STATE OF SPYWARE Q3 2005

An in-depth review and analysis of the impact of spyware, adware and unwanted software on consumers and corporations.

webroot
SOFTWARE, INC.

TABLE OF CONTENTS

webroot
SOFTWARE, INC.

FOREWORD

A Matter of Trust

This past quarter marked the 10th anniversary of Netscape's initial public offering. It seems incredible that the Internet, as we now know it, is only 10-years old. The home computer and access to the Internet represent the same new ubiquity in contemporary American life that the television did in the late 1950s and early 1960s. The Internet has woven itself into the fabric of American life and its presence in our constant interaction with each other and with the business of our daily lives seems inextricable.

Or does it?

The future may hold some tribulation. According to a recent survey by Consumer Reports released this quarter, web shoppers -- the lifeblood of the commercial Internet-- are shying away from online commerce, fearful that their personal data -- credit cards or other identifiable information -- may be compromised. In other words, spyware is striking at the faith consumers have in the Web.

Here are some highlights:

- Nearly nine out of 10 users (86 percent) have made at least one change in their behavior because of a fear of identity theft.
- 30 percent say they have reduced their overall use of the Internet.
- A majority of Internet users (53 percent) say they have stopped giving out personal information on the Internet.
- 25 percent say they have stopped buying things online.
- 29 percent of those who shop online say they have cut back on how often they buy on the Internet.

The Consumer Reports study points to a significant crisis of confidence in the Web, the impact of which has yet to really show itself, but it can't be good. Shopping is a huge part of our collective Internet experience. Brands and experiences that were born in the economic boom of the last decade are now almost iconic. Amazon has become so much more than a troubled rain forest, and Yahoo has changed from a joyous exclaim to an advertising strategy. Google means search just as Xerox means copy or Fedex means to

send overnight. Today, there are online giants, like eBay, whose only provenance is the Web; not to mention the brick and mortar companies that have embraced online commerce, like Target.com.

So let's imagine if one in every four people in your community stopped going to the local mall. And then another quarter cut their mall shopping by half. How long would that mall survive? And it goes beyond just shopping. Nearly a third of the respondents are so fearful of identity theft that they have reduced their use of the Internet all together. Not only are they afraid to go to the mall; they don't want to leave the house!

As an industry we have an obligation to our consumers to restore their faith in the commercial prospects of the Internet. We have advocated vigilance since we first discovered this nemesis called spyware, but we fear this is too blunt a response: cutting the e-tailing nose to spite the face of the Internet and all its many advantages. We are making major progress in the fight against spyware, combating every punch with a counter punch and anticipating many blows with a deft duck out of the way. If the fight has become a matter of trust, we hope the industry as a whole can convince consumers that with proper protection, the Net is safe and trustworthy.

For corporations, the issue is more complex, because trust is a regulated issue. To ensure healthcare records or credit information is kept confidential, corporations must comply with strict standards. So employees, consumers, patients, and investors count on vital information remaining confidential and trust the enacted legislation has outlined policies in their best interest as well as the corporations' best interests.

But professionals responsible for maintaining those confidences still worry about the potential impact of spyware. This quarter, Webroot polled professionals managing the information security compliance initiatives in various corporate organizations. Nearly all (98 percent) thought spyware was a threat to their organizations; over two-thirds thought it was a serious threat. More than 80 percent said the worst kinds of spyware (keyloggers, system monitors and Trojan horses) that can access confidential records represent an immediate threat. And the vast majority (97 percent) worry that spyware

could access employee data, pilfer intellectual property, or access company or customer information. However, despite these figures, many corporations surveyed have yet to protect their information with suitable anti-spyware software.

The compliance issue is tricky. Many corporations have dealt with the hassle of adware and many have deliberately protected their corporate assets with enterprise-class solutions to ensure against some unfortunate intrusion. But the threat of being non-compliant with Sarbanes Oxley, HIPAA, Gramm-Leach-Bliley or even the FTC can impact corporate issues far beyond productivity or even the loss of intellectual property. The matter of trust cuts both ways: do you trust personal data to a company whose security policies may or may not fully protect that data? And can corporations trust that without this kind of protection that they are in compliance?

Clearly, their own staffs have doubts.

We may be entering a new era in the spyware fight. Malware -- Trojan horses, system monitors and the like -- are hovering at or above the infection rates we've seen for the past few months. So maybe consumers have a reason to be apprehensive and maybe compliances officers should worry. But it is the responsibility of the entire industry to regain the trust of consumers and assuage the concern of compliance officers. There is a consistent dialog about whether spyware is a verifiable risk. Should we be concerned about potential risk to our networks and consumer PCs posed by identity theft or threat to compliance issues? Perhaps the risk issues should be characterized differently: If we as an industry cannot address the eroding trust among users we risk not only the theft of credit cards or potential non-compliance, we risk the overall health of the 10-year relationship we all have with the Internet.

C. David Moll
CEO
Webroot Software, Inc.

HIGHLIGHTS

News & Incidents

Global industrial espionage continued to make headlines when U.S. government officials revealed "Titan Rain," an attack on hundreds of U.S. computer systems. Two infamous security breaches that occurred last quarter remain in the news with indictments filed in the Israeli Trojan horse scandal and CyberSource's announcement of their plans to acquire CardSystems, following the largest known data security breach that compromised 40 million customers' data. – page 14

Threat Research/Phileas

Techniques used by spyware writers evolved in complexity during the course of the year. In addition, there has been a large amount of innovation in spyware's ability to evade detection and removal by using polymorphic code and rootkit technology. Spyware authors have increased their installed user-base by utilizing security vulnerabilities and aggressive, persistent, and misleading informational displays that trick users into installing spyware on their computers. To make matters worse, removing new and morphing spyware is nearly impossible without kernel-level technology. – page 20

Enterprise and Compliance

Results from both Webroot and Computerworld spyware surveys reiterate the same message: enterprises are consumed with keeping desktops free of spyware. In fact, 83 percent of IT managers agreed that keyloggers, system monitors and Trojan horses pose an immediate threat to compliance initiatives. It's with good reason that enterprises continue to focus on removing spyware. Just one malicious program can compromise compliance with the FTC, Gramm-Leach-Bliley Act or HIPAA. – page 36

Consumer

Consumer SpyAudit results offer new visibility into the global spyware epidemic. Home computer users in United States, Thailand and United Kingdom had the highest infection rates. Trojan horses and system monitors on PCs are threatening the security of individuals' privacy and negatively affecting e-commerce. According to a Consumer Reports survey, 86 percent of Internet users have made at least one change in their online habits out of fear of identity theft. – page 53

Legal & Legislation

Spyware is a point of discussion for legislators and legal scholars around the globe. In the United States, the FTC launched "OnGuard Online" to educate consumers about online risks, such as spyware. In addition, the FTC filed a spyware case against Odysseus Marketing. Five federal spyware bills and six state spyware bills are pending action. Eight state spyware laws went into effect during the third quarter of 2005. – page 64

THE STATE
of Spyware

During the course of the third quarter of 2005, two important and alarming spyware trends emerged. First, many home computer users are admittedly afraid of becoming a victim of identity theft from using the Internet. Secondly, enterprises are at risk from legal action for failing to prevent spyware from attacking their networks or capturing data.

According to a recent Consumer Reports WebWatch, 86 percent of Internet users have made at least one change in their online habits out of fear of identity theft.

As consumers lose faith in the Internet, e-commerce is directly affected. In addition to limiting time spent surfing the Web, 25 percent of users say they have stopped shopping online altogether.

Spyware concerns are likely behind the growing skepticism, and spyware purveyors are only making matters worse. Despite claims by some adware vendors that they are cleaning up their behavior, many adware vendors use increasingly sophisticated techniques to install programs that are harder to remove than before.

Polymorphic code and rootkit technologies are making their way into the spyware writer's toolbox. Finding and eradicating programs that use these techniques is forcing continuous improvements to anti-spyware engines. This rapid pace of innovation has no end in sight.

The rise in malicious spyware on the desktop, including an 8 percent infection rate in the enterprise as reported by Webroot SpyAudit, is a clear indicator that there are richer fields for cyber-criminals to harvest than the annoying, but relatively harmless adware techniques.

The second spyware trend this quarter focuses more on enterprises and the emerging threat of legal liability for failure to protect against spyware attacks. With consumer notification laws in place in many states, legal action seems inevitable whenever a security breach is discovered.

Furthermore, with the risks of legal action from the Federal Trade Commission, Gramm-Leach-Bliley Act and HIPAA, enterprises need to be hyper-vigilant to monitor security threats as they arise and implement new protective measures when needed.

Enterprises must recognize that back door Trojans, system monitors, keyloggers and adware programs all pose a technological threat to their network. The lurid and well-publicized Israeli Trojan horse incident offered increased visibility into corporate spyware espionage.

While spyware incidents continue to make their way in to the news, the most chilling revelation, dubbed “Titan Rain,” was that Chinese hackers have been systematically launching attacks against American and British resources using system monitors to infiltrate private networks and steal critical information.

It’s important to note that for every publicized spyware attack, many more have gone undetected or unreported by their victims.

The trends are evident. The overall threat to Internet security is rising dramatically as malware is produced for the purpose of stealing information for financial gain.

News
& Incidents

"Titan Rain" Attack and Global Industrial Espionage

On August 25, 2005, U.S. government officials revealed that they were investigating "Titan Rain," an attack on hundreds of U.S. computer systems, including the Departments of State, Homeland Security, Energy and Defense. "Titan Rain" was just one part of a coordinated series of hi-tech attacks on key parts of the world's vital Internet infrastructure. The attacks intended to steal information from computers that would make the perpetrators millions of dollars.

The attacks intended to steal information from computers.

In each attack the method of stealing the confidential information was the same – keystroke logging, a form of spyware that is the equivalent of the skeleton key for the housebreaker or the office thief.

The perpetrators of "Titan Rain" sent e-mail messages containing spyware to the victims. The messages were deliberately written in a manner to compel the recipients to open these e-mails. Analysts working for American and British authorities revealed that the addresses were obtained using viruses previously sent to infect the system.

The criminals left very little to chance. The payload - the Trojan program and keylogger software - was tested against computers loaded with the very latest security software to ensure they would not be detected. As a security source put it: "They are handcrafted and bespoke so they are not on the anti-virus radar."

Britain and the United States are not the only targets. A U.K. spokesman for the National Infrastructure Security Coordination Center says grimly: "We know this is affecting 50 countries - it could be seen as an attack on the Western World." The undoubted aim is to steal vital information that can help rival businesses and organizations catch up with competitors.

This is industrial espionage on a global scale.

This is industrial espionage on a global scale.

Though no one can be completely sure who is behind the attacks, the gang is thought to have the support of or even be backed by a country.

These crimes are a sign that hi-tech criminals now regard everyone as their victim, householder or business, big or small. Even governments are being targeted. For many businesses and individuals this means a rogue program is hiding on their system copying vital information and passing it on to a criminal.

As a computer security expert and former senior FBI agent explains: "The main part of any cyber-criminal's armory at the moment is keyloggers and other spyware. These are the ways to get additional permissions or take over someone's machine."

"The main part of any cyber-criminal's armory… is keyloggers and other spyware…"

Q2 Incidents Update

Israeli Trojan Horse Scandal

As reported in the Q2 State of Spyware Report, in early July, an Israeli prosecutor filed indictments against nine private investigators involved in the industrial espionage case that involved planting malicious Trojan horses on competitors' computers.

The indictments accuse the nine men of industrial espionage, fraudulent receipt, uploading computer viruses, hacking computers with criminal intent, use of wiretaps, invasion of privacy and managing an unauthorized database.

The Trojan horse scandal came to light following an Israeli author's discovery of his unpublished works posted on the Internet. Many stories are surfacing about other individuals and businesses experiencing the same invasion of privacy.

Authorities accuse the private investigators of using two relatively simple attack methods to easily bypass basic security safeguards. One method involved sending a targeted individual a disk that supposedly contained a business proposal. When the victim inserted the disk, however, it would install Trojan horse software on the individual's computer. In other cases, the same process occurred, but the method of delivery was an e-mail instead of a disk.

Companies hired the accused private investigators to gain a competitive advantage over other companies. For example, satellite broadcaster HOT, one of the targeted businesses, sought an injunction against rival broadcaster YES. YES allegedly hired some of the accused private investigators. The injunction bans YES from using any of the information obtained from the spyware attack.

CardSystems Acquired After Security Breach

Following the enormous security breach in Q2 2005, the infamous CardSystems Solutions Inc. is now on the auction block.

CyberSource announced it signed a letter of intent to acquire CardSystems late in September. It is widely rumored that CyberSource will acquire CardSystems at a great discount as to what the price would have been before the security breach.

The breach at CardSystems, the largest known data security breach in the United States, compromised data on 40 million customers. At the time of the incident, 120,000 merchants used CardSystems to process more than $18 billion worth of transactions annually.

CardSystems CEO John Perry admitted that the company stored its records improperly. The blame may not have fallen so heavily on CardSystems if they had taken better security measures.

Following the data theft CardSystems admitted it had violated its contracts with VISA, American Express and other merchants by failing to encrypt credit card transaction data and by storing card verification numbers, which were never supposed to be saved.

Both American Express and VISA responded to CardSystems' admission of guilt by announcing they would terminate their relationships with CardSystems by the end of October. MasterCard will continue its affiliation with CardSystems, but established certain security requirements CardSystems must meet.

CyberSource stressed that the deal is far from final. Its acquisition of CardSystems is still "subject to further due diligence, execution of a purchase agreement, satisfaction of closing conditions and may also be subject to governmental or other regulatory approvals."

If the sale goes through it is unlikely the CardSystems name will remain. That's not the only thing that will die with the deal. Because CardSystems and its senior management violated key provisions of contracts and have not announced any punitive measures, the organization has been widely criticized for failing to accept responsibility.

If VISA or American Express rescind their termination announcements, the deal could be even sweeter for CyberSource. Some say the terminations could cause the deal to fall apart.

No business wants to be known as the next CardSystems.

If all goes well, the deal could be closed before the end of the year.

The publicity from information security breaches have likely resulted in information security investments, such as enterprise anti-spyware solutions, becoming a top priority for business. Instead of the threat being merely theoretical, it is now a viable concern across organizations. No business wants to be known as the next CardSystems.

CSI/FBI Computer Crime and Security Survey

According to the tenth edition of the CSI/FBI Computer Crime and Security Survey security breaches are increasing as is the amount of financial damage these intrusions cause.

Many intrusions are never reported because of the fear of negative publicity.

It is difficult to fully rely on the data that reports security breaches as many intrusions are never reported. Almost half of those surveyed by CSI/FBI (43 percent) did not report security breaches to law enforcement because of the fear of negative publicity.

The concern that negative publicity would hurt their stock or image outweighed the need to recover their financial losses. A third of those surveyed were concerned that competitors would use the attack to their advantage.

The implicit costs of spyware-related security breaches are hard to determine as lost future sales due to negative media coverage following a breach is difficult to estimate.

Respondents to the CSI/FBI survey reported the amount of money lost to unauthorized access to information and theft of proprietary information as greater than ever before – intrusions cost businesses over $300,000, an increase of almost $200,000 just this year.

Even after organizations discover and remove security intrusions, it is nearly impossible to fully assess the extent of the damage or how much confidential information was stolen.

The reported financial losses are minimal compared to the potential long-term financial and public relations damage. The potential fallout for a business struck by a spyware attack is enormous. Seventy percent of all companies go out of business after a major data loss.

70 percent of all companies go out of business after a major data loss.

Perhaps the most frightening development of the third quarter – not only do employers have to monitor computer use to make sure employees are not unwittingly exposing organizations to spyware, but they also have to be increasingly aware that employees are purposefully perpetrating security intrusions.

Organizations must be prepared for attacks from both outside their organizations as well as from within. Security breaches are not always the work of an inside job, as is commonly thought. Respondents detected events orchestrated by insiders about as often as outsiders.

More than half of respondents' organizations detected unauthorized use of their computer systems in 2005, a jump of three percent this year to 56 percent.

THREAT
Research/Phileas

Threat Research

Advanced techniques used by spyware have become more prevalent and more complex over the course of the last year. Spyware authors have increased their installed user-base by utilizing security vulnerabilities and aggressive, persistent, and misleading informational displays that trick users into installing spyware on their computers.

Many of the adware companies seeking the "legitimate" label from anti-spyware vendors still make use of the very reliable "bundled" approach where their adware is included with a free application.

There has been a large amount of innovation in spyware's ability to evade detection and removal. Spyware has been developed to operate under the radar, avoiding all but the most sophisticated detection, firmly implanting itself into programs and computers so that even with expert assistance, users are unable to remove spyware from their computers.

There has been a large amount of innovation in spyware's ability to evade detection and removal.

Techniques like polymorphic code, which enables spyware to change its code repeatedly, require sophisticated detection and removal techniques to mitigate against false positives. Polymorphic code can be easy to implement and requires dedicated researchers to create proper detection and removal procedures on a case-by-case basis.

Spyware Installation Methods

The traditional delivery method of bundling spyware with desirable programs is still widely used. Recent spyware bundles do not offer the option to opt-out of a spyware installation. Additionally, users may be presented with an end-user license agreement (EULA) that can exceed hundreds of pages, and often have to be thoroughly read to determine if something undesirable will be installed.

As users visit malicious Web sites, they are often inundated with pop-up advertisements, browser plug-ins, add-ons, extensions, ActiveX controls, Java applets, and automatic downloads, which may be poised to install something undesirable on an unsuspecting user's computer.

Some of the deluge of unwanted programs can be avoided if the security settings of the Web browser are high, making acceptance by the user the exception rather than the rule.

Spyware authors have found ways to trick users into providing their explicit consent by displaying misleading messages that suggest their plug-in is required to visit a Web site. Some Web sites will repeatedly attempt to install an add-on, even if the user has already clicked "No" or "Cancel," thus requiring the user to shut down their browser or their computer in order to prevent the malicious program from installing.

Spyware authors have found ways to trick users into providing their explicit consent by displaying misleading messages.

The most devious method of installation takes advantage of security vulnerabilities in Web browsers or the operating system. Web sites commonly include specially crafted Java applets, Windows help files, or animated cursors which can be loaded with code that allows spyware to be installed without user interaction. For this inadvertent installation to occur, the user merely visits a site with a Web browser that has not had the latest security patches installed.

Avoidance of Detection and Removal

Spyware writers are continuously searching for new ways to avoid detection and removal once they are installed. Attempts may involve changing file names, folder names, registry names, self-modifying code, or adding components to their payloads to avoid distributing fingerprints that can be easily identified. This is typically accomplished by the Web server, which changes each file prior to its download, or by the installer, which changes files before installing them on the computer. This method of installation is often used to prevent easy detection of malicious components on a computer.

Spyware also uses more advanced methods to evade removal, including "watcher processes." This technique involves multiple components of spyware running simultaneously on the infected computer. Each component continuously checks for the presence of its other components and can re-install them on the computer if they are removed. Sometimes these components lay dormant on the disk and can avoid detection by only executing at Windows startup.

Spyware also has evolved to have greater access and full control over the user's computing environment. These pieces of spyware can execute as a service with system-level privilege or, even more aggressively, as a driver that executes in-line with the core of the Windows operating system.

Spyware also uses more advanced methods to evade removal, including "watcher processes."

Most recently, spyware authors have started injecting their code into other non-spyware processes such as Windows Explorer, or other system components. This is typically achieved by loading a Dynamic Linked Library (DLL) within a running process. Newer techniques create a thread within a legitimate process that runs independently of the process but have no associated file on disk. Using any of these methods can make it nearly impossible for users to detect spyware without assistance from an advanced application.

Enterprises and home computer users alike need to use an anti-spyware program with the ability to delete spyware programs attempting to evade detection and removal. The most advanced generations of anti-spyware programs use adaptive recognition practices to remove processes, applications or files that may have changed during the remediation process or may not have been previously detected.

Evolution to Driver-based Techniques

Initially, spyware was composed of a "Run" key within the registry or an INI file entry and a running executable; cleaning up an infection required closing the executable and deleting the entry. Later, spyware advanced by relying on obfuscation techniques such as injectable threads and API hooks. These techniques, while more advanced, are easily detectable and removable. The new breed of spyware has evolved to a level where detection and removal has become extremely difficult.

Since the introduction of driver-level rootkit procedures, we have seen trends in spyware using similar techniques to obfuscate and protect themselves from detection and removal.

The line between spyware and rootkits is becoming increasingly blurred, as spyware uses techniques previously employed by rootkits. Rootkits can hide an intruder's presence and actions; therefore, spyware using rootkit techniques has become the next evolutionary step. Spyware is now using more Ring-0 or driver-level techniques, including lower-level API hooking and kernel hooking.

These procedures allow the spyware to go below the operating system and physically alter the data being sent between the user and computer, making new detection and removal techniques increasingly important to stay ahead of the threat.

These procedures allow the spyware to go below the operating system and physically alter the data being sent between the user and computer.

When an application sits at this level, spyware has complete control of an entire computer, and it can hide data and files as well as its own actions. Detection and removal of spyware that uses a driver is more difficult because any data that Windows returns may be invalid since it may have been modified by the spyware application's driver.

Anti-spyware software armed with an advanced spyware removal engine to delete the toughest spyware programs is required for all computer users. With a solid removal engine, anti-spyware programs can remove even mutated or rootkit spies.

Keylogger News

Currently, multiple system monitors use process blocking to actively stop anti-spyware programs from running. Keyloggers such as 007 Spy can, when enabled by the user, block the running processes of several of the mainstream anti-spyware products.

Keyloggers are no longer simply hiding from the operating system, file system, and anti-spyware software; they are actually beginning to target the anti-spyware software itself. These types of behaviors and features are becoming more prevalent throughout the range of commercial and non-commercial system monitors.

There are also more keyloggers using kernel-level drivers. Upon installation, this type of keylogger takes over as the driver for the keyboard, mouse, or both. This creates significant removal issues. This may eventually become the standard throughout the next generation of keyloggers. This behavior has been observed in top level keyloggers such as Spector Pro and Elite Keylogger as well as in products from smaller software publishers.

Keyloggers are actually beginning to target the anti-spyware software itself.

Changes in Adware

A few adware companies claiming to have improved their behavior are AbetterInternet/Best Offers/Direct Revenue and 180search Assistant.

AbetterInternet has announced they are ending their contracts with third-party affiliates who distribute their software. They have also joined with Sharman Networks, or KaZaA. Their software is now bundled with the KaZaA peer-to-peer client.

180search Assistant/Zango released their new search assistant technology named Safe and Secure Search, or S3. This technology enforces the display of an installation consent screen prior to installation, to attempt to notify users what they are downloading and installing.

Although some companies are trying to escape negative associations with their products, Elitebar and Apropos are examples of applications that are still malicious.

Elitebar downloads other adware applications onto a machine without the user's consent. It is primarily a toolbar, but also serves advertisements and hijacks browser settings. Elitebar is particularly challenging as it uses some rootkit-like techniques to hide itself from Windows in order to avoid detection thus making it difficult to detect and remove.

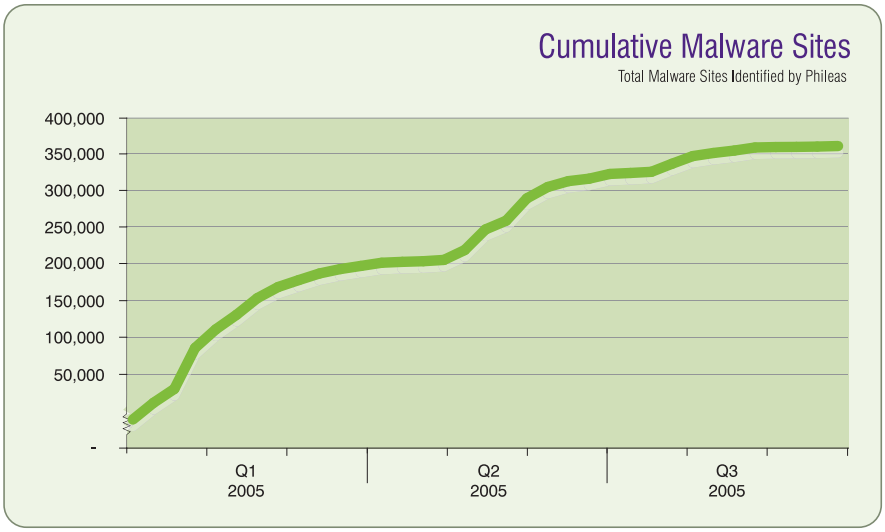
Elitebar is particularly challenging as it **uses some rootkit-like techniques to hide itself.**

Apropos can also cause major instability on systems, including BSOD (Blue Screen of Death). Apropos is an adware program that previously released a very unstable version of itself that caused serious system stability problems like spontaneous system reboots. They have fixed the stability issues. However, the newer version of Apropos uses rootkit-like techniques to hide itself and evade detection.

Web Crawler Automation

This quarter, Webroot's data indicates a 26.56 percent increase in the number of sites that host spyware, for a total of more than 360,000. An effective and efficient means of identifying spyware is to use web crawler technology to find new threats before they can infect end users. Webroot employs this methodology by using Phileas, a malware crawler that is capable of searching the internet for Web sites containing malware.

Webroot's data indicates a **26.56 percent increase in the number of sites that host spyware.**



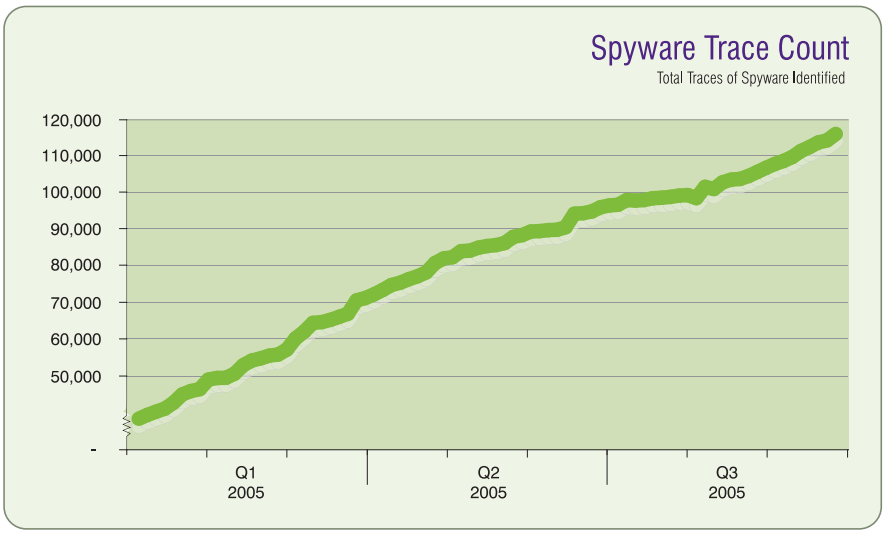
Phileas is continually updated with discovery techniques developed by Webroot's Threat Research team to ensure detection of the latest threats. Dozens of servers with high bandwidth Internet connections are utilized, controlling an army of "bots" that scour the Web for sites containing malware.

An example domain name like what Phileas finds is: http://4pokertips.com

Warning: Do not look at the Web site listed above, unless you are fully protected with an anti-spyware solution. This URL uses an exploit (Microsoft Security Bulletin MS03-014) to install a toolbar.

Phileas data, which references the increasing number of existing, potentially malicious Web sites, supports evidence that malware creators are working overtime with a goal of distributing malicious threats to users. An automated tool such as Phileas is the best way to track growth of this magnitude. Phileas has been developed as a scalable solution, so as the spyware problem grows, the architecture can keep pace.

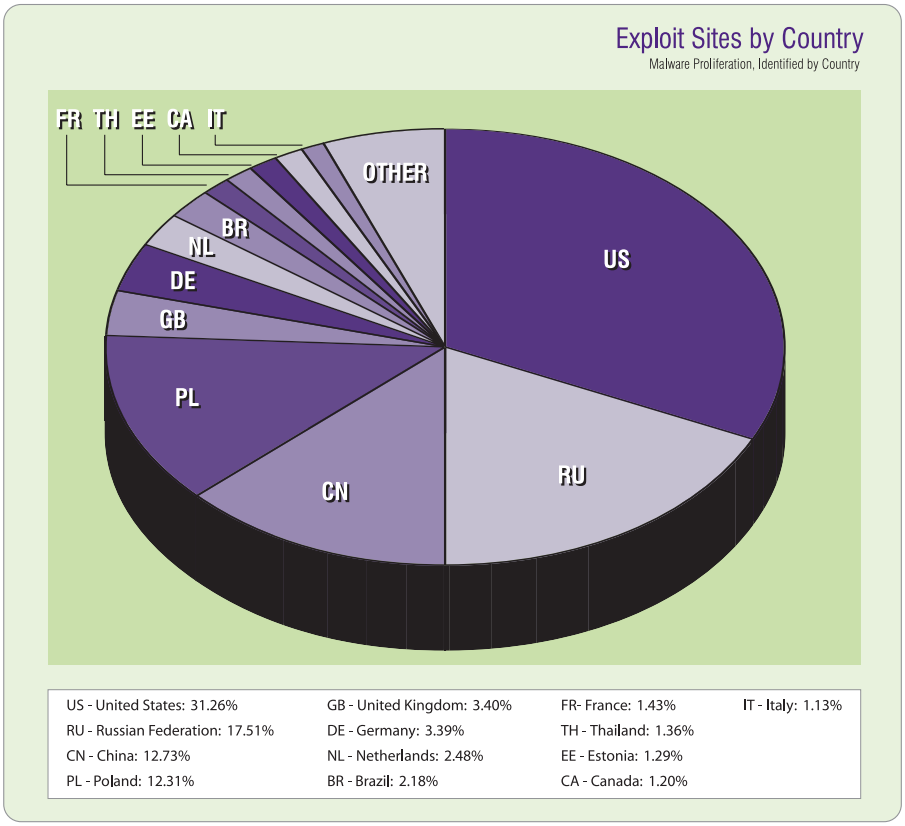
As spyware purveyors continue to modify their programs to evade detection, each program becomes more and more complicated with supplementary traces associated with it. In other words, a single spyware program has more traces associated with it than earlier generation of less sophisticated programs.



Phileas can identify new spyware programs as well as programs that have morphed or changed their identifying traits. By using this methodology, Webroot is able discover new spyware and update its definition database of spyware protection.

Worldwide Problem

As Phileas data indicates, spyware distribution points continue to increase and diversify.



More than 31 percent of the spyware exploits originate from the United States.

According to recent Phileas statistics, more than 31 percent of the spyware exploits originate from the United States, followed by the Russian Federation at 17.5 percent. China and Poland are nearly tied for third at 12.7 percent and 12.3 percent, respectively. The proliferation and attainability for high-speed Internet connections in the United States may cause these high numbers.

False Positives

Identifying spyware is only the first step towards eradicating it from your computer. After identifying a spy, a definition is created which is capable of detecting and removing this particular piece of spyware from your computer. Each definition undergoes testing to ensure that it can correctly identify malicious code and more importantly, that it does not remove or interfere with legitimate files. This incorrect identification, also known as a "false positive," is one of the most challenging aspects in creating an effective anti-spyware application.

A false positive is when an application misidentifies a good file or procedure and marks it for further action. Identifying and removing important or system critical files can cause severe problems and system instability.

Despite these issues, not all anti-spyware vendors take the necessary steps during the quality assurance cycle to prevent false positives. The key to an effective anti-spyware product is not only its ability to correctly identify and remove malicious files, but also to protect legitimate files.

Phileas provides information that constantly feeds Webroot's spyware repository. The Webroot Threat Research team ensures that new spyware definitions, which are under consideration for addition to the spyware database, are thoroughly tested to ensure these definitions detect and remove files and components that are spyware-related.

Top Threats

This quarter, the top threats are not only the most prevalent, but also the most complex. During the last six months, spyware has exhibited the use of packing and encryption algorithms, which is now very common. Spyware that is based on Trojan horse code, viral installation procedures, and polymorphic engines has required new detection and removal methodologies to stay ahead of the threat.

Spyware has exhibited the use of packing and encryption algorithms.

AbetterInternet

Short Description: AbetterInternet is a Browser Helper Object (BHO) that may hijack any of the following: Web searches, home page, and other Internet Explorer settings.

Characteristics: AbetterInternet is a Browser Helper Object (BHO) that may change your browser settings. A BHO is a file, usually a toolbar, which loads with Internet Explorer. BHOs may route certain domains to false addresses thus hijacking your search.

Method of Installation: AbetterInternet generally propagates itself using dialog boxes, various social engineering methods, or through a java scripting error. Usually adware and BHOs are bundled with various, free software programs.

Consequences: AbetterInternet may display advertisements. It may also cause slowing of your Web browser and system performance issues.

CoolWebSearch (CWS)

Short Description: CWS may hijack any of the following: Web searches, homepage and other Internet Explorer settings.

Characteristics: CWS may redirect your Web searches through its own search engine and change your default homepage to a CWS Web site. This hijacker may also change your Internet Explorer settings.

Method of Installation: Recent variants of CWS install using malicious HTML applications or security flaws such as exploits in the HTML Help format and Microsoft Java Virtual Machines.

Consequences: If this hijacker changes your Internet Explorer browser settings, you may be unable to change back to your preferred settings.

Additional detail: CWS is a difficult piece of adware to identify due to its massive number of variants. CWS is modularly coded meaning that its hijacker, downloader, search algorithm and watcher application code is interchangeable making it easy to swap these sections of code to make completely new variants. CWS also encrypts and packs the code with the UPX algorithm, which is used to hide the executable from detection mechanisms. CWS also installs a watcher executable that saves copies of each other; if one executable is removed or destroyed, then the secondary or "sister" executable reinstalls its counterpart, making removal difficult.

EliteBar

Short Description: EliteBar may hijack any of the following: Web searches, home page and other Internet Explorer settings.

Characteristics: EliteBar may display advertisements on your computer. This program may hijack Web searches, meaning it may reroute your Web searches through its own Web page. It may also change your default home page.

Method of Installation: EliteBar generally propagates through the use of seemingly-innocent dialog boxes, various social engineering methods, or through a java scripting error. Usually hijackers are bundled with various, free software programs.

Consequences: This program can display advertisements. It may also cause slowing of your Web browser and system performance issues. If EliteBar changes your Internet Explorer browser settings, you may be unable to change back to your preferred settings.

ISTbar

Short Description: ISTbar is a toolbar that may be used for searching pornographic Web sites, which display pornographic pop-ups and hijack user homepages and Internet searches.

Characteristics: ISTbar may add a toolbar to your Internet Explorer browser, hijack your homepage, and display pornographic pop-ups.

Method of Installation: ISTbar generally propagates itself using dialog boxes, various social engineering methods, or through a java scripting error. Usually toolbars are bundled with various, free software programs.

Consequences: ISTbar may monitor the Web sites you visit.

Look2Me

Short Description: Look2Me may monitor Web surfing activity and report usage statistics to a centralized server. It also may display pop-up advertisements and may install several other pieces of spyware.

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

Method of Installation: Look2Me generally propagates itself using dialog boxes, various social engineering methods, or through a java scripting error. Usually adware and BHOs are bundled with various, free software programs.

Consequences: Look2Me is very difficult to remove due to its injection into system-level processes. Look2Me may also install other pieces of spyware and adware, which decrease your computer's performance, and may display pop-up advertisements.

Additional detail: Look2Me installs itself in the Windows system directory and places a simple registry key into the Winlogon notify section, making its installed component a dependency to the Winlogon system-level process. It then injects a DLL under explorer.exe giving it the ability to execute. This malicious spyware has the ability to reboot the machine if removal of one of its core executables is attempted, and also alters the Debug programs Local Security Policy for Windows XP machines, limiting the functionality of detection programs. Look2Me is also encrypted with a proprietary encryption algorithm making on-disk detection rather difficult, especially since its ability to update itself on the fly usually leads to multiple installed versions. It also installs other pieces of spyware, creating a massive infection on an infected user's machine.

ShopAtHomeSelect

Short Description: ShopAtHomeSelect redirects visitors to merchants' Web sites via its own servers in order to increase its affiliate commissions.

Characteristics: ShopAtHomeSelect may track the Web pages you visit and send this information to its controlling servers. This program may also reroute visits to certain merchant's Web sites via its own servers, allowing the company to receive extra commissions.

Method of Installation: ShopAtHomeSelect generally propagates itself using dialog boxes, various social engineering methods, or through a java scripting error. ShopAtHomeSelect may be bundled with various, free software programs, such as Grokster and iMesh 4 software. It may also be installed by FavoriteMan.

Consequences: This program can display advertisements. It may also cause slowing of your Web browser and system performance issues.

SurfSideKick

Short Description: SurfSideKick may display advertisements on your computer.

Characteristics: SurfSideKick may display pop-up advertisements on your computer.

Method of Installation: SurfSideKick generally propagates itself using dialog boxes, various social engineering methods, or through a java scripting error. Usually adware and BHOs are bundled with various, free software programs.

Consequences: This program can display advertisements. It may also cause slowing of your Web browser and system performance issues.

Virtumonde

Short Description: Virtumonde may display advertisements on your computer.

Characteristics: Virtumonde may display advertisements on your computer.

Method of Installation: Virtumonde generally propagates itself using dialog boxes, various social engineering methods, or through a java scripting error. Usually adware and BHOs are bundled with various, free software programs.

Consequences: This program can display advertisements. It may also cause slowing of your Web browser and system performance issues.

Web search Toolbar

Short Description: Web search Toolbar may hijack any of the following: Web searches, homepage and other Internet Explorer settings.

Characteristics: Web search Toolbar may hijack your Web browser settings while Internet Explorer is running and install a toolbar. This toolbar may display advertisements on your computer.

Method of Installation: Web search Toolbar generally propagates itself using dialog boxes, various social engineering methods, or through a java scripting error. Usually toolbars are bundled with various, free software programs.

Consequences: Web search Toolbar may monitor the Web sites you visit.

.

180search Assistant

Short Description: 180search Assistant is adware that may direct you to sponsors' Web sites.

Characteristics: 180search Assistant may direct you to sponsors' Web sites, after entering certain keywords into your browser.

Method of Installation: 180search Assistant generally propagates itself using dialog boxes, various social engineering methods, or through a java scripting error. Usually adware and BHOs are bundled with various, free software programs.

Consequences: This program may send information about your Web surfing habits to its controlling servers whenever you are online, which may slow your Web browser's performance. 180search Assistant may download third-party programs on your computer, resulting in unwanted programs being installed without your knowledge or consent.

ENTERPRISE
& Compliance

Enterprise & Compliance

A number of laws and regulations require corporations to protect data – especially customer data. As a result, enterprises have been forced to rethink their data security measures. As U.S. states, such as California and others, mandate notification to consumers of data security breaches, more and more protective actions have been implemented to maintain compliance as well as competitive advantage.

Increasing concern about spyware is at the root of these laws and regulations. Until now, corporations were able to dismiss spyware as an annoyance for consumers rather than a threat to business networks and the valuable information they contain. Today, spyware is viewed as a priority threat that requires a state-of-the-art response. Failure to take spyware seriously may expose an enterprise to substantial risks, including prosecution by the FTC or non-compliance with HIPAA or Gramm-Leach-Bliley Act.

Spyware is viewed as a **priority threat that requires a state-of-the-art response.**

Corporations can't be complacent about the threat that spyware poses to its systems and data. Spyware, whether used to support advertising, direct marketing or outright industrial espionage, is not the work of amateur hackers. Increasingly, spyware is a high-stakes business that will, like all business, follow the path of greatest profit.

These recent legal developments have substantially increased the likelihood that a security flaw or negligence will result in legal action. Threats that used to seem remote or far-fetched are mutating rapidly into immediate high-risk conditions that must be addressed if security incidents – and litigation – are to be avoided.

Corporations can't be complacent about **the threat that spyware poses to its systems and data.**

Of particular concern to enterprise is malicious spyware, such as system monitors and Trojan horses. Evidence suggests that enterprises are relying on legacy anti-virus solutions or free desktop programs to combat these types of spyware. These programs are ineffective in detecting and removing spyware from PCs.

Enterprise Findings

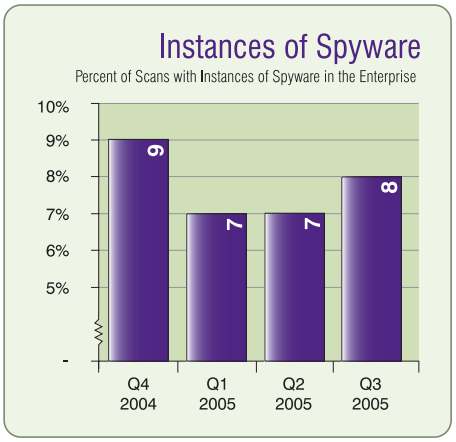
Most enterprises would find themselves engaged in extensive forensic activity in the wake of the discovery of a single instance of a system monitor capturing employee or customer data.

Security and financial auditors alike are becoming concerned about the implications of keystroke loggers on internal machines. Significant loss of proprietary information and even customer trust can occur if a Trojan or system monitor is used to steal company data or proprietary information.

Malicious spyware, which includes system monitors and Trojans, continues to be dangerously prevalent within the enterprise. In Q3 2005, it increased slightly to 8 percent of PCs scanned, according to Enterprise SpyAudit data.

It's important to recognize that anti-virus programs and free desktop solutions are ineffective against these complicated and sophisticated programs. The detection and removal engines used by these programs can't root out these tough programs, which use polymorphic code or rootkit technology to avoid detection.

Malicious spyware, which includes system monitors and Trojans, continues to be dangerously prevalent within the enterprise.



System Monitors

System monitors are growing in sophistication and are being deployed by cybercriminals to capture personal information such as credit card numbers and personal logins to online banking systems.

On PCs with system monitors, the average number of instances held steady at 1.2 instances of system monitors per infected PC in Q3. Industry analysts fear that attackers are customizing system monitors to keep them hidden and undetected.

System monitors
are growing in
sophistication.

Trojan Horses

The presence of Trojan horses within enterprises increased during Q3 to 1.5 instances per infected PC from 1.2 in Q2 2005. During the past few quarters, hackers have relied on Trojan horses to secretly install system monitors on unsuspecting computers.

The high number of Trojans indicates that enterprises are relying on legacy anti-virus programs to protect their computers. These programs are unable to detect and remove the complex and sophisticated Trojans.

Additionally this increased level of Trojans may indicate that the threat from system monitors deployed within Trojans for identity theft could rise dramatically in the next several months.

Because Trojans are usually installed via worms or viruses, their overall existence on enterprise machines can fluctuate with the level of new outbreaks.

Adware

Nearly half (48 percent) of enterprise PCs are infected with adware. Multiple pieces of adware can lead to increased likelihood of system crashes, and other issues that can lead to increased number of helpdesk calls. Removing adware continues to be a pressing issue for enterprises.

Overall, the number of enterprise PCs with adware remains somewhat steady over time. However, PCs with adware had an average of 3.9 adware infections in the third quarter 2005, up from 3.6 in the second quarter.

Tracking Cookies

Although tracking cookies tend to not have a large effect on enterprises, it's noteworthy to mention that during the third quarter, cookie infections remained steady.

SpyAudit found an average of 27 cookies on PCs infected with cookies in Q3 compared to 29 in Q2 2005.

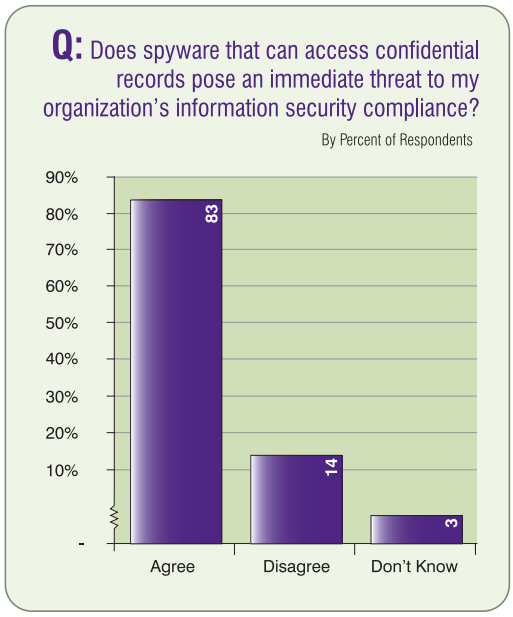
Online marketers and security analysts continue to debate whether cookies should be classified as spyware. As the number of instances reveals, cookie distribution remains high and even brief visits to the Internet can attract cookie files.

Webroot Compliance Survey

As indicated by the results of a recent compliance survey conducted by Webroot, government security regulations are a major challenge facing most enterprises today. Survey respondents identified compliance with Sarbanes-Oxley as a specific challenge to their organization.

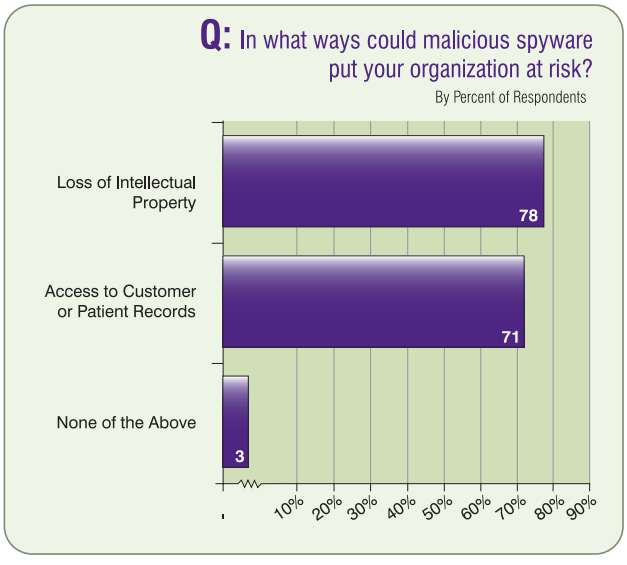
Webroot surveyed high-level, strategic security executives, such as chief executive officers, chief information officers and chief financial officers. In total, the survey respondents represent organizations with more than 350,000 PCs and laptops connected to the Internet.

Many respondents recognize the connection between compliance issues and spyware. More than 70 percent of respondents consider spyware as a potentially serious threat to their enterprise and 83 percent agreed that keyloggers, system monitors and Trojan horses pose an immediate threat to confidential records.

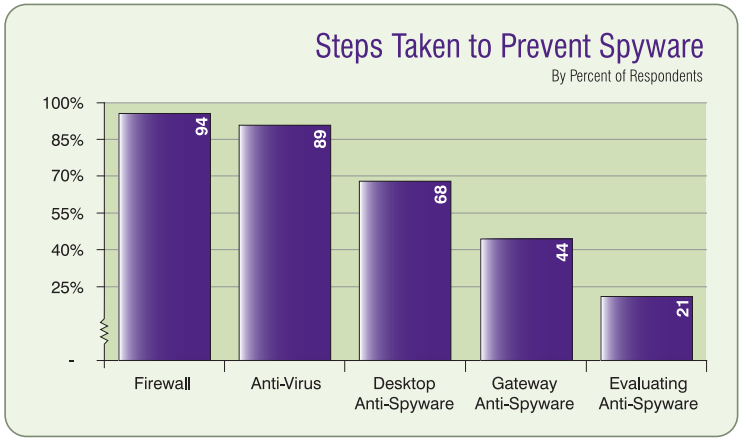


More than 70 percent of respondents consider spyware as **a potentially serious threat to their enterprise.**

The survey data supports evidence that protecting employee data and intellectual property from malicious spyware is a concern for enterprises.



The good news is that 68 percent of enterprises are using and 21 percent are looking to use desktop-based anti-spyware solutions. However, an alarming majority are also dependent on their firewall and anti-virus products which do not provide any protection from spyware. As more enterprises become educated on the risks of spyware and the type of solutions needed to address the problem, desktop-based anti-spyware solution adoption is expected to increase.



Computerworld Spyware Survey

Computerworld recently released the results of a similar spyware survey. Computerworld surveyed IT decision makers such as chief technology officers, chief information officers and others, on the topic of spyware.

Most notably, the results indicate that spyware has a large impact on enterprises with 71 percent identifying spyware as a significant threat. More than 80 percent of respondents don't believe that the spyware threat is being exaggerated or over-hyped.

To combat spyware, nearly 70 percent of those surveyed use a standalone, desktop anti-spyware solution, but only 41 percent have an enterprise-class solution.

The results suggest that enterprises realize the impact spyware can have on their users, including damage to PCs or even identity theft. In fact, close to 85 percent are concerned that spyware could lead to identity theft.

More than 80 percent of respondents **don't believe the spyware threat is being exaggerated or over-hyped.**

Compliance Laws and Regulations

Following the rash of security breaches in the second quarter of 2005, enterprises began to realize the real costs of spyware and the danger of ignoring the risks that spyware posed to their business. These incidents outlined the enormity of the compliance issue and as a result, industry analysts and government agencies offered recommendations during the third quarter of 2005. Much of the following information came from two white papers from cyberlaw and data security and compliance experts, Charles Kennedy, who serves as counsel to Morrison & Foerster, LLP, and Kate Borten, president of The Marblehead Group.

The FDIC urged financial institutions to take several internal steps to fight spyware.

FDIC Issues Spyware Warning

In July, the **FDIC**, in a Financial Institution Letter entitled "Best Practices on Spyware Prevention and Detection," urged banks to enhance their protections against spyware in an effort to limit the risk that customers' personal data may be stolen. The memo stressed that firewall and anti-virus software does not protect computers from spyware.

The FDIC urged financial institutions to take several internal steps to fight spyware, including consideration of spyware in overall risk assessments, regulating employee computer use and altering overall security practices.

Including spyware in overall risk assessments ensures that financial institutions consider all threats to customer information and take proper steps to lessen those risks. The FDIC suggested financial institutions monitor employee's computer use to ensure their employees comply with security and Internet-use practices that prohibit users from accessing risky sites.

Financial institutions must change their overall security practices to protect their confidential information. Firewalls should be in place to monitor inbound and outbound traffic and regular reviews of firewall logs allow for inspection into suspicious activity.

The FDIC also suggested audits of root certificates as spyware can install unique trusted certificates to allow it to intercept secure Internet communications or the execution of malicious code.

Not only do financial institutions need to improve their own response to spyware, but they must also help educate and protect their customers. The FDIC urged banks to educate customers about the risks of spyware and encourage them to take steps to prevent and detect spyware on their own computers.

To read more about the FDIC letter, visit:
www.fdic.gov/news/news/financial/2005/fil6605a.pdf

Spyware Meets HIPAA

Spyware can result in the loss of all three of the prime components of information security: confidentiality, integrity and availability.

Spyware-related privacy and security breaches in the form of unauthorized disclosure of confidential data – personnel data, legal advice, business strategies, and Protected Health Information or PHI (as defined by the Health Insurance Portability and Accountability Act or HIPAA) of patients and health plan members – can lead to public embarrassment, lawsuits and regulatory non-compliance penalties for the affected organization.

Spyware-related breach of patient confidentiality in a health care organization can seriously affect targeted patients as well. Such breaches can lead to embarrassment, mental anguish, job loss, financial loss and even physical harm.

Spyware-related breach of patient confidentiality in a health care organization can seriously affect targeted patients.

Using HIPAA's Security Rule to Fight Spyware

With the advent of HIPAA, security is no longer an option for health care organizations. Instead, the questions today are related to how much security is enough and where to focus security efforts.

By law all PHI must be secured. Implicitly Covered Entities' security programs must encompass their full electronic environment, not just PHI, since PHI systems are not isolated islands. It is also increasingly clear that individually identifiable non-health care data held by any type of organization, including health care providers and plans, should be protected from misuse for identity theft and financial fraud.

Organizations with the most effective security programs recognize the broad scope of the security challenge, and they routinely allocate resources for security infrastructure strategies such as widely deployed desktop controls including anti-spyware solutions.

HIPAA's security rule provides several standards and implementation specifications that logically encompass anti-spyware strategies.

First, the security rule requires workstation use policy and procedures that "specify the proper functions to be performed." Policies and network controls that limit the workforce's use of the Internet, for example, by prohibiting access to pornographic sites, reduce the risk of spyware infection.

Policy and procedures requiring all new software to be approved before loading (downloaded from the Internet or introduced via physical media such as a CD) also reduce the risk. These policy points are often clustered together in a computer and network "acceptable use" policy for the workforce.

Second, the rule requires security incident policies and procedures "to address security incidents," that is, to identify, respond to and mitigate the harmful effects of security incidents – including spyware attacks. Organizations should install anti-spyware software that can identify and deflect spyware attacks.

There should be processes for monitoring and updating the anti-spyware software. As part of the response and mitigation plan, there should also be documented procedures for removal of spyware.

Other necessary technical measures to reduce the risk of spyware infection include hardening the workstation configuration, including the browser configuration, as well as promptly applying security patches to all networked devices.

Finally, HIPAA's security rule requires workforce training on security. Workforce training programs should discuss acceptable and unacceptable uses of computers and the organization's network, based on organization policy.

To meet the implementation specification regarding protection from spyware, training programs should describe the symptoms of an infected workstation; those might include newly persistent slowness and an unexpected change in appearance or functionality – common signs of a spyware infection. Additionally, training should inform the workforce of the procedure for reporting suspected spyware.

While HIPAA's security rule is high-level and technology-neutral, it is clear that in today's networked world, health care organizations are expected to take all reasonable measures to protect their PHI and other information assets from the dangers of spyware and other types of malicious software.

Health care organizations are expected to take all reasonable measures to protect their PHI and other information assets from the dangers of spyware.

The Legal Threat

If your enterprise is attacked by spyware, you are not just a victim: you also are a potential defendant. Today's legal environment makes businesses responsible for failing to prevent foreseeable attacks, including spyware attacks, that result in harm to consumers.

Many enterprises are still unaware of the extent of their exposure for data breaches. Until recent years, government agencies allowed data protection technologies to evolve without regulatory distortion and left businesses free to provide as much or as little data protection as their customers wanted and were willing to buy. With few exceptions, such as those applicable to bank information systems, no statute or regulation required private businesses to conduct security training, make threat assessments, encrypt data, transmit

information over virtual private networks or other secure lines, assign user names and passwords, or take other protective measures.

Perhaps the most comprehensive information security obligations are those imposed on financial institutions by the Gramm-Leach-Bliley Act and the implementing regulations of the various oversight agencies that regulate those institutions. The GLBA, which reinforces a substantial legacy of banking data security regulations, has made U.S. financial institutions some of the most security-conscious businesses in the world.

The most important single enforcer of data protection standards, and the agency that sets the pace for other federal and state initiatives in this area, is the Federal Trade Commission. Beginning at least 10 years ago, when it held a series of hearings on the privacy of information submitted to Internet sites, the FTC has made privacy and data security an enforcement priority under its authority, granted in Section 5 of its enabling statute, to regulate unfair or deceptive acts and practices. The intervening years have only increased the Commission's aggressiveness as a creator and enforcer of privacy rights. The following takes the GLBA obligations, and those adopted by the FTC under Section 5, in turn.

The GBLA has made U.S. financial institutions some of the most security-conscious businesses in the world.

The Data Security Regime of the Gramm-Leach-Bliley Act

The GLB is best known to the public for its restrictions on disclosure by financial institutions of nonpublic personal information to third parties, but the statute also requires various federal and state agencies to set standards for the administrative, technical and physical protection of the customer records and information of financial institutions.

Each institution's information security program, including all "key controls, systems and procedures," must be periodically tested, reassessed and updated as appropriate. Tests of the program's controls, systems and procedures must be "conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs."

Each institution must report to its board, or an appropriate committee of its board, at least annually the "status of the information security program" and the company's compliance with the guidelines.

Each regulatory agency has the authority to examine financial institutions under its jurisdiction for compliance with the guidelines and can determine that those institutions have failed to satisfy the requirements of the guidelines.

Violations of the guidelines can result in substantial penalties and payment of restitution to affected customers. Although penalties specifically related to the guidelines have not been imposed so far, the magnitude of past penalties for unfair and deceptive practices by financial institutions provide an idea of the potential scale of liability.

In a case involving **Providian National Bank**, the institution was required to pay $300 million in restitution to customers for abuses related to guaranteed savings rate, credit protection and other programs.

Similarly, in a case involving the **First National Bank of Marin**, the bank was ordered to establish a reserve to handle restitution payments, with an initial deposit to that fund of $4 million. Other, recent investigations have resulted in restitution by **Direct Merchants Credit Card Bank**, **First Consumers National Bank** and the **First National Bank in Brookings**.

Bank regulators must now make data security a particular focus of their examinations of institutions under their jurisdiction, and protection against spyware has been specifically identified as an enforcement issue.

Providian National Bank was required to pay $300 million in restitution to customers.

Data Security under Section 5 of the FTC Act

The FTC's concern with data security, as distinguished from general privacy, dates at least from its adoption of regulations to enforce the GLBA. The FTC's "Safeguards Rule," which has become the template for all FTC enforcement actions involving data security, took effect on May 23, 2003.

The FTC's Safeguards Rule has had an impact well beyond the financial institutions to which it explicitly applies. The FTC, unlike other agencies that enforce data privacy standards, has a broad consumer protection mandate that applies to businesses generally. In other words the FTC has the means to turn its Safeguards Rule into a de facto standard for most of the U.S. economy.

The FTC's data security enforcement actions under Section 5 have involved a wide range of American industries and lines of business, from software (Microsoft) to pharmaceuticals (Eli Lilly) to entertainment (Tower Records).

Spyware Is an Emerging FTC Enforcement Priority

The FTC's history as a privacy enforcer follows a familiar pattern. First the FTC holds hearings, writes reports or otherwise broadcasts its interest in a privacy-related subject. Concurrently with or soon after the initiation of those efforts, the FTC brings enforcement actions against companies that fail to address the FTC's concerns in a way the Commission thinks appropriate.

The FTC appears to be taking that approach in the area of spyware protection. In April 2004, the Commission held a workshop on the subject of spyware. In further support of its inquiry, the Commission issued a report on the subject to Congress. As should be expected, the FTC also has undertaken its first stage of enforcement proceedings against spyware providers and advertisers of false anti-spyware products.

The FTC has taken its first stage against spyware providers and advertisers of false anti-spyware products.

As the FTC's recent action against **BJ's Wholesale Club** shows, failure to protect networks against intrusions that compromise customer data are considered unfair and will be attacked regardless of the security commitments the targeted company may or may not have made.

The FTC is the lead agency, but not the only protagonist, in the data protection legal drama. Many states are equally aggressive, and private actions – such as the class action suit recently brought against **CardSystems** for its massive loss of credit card data – are just beginning to become a factor.

Finally, as The Wall Street Journal reported in a recent online article, mass data compromise incidents have caused persistent reductions in the shareholder value of the companies involved. Fallout of this kind, even if not accompanied by investigations or lawsuits, amply justifies the attention of management to spyware and other emerging threats.

If the FTC stays true to form, litigation efforts are expected to turn to companies that did not create or knowingly facilitate spyware, but did fail to adequately protect consumer data against spyware threats.

Refer to the **Legal & Legislation** section for more on FTC activities.

Fallout of this kind amply justifies the attention of management to spyware.

SpyAudit Case Study

Current security measures in place at a large retailer aren't effectively protecting the company from spyware, according to the results of Webroot Enterprise SpyAudit.

Webroot conducted an audit for 10,000 desktop computers at the large national retailer. The results concluded that 62 percent of computers had some form of spyware infection.

Most concerning was the infection rate of malicious spyware, such as Trojan horses or system monitors. For retailers that store huge databases of customer confidential records with credit card numbers, even one desktop with malicious spyware can have major security and compliance implications, as noted in the BJ's Wholesale Club case.

Audit Results

Retailer Sample Size of 10,000	Critical		Caution
	Trojans	System Monitors	Adware
Number of Infected Machines	700	100	2,600
Total Threats Found	779	100	14,300
Percent of Machines Infected	7%	1%	26%

Partial List of Spyware Discovered

Threat Name	Significance
MyDoom_M	Mass mailing worm that installs a remote Trojan to monitor TCP port 1034
BackDoor-BDI	May allow hacker access when system is online
Trojan-Backdoor	Capable of providing hacker access to online machines
Ardamax Keylogger	Saves system keystrokes to encrypted log
UFP 007 Spy System Montior	Records system activity and transmits information via email or ftp

Consequences of Malicious Code on the Network

This retailer is just one example of the risks enterprises face from malicious activity aimed at stealing sensitive data. The malicious activity may come from internal or external sources.

As the results of the Enterprise SpyAudit indicate, the retailer is vulnerable to these types of attacks. This vulnerability may cause regulatory compliance issues. For example, a number of laws now require that company executives, such as the CEO or CFO, are personally responsible for the privacy and confidentiality of electronically stored data.

Furthermore, some states require enterprises to report suspected breaches of personal data, like customer information, to the data owners. There is an urgent need for all companies to assess their intellectual property and confidential records security needs and deploy the most effective anti-spyware solution to protect these assets against the widespread spyware epidemic.

This vulnerability may cause **regulatory compliance issues.**

CONSUMER
SpyAudit

Consumer SpyAudit

Each quarter, Webroot Software gathers the results from a continuous Consumer SpyAudit. The tool is free for anyone to use. The SpyAudit is voluntary to use and the results are compiled from scans of PCs that belong to visitors to the www.webroot.com Web site and elsewhere. These results are anonymous. Refer to the methodology section for more details.

As the number of home computers rises, spyware purveyors have more users to target.

Worldwide Problem

Consumer SpyAudit results are a sign of spyware expanding into a global problem. Home computer users increasingly are becoming infected with spyware, particularly malicious spyware such as Trojan horses and system monitors. This increase may signify the prevalence of personal computers and improved Internet access in more and more countries.

According to U.S. Census data, 62 percent of American households had at least one computer in 2003, an increase from 56 percent in 2001. As the number of home computers rises, spyware purveyors have more users to target. The connection is clear: more people online points to increased likelihood of spyware infection.

This worldwide plague is costing consumers millions of dollars in skyrocketing expenses ranging from computer repair costs to damages incurred as a result of identity theft.

As a result of this rising problem, more consumers rely on anti-spyware software to protect their PC from spyware than ever before.

While the spyware problem continues to pose a threat to millions of consumers, scam artists are taking advantage of the demand for anti-spyware products and selling solutions that even install additional spyware. The FTC has brought suit against four such malfeasants to date.

As spyware continues to infect home computer users, many are taking drastic measures to avoid detection. According to a recent Consumer Reports survey, 86 percent of Internet users have made at least one change in their online habits out of fear of identity theft. A number of survey respondents admitted to cutting back on time spent surfing the Internet and others have stopped shopping online.

Global Infection Rates

Consumers from more than 100 countries ran SpyAudit during Q3 2005. Looking at the 38 countries that performed 500 or more SpyAudit scans, the United States had the highest average number of spies detected: 24.4 per scanned PC. Slovakia had the lowest at 6.2 spies per PC scanned.

The average number of spies per PC scanned for the 38 countries is 17.4.

Rates of Spyware Infection

Highest Rates of Machines Infected by Country

Rank	Country	Spies per Scanned PC
1	USA	24.4
2	Thailand	18.7
3	United Kingdom	18.1
Worldwide Average	– – – –	**17.4**

Europe

Following the spyware problem in the United States, European consumers find themselves in a similar situation in regard to infection rates. Industry analysts suggest lower cost Internet-enabled devices as a reason for the increased Internet use among Europeans.

In addition, many countries, such as the United Kingdom, have implemented broadband infrastructure which supports higher speed connections and wireless communication.

Europe - Spy Traces per PC

Average Number of Spy Traces per Consumer PC in Europe

Country	Total Spy Traces
United Kindgom	18.1
Spain	11.9
France	9.9

Asia

Within Asia, consumer PCs in Thailand have the highest average number of spies: 19. Thailand has a very young population of Internet users with 52 percent between the age of 15 and 24. That may account for the top position in Asia.

Asia continues to lead with adoption rates of broadband connections. Industry analysts credit this growth with the large population rates of Asian countries. In addition, lower price computers and Internet-enabled devices are available at a higher rate in these countries.

Consumer PCs in Thailand have **the highest average number of spies: 19.**

Asia - Spy Traces per PC

Average Number of Spy Traces per Consumer PC in Asia

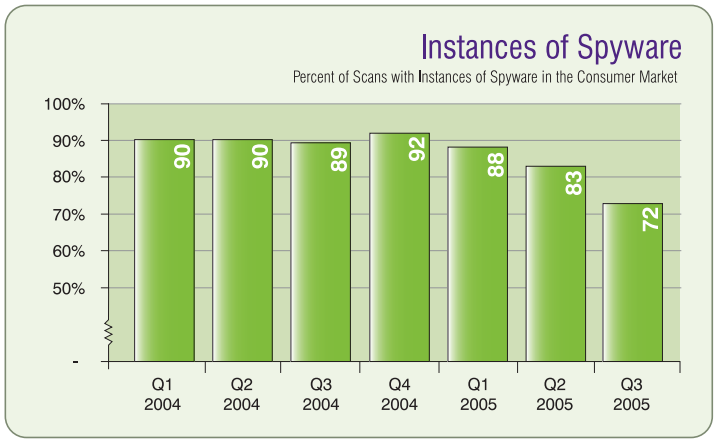
Country	Total Spy Traces
Thailand	18.7
China	14.8
Taiwan	12.4

Spyware Infection Rate

In Q3 2005, the Consumer SpyAudit found that 72 percent of consumer PCs were infected with spyware. Although this infection rate remains high, the improved trend in 2005 is a positive sign.

Webroot attributes the reduction in spyware infection to greater consumer awareness of the threat, a higher penetration of multiple anti-spyware solutions on consumer desktops, and legislation in 10 states that makes illicit downloads and installation illegal.

The commercial adware vendors are modifying their behavior in preparation for federal legislation. With readable EULA's, easy un-install features, and attribution of pop-ups, they are losing penetration.



Commerical adware vendors are **modifying their behavior in preparation for federal legislation.**

Infected consumer PCs have an average of 24 instances of spyware. Fourteen percent of spyware instances are more pernicious spyware such as adware, Trojans and system monitors.

Malicious Spyware

Trojan horses and system monitors on PCs are threatening the security of individuals' privacy and negatively affecting e-commerce. While U.S. census data recognizes the increase in computer and Internet usage, computer users are less trusting than a decade ago.

According to Consumer Reports WebWatch, nine out of 10 U.S. Internet users have changed their online behavior out of fear of identity theft, including decreasing amount of time spent online. Other changes include cutting back on the frequency of online purchasing or ceasing online shopping altogether. Close to 58 percent of online shoppers have started using just a single credit card for all the items they buy online.

Increasingly, Internet users have grown more skeptical of online stores and companies. One in five Internet users almost never trust Web sites offering products for sale. The WebWatch report points out 54 percent of respondents have become more likely to read a privacy policy or user agreement before making a purchase.

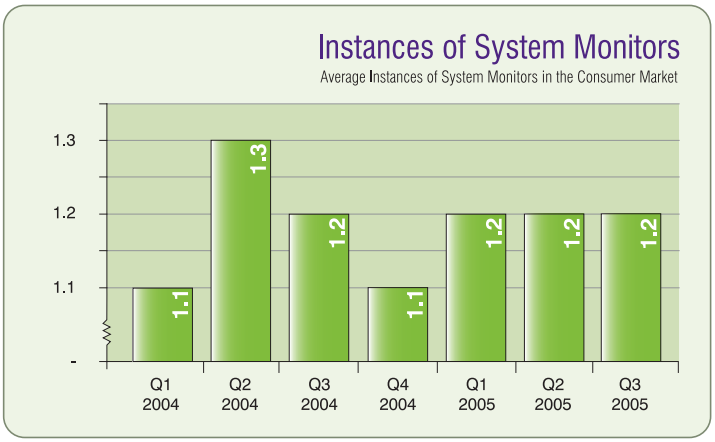
Results from SpyAudit indicate Trojans are present on 21 percent of infected PCs and system monitors are on 5 percent of infected PCs, compared with 6 percent in Q2. In the third quarter there was an increase in the prevalence of Trojan horses on consumer PCs, from 19 percent of infected computers in Q2 to 21 percent in Q3.

There is an average of 1.2 system monitors on computers infected with system monitors and an average of 1.7 Trojans on computers infected with Trojans.

System Monitors

System monitors are growing in sophistication and are being deployed by cyber-criminals to capture personal information such as credit card numbers and personal logins to online banking systems.

On PCs with system monitors, the average number of instances held steady at 1.2 system monitors. Industry analysts fear that attackers are customizing system monitors to keep them hidden and undetected.



The incidence of system monitors is triple the world average in Taiwan and Israel.

The incidence of system monitors is **triple the world average in Taiwan and Israel.**

Rates of System Monitors

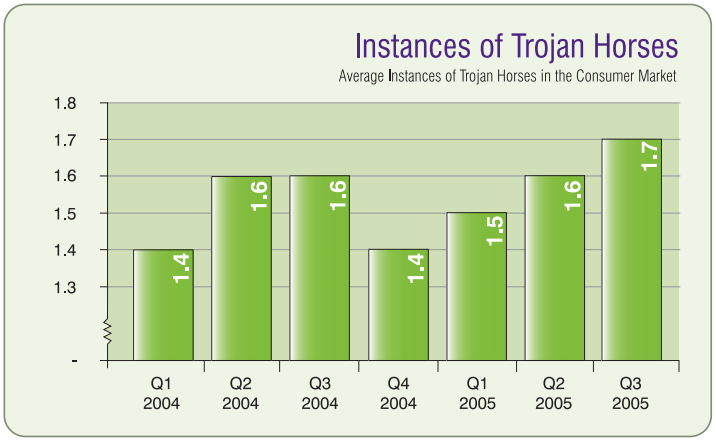
Highest Number of System Monitors per 1,000 PCs Scanned by Country

Rank	Country	System Monitors per 1000 PCs Scanned
1	Taiwan	128
2	Israel	123
3	Belgium	104
US Average	----	**38**
Worldwide Average	----	**42**

Trojan Horses

During the past few quarters, hackers have relied on Trojan horses to secretly install system monitors on unsuspecting computers. The high number of Trojans indicates that consumers are relying on legacy anti-virus programs to protect their computers. These programs are unable to detect and remove the complex and sophisticated Trojans.

Additionally this increased level of Trojans may indicate that the threat from system monitors deployed for identity theft could rise dramatically in the next several months.



Trojan horses have become the tool of choice for the hacker. A Trojan usually implies control of the PC by the attacker. Worms and viruses have been distributing Trojans leading to their greater penetration. Installing a system monitor and then taking action with the data gathered from a keystroke logger is usually a manual process and while paying great dividends to the attacker, it takes longer to execute.

Trojan horses are much more prevalent on PCs in Turkey, Saudi Arabia and Poland than the world average.

Rates of Trojan Horses

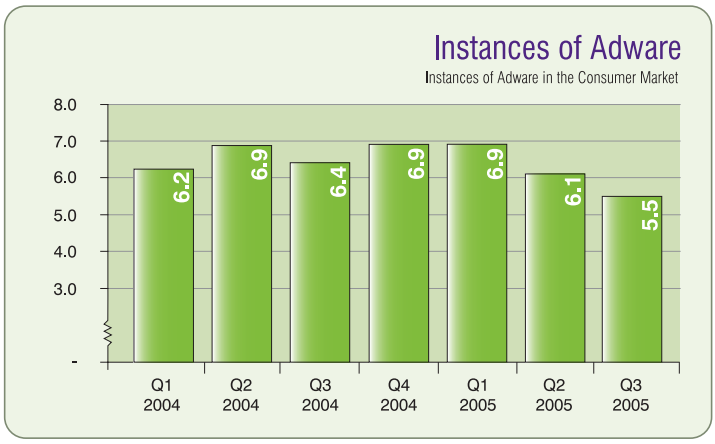
Highest Number of Trojan Horses per 1,000 PCs Scanned by Country

Rank	Country	System Monitors per 1000 PCs Scanned
1	Turkey	493
2	Saudi Arabia	462
3	Poland	426
US Average	----	287
Worldwide Average	----	260

It should be pointed out that ironically, the greatest number of Trojan horse infections were found in the country that gave birth to the original legend of the Trojan horse. Ancient Troy was located in modern day Turkey.

Adware

SpyAudits conducted in Q3 found an average of five instances of adware on infected PCs. More than half of consumer PCs (55 percent) are infected with adware.



Six in 10 PC users who are seeking spyware protection are experiencing a slow computer.

According to a survey of 1,000 new Spy Sweeper customers, six in 10 PC users who are seeking spyware protection are experiencing a slow computer, pop-up windows or another spyware symptom. These symptoms are commonly associated with adware.

180search Assistant is a common adware program that once installed on a PC, may direct that computer to a sponsor's Web site after specific keywords are entered into the browser. This program may send information about Web surfing habits to its controlling servers whenever a user is online, which may slow a Web browser's performance.

In addition to the improved behavior of adware companies (i.e., simpler EULAs, better removal tools and attribution) which leads to fewer installs of their products, more consumers have adopted anti-spyware software for their computers.

While not every program performs the same, even substandard programs can remove the easy-to-find adware programs.

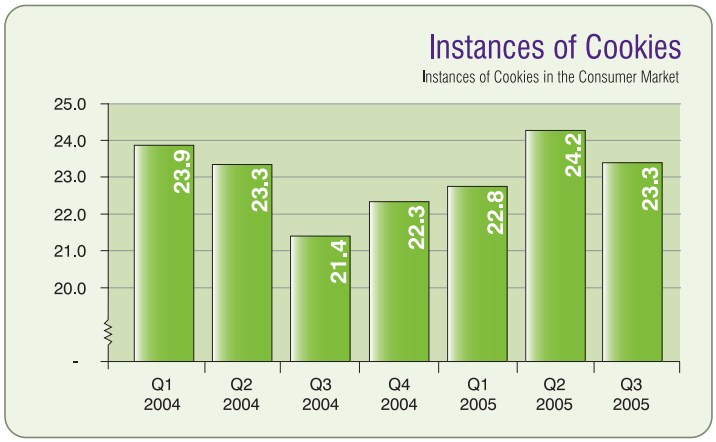
Tracking Cookies

Almost nine in 10 (89 percent) infected consumer PCs have tracking cookies. In the third quarter of 2005, SpyAudit found an average of 23 cookies on consumer PCs infected with cookies.

Online marketers have long used cookies to learn information about their Internet customers and to measure consumer behavior. But as the spyware problem grows more and more insidious, consumers question any files that are downloaded or stored on their personal computers without their consent. Privacy advocates are suspicious about the concept of tracking online behavior.

Walt Mossberg of the Wall Street Journal weighed in on the debate about cookies and spyware. According to Mossberg, tracking cookies meet the definition of spyware and if marketing companies want to use this technique, they should ask a user's permission to install the cookies.

As the debate goes on, Webroot will continue to count cookies as part of the SpyAudit.



LEGAL
& Legislation

Federal Trade Commission Actions

OnGuard Online

Recently, the Federal Trade Commission (the "FTC"), the Department of Homeland Security, the United States Postal Inspection Service and the Department of Commerce launched a new collaborative public education effort called "OnGuard Online." The project's new Web site www.onguardonline.gov is designed to serve as a one-stop-shop for information about online risks such as spyware, identity theft, phishing and spam scams. The Web site also includes important information about how to file a complaint if you are a victim of an online crime.

FTC Testimony on Spyware

FTC Chairwoman Deborah Majoras was the sole witness at an October 5 hearing held by the Senate Commerce Committee's Subcommittee on Trade, Tourism and Economic Development to address the growing problem of spyware and the FTC's jurisdiction and enforcement in this area.

Majoras cited the pervasiveness of spyware and the potential of harm to consumers as primary reasons for making spyware investigations and enforcement a priority and emphasized four additional measures that would enhance FTC efforts to combat spyware.

First, the FTC backs legislation that would improve its ability to take legal action against foreign spyware distributors or those who try to hide their location by using foreign intermediaries.

Secondly, by coordinating with federal and state law enforcement partners, the FTC will be able to prosecute spyware distributors more effectively. An example of this coordinated effort is the August indictment of the creator and marketer of the spyware program "Loverspy" and four others who used the program to break into computers.

The FTC would support legislation that permits it to pursue civil penalites against spyware distributors.

Majoras stressed educating consumers on the risks of spyware and the importance of anti-spyware tools as the third measure that would improve the FTC's ability to protect consumers from spyware.

Lastly, the FTC would support legislation that permits it to pursue civil penalties against spyware distributors as a deterrent.

FTC vs. Odysseus Marketing

FTC File No: 042 3205

The FTC filed a new spyware case in federal court in New Hampshire on Oct. 5, 2005. In FTC vs. Odysseus Marketing, the FTC requested the court to halt the operations of Odysseus Marketing, Inc. ("Odysseus") and its founder, Walter Rines, alleging the defendants' practices are unfair and deceptive and violate the FTC Act.

According to the FTC's complaint, Odysseus offers a freely downloadable software product that Odysseus claims would allow users to engage in peer-to-peer file sharing anonymously. Some of the enticements Odysseus uses to encourage users to download their free software include statements such as: "DOWNLOAD MUSIC WITHOUT FEAR" and "DON'T LET THE RECORD COMPANIES WIN."

The FTC alleges, however, that Odysseus' software does not allow for anonymous file sharing because the peer-to-peer software is bundled with spyware called Clientman that is installed on users' computers without consent.

Clientman, according to the FTC, secretly downloads dozens of other software programs and generates pop-up ads that degrade computer performance and consume memory. Those infected with Clientman can also have their search results corrupted. When users attempt to search the Internet with a search engine such as Google or Yahoo!, they are directed to a look-alike page that lists Odysseus' clients in the results.

When users attempt to search the Internet, they are directed to a look-alike page that lists Odysseus' clients in the results.

The FTC claims that Odysseus deliberately makes its software difficult to detect and impossible to remove using standard software utilities. Although Odysseus offers its own "uninstall" tool, the FTC alleges the tool does not work and triggers additional installations of unwanted software that also capture and transmit information from the users' computers to servers controlled by Odysseus.

Lastly, the FTC argues that Odysseus has an obligation to disclose that its "free" software download is not without cost given that it causes spyware to be installed on users' computers. According to the FTC, the consequences of downloading Odysseus' free software are disclosed only in the middle of a two-page end user license agreement buried in the "Terms and Conditions" section of their Web site.

Other Litigation

In addition to the Odysseus case filed by the FTC, consumers have attempted to find relief directly through the courts in two class action lawsuits filed against alleged spyware vendors. Even though state and federal legislatures are still working on specific spyware legislation, these cases may demonstrate the plaintiffs' ability to bring lawsuits based on existing state and federal laws.

The plaintiffs allege that **the defendants deceptively caused spyware to be installed.**

Sotelo v. DirectRevenue

No. 05 C 2562 (N.D. Ill. Aug. 29, 2005)

In Sotelo v. DirectRevenue, Stephen Sotelo, individually and on behalf of others similarly situated, brought suit against a group of defendants, including DirectRevenue, LLC, DirectRevenue Holdings, LLC, Betterinternet, LLC, Byron Udell & Associates, Inc., d/b/a Accuquote, aQuantive, Inc., and John Does 1-100. Filed in federal court in northern Illinois, the complaint includes among other allegations, trespass to personal property, fraud, negligence and computer tampering.

The plaintiffs allege that the defendants deceptively caused spyware to be installed on the plaintiffs' computers without their consent by bundling their spyware with legitimate software available for free download over the Internet. The spyware then tracked the plaintiffs' Web browsing habits, bombarded the plaintiffs with intrusive pop-up ads, compromised computer performance by consuming bandwidth and memory, and was difficult for the plaintiffs to remove.

The defendants argued that the case should be suspended or dismissed on several grounds, but the federal court ruled that the case may proceed. Notably, the defendants argued that because the end-user license agreement (EULA) provided with the software required disputes to be decided through arbitration rather than litigation, the case should be suspended. However, the plaintiff alleged that the EULA was not always presented to the end user prior to installation of the spyware. The court refused to suspend the case based on the disputed facts as to whether there was consent to the license agreement.

The defendants also argued that the case should be dismissed because the claim of trespass to personal property requires demonstrating that the plaintiffs' personal property was lost or damaged and the defendants' software did not cause such loss or damage. The court, however, refused the defendants' motion and allowed the case to proceed. The court found that demonstrating spyware caused "interference" with the use of a home computer was sufficient to maintain a claim of trespass to personal property.

Simios v. 180Solutions

No. 05 C 5235 (N.D. Ill. Sept. 13, 2005)

In Simios v. 180Solutions, Logan Simios, individually and on behalf of others similarly situated, brought suit against a group of defendants, including 180Solutions, Inc. and John Does 1-100. The complaint was also filed in federal court in northern Illinois by the same law firm that filed the DirectRevenue case.

Similar to the DirectRevenue case, the plaintiffs allege that the defendants deceptively caused spyware to be installed on the plaintiffs' computers without their consent by bundling their spyware with legitimate software available for free download over the Internet or by bundling their software with other spyware, including software distributed by DirectRevenue. Also similar to the DirectRevenue case, the plaintiffs allege the spyware tracks the plaintiffs' Web browsing habits, sends intrusive pop-up ads, compromises computer performance by consuming bandwidth and memory, and is difficult to remove.

Because the DirectRevenue and 180Solutions cases are some of the first class action lawsuits regarding spyware, many will be watching these cases closely as they continue to develop.

Similar to the DirectRevenue case, the plaintiffs allege the spyware tracks the plaintiffs' Web browsing habits.

Congressional Actions

Spyware Legislation

At the U.S. federal level, there are five spyware bills pending action in the Senate Commerce Committee, including the two House-passed bills, H.R. 29 and H.R. 744. The most recently introduced of these bills is the U.S. SAFE WEB ACT (S. 1608).

During the October 5 spyware hearing at which FTC Chairwoman Majoras testified (included previously), Subcommittee Chairman Gordon Smith (R-OR) discussed the strengths of his bill, S. 1608, while Senators Burns and Allen spoke in support of their respective bills, S. 687 and S. 1004. The five bills vary significantly in focus and scope. Thus, in order for a bill to pass the Senate committee, it is likely that a compromise approach will need to be developed. If that is accomplished quickly, passage of a new federal law before the end of the year is still a possibility.

See the Federal Legislation tables on pages 77-79 for more details.

Data Security Legislation

Work on issues like spyware and identity theft earlier in the year increased awareness about the full range of issues that place consumer and business data at risk online. Thus, Congress has increased its focus on the broader agenda of data security related issues over recent months.

Twelve bills dealing with various aspects of information breach and requirements for protecting personal data have been introduced in Congress since March 2005. While it is still unclear which of these bills will move forward to become law, the subject is one of growing interest in Congress. So far there have been hearings in the House Financial Services Committee, the Senate Judiciary Committee and the Senate Commerce Committee.

Most noteworthy is that several of the federal bills include provisions that would require a broad range of companies to develop, implement and maintain an effective information security program. To date, such requirements have been targeted at specific industries, such as financial services and healthcare. If enacted, all companies may need to ensure they have administrative, technical and physical safeguards for the sensitive personal information they hold about their employees and customers.

See the Federal Legislation tables on pages 77-79 for more details.

In addition to the technological solutions available to fight spyware, state and federal government entities continue to increase their efforts to combat spyware and other threats to consumer and business information.

State Spyware Laws and Legislation

At the U.S. state level, there has been considerable legislative activity aimed at fighting spyware over the past two years. Starting with the California Consumer Protection Against Spyware Act, which was signed into law September 30, 2004 and went into effect on January 1, 2005, there are now 12 states, up from 10 states previously, that have enacted laws addressing spyware. Most of these new laws, including those in Arizona, Arkansas, Georgia, Iowa, New Hampshire, Texas, Virginia and Washington, went into effect during the third quarter of 2005. If you are a victim of spyware residing in one of these states, there may be civil and/or criminal actions that could be brought against the spyware purveyors in state courts.

There are now **12 states that have enacted laws addressing spyware.**

In addition to the states that have already enacted laws, there are spyware bills still pending in six state legislatures, including: Illinois, Massachusetts, Michigan, New York, Pennsylvania and Rhode Island. There is also an additional spyware bill pending in California that would allow a person harmed by spyware, the Attorney General, or a district attorney, to file a civil suit for damages under the existing Consumer Protection Against Spyware Act.

See the State Legislation tables on pages 80-82 for more details.

State Data Security Laws and Legislation

In addition to the state laws and bills that deal specifically with spyware, more than 100 bills dealing with the broader issue of data security and the breach of information have been introduced across 35 states. In 21 of these states, one or more of the introduced bills was signed into law by September 30, 2005.

25 states have enacted a total of **54 new identity theft laws.**

There were also numerous legislative initiatives dealing specifically with identity theft. During the first three quarters of 2005, 25 states enacted a total of 54 new identify theft laws. There were also many data security and identity theft laws enacted across the states prior to 2005. All of this is in addition to the wide range of consumer protection laws that have existed in the states for many years.

United Kingdom Spyware Summit

When viruses and spam first arrived on the scene, Internet users were exposed with little means of formal intervention. Industry and regulatory bodies found themselves on the back foot and struggled to contain the problem. However with the advent of spyware, industry and regulatory bodies – having taken onboard the hard lessons learned – are standing to attention and are now applying a more pre-emptive approach to combating the spyware threat.

The United Kingdom's first dedicated Spyware Summit is a recent example of top industry experts, policymakers and parliamentarians gathering together to take the first steps toward gaining a comprehensive understanding of spyware, while drawing on one another's own expertise to illuminate the present threat at both national and international levels.

The summit was held in the historic Astor Suite in Westminster. The suite is named after Nancy Astor, an American who became the first woman Member of Parliament in the United Kingdom.

Invited delegates from leading security organizations such as British Computer Society (BCS), the National Hi-Tech Crime Unit (NHTCU), European Information Society Group (EURIM), Experian and the Association for Payment and Clearing Services (APACS) met to discuss possible measures to eradicate this costly problem that is negatively influencing e-commerce worldwide.

The UK's Spyware Summit is a recent example of **taking the first steps toward gaining a comprehensive understanding of spyware.**

Key developments:

- **Accurate terminology -** A call for further clarification was made on how and in what context 'spyware' is referenced. For legislative purposes, delegates agreed clearer categories are needed.

- **Voluntary code -** Delegates stressed that the marketing community must play a more prominent role and called on organizations like the Direct Marketing Association to establish a uniform industry code of practice for Internet marketing. It was also agreed more guidance is needed on striking a balance between 'knowing your customer and spying on them.'

- **Standardization** – It was agreed that the validity of informed consent and user license agreements must be reviewed and tested in U.K. law. Further collaboration is needed to agree to a set of standardized definitions. Due to adware preying on young Internet users, it was suggested that age should be taken into account and that an age guidance rating be applied to ensure user agreement validity.

- **Global collaboration -** Delegates noted that because the Internet is borderless any ensuing legislation should be global. However the nature of spyware means jurisdiction is unfortunately ambiguous. Delegates called for action on immediate reciprocal legislative arrangements. It will be incumbent on multiple federal governments worldwide to come to a cohesive approach to legislation and the prosecution of spyware purveyors.

- **Awareness and education -** Technology is not the only solution. Further public awareness and education is essential. Delegates agreed that users must be made aware of the scale of potential loss on the Internet; however extreme caution must be taken so not to compromise confidence.

Spyware is now high commerce. Although more aggressive action is being taken, there is still a long battle ahead. For spyware to be successfully contained, local and international bodies must work together to agree an open and collaborative plan of action and form a united, borderless front.

CONCLUSION

As the Q3 2005 State of Spyware Report reveals, spyware continues to evolve into more complex and more harmful programs. This evolution has affected consumer confidence, while enterprises scramble to maintain regulatory compliance with the FTC, HIPAA and other initiatives.

State and federal legislation is on the rise in efforts to protect home computer users and corporations alike from the threats of spyware. New state spyware laws took effect during the third quarter. Federal legislators are working through a number of bills aimed at fighting spyware.

As states enact consumer notification laws, an increase in the public disclosure of security breaches and incidents may occur. Some of those incidents will be caused by insiders using simple to deploy keystroke loggers to spy on their co-workers and supervisors. And, industrial espionage on the scale of the Israeli Trojan fiasco will surface as a real and present danger in European, Asian and North American countries.

Earlier in the year, spyware writers began using Trojans to commit cyber-crimes and the trend hasn't slowed. According to the Enterprise SpyAudit, 8 percent of desktop PCs are infected with malicious spyware. This high number is reason for concern for enterprise, in light of the new regulatory compliance initiatives from the FTC, HIPAA and Gramm-Leach-Bliley.

Looking forward to Q4 2005, industry analysts anticipate that new spyware laws may contribute to increased prosecution of adware vendors, but more malicious forms of unwanted software will continue to proliferate. They will use root-kit techniques to avoid discovery and removal.

The trend is evident. The overall threat to Internet security is rising dramatically as malware is bent to the purpose of stealing information for financial gain.

APPENDIX

Federal Legislation – Enacted

Bill Title & Number	Primary Supporters	Summary	Status as of 9.30.05
"SPY ACT" **Securely Protect Yourself Against Cyber Trespass Act of 2005** US House Bill HR 29	Rep. Joe Barton (R-TX) Rep. Cliff Stearns (R-FL) Rep. Mary Bono (R-CA) Rep. Ed Towns (D-NY)	• Prohibits certain kinds of programs installed without the users knowledge. • Regulates "information collection programs" by prescribing in detail the type of notice and consent required of such programs. • Provides a limited "Good Samaritan" provision to protect anti-spyware producers. • Damages of $11,000 for single violations and up to $3 million for the most egregious patterns and practices. • Preempts state laws. • No civil actions. • FTC to study impact of tracking cookies, and report to Congress. • Effective 12 months after enactment. • Sunsets December 31, 2010.	• Sent to Senate May 24, 2005 referred to Commerce Committee • Approved by the House with a vote of 393-4 May 23, 2005 • Passed Commerce committee 43-0 April 12, 2005
"I-SPY Act" **Internet Spyware Prevention Act of 2005** US House Bill HR 744	Rep. Bob Goodlatte (R-VA) Rep. Lamar Smith (R-TX) Rep. Zoe Lofgren (D-CA)	• Criminal penalties (up to 5 years jail time) for the unauthorized access or download to a computer. • Expresses the sense of Congress that the Department of Justice should vigorously prosecute those who use spyware to commit crimes and those that conduct phishing scams. • Preempts state laws. • Authorizes $10 million for the U.S. Attorney General for prosecutions and enforcement activities.	• Sent to Senate May 24, 2005 referred to Commerce Committee • Approved by the House with a vote of 395-1 May 23, 2005 • Passed Judiciary committee by voice vote May 18, 2005
"SPY BLOCK Act" **Software Principles Yielding Better Levels of Consumer Knowledge Act** US Senate Bill S 687	Sen. Conrad Burns (R-MT) Sen. Ron Wyden (D-OR) Sen. Barbara Boxer (D-CA) Sen. Bill Nelson (D-FL)	• Prohibits certain behaviors related to software, i.e., surreptitious installation. • Prohibits installation of advertising programs that don't label the ads. • Provides the FTC with rulemaking authority. • Provides liability protection for anti-spyware producers. • Provides for regular damages available under the FTC Act ($11,000 per violation). • Criminal penalties (up to 5 years jail time) for the unauthorized access or download to a computer. • Preempts state laws. • No civil actions, but the bill specifically allows State Attorneys General, under certain circumstances, to bring a cause of action on behalf of their citizens	• Introduced March 20, 2005 • Commerce Committee Spyware hearing May 11, 2005

Federal Legislation – Enacted

Bill Title & Number	Primary Supporters	Summary	Status as of 9.30.05
Enhanced Consumer Protection Against Spyware Act of 2005 US Senate Bill S 1004	Sen. George Allen (R-VA) Sen. John Ensign (R-NV) Sen. Gordon Smith (R-OR)	• Expresses the sense of Congress that the FTC should vigorously prosecute spyware cases. • Restates FTC authority over these cases, and allows for them to triple the regular fines allowed by existing law. • No civil actions, but the bill specifically allows State Attorneys General, under certain circumstances, to bring a cause of action on behalf of their citizens. • Criminal penalties (up to 5 years jail time) for the unauthorized access or download to a computer. • Authorizes $10 million for the FTC for enforcement activities.	• Introduced May 11, 2005 • Commerce Committee Spyware hearing May 11, 2005
"U.S. SAFE WEB Act" Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2005 US Senate Bill S 1004	Gordon Smith (R-OR) Daniel Inouye (D-HI) John McCain (R-AZ) Bill Nelson (D-FL)	• Amends the FTC Act to include in the definition of "unfair or deceptive acts or practices," acts involving foreign commerce that: (1) cause or are likely to cause reasonably foreseeable injury in the U.S.; or (2) involve material conduct occurring within the U.S. • Grants the FTC power to transmit to the Attorney General evidence of federal criminal law violations by both domestic and foreign entities. • Prescribes FTC procedural guidelines for sharing investigation information with foreign law enforcement agencies. • Shields certain voluntary providers of information from liability.	• Introduced July 29, 2005

Federal Legislation – Pending

Bill Title & Number	Primary Supporters	Committee Referrals	Actions as of 09.30.05
Notification of Risk to Personal Data Act US House Bill HR 1069	Melissa Bean (D-IL)	• House Energy and Commerce • House Financial Services • House Government Reform	• Introduced March 3, 2005
Consumer Privacy Projection Act of 2005 US House Bill HR 1263	Cliff Stearns (R-FL)	• House Energy and Commerce • House International Relations	• Introduced March 10, 2005
Consumer Data Security and Notification Act of 2005 US House Bill HR 3140	Melissa Bean (D-IL)	• House Financial Services	• Introduced June 30, 2005
Consumer Notification and Financial Data Protection Act of 2005 US House Bill HR 3374	Steve LaTourette (R-OH)	• House Financial Services	• Introduced July 21, 2005
Financial Data Security Act of 2005 US House Bill HR 3375	Deborah Pryce (R-OH)	• House Financial Services	• Introduced July 21, 2005
Consumer Access Rights Defense Act (CARD) of 2005 US House Bill HR 3501	Julia Carson (D-IN)	• House Energy and Commerce • House Financial Services • House Government Reform	• Introduced August 24, 2005
Financial Privacy Breach Notification Act of 2005 US Senate Bill S 1216	Jon Corzine (D-NJ)	• Senate Banking	• Introduced June 9, 2005
Notification of Risk to Personal Data Act US Senate Bill S 1326	Jeff Sessions (R-AL)	• Senate Judiciary	• Introduced June 28, 2005
Personal Data Privacy and Security Act of 2005 US Senate Bill S 1332	Arlen Specter (R-PA)	• Senate Judiciary	• Introduced June 29, 2005 • Placed on Senate Calendar July 12, 2005
Identify Theft Protection Act US Senate Bill S 1408	Gordon Smith (R-OR)	• Senate Commerce	• Introduced July 14, 2005 • Approved by Committee July 28, 2005
Financial Privacy Protection Act of 2005 US Senate Bill S 1594	Jeff Sessions (R-AL)	• Senate Banking	• Introduced June 28, 2005
Personal Data Privacy and Security Act of 2005 US Senate Bill S 1789	Arlen Specter (R-PA)	• Senate Judiciary	• Introduced September 29, 2005

State Legislation – Enacted

State & URL	Legislation	Summary	Status as of 9.30.05
Alaska http://w3.legis.state.ak.us	S.B. 140	Prohibits spyware and unsolicited Internet advertising, in particular "spyware pop-up advertisements".	**Chapter 97 SLA 05** Effective November 28, 2005
Arizona http://www.azleg.state.az.us	H.B. 2414	Prohibits transmission of computer software through intentionally deceptive means that modifies settings, collects personally identifiable information, or takes control of the computer.	Governor signed April 18, 2005 **Public Act 136** Effective Date August 11, 2005
Arkansas http://www.arkleg.state.ar.us	H.B. 2904	Prohibits unauthorized installation of computer software and numerous other deceptive practices as detailed in the bill. Violations are actionable as deceptive trade practices. Establishes a spyware monitoring fund.	Governor signed April 15, 2005 **Public Act 2255** Effective July 1, 2005
	H.B. 2261	Appropriates funds to cover expenses associated with spyware monitoring for the office of Attorney General.	Governor signed April 15, 2005 **Public Act 2312** Effective July 1, 2005
	H.B. 2344	Appropriates funds to cover expenses associated with spyware monitoring for the Department of Information Systems.	Governor signed April 15, 2005 **Public Act 2313** Effective July 1, 2005
California http://www.leginfo.ca.gov	Business & Professions Sec. 22947-22947.6	Consumer Protection Against Computer Spyware Act. Prohibits unauthorized changes to computer settings, collection of personally identifiable information, removal of security, anti-spyware and anti-virus programs, and other acts.	Effective January 1, 2005
Georgia http://www.legis.state.ga.us	S.B. 127	Prohibits deceptive acts and practices with regard to computers and requires notice be given prior to the installation of software programs. Provides for civil and criminal penalties and the recovery of certain damages.	Governor signed May 10, 2005 **Public Act 389** Effective July 1, 2005
Iowa http://www.legis.state.ia.us	H.B. 614	Protects owners and operators of computers from the use of spyware and malware that is deceptively or surreptitiously installed on their computers.	**House File 614** Signed by Governor May 3, 2005
Nevada http://www.leg.state.nv.us/	A.B. 334	Primarily deals with protecting the privacy of a person's social security number and other personal and financial information; however, it includes spyware on the list of prohibited computer contaminants.	**Public Law 486** Effective January 1, 2007
New Hampshire http://www.gencourt.state.nh.us	H.B. 47	Provides that using spyware or similar computer programs to knowingly alter, take control of, or damage a consumer's computer or Internet access will be a violation of the Consumer Protection Act.	**Public Law 238** Effective January 1, 2007

State Legislation – Enacted

State & URL	Legislation	Summary	Status as of 9.30.05
Texas http://www.capitol.state.tx.us	S.B. 327	Prohibits unauthorized collection or transmission of personally identifiable data. Prohibits unauthorized installation or disabling of software. Includes civil penalties.	Signed by the Governor June 17, 2005 **Chapter 298** Effective Date September 1, 2005
Utah http://www.le.state.ut.us	H.B. 104	Amends the Spyware Control Act by removing the prohibition on contextual advertising.	**Chapter 168** Effective Date March 17, 2005
	H.B. 323	Spyware Control Act. Prohibits spyware installations and context based advertising.	**Chapter 363** Preliminary injunction issued by 3rd Judicial District Court, June 2004
Virginia http://leg1.state.va.us	H.B. 2215	Amends the Virginia Computer Crimes Act to prohibit altering, disabling or erasing computer data, computer programs or computer software. Also prohibits causing a computer to malfunction, regardless of how long the malfunction persists.	**Acts of Assembly** **Chapter 812** Effective Date July 1, 2005
Washington http://www1.leg.wa.gov/legislature	H.B. 1012	Prohibits unauthorized installation of software, including opening multiple, sequential, stand-alone advertisements in the consumer's internet browser, as well as other types of deceptive behavior. Providers of computer software and trademark owners adversely affected by a violation of the Act, can bring action to enjoin further violations and to recover damages.	**Public Act 500** Effective July 24, 2005

State Legislation – Pending

State & URL	Legislation	Summary	Status as of 9.30.05
California http://www.leginfo.ca.gov	S.B. 92	Authorizes the recipient of spyware or software transmitted in violation of the prohibitions to recover damages, and also stipulates criminal penalties.	Passed Senate May 23, 2005 Pending action in Assembly
Illinois http://www.ilga.gov	H.B. 380	Prohibits unauthorized installation of programs that take control of the computer; modify settings; collect personally identifiable information through deceptive means, and other actions. Makes a violation of the Act a Class B misdemeanor.	Passed House February 8, 2005 Passed Senate Committee May 4, 2005 Pending Senate floor action
Massachusetts http://www.mass.gov/legis	S.B. 273	Prohibits installation of spyware on another person's computer; or the use of a context based triggering mechanism to display an advertisement that interferes with a user's ability to view a website.	Introduced January 26, 2005 Referred to Economic Development and Emerging Technologies
	S.B. 286	Regulates "unconsented" Internet advertising, and requires a clear "opt-in" choice.	Introduced January 26, 2005 Referred to Economic Development and Emerging Technologies
Michigan http://www.legislature.mi.gov	S.B. 53	Provides sentencing guidelines for the crime of installing spyware on another person's computer without consent.	Passed Senate March 9, 2005
	S.B. 54	Prohibits accessing computers, computer systems, and computer networks for fraudulent purposes. Prohibits intentional and unauthorized access, alteration, damage, and destruction of computers, networks, computer software, or data. Prescribes criminal penalties.	Passed Senate March 9, 2005
	S.B. 151	Prohibits and provides civil remedies for installing spyware or adware onto another individual's computer without consent.	Passed Senate March 9, 2005
New York http://assembly.state.ny.us	A.B. 549	Establishes the unlawful use of spyware and malware as a class A misdemeanor; and a class E felony for a person who has been previously convicted within the last five years of violating this section.	Introduced January 13, 2005 Referred to Codes
	A.B. 2682	Establishes the unlawful dissemination of spyware as a class A misdemeanor. Expands eavesdropping to include information intercepted by spyware. Requires an authorization agreement be provided to computer users prior to software downloads.	Introduced January 28, 2005 Referred to Codes
	S.B. 186	Same as A.B. 2682	Passed Senate June 23, 2005
	S.B. 3600	Same as A.B. 549	Introduced March 23, 2005 Referred to Codes
Pennsylvania http://www.legis.state.pa.us	H.B. 574	Prohibits the misuse of adware or spyware and defines what actions would constitute misuse.	Introduced February 16, 2005 Referred to Judiciary
	H.B. 1697	Prohibits the unauthorized transmission of computer software, adware or spyware to a computer owned by another person.	Introduced June 13, 2005 Referred to Commerce
	S.B. 711	Prohibits deceptive installation of spyware and provides for enforcement and for civil relief.	Approved by Communications & Technology Committee June 13, 2005 Introduced June 3, 2005
Rhode Island http://www.rilin.state.ri.us	H.B. 6211	Defines unlawful modification of computer settings, unlawful control of a computer and prohibits the deceptive sale of software.	Introduced March 10, 2005 Referred to House Corporations

Categories

Adware

Adware is advertising-supported software that displays pop-up advertisements whenever a program is open. Adware software is usually available via free downloads from the Internet. Adware is often bundled with or embedded within freeware, utilitarian programs like filesharing applications, search utilities, information-providing programs (such as clocks, messengers, alerts, weather, and so on), and software such as screensavers, cartoon cursors, backgrounds, sounds, etc. Although seemingly harmless, adware applications may monitor your Internet surfing activities and display advertising including targeted pop-up, pop-under, and other advertisements on your computer. Some adware may track your Web surfing habits. Deleting adware may result in the deletion of the bundled freeware application. Most advertising supported software doesn't inform you that it installs adware on your system, other than via buried reference in a license agreement. In many cases, the downloaded software will not function without the adware component. Some adware can install itself on your computer even if you decline an advertisement offer.

System Monitors

System monitors have the ability to monitor your computer activity. They range in capabilities and may record some or all of the following: keystrokes, e-mails, chat room conversations, instant messages, Web sites visited, programs run, time spent on Web sites or using programs, and even usernames and passwords. The information is transmitted via remote access or sent by e-mail.

A keylogger is a type of system monitor that has the ability to monitor all keystrokes on your computer. A keylogger can record and log your e-mail conversations, chat room conversations, instant messages, and any other typed material. They may have the ability to run in the background, hiding their presence. Keyloggers and system monitors may be used for legitimate purposes but can also be installed by a user to record sensitive information for malicious purposes.

Traditionally, system monitors had to be installed by someone with administrative access to your computer, such as a system administrator or someone who shares your computer. However, there has been a recent wave of system monitoring tools disguised as e-mail attachments or “freeware” software products.

Tracking Cookies

Tracking cookies are one type of spyware. These are pieces of information that are generated by a Web server and stored on your computer for future access. Cookies were originally implemented to allow you to customize your Web experience, and continue to serve a useful purpose in enabling a personalized Web experience. However, some Web sites now issue tracking cookies, which allow multiple Web sites to store and access cookies that may contain personal information (including surfing habits, user names and passwords, areas of interest, etc.), and then simultaneously share the information it contains with other Web sites. This sharing of information allows marketing firms to create a user profile based on your personal information and sell it to other firms. Tracking cookies are usually installed and accessed without your knowledge or consent.

Trojan Horses

A Trojan horse is a malicious program, disguised as a harmless software program. Trojans do not replicate themselves like viruses, but they are spread through e-mail attachments and Web downloads. After opening the file, the Trojan may install itself on your computer without your knowledge or consent. It may manage files on your computer, including creating, deleting, renaming, viewing, or transferring files to or from your computer. It may install a program that allows a malicious user to install, execute, open, or close software programs or take full control of the infected machine. The malicious user may also open and close your CD-ROM drive, gain control of your cursor and keyboard, and may even send spam by sending mass e-mails from your infected computer. They have the ability to run in the background, hiding their presence.

Methodology

Data Collection

Both the Consumer SpyAudit and Enterprise SpyAudit collect data from individuals or corporations who visit the Webroot website www.webroot.com, or some other affiliated site where the SpyAudit is available, and elected to download and run a SpyAudit scan. Additionally, Webroot may use the tool to help customers evaluate spyware problems. Because of this self-selecting sample, the data may not reflect the "general" Internet population and may be skewed to an audience who believes they may have a spyware issue.

Data for the Enterprise SpyAudit have been collected since October 2004. The Consumer SpyAudit has collected data since January 2004. SpyAudit data is collected and aggregated anonymously. No personal or specific computer data is collected with the audit results.

Instances of spyware detected are collected from each scan and grouped into one of four categories (adware, cookie, system monitor, Trojan). If an entry is made into a category, a scan is added to that category's scan count (Category Infected Machine - a), and a flag is triggered indicating a scan that included an infection (Infected Machine - b). Regardless of whether any instances are found, a scan is always added to the total scan count (Scanned Machine - c). These counts are used as the denominators for the statistics quoted in this report.

Calculations and Formulae

Using the denominators above, below are the formulae used in calculations:

- Percentage of Infected Machines: B / C
- Avg Instances per scan: Total Instances / C
- Avg Instances per Infected Machine: Total Instances / B
- Percentage of Infected Machines (excluding cookies): (B less Cookie A) / C
- Avg Instances (excluding cookies) per Machine: (Total Instances – Cookies) / C

The Webroot Consumer and Enterprise SpyAudits can be accessed by visiting:
Corporate: http://www.webrootdisp.net/entaudit/start.php
Consumer: http://www.webroot.com/services/spyaudit_03.htm
Webroot Software, a privately held company based in Boulder, Colorado, creates innovative privacy, protection and performance products and services for millions of users around the world, ranging from enterprises, Internet service providers, government agencies and higher education institutions, to small businesses and individuals.

Webroot Compliance Survey

Webroot polled readers of Chief Security Officer magazine on the topic of spyware and information security compliance. The 63 respondents represent 63 organizations with a total of 351,149 PCs and laptops connected to the Internet.

CREDITS

Credits

Webroot would like to recognize and thank the following professionals who contributed to this report.

- Threat Research Team, Webroot Software
- Kate Borten, CISSP, CISM, President, The Marblehead Group, **Spyware Meets HIPAA** http://www.webroot.com/pdf/wp_hipaa_q305.pdf
- Charles H. Kennedy, Counsel, Morrison and Foerster LLP, **The Emerging Threat of Legal Liabilty for Failure to Prevent Spyware Attacks** http://www.webroot.com/pdf/wp_glb_q305.pdf
- Peter Warren, Future Intelligence, **Global CyberCrime: The Technical Sophistication of Cybercriminals and their Effect on the Global Economy**

Citations

Webroot would like to acknowledge and credit the following resources used in this report.

- Computer Security Institute (CSI) with the involvement of the San Francisco's Federal Bureau of Investigation's (FBI) Computer Intrusion Squad, **Computer Crime and Security Survey**, July 14, 2005
- Walter S. Mossberg, Wall Street Journal, Despite Others' Claims, **Tracking Cookies Fit My Spyware Definition**, July 14, 2005
- Princeton Survey Research Associates International and Consumer Reports WebWatch, **Leap of Faith: Using the Internet Despite the Dangers**, Oct. 26, 2005
- U.S. Census Bureau, **Computer and Internet Use in the United States: 2003**, October 2005
- Computerworld, **The Computerworld Spyware Survey: Methodology and Detailed Results**, October 31, 2005

ABOUT
Webroot Software

The company provides easy-to-use anti-spyware software that guides and empowers computer users as they surf the Web, protecting sensitive information and returning control over computing environments. Webroot's software consistently receives top ratings and recommendations by respected third-party media and product reviewers. The company is backed by some of the industry's leading venture capital firms, including Technology Crossover Ventures, Accel Partners and Mayfield.

In addition to selling these products online at www.webroot.com, Webroot products are found on the shelves of leading retailers around the world, including: Best Buy, Circuit City, CompUSA, Fry's, MicroCenter, Office Depot, Staples, Target and Wal-Mart. Webroot products are also available as either branded solutions or on an OEM basis. To find out more about Webroot, visit www.webroot.com or call 1.800.870.8102.

NO WARRANTY. The technical information is being delivered to you AS-IS and Webroot Software makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Webroot reserves the right to make changes without prior notice.

Certain data is available upon request.

Webroot Software, Inc.
P.O. Box 19816
Boulder, CO 80308-2816
USA

www.webroot.com
Company: (303) 442-3813
Corporate Sales & Support: (800) 870-8102
Consumer Sales & Support: www.webroot.com/support
Fax: (303) 442-3846