MessageLabs®

Be certain

Spyware: Know Your Enemy
White Paper

Mark Sunner, Chief Technology Officer, MessageLabs

Table of Contents

Introduction

Like Macavity, the fictional feline in T. S. Eliot's well-known poem, spyware may be considered to be responsible for a whole host of present-day crimes; but unlike the Mystery Cat, not all spyware is clever enough to leave no trace of its guilt – although that may already be changing.

This White Paper profiles spyware and prescribes the various ways organizations can meet the threat head on.

Spyware may be considered responsible for a whole host of present-day crimes.

History of Spyware

Firstly in terms of history – in order to better understand where spyware is going, or more importantly, where it's evolved from, we actually need to wind the clock back a lot further than may be first imagined; in fact, over fifteen years. If we look at the embryonic stages of the anti-virus industry, around sixteen years ago there were the first boot-sector viruses. It has taken this time for viruses as we've traditionally known them to evolve towards the more commercially viable, or intellectual-property-theft status that we now associate with contemporary viruses, a fact not realized by many. So only in the last few years have viruses actually stopped being mainly malicious and become about commercial gain of some kind.

This has only really started in earnest within the last four years, which is also quite compelling. We can pinpoint this transition back to the advent of the Sobig.A strain, in January 2003, the first virus that we could really say was all about commercial gain. Since then, much has happened, but we can also say that the profile of the person creating these viruses has changed profoundly. Only a few years prior to this were viruses such as Melissa or LoveBug in the year 2000. It was still largely individuals who were responsible and the goal was either malicious or to gain notoriety within those circles. With the advent of Sobig we see a wholly different type of person responsible – someone not motivated to write viruses or malware for malicious reasons, but motivated very much to create these weapons for commercial gain.

Viruses continued to be developed further and refined throughout the remainder of 2003. In 2004 significant outbreaks caused disruption on a massive scale, as writers started to get to grips with the technology, where we witnessed events like Sobig.F and MyDoom.A, and the NetSky vs. Bagle 'bot wars.' All of these events played themselves out on a world stage and became major blips on the radar as huge numbers of "zombie" computers were being infected and subsequently harvested. Without a doubt they were actually too successful from the writers' perspective – because they were too big as blips on the radar. The whole security community was very aware that these were in circulation, vendors were racing to issue patches, media sources were giving them more oxygen, and so the level of awareness in both corporates and home-users was high. People were responding quickly and updating their computers more rigorously than before.

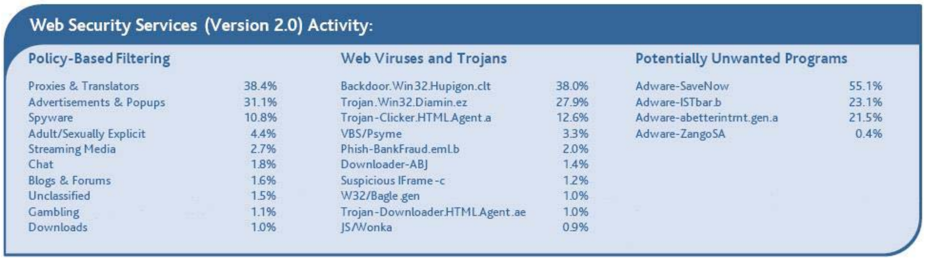
Throughout 2005, we saw the perpetrators rein the botnets in to become much more stealthful. Ostensibly, we have seen botnets shrink in size, but increase in number, with malware like Trojan horses being issued hidden inside Microsoft® Word documents and the like. They also relied much more on the social engineering aspects (or "head hacking"), to keep the attacks below the radar. So far, this entire backdrop has been about viruses, and when we look across at the spyware scene, there is something very important that needs to be taken into consideration. Spyware as we have come to understand it is, relatively speaking, very new, and has only really been with us for three or four years.

Around four years ago, we began to see the use of “pop-up windows” becoming more commonplace in the social engineering arsenal. For example, with a Browser Helper Object (BHO) installed with Internet Explorer, the BHO will have access to the same information as the browser itself. Now all of a sudden, a victim may be searching for something like a car on the Internet using their browser, and the BHO could then trigger a pop-up window to appear containing an advertisement for a car website. This was completely unprecedented, and now through the casual use of the Internet these pop-up windows when clicked-on could install some software onto the victim’s computer behind the scenes. The social engineering involved also paved the way for pop-up windows to spoof other windows and applications, such as an “ok” button, or a message suggesting the user has received an email – ‘click here to read,’ and so on.

What was already becoming known as spyware, or sometimes “adware” to countenance some legitimacy, could now hijack a user’s browser and install all kinds of unwanted software capable of snooping on that person’s browsing activities. This meant that the spyware was able to serve up advertizements depending on the user’s browsing profile. Pop-up windows consequently became a real nuisance for anyone who became a victim, and the software was already much more difficult to remove as the problem spread.

Spyware today

Bearing in mind that this all happened only a few years ago, and in a very short space of time, we can see that spyware has evolved rapidly. While these early incarnations still do exist, the more insidious forms of spyware are extremely stealthful. Contemporary spyware applications can tightly enmesh themselves into the Windows environment, comprizing several components. Removing just one element would not be enough and the software could automatically recover from a botched attempt to remove it. Specialist anti-spyware software was called for as it was already clear that traditional anti-virus software could not cope. A new battlefield had now been created and the lines were already being drawn.



Web Security Services (Version 2.0) Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Proxies & Translators	38.4%	Backdoor.Win32.Hupigon.clt	38.0%	Adware-SaveNow	55.1%
Advertisements & Popups	31.1%	Trojan.Win32.Diamin.ez	27.9%	Adware-ISTbar.b	23.1%
Spyware	10.8%	Trojan-Clicker.HTML.Agent.a	12.6%	Adware-abetterintmt.gen.a	21.5%
Adult/Sexually Explicit	4.4%	VBS/Psyme	3.3%	Adware-ZangoSA	0.4%
Streaming Media	2.7%	Phish-BankFraud.eml.b	2.0%		
Chat	1.8%	Downloader-ABJ	1.4%		
Blogs & Forums	1.6%	Suspicious IFrame-c	1.2%		
Unclassified	1.5%	W32/Bagle.gen	1.0%		
Gambling	1.1%	Trojan-Downloader.HTML.Agent.ae	1.0%		
Downloads	1.0%	JS/Wonka	0.9%		

Fig.1: Web threats from the MessageLabs Intelligence Report: Oct 2006

Contrast this with the virus landscape from which spyware evolved. The early pop-up ads are akin to the early forms of computer virus – and were for the most part nothing more than a benign annoyance. It has taken sixteen years for the commercial element to become involved and make them much more aggressive. Similarly, the same development lifecycle has taken place in the world of spyware in little under three years. This is very worrying, because it is way ahead of the type of adoption curve that the security community has traditionally been accustomed to.

What we are now seeing is the kind of spyware using more aggressive social engineering techniques, such as ‘drive-by-installs’. Just by casually searching for something and following the link from a search engine, the site immediately presents a pop-up box that suggests a virus or trojan has been installed on the user’s computer – click “ok” to remove it. Unfortunately, it is doing nothing of the kind – what follows is the installation of some adware, for which an adware company is paying someone a small fee, typically around $0.25 each time, to install their product. Of course this is supposed to be with the permission of the user, but by tricking people into believing that what they are actually installing is something quite different, they can bypass the end-user license agreement quite easily, thereby earning good money.

In many countries, adware is very close to the grey area between what is considered legitimate and what is not. It is often bundled with many other applications that purport to be free, such as popular peer-to-peer file-sharing tools like KaZaA (currently outlawed in Australia, pending a court case into alleged widespread copyright infringements by KaZaA users). This is generally made quite clear by the program makers that they use “ad-supported” revenue to finance the development of the application, but that there are often ad-free versions that can be purchased should the user wish. Such adware is able not only to generate advertizing banners and pop-ups, but also to send information about the user’s Internet surfing habits to third-party advertizing companies, slowing down the computer’s performance in the process – or in some cases causing the computer to crash.

In many countries, adware is very close to the grey area between what is considered legitimate and what is not.

So, in order to distinguish between adware and spyware, we need to look at the motivation behind the software as well as the means by which it came to be installed. This presents a problem for anti-virus software again, in that it cannot know how that software came to be installed on the user’s computer. It cannot know if the user granted permission in the full knowledge of what they were doing, or if the software is there as a result of visiting an unscrupulous website, or buried within another Trojan horse program.

Convergence and targeted attacks

Malware, botnets and spyware are all now inextricably interlinked; bot-controllers readily install adware and spyware onto their victims’ zombified computers and cyber-criminals are able to harvest an incredible amount of information on the user communities over which they have control, with potentially more knowledge on home users’ casual internet use than many large Governments! A computer thus compromised is tracking the user’s behaviour, recording passwords, online purchases and other preferences. Consider that any number of applications may come to be installed on the same computer, each one potentially bundled with some form of parasitic software. Over time the computer becomes engorged on this Internet baggage and performance is affected severely.

Carefully targeted attacks may go unnoticed for many months.

Businesses are increasingly being confronted by this problem. Despite these invasions to our privacy, however, and the profiling of our individual online habits in order to target us with more advertising, the major spyware goal right now surrounds intellectual property theft. As spyware evolves as such a rapid pace, it can also become increasingly more targeted. With the intelligence gathered in this way, it is possible to use that information to conduct further spear-phishing sorties, covertly gathering yet more confidential business information. Companies and individuals targeted in this way have no knowledge that they may be a target and where previously a virus outbreak may cause some disruption, a carefully targeted attack may go unnoticed for many months.

More recent examples include the use of "root-kit" type technology that enables the spyware to conceal itself from the operating system and from even some of the more advanced desktop anti-spyware or anti-virus applications. This is at the cutting-edge of virus development, but we are already seeing these techniques being employed by spyware, highlighting the fact that spyware is really at the sharp end of the more advanced developments. The purpose of course is to obtain access to the really high value data, from online banking and other commercial portals, including eBay and PayPal. As banks move towards embracing two-factor authentication schemes to counter losses from phishing, the criminals are expected to step-up development of very specialized spyware that will be able to remotely hijack online banking sessions after the user has authenticated using their secure two-factor devices. This is already a reality as examples of this were discovered two years ago, but traditional phishing techniques are still reaping the rewards, so it is only a matter of time before this becomes more commonplace.

With botnets becoming more agile and more difficult to uncover and disrupt, the connection between botnets and spyware is often overlooked. Botnets are being used to send out spam, viruses and phishing attacks directly to other victims; and spyware conversely resides on an individual computer and harvests information about the user. More recently, however, it is feared that by deploying spyware onto the individual zombie computers within a botnet, the botnet can be used to target these attacks more intelligently, targeting individuals within the botnet itself and the contacts harvested from the users' address books with spear-phishing emails, spam and viruses that appear to be more realistic. By profiling the users behind the zombie computers, the cyber-criminals can gather very personal information, such as age, sex, location, which bank and websites are used and use this information to target them. While the traditional view is of the bot as the spam sender, now the bots are also being profiled as recipients.

Only a year ago, spam was really thought of as 'big-bang,' a 'splatter-gun' approach that would result in millions upon millions of emails being sent. Phishing attacks would not specifically target only the customers of a particular bank or commercial website, but several attacks would be launched in sequence, targeting many different banks and organizations in the hope that one of them may strike a chord with the recipients. No attempt was being made to try and profile the recipients, so the actual return would be very low indeed, but with almost no overhead involved, this was of little concern to the criminals. However, what would happen is those attacks could be targeted? What if there were some way of mapping huge communities of people and profiling them into the appropriate categories of recipients? If the criminals could determine exactly who banked with which bank, what their name was, where they lived, what their address and telephone number were – with a little social engineering such as making a reference to a recent transaction, they could make their phishing attacks appear even more compelling, either via email or with a simple telephone call.

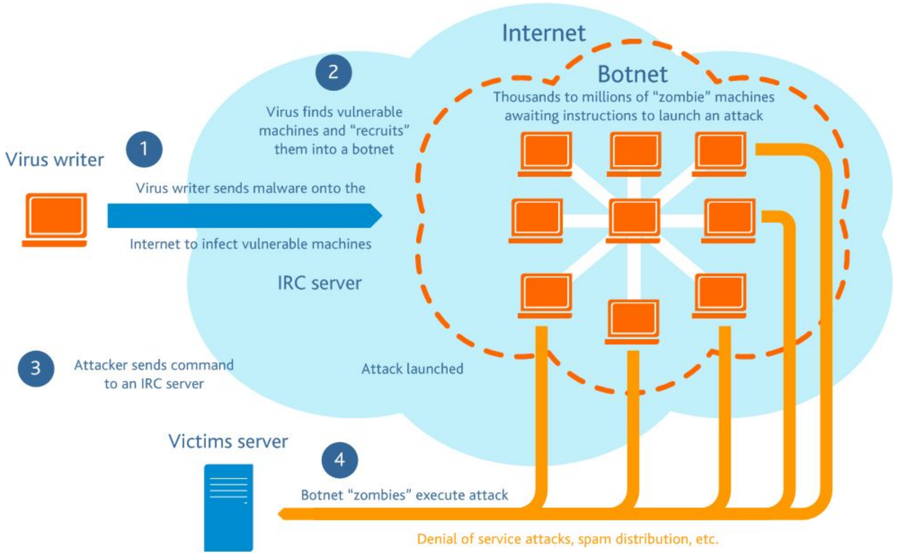

Internet
Botnet
Thousands to millions of "zombie" machines awaiting instructions to launch an attack
2
Virus finds vulnerable machines and "recruits" them into a botnet
Virus writer
1
Virus writer sends malware onto the Internet to infect vulnerable machines
IRC server
3
Attacker sends command to an IRC server
Attack launched
Victims server
4
Botnet "zombies" execute attack
Denial of service attacks, spam distribution, etc.

Fig. 2: Converging threats

There are already plug-in components available for some botnet code that will enable the controllers to decrypt stored passwords on a computer, including usernames and passwords that may be stored within the browser itself. This is often a useful facility that enables a user to bookmark their credentials for particular websites, including eBay, PayPal and many other sites. The information cached in this way is salted away in Windows Protected Storage, a special area for sensitive information, which is encrypted to secure the data from casual access by other applications or users that may have access the same computer. With the appropriate tools and resources, however, this data may be cracked with relative ease, remotely via the bot spyware software, and the information harvested.

Businesses that rely on Microsoft® Outlook and use Personal Storage folders, or PST files to secure data offline will be aware of the inherent insecurity and the ease with which it is possible to gain access to a supposedly encrypted email archive. Early waves of virus outbreaks that spread via email would use the address book of the recipient to further propagate to other users. No consideration was given for the potential value of this information in the early days, as it was used solely as means to spread the virus. Now, with access to local PST files, there now exists the very real possibility that the same spyware code controlling the bot will also be used not only to profile the victim, but also most of the people the victim corresponds with on a regular basis.

This is by no means stargazing, as much of the apparatus to achieve this already exists. It represents the cutting edge of how spyware has become intrinsic to the means by which bot technology converges further with viruses, trojans and spam, and the boundaries between them are now almost impossible to distinguish. For example, in a recent experiment a Windows XP SP1 honeypot computer was soon compromised and within a few hours was already attempting to send around 5-million spam emails per hour. In this case, the technology had been finely honed. The traditional botnet may be likened to peas in a tube; by pushing one pea in, another pea pops out at the other end. Botnets provide this degree of anonymity, but are not often very scalable. The latest techniques, on the other hand, use a mail-merge tactic that combines lists of harvested names and email addresses with email templates – all downloaded from a control server on demand – thus transforming the pea-shooters of old into a veritable “spam cannon.” By merging names and addresses in this way and using the advanced mass-mailing engines from viruses such as MyDoom or Sobig, millions of emails can be blasted out every hour from a single zombie computer.

Further analysis of this honeypot also revealed that the contact details were harvested from a number of different individuals’ address books, enabling the spammer to become much more targeted. If a user’s computer were compromised in such a way, the contacts in the address book would certainly expect to receive emails from the user’s address, and would be much more likely to have white-listed that user. Of course, anyone using online social networking tools integrated with their address books ensures that these contacts are always kept up-to-date.

Anti-virus software can only detect and prevent the installation of malicious software that it has some knowledge of.

Microsoft and Spyware

One of the big problems in this respect now is that much of the bot software in use is actually based on legitimate applications. Variants of open-source bots such as Agobot or Phatbot were firm favourites at one time, but are relatively easy to detect. A more fashionable approach is to use an IRC (Internet Relay Chat) client that can be controlled remotely using specialized scripts. A good example of this is mIRC – a popular, but powerful IRC client. Once installed covertly, it can be scripted to run silently in the background and connect to the command and control channel for the botnet, and yet remain undetected by the locally installed anti-virus software. Anti-virus software can only detect and prevent the installation of malicious software that it has some knowledge of. It is unable to determine how some legitimate software may have been installed on the computer – with or without permission – without entering a potential legal minefield.

Users behind firewalls are afforded a little more protection, but the built-in firewall enabled with Windows XP SP2 allows any outgoing traffic to the Internet unchecked. Once connected to the botnet any local countermeasures such as anti-virus, anti-spyware or firewall software can be rendered unusable or broken as part of the installation process.

Spyware is now such big business, an estimated multi-billion dollar industry. This has had the effect of creating a budding anti-spyware industry, which for the most part goes virtually unregulated. There is a glut of rogue anti-spyware applications available now, products that have dubious provenance and are of questionable value in offering anti-spyware protection. Some of these may be prone to high numbers of false-positives (mistakenly identifying something as spyware when it is not). Others may use inappropriate and misleading tactics to frighten gullible and confused users into parting with some money to increase sales. In many cases this software is touted by the same organizations responsible for creating the spyware and adware in the first place. Pop-ups purporting to alert the user to spyware detected on the computer may lead to more spyware being installed as we have already seen. In in order to remove the spyware, the user is also being asked to pay $50 for the privilege of purchasing and registering some rogue anti-spyware software to remove something that was put there by the same people.

Because of the lack of geography that the Internet brings, attacks can come from many directions, and of course they come from many different legal landscapes, including countries for which no regulation or legislation exists. The economic impact of fraud committed in this way may only be the tip of the iceberg as we consider what is possible when all of these techniques are combined to their full potential. Coupled with the ability for these attacks to surface from countries where no legal protection exists, the irresistible lure of such ill-gotten gains has become a quite potent impulse.

The terms “spyware” and “adware” are often confused and can mean many things to many people, especially those within the security community, and is in essence a relatively new term. What it actually means has also changed over time as the threat has evolved. Three years ago, what was considered “spyware” then often referred to nuisance pop-ups, and was relatively benign when compared to its modern-day progeny. As pop-ups progressed into browser tracking, “cookies” became anathema and a byword for spyware. Then, as the tracking of personal information advanced towards tracking more information more covertly, white-collar cyber-criminals, attracted by the lure of identity theft and online credit card fraud, joined the fray.

Over the years, Microsoft has sustained some considerable criticism as the creator of the world’s most popular desktop operating system – Windows – which continues to be targeted by cyber attacks. The recipe of global popularity and an ever-increasing threat, combined with a determined attitude to social responsibility, has led Microsoft to suggest that the next incarnation of the Windows – Windows Vista – “is engineered to be the most secure version of Windows yet.” With its much anticipated built-in security, Vista is expected to have as significant an impact in terms of security as the arrival of 32-bit Windows, with its “protected mode kernel” and “virtual 8086 mode” had over its 16-bit DOS-based ancestors in the early 1990’s. With improved memory management and process isolation and other built-in security measures including Windows Defender and an all new Vista firewall to safeguard outgoing as well as incoming traffic, Vista is expected to make it much more difficult for malware to exploit the underlying operating system.

Whether we will see viruses in the future engineered in completely different ways to exploit the new operating system, or whether the cyber-criminals will position their targets over other operating systems such as Mac OS X or Linux remains to be seen, and will largely depend on the global adoption of Vista over Windows XP. It is sometimes difficult to reconcile that possibility when many people around the world continue to use Windows 95 and Windows 98.

It is clear that viruses that work perfectly well against Windows XP or Windows 98 just cannot survive in the Vista environment, just as old DOS viruses couldn’t spread on Windows NT. Such attacks will need to be redesigned from scratch, perhaps affording some breathing space. Conversely, recent attacks are increasingly targeting application vulnerabilities, rather than attempting to exploit the underlying OS. In 2005 it became apparent that highly targeted attacks were using zero-day vulnerabilities within Microsoft Word to attack against certain businesses. These attacks could cause Word to behave in an unexpected way, deploying the hidden payload – a spyware application – undetected onto the recipient’s computer.

However, as everyone in the security industry knows, there is no such thing as a panacea that will make this problem suddenly disappear. It is likely that Vista will have an impact, but businesses are often slow to respond to major operating systems upgrades; just take a look at how long it has taken for Windows XP Service Pack 2 to find its way onto corporate desktops.

Deploying such upgrades can be a major operational and logistical problem for the IT department, and only after comprehensive testing with internal applications will the go-ahead be granted. Even deploying something as simple as anti-virus updates across a large organization is not without its own problems, requiring careful planning; many desktops may never be running with the very latest malware detection capability.

No matter how secure the operating systems become, no matter which operating system is in use, or which security software may be running; on balance, the weakest link in the chain will always be the user. Arguably, the problem can never be solved on the PC using technology – technology alone will never be able to control users' behavior. Perhaps in the short term cyber-criminals will lean more and more heavily towards social engineering, baiting users into making mistakes that will result in them losing confidential data. In the longer-term, security weaknesses will be uncovered, and viruses and spyware will find a way to further exploit the technology. It is only a question of time.

The traditional model for computing requires the operating system to control applications and users' access to the computing resources. However, more recently, on-demand computing has begun to etch-out a 'utility model' for the corporate computing environment, where different aspects of the computing resource can be 'virtualized.' For example, terms such as 'grid computing,' 'virtual storage,' 'virtual networking,' 'virtual hardware' are now becoming more recognizable vernacular when designing scalable operating environments for the enterprise.

Many businesses already deploy server-centric environments such as Microsoft Terminal Services or Citrix Presentation Server to provide greater centralized control to applications and access to networked resources. More latterly, 'application virtualization' software such as Softricity SoftGrid, allows applications to run independently of the operating system and independently of each other. This environment differs from "server virtualization" software, such as VMware Server or Microsoft Virtual Server, where the applications are still dependent upon the underlying OS in each virtual environment. With seemingly greater overheads required for each application to exist in its own virtual instance and never fully installed on the user's own system, centralized application virtualization is already being considered by some financial institutions as a more secure and controlled environment, and more importantly to safeguard against application orientated attacks.

Essentially the transition from a product-orientated environment to a services-orientated environment has also been endorsed by Ray Ozzie, the Chief Technology Officer at Microsoft, who has mandated that the company will move towards a services-based focus, including the Office productivity suite and the Exchange messaging and collaboration application. Of course this will take time, perhaps even years, but will affect the security landscape enormously. The application environment will be controlled much more rigorously as it will become less dependent upon the derivation of the desktop itself, thus making the job of the cyber-criminals much harder.

As domestic and small business bandwidth increases, reaching 20Mbps or more will also affect the way people use the internet and what may seem impractical now will almost certainly become a reality in a few years time. Email even ten years ago used to be considered a relative luxury – a corporate perk that could only be accessed from the office, and the possibility of being able to send an email to the person across the street was almost non-existent. And yet, in those past ten years, the whole developed world and a good portion of the undeveloped has become cemented on the internet and now email has become more prevalent than the telephone.

Remedies for Spyware

Until the internet can be considered a perfectly secure environment, in an Internet utopia based on a services-orientated architecture, businesses need to consider their security environment and move towards a services based model, now. This is the only way to fully counter the increasingly sophisticated and aggressive real-time threats that the cyber-criminals already have at their disposal.

The principal security defences should be concentrated on the ingress points rather than the desktop.

In the short term, a high-degree of vigilance can only prevail against some of the more contemporary attacks for so long. As cyber criminals become more organized and highly developed, attacks are becoming more targeted, using social engineering to bypass technological barriers. Even the most cautious amongst us may fall prey to such an attack; curiosity in humans, as in cats, can have a very powerful and dangerous influence – sometimes overtaking any consideration for safe computing practices. Accordingly, businesses must consider the primary conduit through which these threats flow in order to mitigate them effectively.

To do this securely, the principal security defences should be concentrated on these ingress points rather than at the desktop – where often it can already be too late when a breach occurs. Taking this to another level, protocol independent defensive countermeasures built into the Internet conduit itself will become the key component of any services-orientated solution. In the same way, domestic broadband connections are the most heavily abused in terms of botnet dispersion, and in turn home users will be looking to their ISP to provide solutions at the Internet level itself as well.

We already know that the time between a vulnerability being disclosed and an exploit created to capitalize on that vulnerability has all but vanished. Only two years ago, it could take several months for an exploit of a new vulnerability to be created and appear in the public domain, but now with so much at stake, it only takes days. Rather than buying ‘zero-day’ exploits to use in their attacks, cyber-criminals are now investing in their own research and development to uncover new vulnerabilities and keeping them very much to themselves in order to create new exploits before they become public.

Over time, legislation and enforcement in this area will improve and through greater international cooperation and coordination it will become much more difficult for the cyber-criminals to exploit the differences in cross-border jurisdiction. However, this is fundamentally a technical problem and as such will always require a technical solution, first and foremost. By addressing the problem ‘in the cloud’ at the Internet level, it is taking the fight one step closer to the criminals.

Not only does tackling the issue inside the fabric of the Internet itself take the struggle just that bit closer to the source of the problem, it also enables such an approach to stand back from the minutiae and cultivate a more refined understanding of the wider nexus.

Only when technology has caught-up will the criminals realize that they can no longer hide behind the mystique and the antiquated technology we have become accustomed to. As the Internet of today becomes the Internet of yesterday only then can legislation itself become a deterrent.

Although many companies have already tightened their security as a result of increasing attacks, there is still room for improvement beyond reactive security software. The reality is that traditional anti-spam and anti-virus solutions are providing inadequate protection that can and are being easily circumvented by criminals who are one step ahead of contemporary security systems that only combat existing, known threats.

For a business, there are many benefits of using a service that controls content, enforces company policy and delivers value to enterprise messaging within the Internet level. With no hardware or software required by the customer, time and resources are saved, in-house IT resources are released, employee productivity is increased and the efficiency and operability of email systems is enhanced. This in turn can raise network utilization levels through reduced email volumes and place less demand on Internet bandwidth. With constant monitoring and analysis of the evolution of threats and as businesses adopt best practices in email security, the virus and spam problems can be eliminated. This leaves security specialists like MessageLabs to combat the next generation of cyber criminals.

www.messagelabs.com
info@messagelabs.com

Freephone UK
0800 917 7733

Toll free US
1-866-460-0000

Europe
HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom

T +44 (0) 1452 627 627
F +44 (0) 1452 627 628

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom

T +44 (0) 207 291 1960
F +44 (0) 207 291 1937

NETHERLANDS
Teleport Towers
Kingsfordweg 151
1043 GR
Amsterdam
Netherlands

T +31 (0) 20 491 9600
F +31 (0) 20 491 7354

BELGIUM / LUXEMBOURG
Cullinganlaan 1B
B-1831 Diegem
Belgium

T +32 (0) 2 403 12 61
F +32 (0) 2 403 12 12

DACH
Feringastraße 9
85774 Unterföhring
Munich
Germany

T +49 (0) 89 189 43 990
F +49 (0) 89 189 43 999

Americas
AMERICAS HEADQUARTERS
512 Seventh Avenue
6th Floor
New York, NY 10018
USA

T +1 646 519 8100
F +1 646 452 6570

CENTRAL REGION
7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA

T +1 952 886 7541
F +1 952 886 7498

Asia Pacific
HONG KONG
1601
Tower II
89 Queensway
Admiralty
Hong Kong

T +852 2111 3650
F +852 2111 9061

AUSTRALIA
Level 6
107 Mount Street,
North Sydney
NSW 2060
Australia

T +61 2 8208 7100
F +61 2 9954 9500

SINGAPORE
Level 14
Prudential Tower
30 Cecil Street
Singapore 049712

T +65 62 32 2855
F +65 6232 2300