STATE OF SPYWARE

Q2 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

Famed robber Willie Sutton was once asked why he held up banks. His reported response: “Because that’s where the money is.” In the simplicity of this trite maxim, there is also a truism that illustrates the current state of the spyware market.

Spyware’s underlying principle: it is a business. The shadowy – and sometimes very up-front - purveyors of this insidious practice are distant cousins to their counterparts in the virus world. Although some protest that spyware is just another form of viruses, cursory inspection reveals one significant difference: money.

In 2003, when we at Webroot began to evangelize the coming storm of spyware to the industry and the press, we used an appreciable simile to portend the future. Virus writers are, we proffered, like graffiti artists, unleashing cyber-havoc on the world for their own voyeuristic enjoyment and for the renown within their own twisted, hacker circles. Viruses were -- to our thinking -- simply vandalism.

Spyware is different. It is an enterprise, designed as a profit-making venture to inflict users, at best, with an onslaught of pop-up ads that translates in micro-charges and eventually amounts to real money; or at worse, just to steal from an unsuspecting user who wandered into the wrong place or clicked on the wrong OK button. Virus writing may gain some twisted fame, spyware brings fortune.

To their credit, lawmakers, the press and anti-spyware developers all saw the issue and with relatively quick and effective action took major steps toward eradicating the problem. Legislation is now pending in 19 states and no less than four bills affecting spyware are now in consideration at the Federal level.

Last winter, a massive education campaign was waged serendipitously by the national media and the word got out about the scourge. Even some adware vendors have begun to take steps to change their business models to be on the right side of the law and public opinion. Users themselves started refraining from some Internet practices and, according to the Pew Institute, rolled back surfing time to avoid having their computers invaded.

But, along the way we may be missing one seminal issue: spyware is a business and, when one market starts to wane, a capable business does one of two things. Either, they defend their franchise and/or they find new markets to exploit. In this past quarter, we have seen an alarming rise in the sophistication of certain spyware in how they invade a machine, how they remain on that machine and how they transmit the valuable information they find there back to whomever or whatever. Infection rates and the number of sites hosting spyware are up significantly in the quarter.

Spyware routinely now has a hydra-like capability to morph into new forms when the original executable is detected and removed. Spyware programs are now using new and ingenious tactics to send information. Spyware writers understand that their business model is under siege and to survive they are employing every tactic they can.

The second tact a threatened business will take is to look for new products and new markets. The incidents of Trojans and system monitors are growing much faster than more tolerable ad-pushing software. Also the number of traces - the ancillary components of a given piece of spyware that essentially do the dirty work - doubled in the first half of the year.

Basically, spyware writers are creating new and more innovative products to flood the market. And we are seeing evidence of the nightmare scenario: spyware emerging from the darker corners of the Web - like peer-to-peer file sharing services and pornography sites - and brazenly coming into the light of much more legitimate confines. A user we know was invaded while shopping for movie posters on seemingly benign art e-commerce sites. We have seen spyware on music lyric sites. We have even heard of spyware residing inside a listing on a popular auction site (although that incident was not replicable).

And then there are the highly publicized corporate spyware intrusions. Card Systems compromised the credit card numbers of thousands of customers, a transgression that will certainly threaten the company's existence. BJ's Wholesale Club, a $6.6 billion retail conglomerate, was targeted by the Federal Trade Commission, in a potential landmark case in which the FTC sued the company, not because their security was attacked by spyware, but more interestingly because their security was lax enough to let it happen. There are several more incidents recounted in this report, but remember, these are the ones we know about. Undoubtedly, there are countless others which wary executives are deftly keeping from public scrutiny.

Users are protecting themselves more and legislators and other government entities are ensuring that there is a credible and substantial penalty. Even some vendors of conventional adware have openly said they will reassess their practices. The problem is that spyware is now high commerce and for every senator, FTC lawyer or even Webroot Threat Research professional, there are many more programmers in some dark place devising an ingenious method for getting spyware on a computer, keeping it there and harvesting information for a profit.

Webroot and others are continually developing defenses and we are certainly up to the task. And we applaud elected and appointed officials fighting this battle with every legislative weapon in their sizeable arsenal. But there is still one point of caution: armed robbery can get you 20 years in a maximum security penitentiary and yet Willie Sutton still robbed banks, because that's where the money is.

C. David Moll
CEO
Webroot Software, Inc.

HIGHLIGHTS

Incidents

Every day it seems like there's another story about loss or theft of customer or employee data, often through the use of Trojans and system monitors. In total, the incidents section covers a dozen stories of this nature that have cropped up across the globe in the past three months. Corporations like MasterCard International, Bank of America, BJ's Wholesale Club, DSW Warehouse and others have jeopardized the personal information of millions of customers. Spyware is to blame for some of these incidents. And these are just the attacks we know about. According to the FBI, only one in five corporations reports cyber-attacks out of fear of losing consumer confidence. – page 15

Threat Research/Phileas

The number of spyware-producing Web sites Phileas has identified has quadrupled from the start of Q1 2005, and the number of spy traces that Webroot detects and removes has doubled for the first half of 2005. These results show that spyware writers are more and more active.

Even more concerning is that Webroot's Threat Research Team has witnessed an increase in the more malicious types of spyware, which are smarter at avoiding detection and removal, and capable of ensuring survival through new tactics never seen before. The majority of spyware is coming from the U.S., with Poland coming in second and the Netherlands in third. – page 29

Enterprise

In the second quarter of 2005, the Webroot Enterprise SpyAudit identified at least one form of unwanted program (Trojan, system monitor, cookie or adware) on more than 80 percent of the PCs it scanned. What's more concerning is that the frequency of malicious spyware on an infected PC rose 19 percent over last quarter. – page 35

Compliance

In today's business, keeping desktops spyware-free isn't just about reducing help desk calls. It's about maintaining compliance with federal regulations, and even one piece of malicious spyware can throw a company out of compliance. The compliance section provides an in-depth look at how spyware can affect compliance with Sarbanes-Oxley. – page 40

Consumer

In Q2 of 2005, the Webroot Consumer SpyAudit results showed that 80 percent of scanned PCs had at least one form of unwanted program. The number of spyware instances per machine has increased to an all-time high of 25.4 per machine, up from 22.8 instances per PC from Q1 of 2005. The repercussions of the presence of illegitimate adware programs along with malicious spyware applications like system monitors and Trojans continue to plague Internet users. – page 46

Legislation

Spyware is on the minds of legislators across the world. In the U.S., the FTC has been very active in pursuing and punishing companies like BJ's Wholesale Club, which grossly mishandled customer data. On the federal lawmaking level, four bills are in consideration in the Senate Committee for Commerce, Science and Transportation. And 10 states have enacted anti-spyware legislation, with 10 additional states considering close to 20 total bills. In Germany, the country's constitution provides groundbreaking guidance regarding spyware. – page 52

THE STATE
of Spyware

The Webroot Q2 2005 State of Spyware Report offers several insights regarding spyware trends. First, adware vendors continue to generate revenue using the proven infection methods of pop-up ads and click-throughs. Secondly, online privacy and security are at a greater risk as spyware writers use malicious techniques to steal personal information for faster financial gains. Not to mention that new spies are constantly evolving in attempts to avoid detection from anti-spyware solutions. The number of known spy traces has doubled in the first half of this year. In addition, spyware distribution sites have quadrupled this year totaling more than 300,000 Web sites. End users have to be extremely cautious to avoid Web sites that covertly distribute spyware.

The number of spyware distribution sites have **quadrupled this year.**

This report includes the results from separate consumer and enterprise SpyAudits run on thousands of PCs. Infection rates of system monitors and Trojans are holding steady at the alarming numbers revealed in the Q1 report while less harmful tracking cookies are on the rise. However, in response to public outcry, adware distributors in the United States have attempted to improve the behavior of their products. As a result, the penetration rates of mainstream adware companies are slowing, however, extremely pernicious forms of adware such as CoolWebSearch (CWS) are filling the void.

Motivating adware vendors to improve their behavior is the high level of legislative activity, both state and federal, targeted at spyware. The U.S. House passed bills HR 29 (Rep. Bono) and HR 744 (Rep. Goodlatte). As of this writing, they reside with the Senate along with bills, S. 687 (Sen. Burns) and S. 1004 (Sen. Allen), all of which are before the Senate Commerce Committee. The Senate is expected to take action on spyware this fall.

But, in the meantime, there continues to be new state actions. There are twelve states that have passed new spyware laws– although some are not yet signed or in effect. There are an additional 19 bills still active and pending in 10 states. Even without federal action on spyware, the adware vendors will have to comply with a myriad of confusing requirements from all of these state actions.

Actions by Elliot Spitzer, the New York State Attorney General, had a particularly chilling effect on the adware industry when he brought suit against publicly traded Intermix, which quickly settled for $7.5 million and assured their stock holders that they were no longer in the adware business. Intermix was then purchased by News Corp. for $580 million.

The nature of cybercrime is evolving.

Meanwhile the Federal Trade Commission (FTC) brought suit against bogus anti-spyware companies that were preying on the high levels of demand for solutions to the spyware problem. And in a separate action, a consensus was reached with BJ's Wholesale Club requiring them to follow what is commonly regarded as industry best practices in security.

The nature of cybercrime is evolving. The number of system monitor incidents reported in Q2 2005 reached a new high. A major Trojan horse incident in Israel rocked the entire business community, while in the United Kingdom authorities issued warnings that targeted Trojan attacks were being launched against United Kingdom government agencies and industrial targets from Asia.

The Webroot Threat Research Team reports that spyware writers are rapidly refining the tools and techniques they use to avoid detection and removal. Because spyware writers significantly outnumber anti-spyware developers, it's difficult for any anti-spyware solution to keep pace with the threat. The Threat Research portion of this report details the methodologies being brought to bear both in discovering the spies as well as countering them. Three research techniques for finding spies are manual discovery, client automation, and Web crawler automation.

Results from Webroot's Phileas automatic Web crawler have allowed Webroot not only to catch up with known spyware programs, but to stay on top of the newly created spies each week. Phileas findings produce more than 300 spyware definitions a week. For the first time, we are reporting on the geographic origin of spyware with some interesting results. While the United States continues to be the largest originator of spyware, Poland has established its position as an up-and-coming contender, and is likely to become even more dominant given the threat of legal action against U.S.-based developers and distributors.

The Q2 2005 State of Spyware Report identifies a disturbing trend in regards to the sophisticated tools and techniques used by spyware writers to install their programs and avoid detection and removal. The Webroot Threat Research Team reports on the best (worst) examples of these techniques such as altered registry settings, encryption algorithms or packers such as UPX, Aspack, FSG, or their own proprietary algorithms, which render previous detection techniques obsolete.

Summary

Spyware developers continue to explore new ways to get installed and avoid detection. System monitors are being installed via targeted attacks against industrial competitors, government agencies and banks to steal login credentials and intellectual property. Legislative efforts in the United States and European Union are slowing the success rate of visible adware vendors, but are having little effect on the most malicious adware vendors. While enterprises initially regarded spyware as an annoyance that could be treated "tactically," they are quickly learning that their infection rates are too high and the costs of remediation are out of control. Strategic use of a centrally managed desktop anti-spyware solution is the only way to gain control over this menace to productivity and security.

Incidents
in the News

Incidents

The tumultuous second quarter of 2005 witnessed more than a dozen incidents involving the corporate loss of data for customers and employees. News stories reported security breaches at some of the largest names in business, including Lexis-Nexis, DSW Warehouse, BJ's Wholesale Club, Time Warner and Bank of America.

Even more sensational reports were published and signify the greatest changes in the threat landscape, including the now infamous Israeli Trojan fiasco and news from the United Kingdom that government agencies and large corporations were under continuous monitoring.

One of the single most compelling data thefts of the quarter occurred at **BJ's Wholesale Club, Inc.** with the loss of thousands of customers' credit card information. The loss of this personal information led the Federal Trade Commission to bring charges against the company using Section 5 of the FTC Act. Section 5 gives the FTC the authority to challenge deceptive or unfair acts and practices that affect commerce. More detail on this Act can be found on page 52.

One of the single most compelling data thefts of the quarter occurred at
BJ's Wholesale Club, Inc.

The Natick, Massachusetts-based BJ's operates 150 warehouse stores and 78 gas stations in 16 states in the Eastern United States. Approximately 8 million consumers are currently members, with net sales totaling about $6.6 billion in 2003.

BJ's Wholesale Club has agreed to settle Federal Trade Commission charges that its failure to take appropriate security measures to protect the sensitive information of thousands of its customers was an unfair practice that violated federal law. According to the FTC, this information was used to make millions of dollars of fraudulent purchases. The settlement will require BJ's Wholesale Club to implement a comprehensive information security program and obtain audits by an independent third party security professional every other year for 20 years. This is an important development because it puts all retail operations on notice that there are minimum practices they should follow to protect customer data.

It's a new world online. These stories are evidence that no company or customer is safe from the probing attacks from hackers determined to get their hands on corporate secrets or personal information.

Time Warner reported in May that a back-up tape containing employee records for 600,000 past and present employees was missing. The data had been in transit to an off-site storage facility. This is one of many incidents reported in compliance with the requirements in California law 1386, which mandates organizations to notify people if their personally identifiable information is lost.

In a similar incident, **Iron Mountain** announced on July 7 that earlier in the spring, the company had misplaced a box full of back up tapes that contained customer data belonging to National City Bank.

In both of these incidents, the data was not encrypted.

In a story that reinforces the need for organizations to review Web-based processes for weaknesses, **Lexis-Nexis** succumbed to an attack from business process hackers. In March 2005, Lexis-Nexis revealed that hackers commandeered one of its databases, gaining access to the personal files of as many as 32,000 people. In this case, the hackers used normal processes to create fake accounts, then gain access to the database. They used this access to pilfer more than 200,000 identities.

All retail operations on notice that **there are minimum practices.**

In April, it was reported that thieves who accessed a **DSW Shoe Warehouse** database obtained 1.4 million credit card numbers and the names on those accounts – 10 times more than investigators initially estimated.

Besides the credit card numbers, the thieves obtained driver's license numbers and checking account numbers from 96,000 transactions involving checks.

Poor security practices by the retailers themselves and weaknesses in the software used to process credit-card payments are blamed for the security breach.

In the meantime, some 6,000 former and current employees of the **Federal Deposit Insurance Corp. (FDIC)**, the agency responsible for insuring Americans' bank accounts from theft, were themselves victims of an identity breach 18 months ago.

During a Senate hearing on identity theft and possible legislation to protect Americans from the recent flood of data thefts or losses, several of the senators mentioned the FDIC's breach, and called it just the latest in a long string of bad news for consumers. Additionally, **Bank of America Corp.** is among the big banks notifying more than 670,000 customers that account information was stolen in what may the biggest security breach to hit the banking industry.

MasterCard International notified its member financial institutions of a breach of payment card data, which potentially exposed more than 40 million cards of all brands to fraud, of which approximately 13.9 million are MasterCard-branded cards.

MasterCard International's team of security experts identified that the breach occurred at Tucson-based **CardSystems Solutions, Inc.**, a third-party processor of payment card data. Third-party processors process transactions on behalf of financial institutions and merchants.

The data security breach, possibly the largest to date, happened because intruders were able to exploit software security vulnerabilities to install a rogue program on the network of CardSystems Solutions. The malicious code was discovered after a probe into the security of CardSystems' network. That investigation, by security experts from Cybertrust, was triggered by a MasterCard inquiry into atypical reports of fraud by several banks. The trail led to CardSystems. No estimates are available of the total amount of money stolen in this incident.

Meanwhile in **Israel**, a story fit for Hollywood revealed that large businesses were hiring private investigators to spy on competitors. The private investigators used modified Trojan horses and social engineering techniques to steal documents from more than 20 companies.

Private investigators used modified Trojan horses and social engineering techniques to steal documents.

It all began when an Israeli author noticed his unpublished works posted to the Internet. Suspecting his step-daughter's ex-husband, he called in the Israeli police. The police discovered the HotWar Trojan on his home computer.

Files, e-mails, and everything the author typed were sent to FTP servers in Germany, the United Kingdom and the United States. Local authorities in each country seized the servers and discovered internal documents from dozens of companies in Israel including the state-owned telephone company, Bezeq, a cell phone company, a car dealer, a satellite TV company, a cell phone company, a water company, and a defense contractor, among others.

The investigation uncovered at least a dozen Israeli companies that had hired private investigators to gather competitive intelligence on their counterparts. Using software purchased from Michael Hephrati in the United Kingdom, the private investigators sent it to the targets disguised as a legitimate e-mail proposal.

Some additional news and discoveries in this case include:

- The CEO of one of the private investigator firms threw himself down a stairwell at the police station and is in critical condition with multiple head and spine injuries.
- The private firms that were in the process of purchasing Bezeq have asked for a new sale to take place.
- The water company that was hacked lost documents that detailed heavy water extraction techniques. Heavy water is critical to the manufacture of H-bombs.
- Israeli authorities themselves have reportedly been using spyware to gather information from the PC of the wife of the Syrian President.

The **National Infrastructure Security Coordination Centre (NISCC)** in the United Kingdom announced that attacks similar to the Israeli espionage case had been going on for more than a year. As in the Israel case, Trojan horses containing spyware were sent to particular e-mail addresses within target organizations.

Trojan horses containing spyware were sent to particular e-mail addresses within target organizations.

Additionally, the personal information of 57,000 **Blue Cross Blue Shield of Arizona** customers was stolen from a Phoenix-based managed care company.

Arizona Biodyne, an affiliate of Magellan Health Services that manages behavioral health for Blue Cross of Arizona, notified customers and providers whose information was lost in the latest theft in which financial, personal or medical records were taken. Biodyne reported to police that a safe containing computer backup tapes was stolen from its office. The stolen information included policyholders' addresses, phone numbers, Social Security numbers and dates of birth. They also contained partial treatment histories for some patients and certain information about the doctors who provided that care.

With the myriad of news announcements about the successful attacks carried out against CardServices, the FDIC, organizations in the UK, and, of course, the Israeli Trojan fiasco, it may have been easy to overlook the consent agreement coordinated between the FTC and BJ's Wholesale Club. Quietly posted on the FTC's Web site, this agreement is the single most important legal action in security to date. The repercussions will be greater than HIPPA, Sarbanes-Oxley, or GLB.

This is the single most important legal action in security to date.

The FTC has used its *existing authorization* provided by Section 5 of the FTC Act to prosecute a company for unacceptable security precautions regarding the way it handled customer data at its stores. The consent agreement requires BJ's Wholesale Club to do what arguably they should have been doing all along:

- Designate an employee or employees to coordinate and be accountable for the information security program.
- Identify material internal and external risks to the security, confidentiality and integrity of consumer information that could result in unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.
- Design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems and procedures.

- Evaluate and adjust its information security program in light of the results of testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that BJ's Wholesale Club knows or has to reason to know may have a material impact on the effectiveness of its information security program.

Part II of the proposed order requires that BJ's Wholesale Club obtain within 180 days, and on a biennial basis thereafter, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) BJ's Wholesale Club has in place a security program that provides protections that meet or exceed the protections required by Part I of the proposed order, and (2) BJ's Wholesale Club security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality and integrity of consumers' personal information has been protected. This is a clear signal to every enterprise to review its own security practices and increase them where necessary to meet the new levels of threats that are now becoming painfully evident.

A complete list of data loss incidents can be found at:

http://www.privacyrights.org/ar/ChronDataBreaches.htm

THREAT
Research/Phileas

In an environment where technology is old before hitting store shelves, it is a daily struggle to maintain an edge over not only other anti-spyware companies, but also those spyware writers who revel in wreaking havoc on computers and their users. To excel in the spyware research field, several methods must be employed. While user submissions aid in researching anti-spyware, the nature and complexity of spyware requires additional assistance. There are three main methods that companies utilize to detect spyware: manual discovery, client automation, and Web crawling automation.

Manual Discovery

Manual discovery involves researchers visiting known spyware Web sites to infect virtual machines with malicious code. This is a time consuming and non-scalable approach to research. It also involves receiving and researching file submissions from users. Researchers can review anti-spyware related Web forums looking for new threats reported. Once researchers know a machine is infected, they run anti-spyware software to eliminate known threats and then research what remains on the system (system changes, network activity, etc.); they attempt to identify both new threats and new variants of existing threats. Subsequently, spyware researchers then create definitions that can be updated and tested across multiple platforms to ensure they are removed properly and as completely as possible.

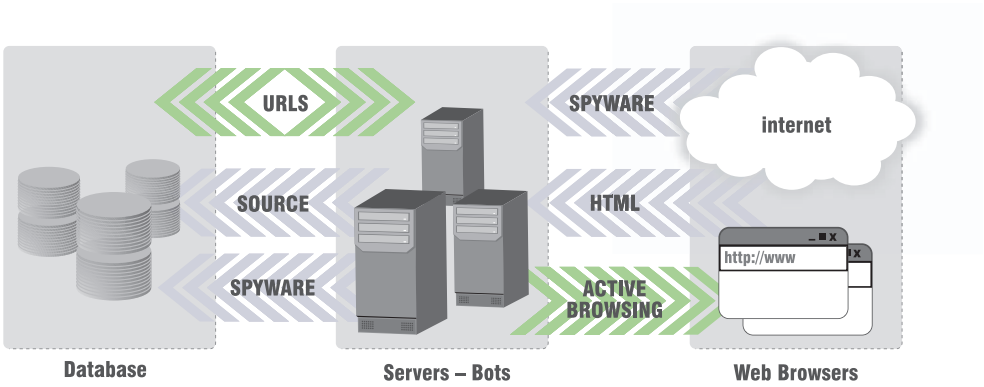
Client Automation

Another methodology used by some anti-spyware companies involves a collaboration of the end-user and their computer's anti-spyware software findings; the end-user submits an automated report of potential spyware found on their computer. These findings are sent to a central repository for further analysis. While this collection method is economical and attainable, it is reliant on end-user infection before providing protection. The frequency of false positives is higher because the reports generated by the system do not provide enough data for deeper analysis before writing a definition.

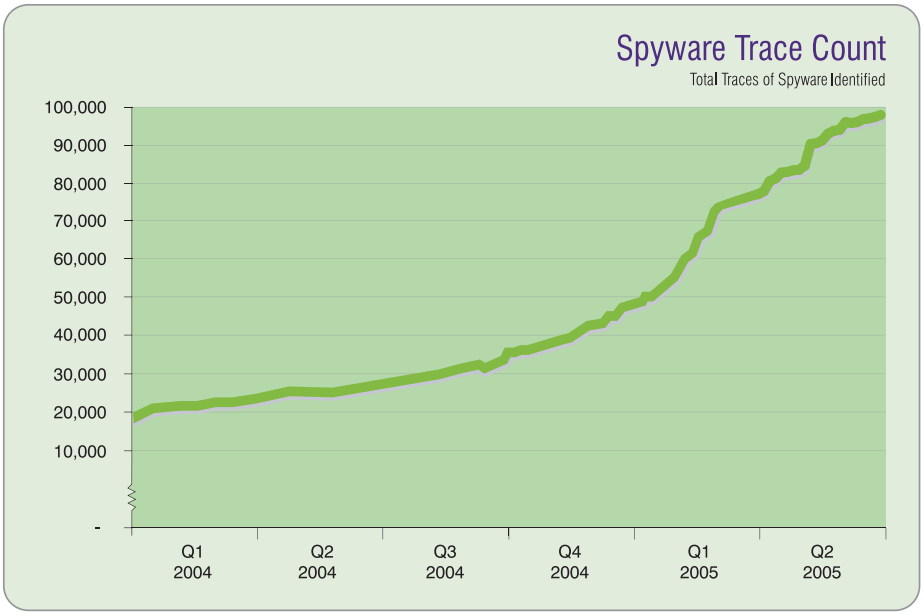
Web Crawler Automation

A very effective and efficient means of identifying spyware is to employ Web crawler technology to find new threats before they can infect end-users. Webroot employs this methodology by using Phileas, a malware crawler that populates a threat database. Phileas utilizes dozens of servers with high bandwidth Internet connections, controlling an army of "bots" that scour the Web for sites containing malware. By using this system, Webroot is able to continually update its definition database. As the problem grows, this architecture can scale to keep pace.

The graphic below depicts the process:



As of July 31, the Webroot Spy Sweeper product identified 97,295 traces of unwanted programs.



False Positives

Identifying spyware is only the first step towards eradicating it from your computer. After identifying a spy, each spy is given a unique definition. Each definition undergoes rigorous testing to ensure that it can correctly identify malicious code and more importantly, that it does not incorrectly identify, or interfere with, legitimate files. This incorrect identification or "false positive" identification is one of the most challenging aspects in creating an effective anti-spyware application.

False positives cause severe problems for application users. Oftentimes, anti-spyware vendors do not take the necessary, additional 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 keep and protect legitimate files. As spyware evolves and newer variants and components are released, it is more difficult for researchers to stay ahead of the growing threat, and also to identify what looks like a threat but isn't.

The key to an effective anti-spyware product is not only its ability to correctly identify and remove malicious files, but also to **keep and protect legitimate files.**

Webroot's Phileas system provides an autonomous relay that constantly feeds Webroot's spyware repository, and it also helps to substantially reduce the number of false positives by finding the newest pieces of true spyware. The Webroot Threat Research team then ensures that new definitions under consideration for addition to the spyware database are thoroughly tested to ensure these definitions detect and remove spyware-related applications, and nothing else. Currently, Webroot is tracking to a false positive rate of one per million desktops deployed per month.

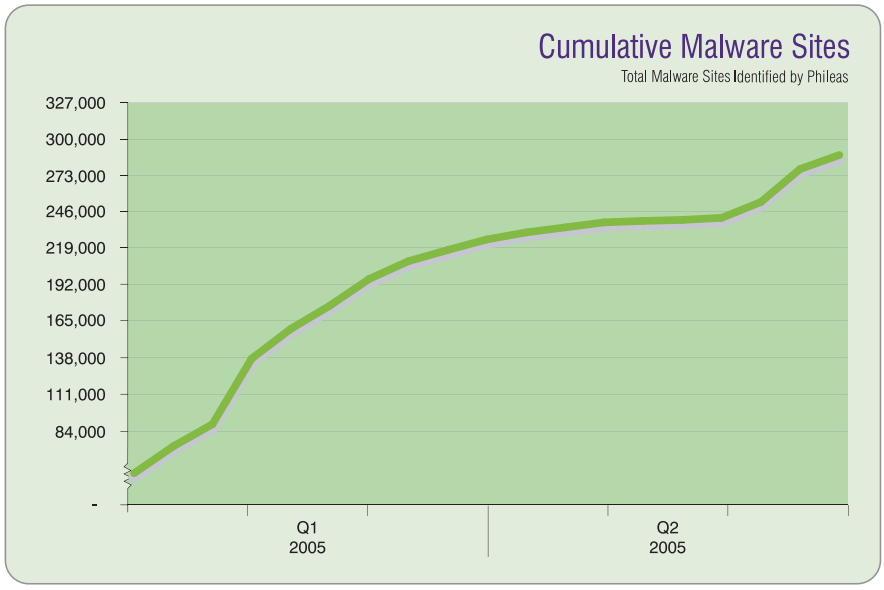
In the second quarter of 2005, Phileas returned results for over 150 million URLs and associated domain names. An example domain name like what Phileas finds is **http://www.zadolbali.com**. **Warning: Do not look at this Web site unless you are fully protected with an anti-spyware solution. This URL uses an exploit (Microsoft Security Bulletin MS03-014) to install a toolbar.**

Additional examples of sites found by Phileas:

Malicious Malware Sites

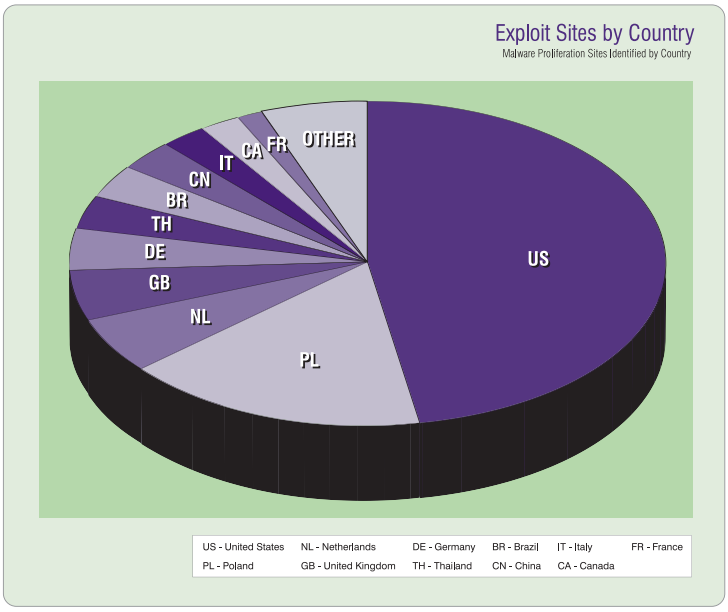
A Selection of Malware Sites Identified by Phileas

Domains	Number of Associated URLs
http://www.mypornfree.com	485
http://www.kellyonline.com	174
http://9sekund.pl	155
http://www.x-shemale.com	136
http://www.prescriptions.1accesshost.com	108



Cybercrime is going **mainstream.**

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. According to the recent statistics, the majority of exploit sites originate from the United States, with 25,385 exploits, followed by Poland with 8,822 and the Netherlands with 4,310. The proliferation and attainability of various Internet connections in the U.S. may be the cause for these high figures.



Spyware is evolving—simple techniques that once worked were things such as modifying an application's file name and placement, to make it appear as a valid system process (i.e. c\windows\system32\svc host.exe). Over the last year, more creative pieces of spyware use the following techniques to evade detection and removal: .dll (dynamic-link library) injection, encryption, and proprietary encryption algorithms that insert themselves as dependencies and threads into system level processes. For example, these .dll injection techniques entail an application placing a .dll into a running process, placing their code into memory, and enabling the application to run specific functions; this can be accomplished utilizing Windows API's.

Spyware is
evolving.

Another technique that spyware practices is to alter registry settings on system level executables, which effectively fools Windows into thinking that the spyware is needed to run core executables. Essentially, Windows promotes the spyware to a "valid and necessary" file, thus making it difficult to remove.

Additionally, spyware is now capable of altering an executable on disk, placing its own malicious code at a file's beginning so that the malicious code runs prior to the normal executable's code. More recently, the majority of spyware developers' encryption algorithms or packers such as UPX, Aspack, FSG, or their own proprietary algorithms, which render previous detection techniques obsolete.

Top Threats

The top threats this quarter are not only the most prevalent in terms of sheer numbers, but also in complexity. Over the last six months, spyware has grown in complexity; the use of packing and encryption algorithms is now very common. Spyware that is based on Trojan horse code, viral installation procedures, and polymorphic engines has yielded new detection and removal methodologies to stay ahead of the threat.

Over the last six months, **spyware has grown in complexity.**

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: CWS may install using malicious HTML applications or security flaws in common applications such as 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 or CoolWebSearch 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 track the Web pages you visit and deliver pop-up advertisements to your computer based on your personal preferences. This toolbar may hijack Web searches, meaning it may reroute your Web searches through its own Web page. It may change your default home page.

Method of Installation: EliteBar is generally bundled with various free software programs.

Consequences: This adware program may track your Web surfing habits and display pop-up advertisements, slowing your Web browser's performance. EliteBar may also download arbitrary code on your computer, resulting in the installation of unwanted programs without your knowledge or consent.

PowerScan

Short Description: PowerScan is a spyware program that may display pop-up advertisements on your computer.

Characteristics: PowerScan may track your Web surfing habits and display pop-up advertisements on your computer. This program may download and execute third-party programs on your computer without your knowledge or consent.

Method of Installation: PowerScan is generally installed via ActiveX drive-by downloads. A "drive-by download" program automatically downloads itself on your computer without your knowledge or consent. Drive-by downloads can be initiated by clicking on an advertisement or visiting a Web site.

Consequences: This spyware program may send information about your Web surfing habits to its controlling servers when you are online.

Look2Me

Short Description: Look2Me is a piece of spyware that may monitor Web surfing activity and report-back 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.

Look2Me is a new breed of spyware.

Method of Installation: Look2Me is generally installed via ActiveX drive-by download sites, or by vulnerabilities in common Web applications.

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 is a new breed of spyware released onto the Internet. 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 and a huge problem on an infected user's machine.

PurityScan

Short Description: PurityScan is spyware that may display pop-up advertisements on your computer.

Characteristics: Once installed PurityScan may update itself and register your computer and system information with its centralized server. The ability to update itself gives PurityScan the ability to install other applications and functionality. PurityScan displays pop-up advertisements based on Web browsing activity.

Method of Installation: PurityScan is generally bundled with popular peer-to-peer music sharing software such as Grokster and Kazaa.

Consequences: Due to the auto-update mechanism, this adware is rather difficult to remove. Populating multiple advertisement windows may degrade browser performance.

Clkoptimizer

Short Description: Clkoptimizer is an adware program that may display advertisements on your computer.

Characteristics: Clkoptimizer may track your Web surfing habits and display pop-up advertisements on your computer. This program may download and execute third party programs on your computer without your knowledge or consent.

Method of Installation: Clkoptimizer is generally installed via ActiveX drive-by download. A “drive-by download” program automatically downloads itself on your computer without your knowledge or consent. Drive-by downloads can be initiated by clicking an advertisement or visiting a Web site.

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. Clkoptimizer may download third party programs on your computer, resulting in unwanted programs being installed without your knowledge or consent.

180search Assistant

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

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

Method of Installation: 180search Assistant may be bundled with various free software programs or downloaded directly.

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.

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 Internet Explorer settings and install a toolbar on your Web browser. This toolbar may also display advertisements on your computer. It has the ability to run in the background, hiding its presence.

Method of Installation: Web search Toolbar is generally installed via ActiveX drive-by download. A "drive-by download" program automatically downloads itself on your computer without your knowledge or consent. Drive-by downloads can be initiated by clicking on an advertisement or visiting a Web site.

Consequences: Toolbars may monitor the Web sites you visit. They also may share your personal information with their business partners in order to offer you more promotions and advertisements through the toolbar.

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 is generally installed via ActiveX drive-by download. A "drive-by download" program automatically downloads itself on your computer without your knowledge or consent. Drive-by downloads can be initiated by clicking on an advertisement or visiting a Web site.

Consequences: ISTbar may install other pieces of spyware on your computer and as with all toolbars, may monitor the Web sites you visit. They may also share your personal information with their business partners in order to offer you more promotions and advertisements through the toolbar.

AbetterInternet

Short Description: AbetterInternet is an advertisement-displaying browser helper object (BHO) that may update itself and install third party applications.

Characteristics: AbetterInternet is a Browser Helper Object that may display targeted advertisements via Internet Explorer. A BHO is a file that loads with Internet Explorer and performs what the author designed it to do.

Method of Installation: AbetterInternet is generally installed via ActiveX drive-by download. A "drive-by download" program automatically downloads itself on your computer without your knowledge or consent. Drive-by downloads can be initiated by clicking on an advertisement or visiting a Web site.

Consequences: AbetterInternet may send information about your Web surfing habits to its controlling servers when you are online, which may slow your Web browser's performance.

ENTERPRISE
SpyAudit

Enterprise SpyAudit

The Webroot Enterprise SpyAudit was initiated in October 2004. The data presented below is for the second quarter of 2005.

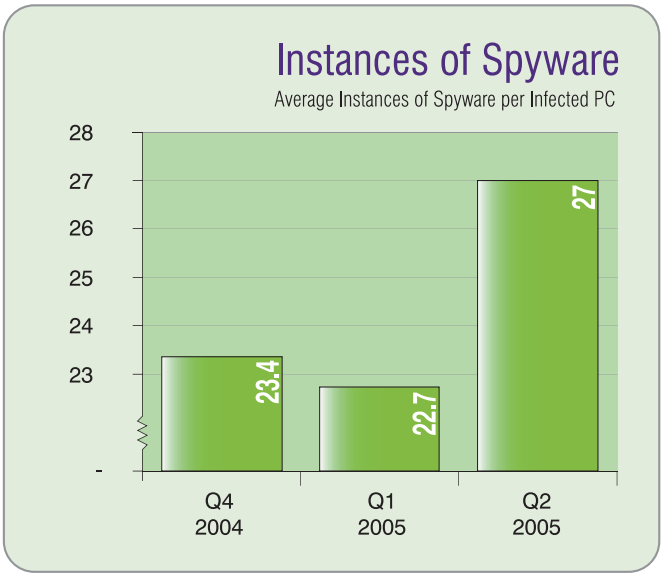
The Enterprise SpyAudit is a tool designed to help IT administrators easily determine the amount of spyware that has penetrated their organizations. By visiting www.webroot.com/enterprise an administrator generates a unique URL that is then visited by each machine he or she wants to audit. A report is automatically generated that presents the results of all of the individual audits run within the enterprise.

Overall Findings

To date, the Webroot Enterprise SpyAudit has scanned nearly 60,000 systems, representing more than 20,000 companies.

Enterprise SpyAudit scanned nearly **60,000 systems.**

The spyware infection rate for enterprise desktops continues to remain above 80 percent. Alarmingly, the number of spyware instances per infected machine has increased by 19 percent - averaging 27 instances of spyware per infected machine.



Infection rate continues to remain above **80 percent.**

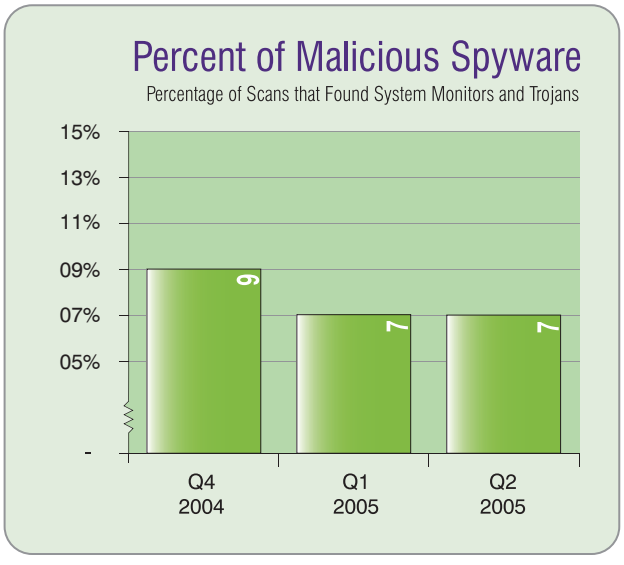
Although cookies tend to make up the largest number of infections per enterprise machine, instances of adware and other more malicious spyware such as system monitors and Trojan horses were found on the scanned machines. Eliminating cookies from the audit, scans of the enterprise machines found an average of 4.4 instances of Trojans, system monitors and adware combined, representing a 17 percent increase from Q1, which saw an average of 3.8 instances per infected PC.

This indicates that the machines that are infected with these more malicious forms of spyware continue to be more susceptible to additional infections. An average of 4.4 infections is a very high number considering a single malicious program can cause a detrimental impact to an enterprise, including loss of intellectual property, customer records or even violation of compliance regulations.

Machines that are infected with malicious forms of spyware **continue to be susceptible to additional infections.**

Malicious Spyware

When the Enterprise SpyAudit was first conceived, it was assumed that infection rates of Trojans and system monitors would be measured in the single digits of instances, if it all. The presence of a single system monitor which could record keystrokes, screen shots, e-mails, even audio or video is considered by most security practitioners and auditors to be a major breach of security. This type of security breach requires immediate response and a forensic investigation.



Malicious spyware, which includes system monitors and Trojans, continues to be dangerously prevalent within the enterprise. It was detected on 7 percent of PCs scanned. The average count of malicious spyware infections held steady at 1.2 per infected machine. In other words, infected machines are likely to have more than one type of malicious spyware.

This high level of malicious spyware present on enterprise machines represents a real and present danger to enterprise security. As a result, auditors and compliance managers alike should begin to check for these types of infections in their regular security assessment programs.

This concern is echoed by the FDIC in their spyware guidelines issued on July 22. "Information collected through spyware can be used to compromise a bank's systems or conduct identity theft," said Michael Zamorski, director of the FDIC division of supervision and consumer protection. "It is critical that banks stay vigilant about the risks involved with this malicious software."

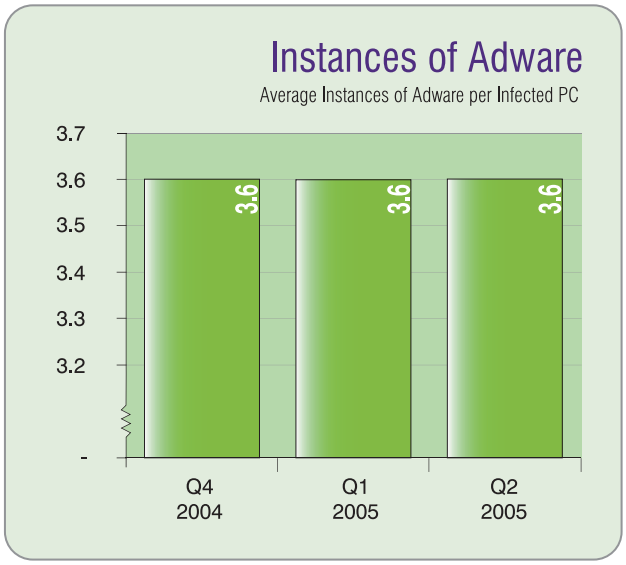
Malicious spyware on enterprise PCs represents a real and present danger to enterprise security.

The FDIC said banks should educate customers about the risks of spyware and encourage them to take steps to effectively manage the spyware threat on their own computers. It was also recommended that banks advise customers of the risks of banking online on public computers -- such as in hotels, libraries or Internet cafés -- where spyware might have been installed.

Adware

Nearly one-third of all machines scanned within the enterprise showed a presence of adware. For machines with adware, the rate continues to be more than three pieces of adware per scan.

This fluctuation in adware infections may be the result of pending legislation aimed at correcting the behavior of adware distributors. Although the adware infection rate has decreased, the complexity of adware programs has grown, often making detection and removal more difficult to ensure their survival on a PC.



Comparatively, the average infected machine had 3.6 instances of adware, which was equal to the previous two quarters.

This number is concerning since multiple pieces of adware can lead to the increased likelihood of system crashes and poor performance that ultimately result in calls to the IT help desk. While help desk calls attributed to spyware continue to increase, combating and removing spyware is becoming among the most pressing IT issues for enterprises.

Multiple pieces of adware can lead to the increased likelihood of system crashes.

Webroot's analysis of this overall trend is that while infections via U.S.-based adware companies may have declined, more pernicious adware programs written for more malicious purposes are surging ahead. Infection rates may be less than before, but the type of infection from these more virulent and aggressive programs is much more serious.

Higher end user awareness. A survey from the Pew Internet Project indicated that end users are much less likely to install software or click on downloads or say "yes" to those pop-ups. Both news coverage and the actions of the federal government, and more than 30 state legislatures have contributed to this awareness.

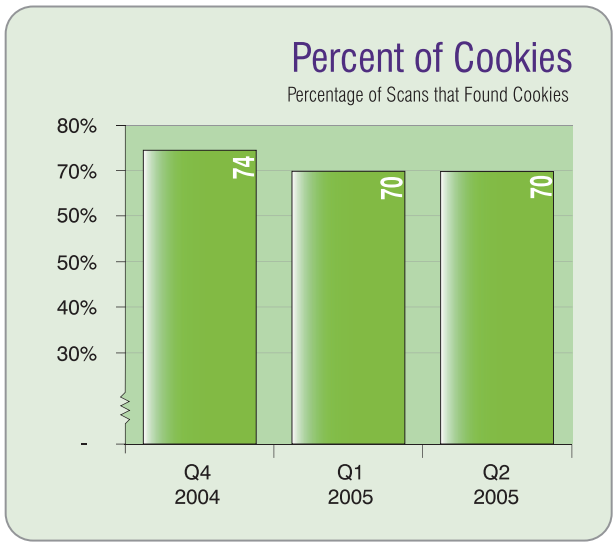
Improved adware behavior. The major U.S. adware distributors, Claria, 180Solutions and WhenU, have taken significant steps to bring their products in-line with proposed legislation. These steps include:

1. Readable End User License Agreements
2. Attributed pop-ups with border titles that give credit to the adware company for the pop-up
3. Removal capabilities, usually by invoking Windows Add/Remove

The first two factors lead to fewer initial installations. The third factor leads to more adware uninstalls, thus reducing the overall penetration of these programs. The overall rate of infection is not falling very rapidly, of course, because the void is being filled by completely illicit adware programs, in particular, the many variants of CoolWebSearch (CWS) and an up-tick in non-U.S. developers and distributors of adware.

Tracking Cookies

While this particular area may be inconsequential to enterprises, it's interesting to note that during the second quarter, cookie infections remained steady. Seventy percent of scanned computers contained cookies, with an average of 29 cookies per infected machine.



An interesting observation is that the online advertising companies that use tracking cookies extensively have entered the spyware debate. Their contention is anti-spyware programs remove the tracking cookies, and damage their ability to accurately track unique users to their customers' sites. Both the enterprise and consumer SpyAudits indicate that cookie distribution is still healthy, so even if the cookies are removed from a PC, a brief visit to the Internet will add more cookies. Webroot will continue to monitor cookies until a definitive decision on whether cookies constitute spyware is determined.

Compliance Update

The connection between government compliance initiatives and spyware has grown closer as each quarter comes to a close. Spyware, in its more nefarious forms as system monitors or Trojan horses, has the ability to push an enterprise out of compliance of the three major initiatives, HIPPA, Gramm-Leach-Bliley Act and Sarbanes-Oxley. It takes just one piece of spyware to place an enterprise in a position of non-compliance or into hot water with the FTC or FDIC. If this occurs, the federal government can post heavy fines or other actions against it, and the enterprise may face bitter fallout from its customers and partners. More recently, given the increasing number of financial institutions being targeted by spyware, the FDIC issued guidelines recommending the internal implementation of anti-spyware technologies.

Each State of Spyware Report includes an in-depth review of one compliance initiative, and a review of the others as spyware relates to remaining in compliance with these strict government regulations. The Q1 2005 report covered Gramm-Leach-Bliley (GLB). In the Q2 2005 report, we include an article on Sarbanes-Oxley, the Federal law pertaining to management responsibility for reporting accurate and true financial information, and a short update on the other major areas of compliance, HIPPA and GLB.

HIPPA, the regulation covering health records data privacy

This compliance initiative presents a quagmire of requirements, and as a result, there have been very few enforcement actions in the case of health record data breach. However, more incidents have been recently reported.

In one of the largest fines ever levied, on June 21, the California Department of Managed Health Care (DMHC) fined Kaiser Foundation Health Plan, a division of Kaiser Permanente, $200,000 for exposing confidential patient health information. Web developers used real data of approximately 150 patients for a test Web site.

This fine was imposed based on California law, not on the Federal HIPPA regulation. However, this fits the type of scenario that HIPPA attempts to prevent.

The Gramm-Leach-Bliley Act or the Financial Modernization Act of 1999

Of the three major provisions of GLB, the Financial Privacy Rule deals with how financial institutions handle consumer financial data. To date, the biggest impact of this clause has been the requirement of a Privacy Notice that must be delivered to every customer by financial institutions. Customers are also given the right to opt-out of any marketing activity that the financial institution may undertake using their information.

The other provisions of GLB are the Safeguards Rule and the Pretexting Rule. The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Pretexting provision of GLB protects individuals from the misuse of their information when it is obtained under false pretenses.

Most of the incidents reported in Q2 2005 involved loss of account and personally identifiable information on the part of financial institutions. MasterCard unintentionally made history when it revealed that more than 40 million credit card records had been exposed to hackers through a credit card processor, CardSystems International. Hackers used Trojans and keystroke loggers to gain access to banking systems. GLB does not

Incidents reported in Q2 2005 involved **loss of account and PII on the part of financial institutions.**

mention encryption, which if implemented properly, would be a tremendous safeguard of customer information. These types of attacks are rampant, and it is necessary that companies responsible for handling customer data take defensible action, including encrypting customer information and deploying a desktop-level anti-spyware solution.

Is Spyware a Sarbanes-Oxley Concern?

This article contains a brief explanation of the Sarbanes-Oxley Act of 2002 (SOX) and how the act implies that the existence of spyware on internal systems could have grave implications for overall compliance.

Following major fraud at publicly-traded companies like Enron, Congress created the Sarbanes-Oxley Act of 2002, which imposes stricter controls over financial reporting by mandating accurate disclosure of corporate information. To be compliant with this act, companies are required to have certification of internal controls (Section 404) and the personal liability of company executives (Section 302). The compliance deadline for public U.S. companies with market capitalization greater than $75 million was November 15, 2004. Companies based outside of the United States must be in compliance by July 15, 2006. The enactment of this law has led to enhanced auditing practices which demonstrate compliance with Sarbanes-Oxley, primarily via the Big Four public accounting firms.

Companies responsible for handling customer data take defensible action, including deploying a desktop-level anti-spyware solution.

The one section of the Act that is most often cited as impacting corporate security practices is Section 404 which requires each annual report of an issuer to contain an “internal control report” that:

(1) states the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contains an assessment, as of the end of the issuer’s fiscal year, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

By delving further into the world of audit, risk assessment and controls you can begin to understand why this simple language has far-reaching implications. It requires corporate management to certify and sign off that these controls are in place when their annual reports are filed, with significant penalties for non-compliance. Ensuring that every part of Sarbanes-Oxley is implemented is the *personal responsibility* of the CEO and the CFO.

The Committee of the Sponsoring Organizations of the Treadway Commission (COSO), developed internal control structures for Sarbanes-Oxley Act compliance, which most companies follow. Under the general guidelines of the COSO, organizations can use one of two well-known information security standards, COBIT or ISO 17799. Either of these information security standards can be used by organizations to implement the five essential components: control environment, risk assessment, control activities, information/communication and monitoring.

Sarbanes-Oxley
302 & 304
COSO Component
- Control Activities
- Information & Communication

Control Guidance for Data Management
Management protects sensitive information logically and physically, in storage and during transmission against unauthorized access or modification.

DS5—Delivery & Support: Ensure Systems Security

5.19—Malicious Software Prevention, Detection, and Correction
Regarding malicious software, such as computer viruses or Trojan horses, management should establish a framework of adequate preventative, detective and corrective control measures, and occurrence response and reporting. Business and IT management should ensure that procedures are established across the organization to protect information systems and technology from computer viruses. Procedures should incorporate virus protection, detection, occurrence response, and reporting.

In Webroot's Q2 '05 State of Spyware Report we find that more than 80% of all corporate desktops are infected with spyware. Within these systems, 7% of computers scanned in our Enterprise SpyAudit were infected with system monitors and Trojan horses. System monitors and Trojans are spyware that often allow an attacker to capture key strokes, files, and screen images and are used to compromise user accounts and then transmit this data outside the network.

These malicious types of spyware are not detected via firewalls or anti-virus software and enable unauthorized access to sensitive corporate data. Cases such as Sumitomo Bank in the UK, the Israeli Trojan horse case and possibly CardServices in Georgia, and many of the organizations that participate in the enterprise SpyAudit indicate that system monitors are a real and present danger to the enterprise.

2.4—Security Levels
Management should define, implement, and maintain security levels for each of the data classifications identified above the level of "no protection required." These security levels should represent the appropriate (minimum) set of security and control measures for each of the classifications and should be re-evaluated periodically and modified accordingly. Criteria for supporting different levels of security in the extended enterprise should be established to address the needs of evolving e-commerce, mobile computing, and telecommuting environments.

The presence of system monitors and trojans indicate an extremely high likelihood that unauthorized access to sensitive information is available to an attacker either on the inside or from outside the corporation. Based on the strict guidance as spelled out in COBIT and COSO (5.19 and 5.20), an organization would not be in compliance with adequate controls over financial reporting if system monitors were present on audited machines even if the company had firewalls and anti-virus deployed.

It is also clear that mobile computers need protection from these malicious spyware types, and is critical that these PCs are free of spyware before they connect to corporate networks. Support for mobile desktops is required to comply with the "Security Levels" identified in SOX.

The increasing number of identity theft cases caused due to spyware has dire implications on the future of online commerce and it is in the enterprise's best interest to ensure that they are putting the most effective solution to combat spyware.

It is clear that as auditors use accepted assessment and testing techniques as defined by the COSO Framework and as detailed in COBIT, they will not be able to attest that an organization is in compliance with Sarbanes-Oxley if system monitors and Trojans are found on internal computers. It is best for organizations to deploy a desktop level anti-spyware solution as part of their security infrastructure to ensure compliance with SOX.

CONSUMER
SpyAudit

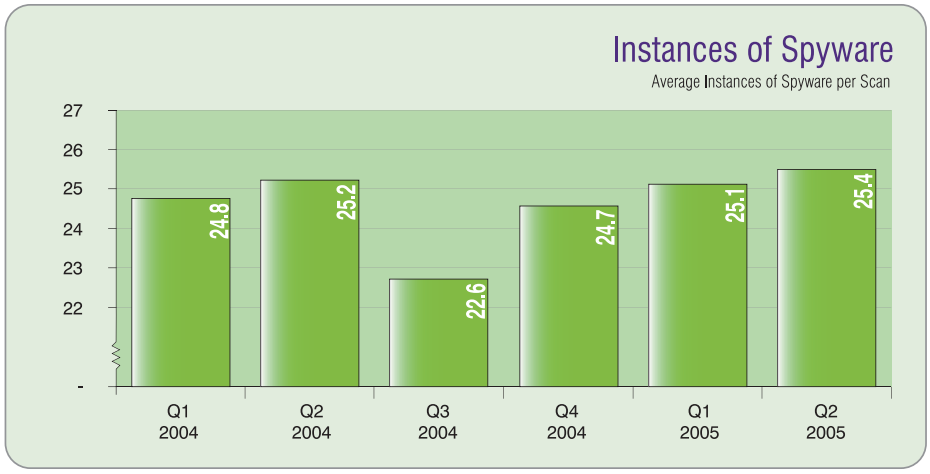
Consumer SpyAudit

Each quarter, Webroot gathers the results from a continuous Consumer SpyAudit. The tool is free for anyone to use. The SpyAudit is voluntary to use, and 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 detail.

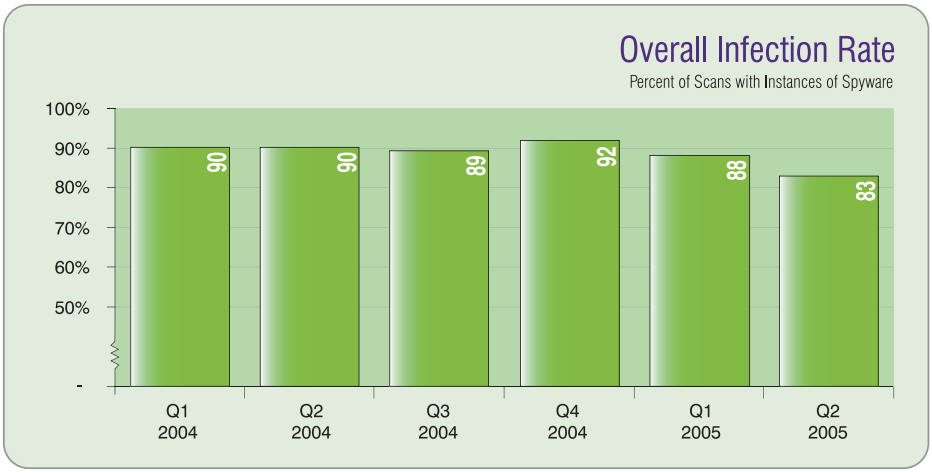
Overall Results

In Q2 2005, the Consumer SpyAudit results showed that the percentage of infected consumer PCs remained elevated at more than 80 percent. The number of spyware instances per machine has increased to an all-time high of 25.4 per machine, up from 22.8 instances per PC from Q1 of 2005.

The percentage of consumer PCs infected with spyware remained elevated at more than **80 percent.**



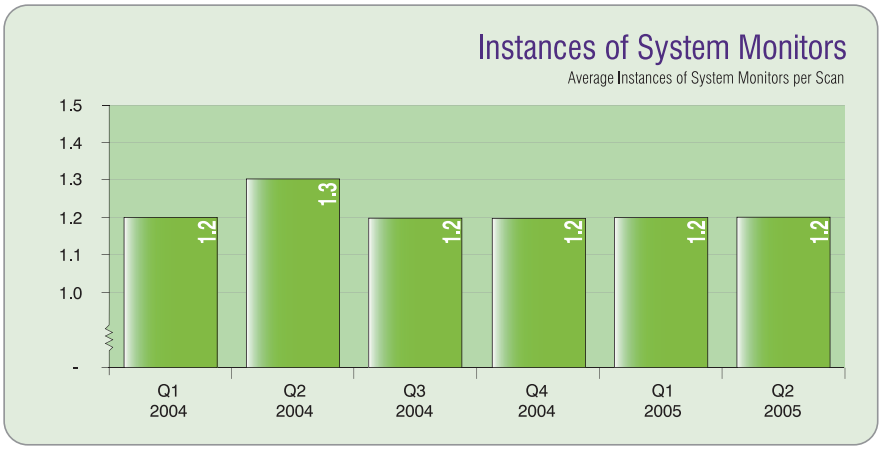
The most harmful elements of spyware, system monitors and Trojans, continue to infect users at similar rates as in prior quarters. Heightened end-user awareness, changing behavior by some of the adware vendors due to impending legislation and increased lawsuits along with an increased usage of anti-spyware products are helping to combat adware.



System Monitors

System monitors continue to remain a threat to consumers. Six percent of PCs scanned showed some form of a system monitor. The continued persistence of these threatening applications, at 1.2 instances per infected machine for five out of six quarters, demonstrates the need for anti-spyware protection.

How do system monitors get on consumer PCs? There are many ways. The most common is for a PC to become infected with a Trojan horse via e-mail or instant messaging borne virus. The Trojan horse gives the hacker the ability to download other malicious code that could be zombie code for denial of service attacks, e-mail programs for sending spam, or even lightweight Web servers that allow a PC to act as a fake Web site used in phishing attacks. A Trojan allows a hacker to “own” the infected machine.



Increasingly, the purpose of system monitors is to steal login credentials to bank accounts and other personal information, especially credit card numbers. System monitors can be very sophisticated. For example, they often capture screen images on each mouse click to thwart the defenses banks use to counter early generations of simple keystroke loggers (Virtual PIN pads for instance).

Trojans

Trojan infection rates fluctuated slightly from 19 percent in Q1 2005 to 16 percent in Q2 2005, but remain in line with previous quarter's results. The instances of Trojans per infected PC also remained steady from 1.5 for Q1 2005 to 1.6 for Q2 2005. Trojans have been prevalent in the news in recent months, and have become the deployment method of choice for hackers seeking to launch system monitors onto target PCs.

Trojans have become the deployment method of choice for hackers seeking to **launch system monitors onto target PCs.**

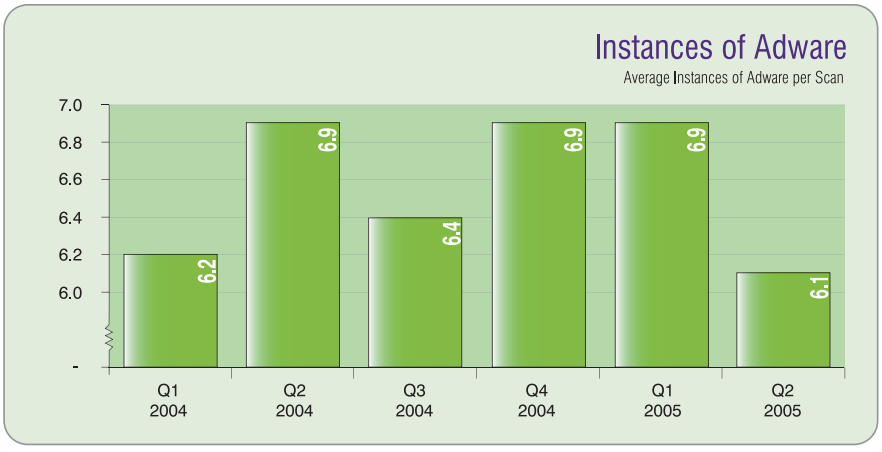
See the "Incidents" section of this report for complete details of the Israeli Trojan fiasco as well as the use of Trojans in the United Kingdom. Both instances highlight the methodology.

> *An attacker uses e-mail to trick a recipient into opening an attachment that contains the Trojan. This type of targeted attack is extremely difficult to counter. Imagine receiving an e-mail apparently from a co-worker in another division of your company with the subject, "New employee bonus plan attached."*

Adware

More than half of the computers scanned by the Consumer SpyAudit showed a presence of adware. For machines with an adware infection, the rate continues to be more than six pieces of adware per scan. Pending legislation in the U.S. Congress may have affected the core activities of adware distributors. However, examples of more pernicious and damaging adware continue to surface in Webroot's research. The resilience and complexity of new and existing adware programs is cause for concern. These more virulent adware programs often make removal more difficult to ensure their survival on a PC. In some ways, this new generation of adware offers the potential to be as damaging to a PC as the presence of system monitors or Trojans are to identity protection.

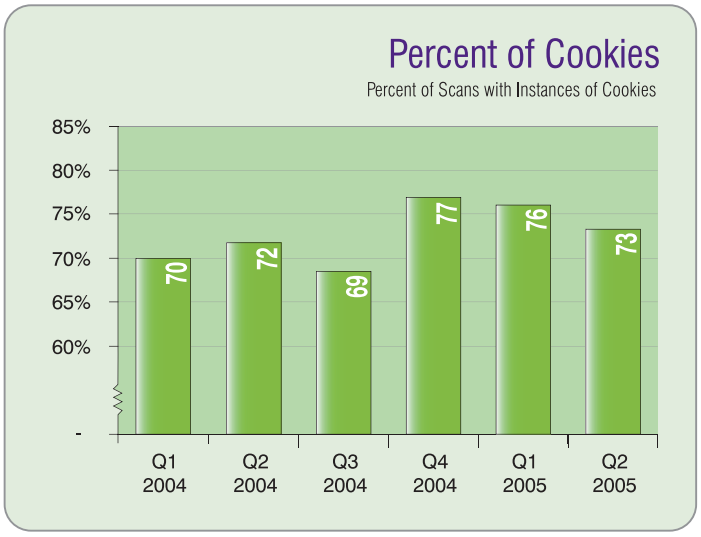
More than half of the computers scanned by the Consumer SpyAudit **showed a presence of adware.**



Note that while the penetration rates of U.S.-based adware companies' software such as Claria, 180Solutions and WhenU have declined slightly, the overall penetration rate of adware is declining less slowly. Webroot attributes this to the more illicit forms of adware such as the 107 variants of CoolWebSearch (CWS) filling the void left by these other programs.

Cookies

The debate continues about whether or not cookies constitute spyware. Many consumers have indicated that any type of application or program, including cookies, placed on their PC without their knowledge is spyware. Others call for features in anti-spyware software that allow consumers to remove cookies as part of an anti-spyware scan. As long as the discussion continues, Webroot will monitor cookie counts as part of this report. Cookie infections continue to be consistent with previous quarters with an infection rate of 73 percent. Instances per infected PC increased 6 percent to 24.2 instances.



LEGISLATION

Using an anti-spyware solution will clean up your PC, but you may also have legal recourse against adware and spyware vendors whose programs infected your machine. The U.S. Federal Trade Commission (FTC) has already filed several spyware-related cases. If you have suffered some material harm as a result of spyware, you can file a complaint with the FTC using the web form located at https://rn.ftc.gov/pls/dod/wsolcq$.startup?Z_ORG_CODE=PU01.

You may have legal recourse against spyware and adware vendors.

In the United States, Section 5 of the Federal Trade Commission (FTC) Act gives the agency the authority to challenge "deceptive" or "unfair" acts and practices that affect commerce. The Commission generally finds an act or practice to be "unfair" if it causes substantial consumer injury that is not outweighed by countervailing benefits to consumer or competition benefits, and consumers could not have reasonably avoided the injury. An act or practice is considered by the Commission to be "deceptive" when consumer harm results from a material representation, omission or practice that is likely to mislead consumers. The FTC has already begun applying these standards to cases like BJ's Wholesale Club, where customer data was not properly secured. It has also been used against spyware companies and businesses providing bogus anti-spyware offerings.

Legal Actions

The most noteworthy case in the second quarter was the New York state case against Intermix Media filed by State Attorney General Eliot Spitzer in the New York Supreme Court.

The People of the State of New York v. Intermix Media, Inc.

In the petition the Attorney General documented at least 10 separate Web sites from which Intermix or its agents were downloading spyware, providing either no warning or other misleading disclosures. In this way, Intermix and its agents downloaded more than 3.7 million programs to New Yorkers alone, and tens of millions more to users across the nation. The filings also outline how Intermix went to great lengths to protect the spyware and adware it secretly installed. The programs were hidden in unlikely locations on the computer and could not be removed through a computer's "Add/Remove" function. In addition, the programs omitted "un-install" applications, and even reinstalled themselves after being deleted.

In the second quarter, the Federal Trade Commission also filed an additional spyware related complaint in Federal Court.

FTC v. Trustsoft, Inc., d.b.a, Swanksoft and Spykiller, and Danilo Ladendorf

FTC File No. 052 3059, Civ. No. H 05 1905

According to the FTC complaint, the operation used bogus "scans" and illegal spam to market its anti-spyware program, SpyKiller, that didn't work as claimed. The company's assets have been frozen. The agency's complaint details violations to federal laws and asks the court to permanently bar the deceptive marketing, and order redress for consumers.

According to the FTC complaint, the operation used bogus "scans" and illegal spam.

Past complaints filed by the Federal Trade Commission that also deal with spyware include:

FTC v. Seismic Entertainment Productions, Inc., SmartBot.net, Inc. and Sanford Wallance

FTC File No: 042 3125

The complaint asked a U.S. District Court to shut down a spyware operation that hijacks computers, secretly changes their settings, barrages them with pop-up ads and installs adware and other software programs that spy on consumers' Web surfing, also often causing computers to malfunction. The FTC complaint also asks the court to order the defendants to give up their ill-gotten gains.

FTC v. Maxtheater, Inc. and Thomas L. Delanoy

FTC File No. 042 3213, Civil Action No.: 05 -CV-0069 - LRS

The complaint detailed the deceptive practices used to market anti-spyware software that does not work. These deceptive practices included offering consumers a free spyware detection scan that "detected" spyware even if there was none.

The deceptive practices included offering a free spyware scan that "detected" spyware, even if there was none.

New Laws and Legislation

In addition to the legal actions filed by the FTC, there has also been a flurry of activity at both the state and Federal levels to provide consumers with even greater protection against spyware. So far this year, new anti-spyware laws have been enacted by eight U.S. states: Arizona, Arkansas, Georgia, Iowa, Nevada, Texas, Virginia and Washington. As of this printing, laws have also been approved by the legislatures and are awaiting Governors' action in two additional states: Alaska and New Hampshire. These are in addition to California and Utah that enacted anti-spyware laws in 2004. (In 2005, Utah enacted amendments to its law to address legal challenges to the Act that was approved in 2004.) If you live in one of these states, you may have some legal remedies available to you. As of June 30, 2005, there were an additional 19 bills still active and pending in 10 states that do not have any existing spyware specific laws.

New anti-spyware laws have been **enacted by 8 U.S. states.**

See the State Spyware Legislation table on page 63 for more details about the state bills.

On a Federal level, the U.S. Congress is interested in avoiding 50 different state bills dealing with spyware. On May 23, 2005, the Unites States House of Representatives passed two spyware-related bills. Those two bills, as well as two Senate originated bills, are now pending before the U.S. Senate Committee on Commerce, Science and Transportation. If Federal legislation is enacted, it will likely preempt the growing number of state laws from coming into effect, but will also provide both the market and consumers with a single legal standard relating to spyware.

See the U.S. Federal Legislation table on page 62 for more information.

Spyware in Germany

Incidents of corporate espionage and cybercrimes caused by spyware have occurred around the globe. The international community is now dealing with the legality of spyware. Similar to the efforts of the U.S. government, many countries are creating laws in response to the spyware epidemic. Germany's lead in creating laws to fight spyware is groundbreaking.

In Germany, the use of spyware is not only against their constitution, but also illegal under certain provisions of the penal code. German laws concerning data offer such extensive criteria for transferring data that a legal provision would have to be created to allow the use of spyware. No such provision can be found in any German law.

Spyware is not only against the German constitution, but also illegal.

The automatic transfer of personal data through spyware violates the constitutional Right of Informational Self-Determination. Thus, the state must protect the individual from the use of spyware. Any individual may take legal actions against private entities using such spyware to collect personal data subject to the provisions of the German Constitution.

German Penal Code and Spyware

Section 202a (Data Espionage) of the German Penal Code was implemented to fight the use of spyware.

Section 202a Penal Code reads as follows:

> "(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.
>
> (2) Within the meaning of subsection (1), data shall only be those which are stored or transmitted electronically or magnetically or otherwise in a not immediately perceptible manner."

This provision gives individuals the right to decide who has access to their personal information contained in data.

The spying can take place in two ways:

- The data can be obtained without any conscious electronic copying, by simply reading it on a computer screen after retrieving it from a secure data storage device (local hard disk, e-mail server, etc.).
- The data can also be procured by consciously producing a copy, i.e. on a disk, the offender's computer hard disk, etc. In these cases the offender gains permanent control over the data so that the copying itself is sufficient to fulfill the elements of offence of Data Espionage according to Section 202a Penal Code.

Even though this provision does not provide a definition of data, it clarifies that it protects electronically-stored data. It's clear that data in its broadest sense, not just personal data, is to be protected. Accordingly, user names, passwords, e-mails, visited Internet sites, used programs, details of use and the like are data in the sense of Section 202a. And, since only the individual or authorized personnel are meant to have access to personal data, they are protected against unauthorized access. As a result the offender, by reviewing or storing such data using spyware, is guilty of data espionage.

A person reviewing or storing data using spyware **is guilty of data espionage.**

This provision equally applies to all sorts of spyware that are subject to the evaluation, i.e. system monitors, Trojan horses, cookies and adware so that no distinction through legal evaluation is necessary.

The second new provision of the German Penal Code, Section 303b Penal Code (Computer Sabotage), protects businesses from third-party attacks to their computers.

It reads as follows:

> "(1) Whoever interferes with data processing which is of substantial significance to the business or enterprise of another or a public authority by:
> 1. committing an act under Section 303a subsection (1); or
> 2. destroying, damaging, rendering unusable, removing, or altering a data processing system or a data carrier,
>
> shall be punished with imprisonment for not more than five years or a fine.
> (2) An attempt shall be punishable."

Generally speaking, installing Trojan horses on a computer changes the data contained on the device on which they are installed. In cases where significant data processing of business enterprises or public authorities is attacked, the installation of a Trojan Horse is a criminal offense according to Section 303b Penal Code.

Cookies, in most cases, also lead to a change of the data being stored on the targeted computer. Accordingly, the installation of cookies without the consent of the owner of the data creates a criminal offence of alteration of data.

The same holds true for adware. Adware may alter the data stored on the target computer as a prerequisite for the transfer of the identified data. Again, the individual adware programs and its effects would decide if it were criminal.

Conclusion

Using spyware to gain access to personal data is in direct conflict with the Right to Informational Self-Determination of the data subject, i.e. a constitutional right that can also be claimed in relation to private entities. If spyware is used to process personal data without consent, such use is also an infringement of the German Act on Data Protection. Finally, the undisclosed/not-consented use of spyware is data espionage and a criminal offence.

CONCLUSION

The Q1 2005 State of Spyware Report revealed that adware creates $2.4 billion in annual revenue. The Q2 2005 State of Spyware Report uncovered that spyware writers are intent on continuing this revenue generation with ads and click-throughs, but are also using more malicious attacks to steal information for financial gain. As a result, online privacy and security are at a greater risk.

Both the rate of consumer and enterprise spyware infections remain alarming high at more than 80 percent for both. Consumer adware infection rates are near 50 percent and continue to receive the majority of attention because of the debilitating effect on computing and productivity. However, there is growing awareness that keystroke loggers and Trojans pose a real and present danger with government, academic and corporate environments.

While legislative action and passionate State Attorney Generals battle adware vendors, cybercrime is going mainstream. Dozens of data loss incidents, from the benign cases of tapes lost in transit to the disturbing thefts at Choicepoint, Lexis-Nexis and CardSystems, are fueling new legislative action. Any organization responsible for the storage of confidential data will have to implement stronger security measures to protect those assets.

The Webroot Threat Research Team reports that spyware writers are rapidly refining the tools and techniques they use to avoid detection and removal. Because spyware writers exponentially outnumber anti-spyware developers, it is a challenge for any anti-spyware solution to stay ahead of the threat in this space.

The most disturbing trend in the spyware arena is the use of sophisticated tools and techniques on the part of spyware writers to insidiously install their malware and to avoid detection and removal. The Webroot Threat Research Team reports on the best (worst) examples of these techniques such as altered registry settings encryption algorithms/ packers such as UPX, Aspack, FSG, or their own proprietary algorithms, which make previous detection techniques obsolete.

Spyware writers continue to explore new ways to get installed and stay installed. System monitors are being installed via targeted attacks against industrial competitors, government agencies and banks to steal login credentials and intellectual property. Strategic use of centrally managed desktop anti-spyware is the only way to gain control over this menace to productivity and security.

APPENDIX

Federal Legislation

Bill Title & Number	Primary Supporters	Summary	Status as of 6.30.05
"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" **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
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

State Legislation

State & URL	Legislation	Summary	Status as of 6.30.05
Alabama http://alisdb.legislature.state.al.us/acas	S.B. 122	Prohibits willfully using computer software to take control of another computer or otherwise attacking operation of another computer.	Died upon adjournment May 16, 2005
Alaska http://w3.legis.state.ak.us	S.B. 140	Prohibits spyware and unsolicited Internet advertising, in particular "spyware pop-up advertisements".	Awaiting transmittal to Governor Passed Senate May 10, 2005 Passed House May 6, 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	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
Delaware http://www.legis.state.de.us	S.B. 124	Prohibits the installation, transmission, and use of computer software that collects personally identifiable information. Authorizes civil action by the Attorney General.	Introduced May 12, 2005 Referred to Judiciary Committee
Florida http://www.flsenate.gov	S.B. 2162	Prohibits certain deceptive acts or practices that involve the computer; and prohibits the collection of certain information without notice and consent. Violations are considered deceptive and unfair trade practice and provides for civil action against violators.	Died upon adjournment May 6, 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
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

State Legislation

State & URL	Legislation	Summary	Status as of 6.30.05
Indiana http://www.in.gov	H.B. 1714	Prohibits the installation of spyware, except when the computer owner consents after full disclosure. Provides for injunctive relief and the greater of actual damages or $10,000 per violation. Permits treble damages for intentional violations. Requires the consumer protection division of the attorney general's office to collect reports of spyware installations.	Died upon adjournment April 29, 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.	Signed by Governor May 3, 2005
	S.B. 465	Relates to the transmission, installation, and use of computer software through deceptive or unauthorized means.	Withdrawn March 30, 2005 (replaced by HB 614)
Kansas http://www.kslegislature.org	H.B. 2343	Prohibits unauthorized copying of software onto a computer, modifying computer settings, and other acts. Provides penalties for violations.	Died upon adjournment May 20, 2005
Maryland http://mlis.state.md.us	H.B. 780	Prohibits unauthorized persons from modifying computer settings, collecting personally identifiable information, and other actions.	Introduced February 9, 2005 Referred to Economic Matters
	H.B. 945	Prohibits actions similar to H.B. 780, with the addition that such acts are undertaken with actual knowledge or conscious avoidance of actual knowledge.	Introduced February 10, 2005 Referred Economic Matters
	S.B. 492	Prohibits unauthorized persons from modifying computer settings, collecting personally identifiable information, and other actions.	Unfavorable report from Finance Committee March 31, 2005
	S.B. 801	Prohibits unauthorized persons from modifying computer settings, collecting personally identifiable information, and other actions.	Withdrawn March 31, 2005
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

State Legislation

State & URL	Legislation	Summary	Status as of 6.30.05
Tennessee http://www.legislature.state.tn.us	H.B. 1742	Prohibits installation of certain "cookies" on another person's computer. Authorizes injunctive relief, civil damages and treble damages. Precludes class action suits against violators. Requires the establishment of reporting procedures.	Died upon adjournment May 28, 2005
	S.B. 2069	Same as H.B. 1742.	Died upon adjournment May 28, 2005
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 Effective Date September 1, 2005
	H.B. 1430	Relates to the installation, copying, or use of computer software for unauthorized purposes and stipulates penalty.	Merged with S.B. 327 and passed May 30, 2005
	H.B. 1351	Prohibits unauthorized copying of, or use of computer software for unauthorized purposes. Includes civil penalties.	Died upon adjournment May 30, 2005
	S.B. 958	Same as H.B. 1430.	Replaced by S.B. 327
Utah http://www.le.state.ut.us	H.B. 104	Amends the Spyware Control Act.	Governor signed March 17, 2005
Virginia http://leg1.state.va.us	H.B. 2215	Amends the Virginia Computer Crimes Act to add unauthorized installation of software, disruption of another computer's ability to share or transfer information and maliciously obtaining computer information as crimes of computer trespass.	Governor signed March 26, 2005 **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.	Governor signed May 17, 2005 **Public Act 500** Effective July 24, 2005
West Viginia http://www.legis.state.wv.us	H.B. 3246	Adds language regarding spyware to the West Virginia Computer Crime and Abuse Act; includes spyware definition, disclosure requirements and criminal penalties for failure to disclose.	Died upon adjournment April 9, 2005

State Legislation

State & URL	Legislation	Summary	Status as of 6.30.05
Tennessee http://www.legislature.state.tn.us	H.B. 1742	Prohibits installation of certain "cookies" on another person's computer. Authorizes injunctive relief, civil damages and treble damages. Precludes class action suits against violators. Requires the establishment of reporting procedures.	Died upon adjournment May 28, 2005
	S.B. 2069	Same as H.B. 1742.	Died upon adjournment May 28, 2005
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 Effective Date September 1, 2005
	H.B. 1430	Relates to the installation, copying, or use of computer software for unauthorized purposes and stipulates penalty.	Merged with S.B. 327 and passed May 30, 2005
	H.B. 1351	Prohibits unauthorized copying of, or use of computer software for unauthorized purposes. Includes civil penalties.	Died upon adjournment May 30, 2005
	S.B. 958	Same as H.B. 1430.	Replaced by S.B. 327
Utah http://www.le.state.ut.us	H.B. 104	Amends the Spyware Control Act.	Governor signed March 17, 2005
Virginia http://leg1.state.va.us	H.B. 2215	Amends the Virginia Computer Crimes Act to add unauthorized installation of software, disruption of another computer's ability to share or transfer information and maliciously obtaining computer information as crimes of computer trespass.	Governor signed March 26, 2005 **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.	Governor signed May 17, 2005 **Public Act 500** Effective July 24, 2005
West Viginia http://www.legis.state.wv.us	H.B. 3246	Adds language regarding spyware to the West Virginia Computer Crime and Abuse Act; includes spyware definition, disclosure requirements and criminal penalties for failure to disclose.	Died upon adjournment April 9, 2005

More on 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. 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

CREDITS

CREDITS

Webroot would like to thank the following professionals who compiled this data, analyzed it and have communicated in a way that is both compelling and educational.

Richard Stiennon, Vice President of Threat Research, Webroot Software Inc.
Paul Piccard, Director of Threat Research, Webroot Software Inc.
The Webroot Threat Research Team

ABOUT
Webroot Software

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.

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 1-800-772-9383.

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.