the cost of sending mobile spam may be sufficient to deter indiscriminate mobile spamming, it is also aware of the difficulty for any mobile user to switch his mobile phone number for the purpose of avoiding mobile spam. The physical closeness and personal attachment of the mobile phone to the user further amplifies the negative effects caused by indiscriminate mobile spam activities. According to the iDA, mobile spam includes unsolicited, commercial electronic messages such as short text, graphics, video clips or sound files, sent to any mobile telecommunication devices. Consistent with email spam, an opt-out approach is recommended for mobile spam. The exclusion of unsolicited fax transmissions and telemarketing from the proposed Bill remains.

The Bill also proposes that anyone who suffers damages or loss arising from spam (both e-mail and mobile) be given the right to initiate legal action against non-compliant spammers. If found guilty, non-compliant spammers can be directed by the court to stop their spamming activities or pay damages to the affected parties. It was previously proposed that only service providers or organizations which operate its own servers could do so. As with all other legal proceedings, damages will need to be proven by the affected party before a court case can commence.

Civil suits can also be brought against non-compliant spammers or persons responsible for sending spam via the use of dictionary attacks and address harvesting software. If such persons are proven guilty, the court can order them to stop their spamming-related activities. They can also be made to pay damages amounting to the loss or damage suffered by the affected party or statutory damages of up to S$25 per spam message subject to a maximum cap of S$1 million.

The Direct Marketing of Singapore has been working closely with the iDA on the new proposed bill and giving their feedback and views. DMAS chairman, Lisa Watson says that the Association is in favor of self-regulation but fundamentally, they agree with the proposal, and that this makes everything related to spam more official. She adds that in permission-based it is important to have:

- **Transparency:** There needs to be transparent you are using data for marketing purposes. Do not trick people, this gives all marketers a bad name.
- **Consent**: Within this is opt-in versus opt-out. Ensure you always have this option. If a customer unsubscribes, make sure it is done in a timely fashion. Emarketers have to make a judgment call about how much consent the customer has given them. There should be an option for them to decline from being contacted for certain things like third party offers. Having options like this will improve the positive forms of your communication.
- **Proportionality**: As a marketer, you have the responsibility to adhere to the level of consent the customer has given you. Frequency comes into play here, and this should be up to the customer.

Stressing the opt-out version, the Association favors this because the U.S. system is a big opportunity for Singapore businesses or organizations. Watson says that Singapore business entities would have a big disadvantage if there is an opt-in system. This is especially so for small entrepreneurs because it is costly and time-consuming.

Watson notes that she believes that spam is less of a concern to her now than it was a year ago and this may be due to users receiving less spam, improved technology (for example, the ISPs have brought in spam-filter technology) and finally, because more emarketers are following email best practices, thereby ensuring that it remains an effective and viable channel. In addition, consumers are also learning how to handle emails more effectively.

She summarizes that the DMAS and especially its eMarketing Council represents the interests of the emar-

continues on Page 19

Spyware just messed with the wrong IT guy.

For spyware, it's the wrong place at the wrong time. Symantec antispyware solutions continually scan for, detect and remove spyware and other invasive code before they can create problems. Which means those unwanted programs that could accidentally be installed on your computers never get their virtual foot in the door. And you can deal with more important issues than nonstop popups, hijacked browsers, and frustrated users. Want to see how the right antispyware can keep your business protected and productive? Visit www.symantec.com/antispyware or speak with your Symantec Certified Partner.

BE FEARLESS.

symantec.

ANTI-SPYWARE LEGISLATION: WHEN WILL IT BE?

Currently, most governments of the developed countries are working on their anti-spam laws – if not already implemented - to protect their citizens and economy. And as if this wouldn't be enough work yet, spyware is appearing on the scene, which is in my opinion the most dangerous threat at all. Spyware is software that monitors your online activities, transmits gained information to remote servers and annoys you with pop up advertisements. Internet users are often unaware that spyware has been downloaded to their computers and owners of computers infected with spyware generally claim that they never authorized the installation. This problem has started to get attention from legislators, as gaining unauthorized access to a computer is illegal under computer crime laws.

As spyware is installed quite often bundled with useful and desired software (shareware) the producers of the malicious applications primarily argue in defense of the legality of their acts that, contrary to the users' claims, in fact consent to the installation is given. The legalese text of the end-user licence agreement (EULA) would include the description of the spyware. Spyware companies play with the fact that many users habitually ignore these purported contracts and insist that users have consented to the installation of their software. In addition, these EULAs seem to be made intentionally ambiguous with unobtrusive key contract terms and excessive in length. Such kind of agreements which cannot be binding could occur in the case of fraudulently installed spyware like e.g. drive-by downloads where the user receives no opportunity to either agree or refuse the contract terms.

Lawmakers should prohibit anyone other than the owner or operator of a computer to install software that alters Web-browser settings, collects personally identifiable information, monitors keystrokes, disables computer security software, or takes control of the computer (by accruing dial-up charges, or by opening a series of advertisements that can only be stopped by turning off the computer).

A "Spyware Control Act" should take into consideration:

- To force spyware manufacturers to notify consumers when their products include spying applications - the notice should describe what information would be collected and to whom it would be sent. The spyware would then be forced to lie dormant unless the consumer chooses to enable it.
- To force spyware manufacturers to ensure that the information gathered from their products is properly encrypted and adequately protected from malicious hackers.

To include some right-minded exceptions to the notice and consent requirements (if e.g. spyware is used to collect information that would only be used to provide technical support for the software, or to determine if a given user is a licensed user of the product, or for employers using spyware to monitor Internet usage by their employees etc.)

The fact is that sooner or later a law to control spyware has to be proposed and for sure it will be a challenge for governments to establish it appropriately.

At the inaugural Asian Internet Security Summit 2005, we intend starting the discussion about Asia's concerns to address the harms associated with spyware in an open forum targeted at the ICT industry, governments, and academia. Be part of this brainstorming session to STOP SPYWARE threats!♦

By Daniela La Marca

From Page 17— Round 2 of Singapore's proposed Spam Bill and DMAS views

keting sector and will promote and as protect it as a communication channel. One of its primary objectives is to help people and organizations use emarketing effectively. As she says, "We would hate to have Singapore become known as a spam nation." On a positive note, Watson says, "In Singapore, we find that the level of trust among consumers in emarketing is still high especially when compared to the US." She adds that as a very wired and online society, email and emarketing are a very highly used medium, yet "because we are such a small market, our direct marketing skills are not yet as sophisticated as some other countries like the U.S. where for example, they use email in a smarter way like testing what means is most effective, use teasers, reminders and so on.

Watson's hope for emarketing in Singapore is to ensure that the Internet remains a viable marketing channel for companies doing business here. "From a marketing perspective, it should be a bridge between the industry and the consumers", she adds.♦

By Shanti Anne Morais

ASIAN INTERNET SECURITY SUMMIT 2005

The goal of the event is a far-reaching analysis of SPYWARE & SPAM from a legal, economic, technical and organizational perspective.

DATE	**24th & 25th November 2005**
VENUE	**The Pan Pacific, Singapore**
FOR WHOM?	**Top management, key decision makers and professionals of the ICT industry**

HIGHLIGHTS

- Asian Anti Spam Symposium
- Asian Anti Spyware Symposium
- Open Forum & Formation: Asian Internet Security Task Force

Register NOW!

Seats are limited to 500 qualified participants.
Participation is free of charge.

Platinum Sponsor

symantec

Gold Sponsor

Computer Associates

Silver Sponsor

BlueCoat

Supported by:

Singapore Computer Society

Singapore Infocomm Technology Federation

Singapore Exhibition & Convention Bureau

SIG²

Suruhanjaya Komunikasi dan Multimedia Malaysia
Malaysian Communications and Multimedia Commission

Official Research House:

IDC
Analyze the Future

Conference Material Sponsor

CipherTrust

EDITORIAL

Dear Reader,

Nowadays, computers are more than ever vulnerable to all types of attacks and the need for security has grown tremendously. That's the reason why the focus of this quarter's issue of Asian eMarketing is dedicated to security threats and it especially gets granular on spyware and how to fight it.

Enjoy getting more insights and knowledge to protect yourself effectively!

I look forward to receiving your feedback at daniela@mediabuzz.com.sg

Best Regards,

Daniela La Marca
Editor, Asian e-Marketing

If you want to make sure that you receive Asian e-Marketing or recommend it to a friend please subscribe by visiting this link: http://www.mediabuzz.com.sg/subscribe.html

MediaBUZZ Pte Ltd respects the privacy of its readers.

If you no longer want to receive our e-InfoSource Asian e-Marketing follow this link, enter your email address and write unsubscribe into the subject line.

Empowering Asian eMarketing
Asia's Electronic Marketers

TEAM

Editor
Daniela La Marca

Contributing Editor
Shanti Anne Morais

Circulation Manager
Sean Wong

Graphic Designer
Evelyn Valente

Published
quarterly by
MediaBUZZ Pte Ltd
60 Havelock Road,
Tower A3
10-08 River Place
Singapore 169658

Tel: +65 6836 1607
Tax: +65 6235 1706

Empowering Asian eMarketing
Asia's Electronic Marketers