STATE OF SPYWARE

2005: THE YEAR IN REVIEW

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

"**The Former Prince of Freedonia Needs Your Help"**

How many of us have received this e-mail or something like it: the former prince of Freedonia has been bilked of his family's fortune, and he needs your help because he has heard you are an honest person and can be trusted. Won't you please respond and help?

So begins one of the oldest con games in the world.

Here's how it goes. The prince says he has all this money but can't get at it because he doesn't have a U.S. bank account. You agree to help by accepting the money into your bank account. He says 'Wait, how do I know you won't run off with my money' and asks you to put up some money as collateral. You agree to wire your money to his account, and once his money is in your account and safe he'll wire your money back. A variation on this con almost snagged a friend of mine in college and another variation is what gets Robert Redford in trouble with the mob in "The Sting."

But, you'd never fall for that. And yet, I get this e-mail or one like it about three times a month, for the simple reason that it must work on somebody. That's how con artists operate; it's all about numbers.

Ask enough people, and eventually you'll find a mark and gain their confidence, so they are willing to do something that common sense would tell them is probably not the smartest move in the world. Con games are also very high on the food chain of criminal activity. They rarely get reported because the victims feel foolish. They rarely include violence or even a threat of violence.

We have begun to think of many forms of spyware as the con game of cybercrime. After all, one of the most prevalent and dangerous spies around, the Trojan horse, is named after one of the greatest cons in history. There is the blunt instrument of pop-up ads that intrude on users and slow computer performance to a crawl.

With the onslaught of governmental intervention and public outcry, the purveyors of that kind of marketing have either changed their ways, eventually will change their ways, or will run that business into extinction.

But the real threats trick consumers into opening their computer and letting spies waltz into their private information. The true con sees an opportunity, never evidences itself until the hook is set and the game is done, and is gone before the mark realizes what has happened.

In December, spyware writers took advantage of another flaw in Windows security, and a new wave of Trojan horses hit the market just in time to snap up information from unsuspecting holiday shoppers. A seemingly benign flash image on a Web site infected passing surfers with nasty and difficult to remove spyware before they could say Merry Christmas.

This kind of "conware" continues to be the bane of computer security. Webroot's surveys continue to show steady rise in Trojan horses quarter over quarter. System monitors have increased by 50 percent in the last three quarters. These kinds of malicious spyware are growing stronger and show no signs of slowing down. And why should they?

In a previous report, we used this space to discuss the criminal enterprise of spyware. This past quarter, the FBI attempted to quantify that for the industry. In a survey the Bureau conducted in 2005, it polled over 2,000 organizations and estimated that as much as 64 percent of the respondents had suffered some financial loss from spyware and other computer-related crimes. The Bureau extrapolated the costs across U.S. businesses, and surmised that these kinds of crimes cost as much as $62 billion. That is 10 percent more than all identity fraud and over 60 times the cost of telecommunications fraud.

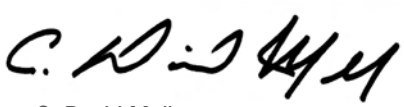
To put it in another perspective: that puts the cost at just under the annual revenue of Bank of America, number 20 on the Fortune 500. What's incredible to me is that while figures like that sound astronomical, the FBI actually applied a highly conservative model

to the extrapolation from the study sample to the overall business population. Had they done straight math, the estimates would approach $200 billion – pretty soon we're talking real money.

Unfortunately, the great spyware con is not just developers preying on consumers and businesses. Webroot's recent research has found there is a fox in our own hen house. Hundreds of "rogue" anti-spyware programs have emerged attempting to cash in on the crisis. These illicit programs that frighten surfers into thinking their systems are replete with spyware, and then sell them software that can't fix the problem and was probably never designed to do so. Luckily, smart consumers are buying quality products, keeping them current, and sleeping comfortably at night. But, there is so much hype around spyware that some consumers and businesses don't know where to turn. Vendors tell them the threats are growing. Some vendors say an anti-virus tool is good enough. Some vendors say your PC is feeling sick and you should buy this snake oil. And then the spyware developers are subtlety enticing webizens into their confidence schemes.

Suddenly, choosing the right anti-spyware seems more important than ever.

On the silver screen, people love a good con game. The top 40 grossing con game movies have hauled in nearly $900 million, so clearly movie-watchers enjoy someone tricking someone else into giving up money. Perhaps that's because most people would never believe it could happen to them. Yet, Trojan horse infection rates are at an all time high, and many fall further into the trap they are trying to escape as they pick spyware in anti-spyware clothes. For all the people who think they could never be conned, these numbers tell a different story. Perhaps the con is more interesting at the movies than on our real-life computers. Look out, the Prince of Freedonia just wrote back...



C. David Moll
CEO
Webroot Software, Inc.

HIGHLIGHTS

News & Incidents

Security analysts may consider 2005 as one of the worst years ever for data security losses. In all, more than 130 different security breaches exposed over 55 million Americans to a wide range of illegal activities, including the possibility of identity theft. Many organizations and businesses, like H&R Block, University of California and Ford Motor Company, suffered security breaches, compromising personal customer and employee data. Sony BMG made headlines following its use of rootkits in its digital rights management software. Following these scandals, Microsoft revealed a major vulnerability, a WMF flaw that hackers could use to access and take control of a system. – page 14

Threat Research/Phileas

During 2005, Webroot identified more than 400,000 sites that host spyware. Throughout the year, evading detection and removal became the primary focus of spyware authors. To this end, spyware writers continue to increase their user base by targeting security vulnerabilities and using advanced techniques, such as polymorphic code, to operate under the radar. It is now common for keyloggers to use kernel-level drivers, not only making them more robust and stable, but also extremely difficult to detect. – page 26

Enterprise and Compliance

Complying with government regulations became a high priority for businesses of all sizes during 2005. An increasing number of enterprises found themselves confronting a high number of complex spyware programs, such as system monitors and Trojan horses. From Q2 to Q4, system monitors increased 50 percent each quarter. The continuous spyware offensive caused many of these enterprises to scramble to stay ahead of these threats. According to a Webroot Internet Security survey, more than half of the businesses hit with spyware lost revenue as result. – page 41

Consumer

Despite a high awareness level about spyware, more and more consumers are becoming infected with unwanted programs, particularly with malicious programs such as Trojan horses and system monitors. Home computer users in United States, Thailand and United Kingdom continue have the highest infection rates. To make matters worse, scam artists are cashing in on the heightened awareness and high infection rates by offering bogus, or "rogue" anti-spyware products. To guard against new spyware programs, home computer users must use an anti-spyware program with frequent definition updates. – page 53

Legal & Legislation

Throughout the past year, legislators at the state and federal levels tackled the growing spyware threat. By the end of 2005, 12 states have passed spyware laws – 11 of which are already in effect. The FTC stepped up its enforcement activity in 2005 by filing several actions against purported purveyors of spyware and bogus anti-spyware software, as well as actions against companies that, according to the FTC, failed to adequately protect customer data. – page 68

THE STATE
of Spyware

During 2005, spyware became the leading threat to safe and secure computing. In response to this rising threat, a number of security product vendors introduced their enterprise anti-spyware products, arriving late to the game while attempting to cash in on market demands.

The wide availability of anti-spyware solutions, including freeware products, has had an effect on the prevalence of spyware on consumer and enterprise computers. Despite this increased adoption rate, new infections, new malware and major incidents dominated industry news throughout the year.

Spyware evolved dramatically during 2005. New propagation methods emerged targeting Internet browsers as a way to spread malicious infections. Polymorphic code and advanced encryption techniques are used increasingly by spyware writers to avoid detection.

File obfuscation techniques received a great deal of attention in the mainstream media. These techniques, also called rootkits, allow spyware to avoid detection and removal. Sony BMG made the news following the use of rootkits in their digital rights management software, bundled with various music CDs. The immediate outcry from industry watchers and class action lawsuits filed by consumers should serve as a warning to other commercial entities wishing to invade the desktop.

Following the highly publicized announcement of the Windows Meta File (WMF) vulnerability, the Webroot SpyAudit results indicated a sharp rise in the occurrence of Trojans on desktops in the fourth quarter of 2005.

The WMF flaw opened a security hole in the image viewing engine in Windows to allow remote code execution. In other words, any time an image is displayed, it gives that image the option of installing anything it wants on the computer. This vulnerability went unpatched for weeks – jeopardizing the security of Windows computer users worldwide.

Many industry analysts consider the WMF flaw and the subsequent rise in Trojan horses as yet another sign that malicious spyware infection rates are climbing.

As spyware infection rates soar, it reinforces the need for home computer users and enterprises alike to keep their anti-spyware programs up-to-date with current definitions. Definitions that defended against last week's spyware programs may be unable to protect against today's malicious programs.

Moreover, reputable anti-spyware programs offer improved detection and removal capabilities with product updates. Computer users need to start the habit of updating to the latest version available to defend against these unwanted programs.

Also during 2005, Congress struggled to bring a spyware bill to the Senate floor. Three competing bills were debated in committee throughout the course of the year. One bill, SB 1608, "Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond Borders Act of 2005" sponsored by Senator Gordon Smith (R-OR), passed the committee by voice vote and without amendments. The next step is to resolve the two bills that have made it through committee with an additional House-passed bill.

It has been a productive year for the FTC, the body tasked with enforcing fair trade on the Internet. The FTC settled two cases it brought against scam anti-spyware purveyors. And earlier in the year, in a landmark case, the FTC extracted a consent agreement from BJ's Wholesale resulting from BJ's loss of millions of customer credit cards.

Read on to get a complete update on the current State of Spyware, including fourth quarter SpyAudit data as well as a look back at 2005 results.

News
& Incidents

2005 News and Incidents

Security analysts may consider 2005 as one of the worst years ever for data security losses. In December alone, both Ford Motor Company and Sam's Club revealed that they had suffered data security breaches, which compromised personal customer and employee data, such as Social Security and credit card numbers.

In all, more than 130 different security breaches exposed over 55 million Americans to a wide range of illegal activities, including the possibility of identity theft.

These high-profile breaches continue to affect consumers' pockets. ChoicePoint, a data broker firm, and victim of fraud in early 2005, had to adjust second quarter earnings to cover costs associated with their security breach.

These high-profile breaches continue to affect consumers' pockets.

When determining its profits for Q2 2005, ChoicePoint deducted $.04 per share from its shareholders to cover the company's legal expenses and professional fees as well as expenses incurred in its fight to tighten security, deal with consumer lawsuits, and pay for the credit-monitoring services offered to the thousands of people affected by the data loss.

Q4 2005 Incidents Update

Sony BMG

Following a firestorm of protests and class-action lawsuits, Sony BMG recalled thousands of CDs bundled with rootkit software designed to prevent piracy. The software was developed to restrict the number of times music on a single disc could be copied.

Sony BMG used digital rights management software developed by First4Internet, Ltd., a British software company.

The disputed software reportedly opened customers' computers to hackers and viruses. The lawsuits claimed that Sony BMG has surreptitiously installed spyware on the CDs.

In addition, security analysts report that manual attempts to remove the software can harm the computer.

Ironically, claims of copyright infringement were made against First4 Internet, Ltd. The Sony BMG software in dispute contained free software code, covered by the Free Software Foundation's Lesser General Public License.

Refer to the Legal and Legislative section for more details on the Sony BMG incident.

This vulnerability illustrates that the security threats have evolved.

Microsoft WMF vulnerability

In late December, Microsoft issued a security advisory related to a flaw in some Windows graphics files, known as Windows Meta File (WMF). Immediately following the announcement, criminal hackers began exploiting the vulnerability.

This vulnerability was particularly dangerous because even simple activities such as viewing a Web page or reading an e-mail were no longer safe. If the Web page or e-mail message contained an infected image, the user's computer would be infected.

Experts claim that about 90 percent of computer users worldwide use some variation of Windows operating system.

This vulnerability and the hacker activity around it illustrate that the security threats have evolved. For example, criminal hackers didn't follow the previous patterns of other exploits such as Blaster and Code Red, which were widespread in nature.

Rather, they fit the model of current online threats, which aren't designed for bragging rights, but instead are tied to online theft and fraud and focus on specific monetary goals.

The Microsoft security advisory characterized the attacks as limited in scope, but a large number of technical Web sites focused on the dangerous possibilities the vulnerability could cause.

Before Microsoft could issue a patch to the WMF flaw, an unofficial third-party patch was made available on the Internet. The availability of this patch illustrates the urgency in correcting this flaw before more exploits could occur.

In early January, Microsoft issued an official patch. Given the urgency of the situation, Microsoft released the patch separately instead of including it with its monthly security bulletin, due out later in the month.

University of California

In the largest disclosure under California's anti-identity theft law, University of California revealed a data security breach affecting more than 1.4 million Californians who participated in a state social program.

The exposed data includes the names, addresses, phone numbers, social security numbers and birth dates of everyone who participated in California's In-Home Supportive Services program since 2001.

The database is made available to university researchers on the Berkeley campus. Following the data breach, the state has withdrawn the researcher's access to the records. The university had not been in compliance with security rules the state established for research access to sensitive data.

University of California revealed a **data security breach affecting more than 1.4 million Californians.**

H&R Block

H&R Block inadvertently exposed customer Social Security numbers during a mailing offering free copies of the company's tax software. The tracking number on the mailing contained the Social Security numbers.

H&R Block blamed user error and said no customer data had been lost or stolen as a result of the mistake.

Ford Motor Co.

Late in 2005, Ford Motor Company began notifying some 70,000 current and former white-collar workers that their sensitive personal and financial data had been stolen. The confidential information, which included employees' names, addresses and Social Security numbers, was contained on a stolen computer.

Although the company maintains that there is no evidence that any of the information has been misused or used for the purpose of identity theft, there is no guarantee that it will not be. Thus, Ford has notified the FBI, the Federal Identity Theft Task Force, the U.S. Secret Service, and the three major credit reporting services of the theft.

In an effort to guard against misuse of the stolen personal data, Ford plans to pay for a credit monitoring service and other services for those affected by the theft.

Hirayama used a Trojan horse hidden in an e-mail to install keylogger software.

Japanese Bank Thief

In November, Tokyo police arrested Kiichi Hirayama, a 34-year old computer hacker, for allegedly transferring 210,000 yen from a jewelry company's bank account. Police suspect that he completed the transaction by illegally obtaining the firm's banking identification number and password.

Police believe that Hirayama transferred 1.4 million yen from at least 10 corporate bank accounts. The banks include JapanNet, E-Bank, Mizuho and Okawa Shinyo Kinko. Experts suspect that Hirayama used a Trojan horse hidden in an e-mail message to install keylogger software on computers at the various businesses.

Sam's Club

Sam's Club, a division of Wal-Mart Stores Inc., continues to investigate a security breach that exposed credit card data belonging to a number of customers who bought gas at the wholesaler's stations in late September and early October.

In a statement, the Bentonville, Ark.-based company said credit card issuers who reported customers complaining of fraudulent charges on their statements alerted the

company to the problem. It's still unclear how the data was obtained. Sam's Club is cooperating with both Visa International Inc. and MasterCard International Inc. to investigate the breach. The company also has notified the U.S. Attorney's Office and the U.S. Secret Service.

Guidance Software

In November, computer hackers broke into a Guidance Software database and captured close to 4,000 customer credit cards.

While the number of records stolen is relatively low, it's alarming given the nature of Guidance Software's business. The software company is the leading provider of software used to diagnose hacker break-ins. Many of their customers are law enforcement agencies worldwide, including the U.S. Secret Service, the FBI and New York City police.

Guidance failed to follow the guidelines used by Visa and MasterCard that require vendors to encrypt customer credit card databases. This incident illustrates that every company is vulnerable to security intrusions.

Guidance failed to follow the guidelines used by Visa and MasterCard.

U.K. Charity, Aid to the Church in Need

A U.K. charity revealed that its online security systems had been breached by hackers in December. The charity didn't disclose how much money the criminals stole, but identified that the addresses of 2,800 online donors were stolen.

The hackers took things a step further and contacted the charity's donors and tried to extract more money. Security analysts warned other charities to guard against Internet fraud.

Google

A Trojan horse designed to create Web pages that mimic Google ads was identified in December. The Trojan tries to incorporate its ads in Google AdSense publisher program.

The Trojan produces its own set of ads, which lead the user to different sites and causes legitimate Google advertisers and publishers to have poor revenue.

Once a user downloads the Trojan, the malicious program replaces the original ads with its own ads.

British Rogue Dialers

Effective Dec. 30, 2005, British Parliament raised the penalty for companies using rogue dialers.

Companies caught using U.K. premium rate phone services, similar to American pay-per-minute telephone numbers, can be fined up to £250,000 or $434,281. The action comes after a high number of dial-up Internet users have fallen victim to rogue dialers in 2005.

Rogue dialers are frequently spread using Trojan horses hidden in e-mail. The dialer program automatically call premium-rate phone numbers, running up big bills that people don't discover until after the fact.

Rogue dialers are frequently spread using Trojan horses hidden in e-mail.

2005 Incidents

The following is a snapshot of several other high-severity security incidents that made headlines in 2005.

'Titan Rain' Attack

In August 2005, U.S. government officials revealed that they were investigating 'Titan Rain,' an attack on hundreds of U.S. computer systems, including the Departments of State, Homeland Security, Energy and Defense.

'Titan Rain' was just one part of a coordinated series of hi-tech attacks on key parts of the world's vital Internet infrastructure. The attacks intended to steal information from computers that would make the perpetrators millions of dollars.

Israeli Trojan Horse Scandal

In Israel, it was discovered 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.

The private investigators used modified Trojan horses to steal documents.

In early July 2005, an Israeli prosecutor filed indictments against nine private investigators involved in the industrial espionage case that involved planting malicious Trojan horses on competitors' computers.

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

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, United Kingdom and 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 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 the keylogging software to the targets disguised as a legitimate e-mail proposal.

BJ's Wholesale Club, Inc.

One of the single most compelling data thefts of the year 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 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.

In June 2005, BJ's Wholesale 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 requires BJ's to implement a comprehensive information security program and obtain audits by an independent third-party security professional every other year for 20 years.

Spear-Phishing and United Kingdom's National Infrastructure Security Coordination Centre

In June 2005, the National Infrastructure Security Coordination Centre, a government bureau that keeps an eye on computer security in the United Kingdom, issued a public warning about a spear-phishing campaign targeting industrial and government computer networks.

Spear-phishing, a hybrid form of phishing, is an e-mail scam aimed at specific victims instead of casting a wide net across e-mail hoping to catch a wide range of victims. Security analysts claim that spear-phishing is the work of sophisticated hackers in search of financial gain, trade secrets or military information.

The U.K. warning called the spear-phishing incident a "targeted Trojan e-mail attack" and noted that the e-mail messages appear to come from a trusted sender. In addition, traditional anti-virus and firewall software didn't protect recipients from the e-mail message.

The U.K. warning called the incident a "targeted Trojan e-mail attack."

CardSystems and MasterCard International

MasterCard International notified its member financial institutions of a breach of payment card data that occurred in May 2005, 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 CardSystems Solutions' network. 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.

DSW Shoe Warehouse

In April 2005, 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.

A keylogger is to blame for the attempted heist of $423 million.

Sumitomo Mitsui Bank

At Sumitomo Mitsui's London offices, a keylogger is to blame for the attempted March 2005 heist of $423 million. Keylogger programs, a type of spyware, are used by hackers to snatch user account information – like login names and passwords – and grab other lucrative data including account numbers.

Authorities have confirmed that the cleaning staff planted a keylogger on the bank's computer network.

Lexis-Nexis

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 and then gain access to the database. They used this access to pilfer more than 200,000 identities.

Oklahoma Sheriff's Department

A sheriff's department in Oklahoma discovered surveillance spyware installed on computers in their office. The installed spyware allowed unauthorized access to sensitive information about prisoner movements, personnel files and confidential homeland security information.

ChoicePoint

The perpetrator behind the February 2005 ChoicePoint data breach, which exposed the personal information of 145,000 people, pleaded guilty to charges of conspiracy and grand theft. Nigerian-born Olatunji Oluwatosin will be sentenced on February 10, 2006. He is currently incarcerated for a previous felony count of identity theft.

ChoicePoint is a data broker that specializes in providing records of consumer activity to government agencies, employers and third-party businesses. The company has nearly 20 billion records on individuals, including motor vehicle registrations, license and deed transfers, military records, addresses and Social Security numbers.

Despite its security mistakes, ChoicePoint continues to supply information and records on individual citizens to government and law enforcement agencies. However, following the well-publicized theft, ChoicePoint altered its security practices, including restricting the sale of reports that contain Social Security numbers.

Refer to the Legal & Legislation section for details on many of these incidents.

THREAT
Research/Phileas

Threat Research

Throughout 2005, evading detection and removal became the primary focus of spyware companies and spyware authors. To this end, spyware writers continue to increase their user base by targeting security vulnerabilities and using advanced techniques, such as polymorphic code, to operate under the radar.

As spyware companies strive to create stronger, more persistent programs, there has been an increase in spyware using driver-based technologies. These programs sit at the lowest level of the operating system, embedding themselves deeper than early generations of spyware into the computer with the ability to extensively damage the user's operating system.

Current spyware development not only focuses on hiding spyware from the user, but also on implementing auto-updating technology to avoid detection. The constant changing of threats requires the anti-spyware industry's undivided attention.

The constant changing of threats requires the anti-spyware industry's undivided attention.

Spyware Installation Methods

Bundling software remains one of the most favored and widely employed methods for spyware delivery. Often, users intend to download one program contained within a bundle of programs, but are forced to download the entire package of software. Bundles usually contain other extraneous and often undesirable programs, and do not give users the ability to choose which specific programs to download.

Many of these bundles use the end-user license agreement (EULA) to inform users that they are installing a group of programs. EULAs continue to be cumbersome to decipher and actually hinder a user's understanding of what is being downloaded within a software bundle. Once the bundle is downloaded, the undesirable programs contained within this package become active and install spyware and adware programs, which often results in a massive spyware infection on a user's computer.

Spyware also takes advantage of the vulnerabilities found in unpatched Web browsers and operating systems. Malicious Web sites include specially crafted Java applets, Windows Help file, or animated cursors which contain code allowing spyware installation without a user's consent.

While both bundling and exploiting Web browser and operating system vulnerabilities are standard methods of distribution, many new threats require users to install special and "necessary" programs to view a Web site. Some programs claim to be anti-spyware software.

These rogue anti-spyware programs "scan" the user's system, reporting malicious threats that require removal. These programs scare the user into downloading and often paying for the program based on these false results. Refer to News and Incidents to read more about rogue anti-spyware programs.

Rogue anti-spyware programs scare the user into downloading and often paying for the program based on these false results.

Preventing Detection and Removal

Spyware writers employ a number of tricks to avoid detection and removal, including changing file names, folder names, registry names or adding components to their payloads to avoid distributing fingerprints that can be easily identified. These traditional tactics are well known in the industry and only prevent easy detection of malicious components on a computer.

Spyware is becoming more advanced with each newly created piece of malware. Spyware authors have started injecting code into program processes, or into other system components such as Windows Explorer. This is often achieved by loading a dynamically linked library (.dll) within a running process, or by creating a "thread" within a legitimate and independently running process. Using these methods make it nearly impossible for users to detect spyware without assistance from advanced programs.

These advanced programs demonstrate that spyware and adware developers are on the cutting edge of utilizing persistence techniques and no longer have to rely on antiquated viral methods. In addition, these sophisticated programs can completely overtake a computer to execute a service or process with system-level privilege or, even more aggressively, as a driver that executes in step with the operating system.

Evolution to Driver-based Techniques

The new breed of spyware is at a level where detection and removal becomes extremely difficult. The line between rootkits and Trojans is becoming increasingly blurred as spyware utilizes techniques that were previously reserved for extensive use in rootkits.

After using a Trojan to gain access to a computer, some online criminals will use a rootkit to help maintain access to a computer without the user's awareness. Rootkits typically hide logins, processes, files and logs, and may include software to capture information from desktops or a network. Because rootkits hide the presence of an intruder and the intruder's actions, it is understandable that new threats are adopting these techniques.

The new breed of spyware is at a level where **detection and removal becomes extremely difficult.**

The term "rootkit" became mainstream during the Sony BMG copy protection controversy, following Sony's decision to include a rootkit in its digital rights management software bundled with music CDs.

In addition to rootkits, spyware is using more "Ring-0" or driver-level techniques, including lower level API hooking and thread injection. When a program sits at this level, it has complete control over an entire computer. Programs can hide data, files or actions.

Detection and removal of spyware that uses drivers is more difficult because no data that Windows returns can be considered reliable as it may have been modified by the spyware program's driver.

Keylogger Advances

It is now common for keyloggers to use kernel-level drivers, not only making them more robust and stable, but also extremely difficult to detect. It has also become common for keyloggers and system monitors to use process blocking to actively stop anti-spyware programs from running.

Keyloggers attempt to block the running processes and services of several mainstream, anti-spyware products. Therefore application protection procedures are a must for any anti-spyware application.

Throughout the range of commercial and non-commercial system monitors, keyloggers are becoming more aggressive and are no longer content to merely evade a computer's operating system. Anti-spyware as well as other detection software programs are now common targets.

Keyloggers attempt to block the running processes and services of several mainstream anti-spyware products.

Changes in Adware

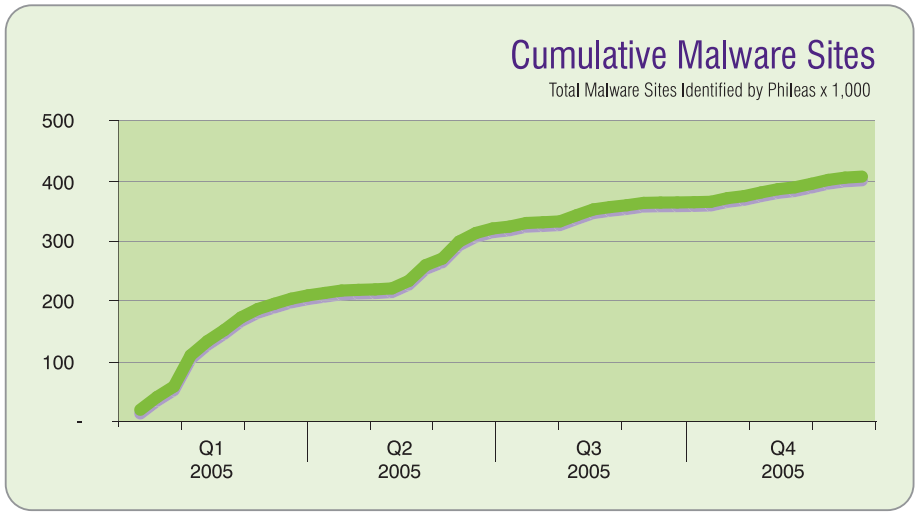
As a result of pending state and federal legislation, a few adware companies claim they have modified their behavior for the better. Some companies have incorporated new technology to enforce the display of an installation consent screen prior to installation to ensure that users are aware of what they are downloading and installing.

Although some companies are trying to escape negative associations with their products, other applications are still malicious by nature. A few of these programs continue to download adware programs onto a machine without the user's consent. Frequently, it's primarily a toolbar that is downloaded, but also serves advertisements and hijacks browser settings.

Web Crawler Automation

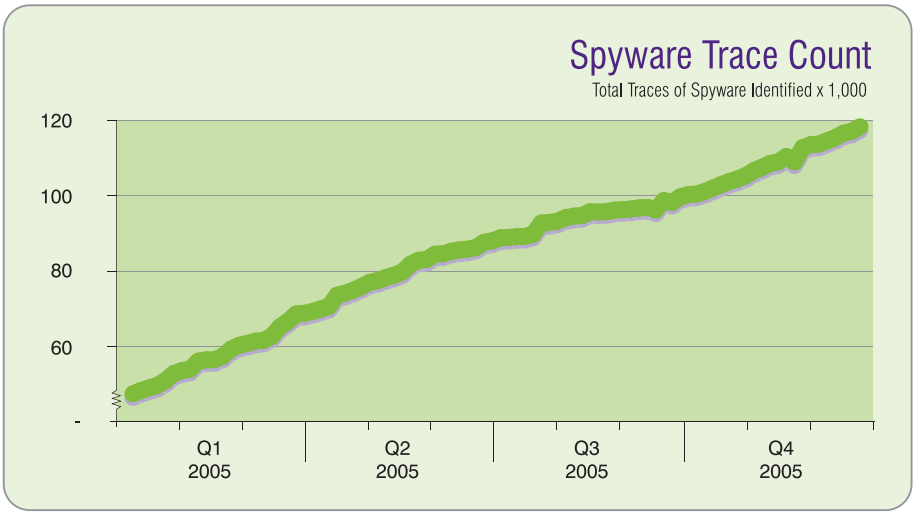
During 2005, Webroot identified more than 400,000 sites that host spyware. An effective and efficient means of identifying spyware is to use Web crawler technology to find new threats before they can infect end users. Webroot employs this methodology by using Phileas™, a malware crawler that is capable of searching the Internet for Web sites containing malware.

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



Phileas data, which references the increasing number of existing, potentially malicious Web sites, supports evidence that malware creators are working overtime with a goal of distributing malicious threats to users. An automated tool such as Phileas is the best way to track growth of this magnitude.

Phileas has been developed as a scalable solution, so as the spyware problem grows, the architecture can keep pace.



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

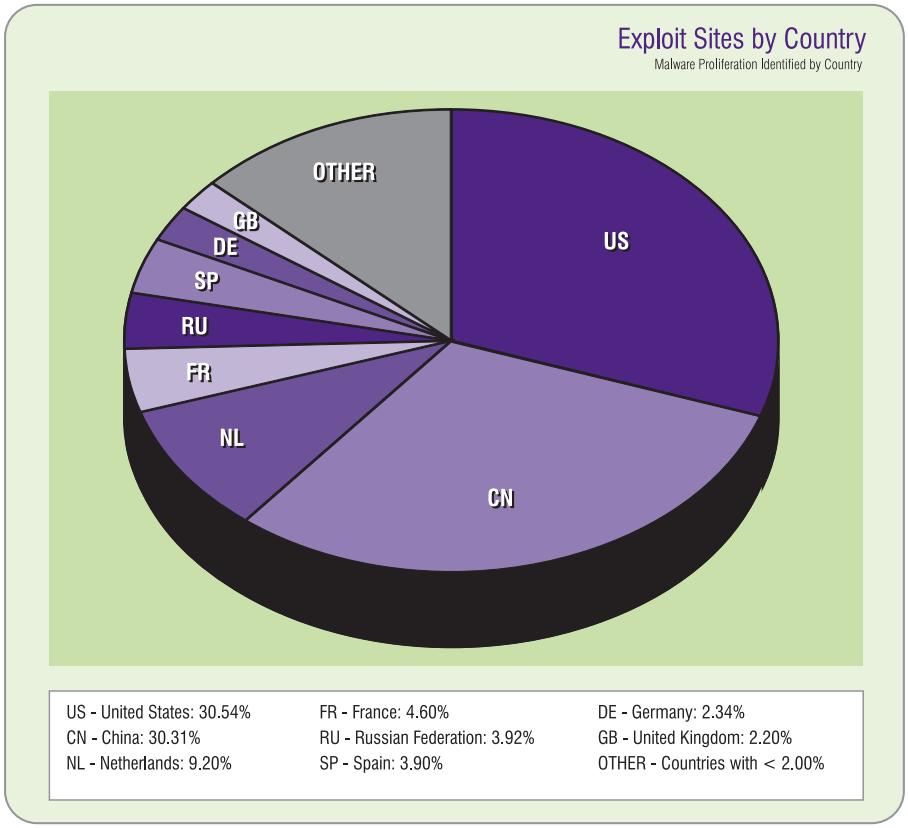
At the start of 2005, Webroot had identified more than 40,000 traces of spyware. During 2005, Webroot nearly tripled the total number of spyware traces identified, bringing the total to 120,000.

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

Webroot has identified **120,000 traces of spyware to date.**

Worldwide Problem

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



According to recent Phileas statistics, 30.5 percent of the spyware exploits originate from the United States, followed very closely by the China at 30.3 percent. The proliferation and attainability for high-speed Internet connections in the United States may be responsible for these increasingly high numbers. Even more alarming, it is suspected that some Web site hosting companies are knowingly permitting spyware Web sites, turning a blind eye to this malicious activity.

False Positives

Identifying spyware is only the first step towards eradicating it from a user's computer. After identifying a spy, a definition is created that is capable of detecting and removing a particular piece of spyware from a computer.

Each definition undergoes testing to ensure that it can correctly identify and remove malicious code and more importantly, that it does not remove or interfere with legitimate files. Incorrect identification, or a false positive, presents one of the most challenging aspects in creating an effective anti-spyware program.

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

Despite these issues, not all anti-spyware vendors take the steps necessary during the quality assurance cycle to prevent false positives.

Phileas provides information that constantly feeds the Webroot spyware repository. The Webroot Threat Research team ensures that new spyware definitions are thoroughly tested to guarantee that the definitions detect and remove spyware-only related files and components.

Top Threats

The top threats this quarter displayed the continued use of packing and encryption algorithms. Spyware based on Trojan horse code, a viral installation procedure, or a polymorphic engine requires new detection and removal methodologies to stay ahead of the threat.

It's important to note that two of the top 10 programs listed are considered rogue anti-spyware programs.

The top threats this quarter displayed the continued use of packing and encryption algorithms.

180 Search Assistant

Short Description: 180search Assistant is adware that may direct you to sponsor's 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.

Apropos

Short Description: Apropos is adware that may display advertisements on your computer.

Characteristics: Apropos may display advertisements on your computer.

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

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

Virtumonde

Short Description: Virtumonde may display advertisements on your computer.

Characteristics: Virtumonde may display advertisements on your computer.

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

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

SpywareStrike

Short Description: SpywareStrike is a system maintenance and security application that may install without consent and load at Windows startup.

Characteristics: SpywareStrike may have been installed without your consent.

Method of Installation: SpywareStrike may be installed by a direct download or may install via a Trojan horse or pop-up advertisement.

Consequences: This software may have been installed without your consent.

EliteBar

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

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

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

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

ISTbar

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

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

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

Consequences: ISTbar may monitor the Web sites you visit.

CoolWebSearch (CWS)

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

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

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

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

PSGuard

Short Description: PSGuard is a "spyware remover" that may hijack your desktop until you install the program.

Characteristics: PSGuard may redirect your Web searches through its own search engine and change your default home page to the author's Web site. This hijacker may also change your other Internet Explorer settings.

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

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

SurfSideKick

Short Description: SurfSideKick may display advertisements on your computer.

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

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

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

DirectRevenue-ABetterInternet

Short Description: DirectRevenue-ABetterInternet, commonly known as VX2 or Transponder, is an adware program that may display pop-up advertisements on your computer.

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

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

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

ENTERPRISE
& Compliance

Enterprise & Compliance

As the News and Incidents section reveals, 2005 may go down in history as one of the worst years ever for data security breaches. Stories ripped from the headlines illustrate that corporations can no longer be complacent about the evolving spyware threat. As Webroot's SpyAudit data suggests, no company is immune. Unsuspecting companies that feel that they do not need protection from spyware have fallen victim to this evolving threat.

Many of these security incidents came to light as a direct result of state legislation requiring corporations to reveal when customer data has been compromised, such as the California security breach notification law. Corporations are now faced with meeting this mandate as well as others, such as the FDIC advisory, HIPAA, Gramm-Leach-Bliley Act and Section 5 of the FTC Act.

To maintain compliance with these initiatives, corporations have been forced to rethink their data security measures. Of particular concern is the looming question of how spyware may jeopardize compliance with new laws and regulations.

The business may lose considerable customer and shareholder confidence.

Many corporations today recognize that just one piece of malicious spyware, such as a Trojan horse or system monitor, can push them out of compliance. If this occurs, the federal government can levy significant fines against the corporation. Even worse, the business may lose considerable customer and shareholder confidence, directly affecting revenue and market share.

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

The following is a recap of the connection between spyware and government compliance initiatives.

FDIC

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

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

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

HIPAA

With the implementation of the Health Insurance Portability and Accountability Act (HIPAA), health care organizations began to seriously examine security measures within their organizations. Under HIPAA, personal information must be secured from the possibility of misuse or fraud.

In many cases, the strict provisions outlined in HIPAA have led to extensive overhauling of security programs with regard to medical records and billing systems. As such, many organizations have routinely allocated resources for security infrastructure strategies, such as widely deployed desktop controls including anti-spyware solutions.

Specific security rules regarding workstation use can reduce the risk of spyware infection, such as prohibiting access to gambling or pornographic sites. Other policies limiting the ability to install new software on desktops also reduce risk.

In response to the HIPAA provision requiring health care organizations to address security incidents, many organizations have turned to anti-spyware software that can identify and deflect spyware attacks.

To comply with HIPPA, health care organizations should take all reasonable measures to protect patient personal information from the dangers of spyware.

Gramm-Leach-Bliley Act

Like HIPAA's provisions for the health care industry, the Gramm-Leach-Bliley Act (GLB) issues similar rules for protecting customer information for the financial industry. Under GLB, individuals are protected from the misuse of their information when it's obtained under false pretense.

The majority of the incidents reported in 2005 involved loss of account and personal information from financial institutions. Many of these incidents opened the targeted enterprises to legal action for failing to comply with GLB.

The majority of incidents involve a loss of account or **personal information.**

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

In a case involving **Providian National Bank**, the institution was required to pay $300 million in restitution to customers for abuses related to guaranteed savings rate, credit protection and other programs. Similarly, in a case involving the **First National Bank of Marin**, the bank was ordered to establish a reserve to handle restitution payments, with an initial deposit to that fund of $4 million. Other recent investigations have resulted in restitution by **Direct Merchants Credit Card Bank**, **First Consumers National Bank** and the **First National Bank in Brookings**.

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

Section 5 of the FTC Act

The FTC's concern with data security, as distinguished from general privacy, dates back to its adoption of regulations to enforce the GLB, otherwise known as the FTC's "Safeguards Rule."

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

As the FTC's recent action against **BJ's Wholesale Club** shows, failure to protect networks against intrusions that compromise customer data are considered unfair, and will be attacked.

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

Refer to the Legal and Legislative section for more on FTC activities.

Enterprise Findings

During 2005, an increasing number of enterprises found themselves confronting a high number of complex spyware programs, such as system monitors and Trojan horses. The continuous spyware offensive caused many of these enterprises to scramble to stay ahead of these threats.

Facing a loss of customer trust that can easily domino into loss of revenue, enterprises now concern themselves with the implications of keystroke loggers on internal computers.

Malicious spyware, which includes system monitors and Trojans, is increasing in prevalence within the enterprise. Between Q3 and Q4 2005, Trojan horses increased 9 percent. From Q2 to Q4, system monitors increased 50 percent each quarter.

As malicious spyware grows in complexity, it presents a problem for traditional virus detection methods. Most spyware behaves drastically different than viruses.

Most spyware behaves drastically different than viruses.

It's important to recognize that anti-virus programs and free desktop anti-spyware solutions are ineffective against complicated and sophisticated spyware programs. The detection and removal engines used by anti-virus and freeware anti-spyware programs are unable to root out these insidious programs, which use polymorphic code or rootkit technology to avoid detection.

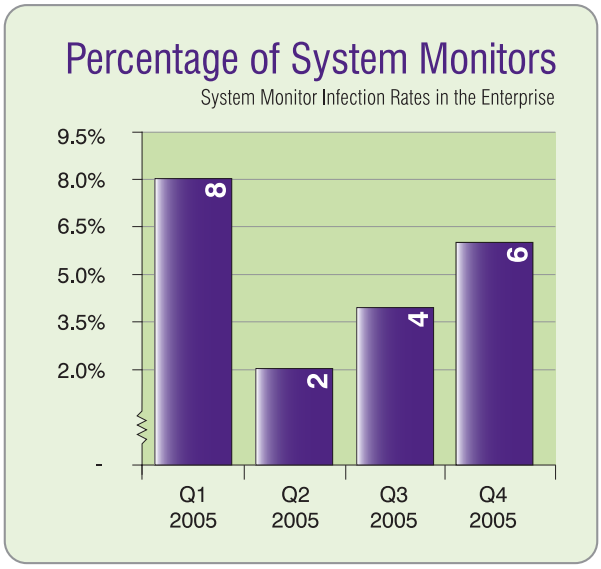
Additional Enterprise Findings

System Monitors

System monitors are growing in sophistication and are now being deployed by cyber-criminals to capture personal logins and other passwords to gain access to networks.

Six percent of infected PCs had system monitors in Q4, up from 4 percent in Q3, a 50 percent increase. Industry analysts fear that attackers are customizing system monitors to keep them hidden and undetected.

Just as mainstream companies adjust their business models to continue to be effective, spyware developers have resorted to increasing their penetration of keyloggers, especially during the heavy online commerce season to gain access to sensitive corporate information.

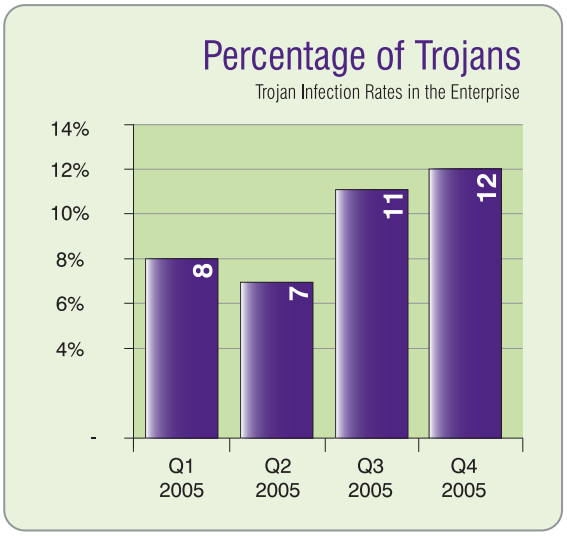


Trojan Horses

The infection rate of Trojan horses increased in the last three quarters of 2005 – from 7 percent to 11 percent to an all-time high of 12 percent in Q4. During the past few quarters, hackers have relied on Trojan horses to secretly install system monitors on unsuspecting computers.

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

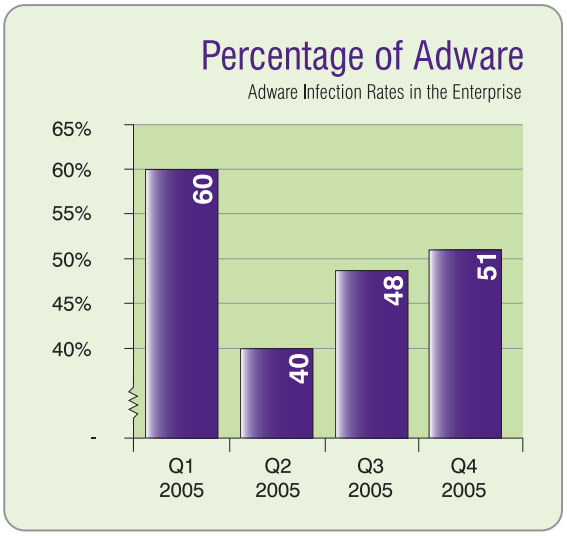
Additionally this increased level of Trojan horses may indicate that the threat from system monitors deployed for identity theft within Trojans could rise dramatically in the next several months. Because Trojans are usually installed via worms or viruses, their overall existence on enterprise machines can fluctuate with the level of new outbreaks.



Adware

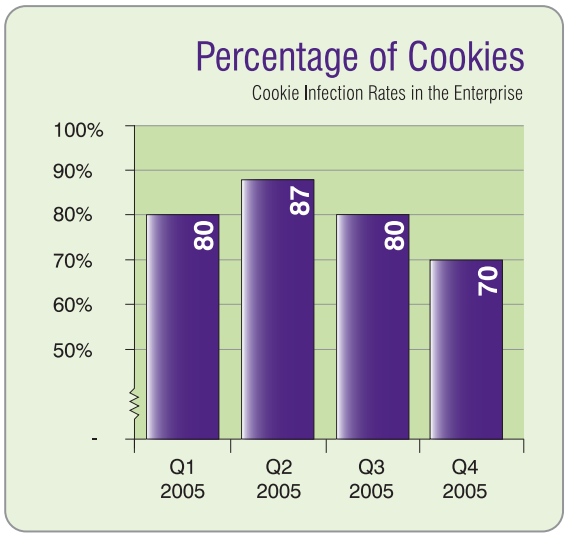
Adware infection rates climbed from 48 percent in Q3 to 51 percent in Q4. Multiple pieces of adware can lead to increased likelihood of system crashes, and other technical issues that can lead to increased number of help desk calls. Removing adware continues to be a pressing issue for enterprises.

Removing adware continues to be a pressing issue for enterprises.



Tracking Cookies

Although tracking cookies tend to not have a large effect on enterprises, it's noteworthy to mention that during the third quarter, cookie infections declined slightly. The infection rate of cookies dropped to 70 percent of infected enterprise PCs in Q4 2005.



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

Webroot Internet Security Survey

As indicated by the results of a recent Internet security survey conducted by Webroot, spyware directly costs businesses time and money.

Almost two-thirds of survey respondents indicated experiencing spyware infection. Of those companies that experienced spyware infections, 54 percent reported that spyware triggered business disruptions that caused loss of revenue.

54 percent reported that **spyware triggered business disruptions that caused loss of revenue.**

Webroot surveyed high-level executives and information technology managers primarily in small and medium-sized businesses to determine the actual cost of spyware to these businesses. The responding companies represent a total of 148,000 enterprise PCs. The respondents came from a wide cross-section of industries, including health care, finance, insurance, education and manufacturing.

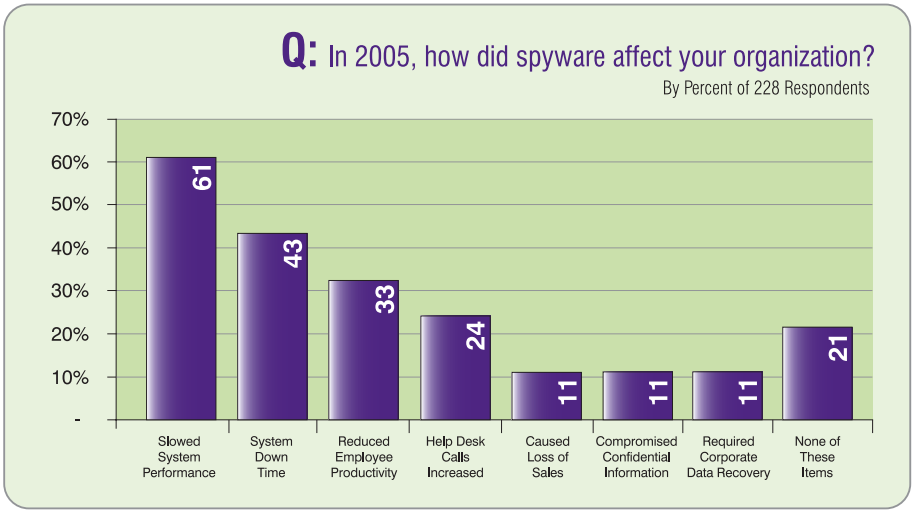
Webroot's survey results mirror the results of a recent FBI survey, which shows that nine out of 10 businesses suffered from a computer virus, spyware or other online attack in 2004 or 2005. Many of the attacks occurred at a time when anti-virus programs were used as a standard security tool.

The repercussions of spyware infections are felt throughout an organization. In 2005, spyware slowed system performance (61 percent of respondents), caused computer down time (43 percent), reduced employee productivity (33 percent), and increased help desk calls (24 percent).

Spyware directly affects the bottom line in some cases. Eleven percent of companies said that spyware caused of loss of sales in 2005.

Spyware directly costs businesses **time and money.**

Spyware endangers the security of confidential information. In 2005, 11 percent of organizations reported that spyware compromised confidential information and required recovery of corporate data. According to one IT director in the finance industry:
"We were pretty much shut down for a week."



Close to two-thirds of the companies surveyed believe that spyware could have a medium to high negative impact on their compliance with information security regulations. Four out of 10 companies also say that spyware could have a medium or high negative impact on revenue and corporate image.

Spyware caused a loss of sales.

SpyAudit Case Study

Legacy security measures at a small health care organization have not effectively protected the company from spyware, according to the results of a Webroot Enterprise SpyAudit. Webroot conducted a SpyAudit for 300 desktop computers at a regional hospice organization. The results concluded that 73 percent of computers were infected with some type of spyware.

The most concerning was the 13 percent infection rate of malicious spyware, such as Trojan horses or system monitors.

For health care organizations with large databases full of confidential patient records including social security numbers and health history, just one desktop with malicious spyware can have major security and compliance implications, even for a smaller organization. Smaller organizations may have the most to lose from a spyware-related data loss, as they don't have shareholders to fall back on or extra money to pay fines.

Audit Results

Health Care Organization Sample Size of 300	Critical		Caution
	Trojans	System Monitors	Adware
Number of Infected Machines	21	18	180
Total Threats Found	13	7	423
Percent of Machines Infected	7%	6%	60%

CONSUMER

Consumer

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

Worldwide Problem

During 2005, nearly 2.4 million scans performed by consumers contributed to the Consumer SpyAudit. That's 200,000 more scans in 2005 than occurred in 2004. Skeptics can no longer claim that spyware is just a passing trend. Due to the increasing awareness about spyware, home computer users are turning to tools like Webroot SpyAudit to assess their infection level.

Despite this high awareness level, more and more home computer users are becoming infected with spyware, particularly with malicious programs such as Trojan horses and system monitors.

While it's difficult to identify just one reason for this increasing spyware infection rate, security analysts point to lowering costs of both personal computers and higher adoption rates of broadband due to lower prices and increased access. As computers become more and more affordable, the rise of multiple computers in each household has increased.

In addition, spyware writers frequently modify their programs to avoid detection. To guard against new spyware programs, home computer users must use an anti-spyware program with frequent definition updates. Unfortunately, users who just install an anti-spyware program, but fail to update definitions and versions, aren't as protected as those who update on a frequent basis.

It's easy to connect the dots. As the number of home computers rises, spyware sources have more users to target.

As the number of home computers rises, **spyware has more users to target.**

Rogue Anti-Spyware

To make matters worse, scam artists are cashing in on this heightened awareness by offering bogus, or "rogue" anti-spyware products. Some of these rogue anti-spyware products are associated with known distributors of spyware and have been known to install spyware themselves.

Other rogue products use deceptive or scare tactics to drive up sales from confused computer users searching for protection from spyware.

The FTC has filed actions against a number of these vendors, such as Seismic Entertainment Productions, creators of Spy Wiper and Spy Deleter, and MaxTheater, creator of Spyware Assassin. Refer to the Legal and Legislative Section for more details about these actions.

Other rogue anti-spyware programs include SpyAxe, Spyware Strikes, SpySheriff, WorldAntiSpy and PSGuard. Each of these programs are known for their illicit installation methods, desktop hijacks and deceptive, aggressive advertising.

Global Infection Rates

Consumers from 107 countries ran scans in Q4 2005. Looking at the 44 countries that performed 500 or more SpyAudit scans, the United States had the highest average number of spies detected: 27 per scanned PC. The Czech Republic had the lowest infection rate at 9.1 spies per PC scanned. The average number of spies per PC scanned for the 44 countries is 15.

Note: Webroot Software began collecting country-specific data, including spyware infection rate per country in Q2 2005.

International - Rates of Spyware Infection

Highest Spyware Infection Rates per Scanned PC by Country

Q4 Rank	Country	Q4 2005	Q3 2005	Q2 2005
1	USA	26.7	24.4	26.7
2	United Kingdom	21.6	18.1	21.8
3	Thailand	21.1	18.7	18.5

Europe

In recent years, the digital divide in Europe has become considerably smaller as the IT infrastructure has grown to provide improved Internet accessibility for more citizens. In addition, European telecommunications regulators have recommended drastically cutting telephone prices to encourage Internet use through dial-up Internet connections.

As a result, more people are online in Europe these days than ever before. In fact, Internet usage statistics indicate a 171 percent growth in use for all of Europe between 2000 and 2005. The average number of spies per PC scanned for the European countries is 15.1.

Compared with Q3 2005, United Kingdom still records the highest number of spies per PC in Europe. Norway replaces Spain for the second place. France is no longer on the list either, replaced by Sweden.

The average number of spies per PC scanned for the 44 countries is 15.

Europe - Rates of Spyware Infection

Highest Spyware Infection Rates per Scanned PC in Europe

Q4 Rank	Country	Q4 2005	Q3 2005	Q2 2005
1	United Kingdom	21.6	18.1	21.8
2	Norway	20.3	14.8	16.5
3	Sweden	19.1	14.2	17.3

Asia

Within Asia, consumer PCs in Thailand continue to have the highest average number of spies: 21. Overall Internet usage in Thailand has grown more than 266 percent between 2000 and 2005, which may contribute to this high infection rate.

In the three Asian countries tracked, the average number of spies per PC increased for all between the third and fourth quarters of 2005.

The Asian region accounts for about 25 percent of the world's Internet users. This relatively low degree of Internet penetration, however, is changing very rapidly as the Internet grows quickly in such large populated countries as China.

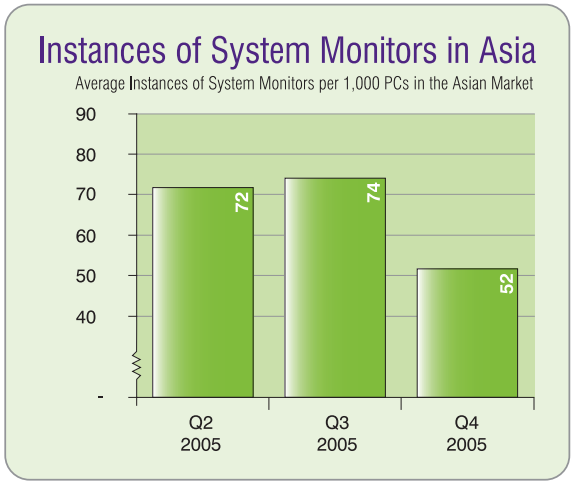
Penetration of Internet use and its stabilization in the Asian market are the result of Internet user promotion by various government initiatives such as expanding broadband infrastructure and increasing accessibility to Internet-enabled devices.

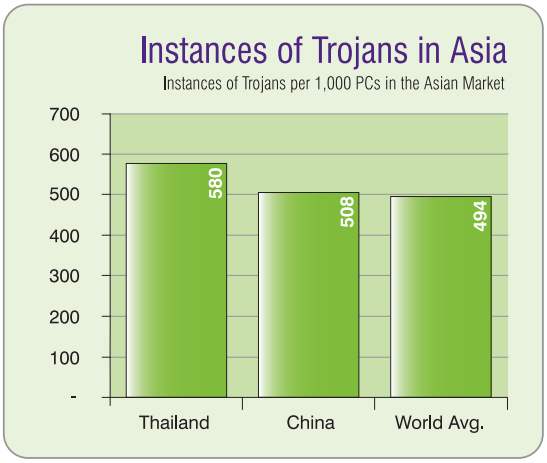
Asia - Rates of Spyware Infection

Highest Spyware Infection Rates per Scanned PC in Asia

Q4 Rank	Country	Q4 2005	Q3 2005	Q2 2005
1	Thailand	21.1	18.7	18.5
2	Hong Kong	16.6	14.8	13.0
3	China	13.6	14.8	15.4

Compared with world averages, consumer PCs in Thailand and China have higher rates of malicious spyware.





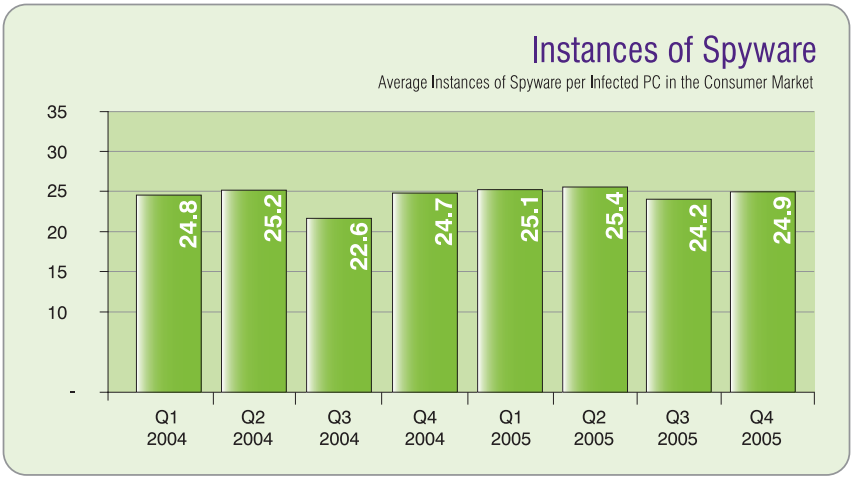
2005 Overall Findings

Webroot performed spyware scans on 2,163,838 consumer PCs in 2004 and 2,356,932 in 2005. The spyware scan results showed that the percentage of infected consumer PCs remained elevated at more than 81 percent.

Although only a slight decrease from 91 percent in 2004, this improved trend is a positive sign that consumers are taking steps to protect their PCs from spyware.

New legislation in more than 10 states criminalizes the download and installation of spyware, which may contribute to the slight reduction in infection rate. Other contributing factors include greater consumer awareness about spyware, which is tied directly to a higher penetration of multiple anti-spyware solutions on consumers' desktops.

Additionally, commercial adware vendors are modifying their behavior in preparation for federal legislation. These modifications include understandable EULAs, simple un-install features and attribution of pop-up ads. These changes may also contribute to the loss of penetration.



The percentage of infected consumer PCs **remained elevated at 81 percent.**

In 2005, the Consumer SpyAudit found that the infected consumer PCs have an average of 25 instances of spyware. This is a slight increase of 2 percent from an average of 24.4 instances of spyware in 2004.

While overall infection rate reduced slightly between 2004 and 2005, the average number instances of spyware per machine increased. This juxtaposition may indicate that consumers infected with spyware are suffering more harm than ever before.

It's important to note that in Q4 2005, almost 18 percent of spyware instances are more pernicious forms of spyware such as adware, Trojans and system monitors. In Q3 2005, these destructive forms of spyware accounted for just 14 percent.

Malicious Spyware

Throughout 2005, malicious spyware, such as system monitors and Trojan horses, threatened the security of consumers' privacy while negatively affecting e-commerce. Computer and Internet use increased along with concerns about identity theft and other online threats.

Unfortunately, malicious spyware infection rates from the Consumer Spy Audit results are unable to offer any comfort. In 2005, Trojan horses increased dramatically to 21 percent, up from 15 percent in 2004.

Consumers infected with spyware **suffer more harm than ever before.**

Trojan horses are particularly harmful because they may install a program that allows a malicious user to take control of the infected machine. Trojans can run in the background, hiding their presence from the computer user.

During Q4 2005 alone, Webroot SpyAudit results revealed that Trojans are present on 24 percent of infected machines, an increase of three percentage points from Q3 2005. System monitors also fall under the umbrella of malicious spyware. Webroot SpyAudit results indicate an overall decline from 17 percent in 2004 to 7 percent in 2005. However, during the last two quarters of 2005, infection rate held steady at 5 percent.

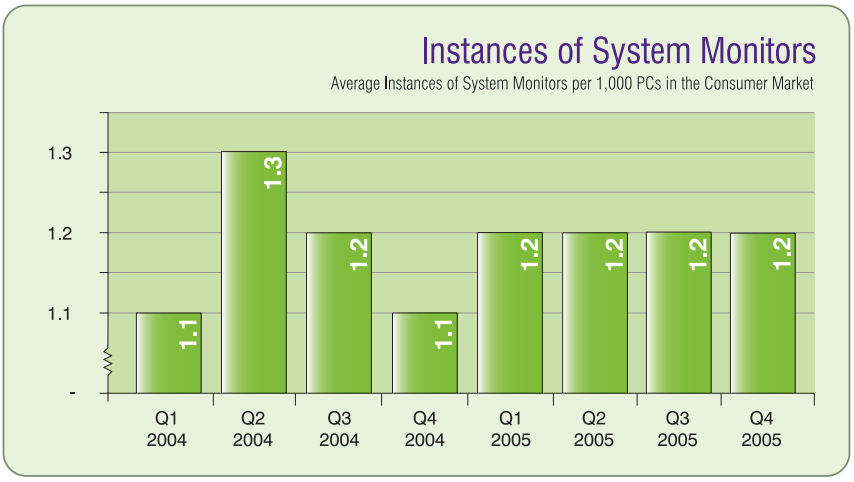
Moreover, the average number of instances of malicious spyware remained relatively unchanged between Q3 and Q4 2005, averaging 1.2 system monitors on computers infected with system monitors.

In Q4, there is an average of 1.9 Trojans on computers infected with Trojans, up from 1.7 in Q3. This stable infection rate for the last two quarters of 2005 is in line with annual infection averages as well. In 2005, the average number of instances of Trojans was 1.7, a slight increase from 1.5 in 2004. Systems monitors remained unchanged at 1.2 instances in both 2004 and 2005.

System Monitors

System monitors continue to increase in sophistication and prevalence. Frequently, they are deployed by online thieves to steal personal information such as bank account information or credit card numbers.

During Q4 2005, on PCs with system monitors, the average number of instances held steady at 1.2 system monitors. Because of the growing sophistication, industry analysts believe online criminals are modifying system monitors to keep them hidden and undetected.



In the fourth quarter of 2005, the incidence of system monitors in Saudi Arabia and Israel was triple the world average. In Q3 2005, Taiwan recorded the highest world average of incidence of system monitors.

Rates of System Monitors

Highest Number of System Monitors per 1,000 PCs Scanned by Country
** fewer than 500 scans*

Q4 Rank	Country	Q4 2005	Q3 2005	Q2 2005
1	Saudi Arabia	144	67	133
2	Israel	134	123	152
3	Egypt	128	94*	281*

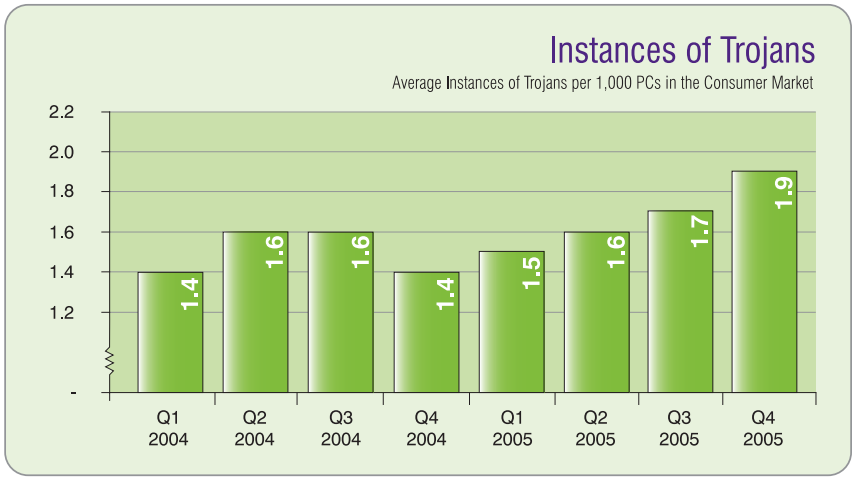
Trojan Horses

In Q4 2005, Trojan horses increased on consumer PCs. Security analysts link this spike in Trojan attacks to the Microsoft Windows Meta File (WMF) vulnerability, which threatened the security of nearly every PC user.

Hackers created a range of Trojans to exploit the WMF vulnerability. This vulnerability was particularly dangerous because even simple activities such as viewing a Web page or reading an e-mail were no longer safe. If the Web page or e-mail message contained an infected image, the user's computer would be infected, most likely with a malicious Trojan designed to download other spyware programs. Before this vulnerability was patched in early January 2006, Webroot spyware scans recorded a three-fold increase in Trojan horse infections.

Refer to the News and Incidents section to read more about the WMF vulnerability.

The Microsoft WMF vulnerability **threatened nearly every PC user.**



For every 1,000 PCs scanned by SpyAudit worldwide, 494 are infected with a Trojan horse. Trojan horses are much more prevalent on PCs in Poland, Sweden and Colombia. Trojans in Poland doubled from 426 per 1,000 PCs scanned in Q3 to 863 in Q4. In Q3 2005, Turkey recorded the highest world average of incidence of Trojan horses.

Rates of Trojan Horses

Highest Number of Trojans per 1,000 PCs Scanned by Country

** fewer than 500 scans*

Q4 Rank	Country	Q4 2005	Q3 2005	Q2 2005
1	Poland	863	426	438
2	Sweden	791	252	391
3	Colombia	743	459*	496*

Adware

SpyAudits conducted in Q4 2005 found an average of 6.1 instances of adware on infected PCs. Almost two-third of infected consumer PCs (63 percent) have adware. During 2005, the average instances of adware on infected PCs is 6.4, a slight decline from 6.7 in 2004.

Two-thirds of infected PCs **have adware.**

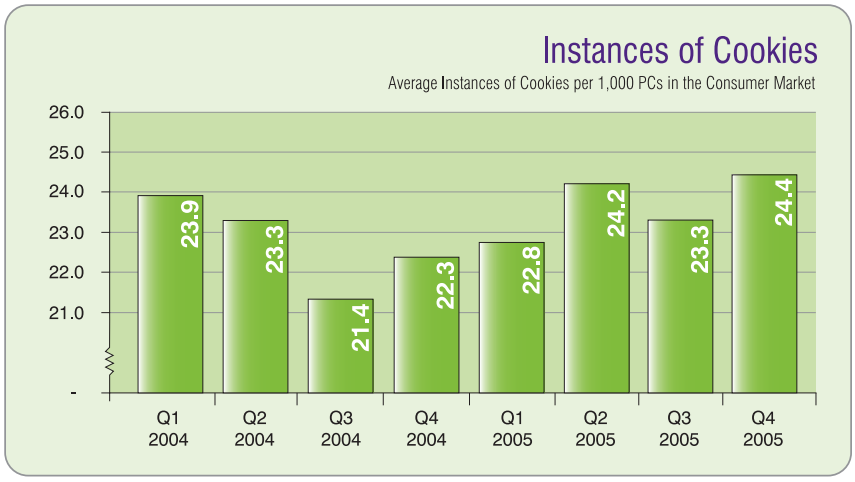
Despite the high number of consumers using an anti-spyware program, a relatively stable number of computer users remain bothered by adware. Industry analysts believe that some substandard anti-spyware programs are unable to completely remove all adware programs from an infected PC.

Tracking Cookies

During 2005, industry analysts continued to debate counting cookies as part of spyware scans. Online marketers argue that cookies help measure consumer behavior. Privacy advocates, on the other hand, remain skeptical of the monitoring of online behavior. Until the debate is resolved, Webroot will continue to count cookies during a scan.

In Q4 2005, eight in 10 (84 percent) infected consumer PCs have tracking cookies. SpyAudit found an average of 24 cookies on consumer PCs infected with cookies in the fourth quarter of 2005.

During 2005, the average instances of cookies per infected PC increased to 23.5, up from 22.6 in 2004.



Spyware can seriously damage a PC.

Quantitative Analysis of the Effects of Spyware on a PC

A large portion of home computer users understand the major privacy and online security risks associated with spyware – the possibility of identity theft and the loss of personal information like credit card or bank account information. But if spyware takes hold of a PC, it can seriously damage the performance of a PC, rendering it practically useless for the user. To demonstrate the pain a home computer user feels when their PC is infected with spyware, Webroot conducted a series of tests in our research laboratory.

Test #1: File-sharing Downfalls

Webroot researchers downloaded a very common peer-to-peer program, frequently used to share music files. Following the program installation, researchers tested a variety of activities in an attempt to measure pain points for an average home computer user. Items measured include:

- Number of times a computer freezes or crashes during a period of two hours online
- Number of pop-up ads delivered during a period of two hours online
- How quickly a browser or search is hijacked by spyware
- Number of items added to Start menu and desktop
- Number of toolbars added to browser
- Amount of CPU usage

At the conclusion of the test, researchers used Webroot's spyware scan to assess the infection level on the test computer. The results were frightening – the infection level ranked dangerous on the spyware scan tool scale. Even worse, in less than the two hours it took to conduct the test, two Trojan horses, 34 adware programs and eight cookies had installed on the machine. The spyware scan identified one of the Trojan horses as "2nd-thought," a treacherous program that may open a computer to hackers trying to gain remote control of the computer.

Test Result Details:

- Within 38 seconds of program installation, pop-up ads began appearing on the screen.
- CPU usage measured 95 percent just 54 seconds after the program was installed, bringing the system to a crawl as adware programs bundled with the downloaded music program began to install and run.
- Within six minutes, more than 25 illegitimate processes were running – using up more than 138 megabytes of memory.
- After 30 minutes, the infected computer was unable to open Internet Explorer. The high number of illegitimate processes as well as the number of spyware programs running caused the computer to freeze. A manual restart was required by the testers.

- Restart triggered three application errors and one system error notification.
- Following the restart, Webroot researchers noted additional icons had been added to the Start menu and desktop. In addition, an unwanted toolbar was added to Internet Explorer.
- Even more alarming, the Internet search had been hijacked with the results appearing in a format that mimicked msn.com. Once the researchers attempted to browse the Internet, the computer froze again, requiring another manual restart. CPU usage remained above 75 percent.
- After repeatedly restarting the computer, researchers declared the machine too damaged to continue with the tests.

The Internet search had been hijacked.

Test #2: Emoticons – how can something so cute cause so much damage?
Meanwhile on a separate PC, Webroot researchers conducted another series of tests to measure how likely a home computer user can pick up troublesome adware programs while surfing the Internet.

After performing searches on a mainstream search Web site, Webroot researchers clicked on a banner ad for free emoticons which initiated a download. Emoticons, also called smileys, are little facial expressions used commonly in e-mail or on instant messaging to represent a human expression. The researchers tested the same activities listed previously.

At the conclusion of the test, the researchers used Webroot's spyware scan to measure any possible spyware infection. The results were surprising. In less than two hours, 13 adware programs and six cookies installed on the PC.

Webroot researchers believe that one of the programs, Hotbar, was initially installed with the free emoticons. Hotbar may collect detailed information about the Web pages you view and the data you enter into online forms (such as your name, e-mail address, telephone number and home address).

Test Result Details:

- Immediately after the download completed, a dynamic toolbar was added to Internet Explorer. The toolbar's contents changed to match the contents of the page.
- Less than a minute after clicking the emoticon ad, additional pop-up ads for a variety of sweepstakes began to appear. The sweepstakes ads collected detailed personal information such as Social Security number and mother's maiden name.
- After 10 minutes, two additional toolbars, including a vertical toolbar, were also added to Internet Explorer.
- After 30 minutes, three icons were added to the desktop and two were added to the Start menu.
- Following a restart of the computer, a weather service icon was added to the notification area on the task bar.
- Eleven illegitimate processes were running at the conclusion of the test. These processes consumed 43 megabytes of memory.
- CPU usage was steady at just over 25 percent throughout the test. This level of usage slowed performance, but the computer was still usable.

Eleven illegitimate processes were running at the conclusion of the test.

Conclusion

Both tests indicate that the substantial impact of spyware on a PC is not acceptable for consumers trying to quickly browse for needed information such as movie tickets or directions to a restaurant.

Privacy remains an important issue for online computer users, but performance continues to sting as well and can hit home computer users in the pocketbook – whether it's in repair costs, system degradation or bandwidth consumption.

Given these dangers, it is essential that home computer users protect themselves with a reputable anti-spyware solution that offers frequent definition updates. For a true sense of security, home computer users need to pick up the habit of checking for updates often.

LEGAL
& Legislation

Legal Actions

FTC Actions

Following the passage of several state spyware and identity theft bills, several states brought legal action against alleged spyware purveyors. In addition, the Federal Trade Commission also filed actions.

After filing its first spyware case against an alleged spyware operator in October 2004, the FTC stepped up its enforcement activity in 2005 by filing several actions against purported purveyors of spyware and bogus anti-spyware software, as well as actions against companies that, according to the FTC, failed to adequately protect customer data.

FTC v. Seismic Entertainment Productions

FTC File No. 042 3125 – Pending

In October 2004, the FTC filed its inaugural enforcement effort against an alleged spyware purveyor. The defendants included Seismic Entertainment Productions and SmartBot.net, which, according to the FTC, operated Web sites that distributed spyware and bogus anti-spyware software.

The FTC requested that the court shut down the alleged spyware operations.

In its complaint, the FTC requested that the court shut down the defendants' alleged spyware operations, which allegedly exploited a vulnerability in Microsoft's Internet Explorer browser to hijack computers, secretly change computer settings, bombard consumers with pop-up ads and install adware and other software programs that monitored consumers' Web surfing, often causing computers to malfunction.

The FTC complaint identified specific deceptive marketing activities in which the defendants engaged, including allegedly installing spyware on consumers' computers and then offering to sell consumers the defendants' Spy Wiper and Spy Deleter software that purportedly removed spyware from the users' computers.

Shortly after the action was filed, the court granted the FTC's request for a temporary restraining order. The court ruled that the defendants must refrain from exploiting Internet security vulnerabilities and gave the defendants 24 hours to remove from any Web site, bulletin board or Internet server script that exploits those vulnerabilities to install, download or deposit software onto a computer without a user's knowledge. The litigation is proceeding and trial is currently set for March 2006.

FTC v. MaxTheater, Inc. et al.

FTC File No. 042 3213 – Settlement Announced January 5, 2006

In March 2005, the FTC filed an action against MaxTheater, claiming that to market its non-functional anti-spyware software, Spyware Assassin, MaxTheater offered free spyware "scans" that detected spyware even when there was no spyware on a consumer's computer.

The free "scans" detected spyware even when there was no spyware on the PC.

MaxTheater used Web sites, e-mail, banner ads and pop-up ads to drive consumers to the Spyware Assassin Web site. After exposing consumers to the variety of dire consequences resulting from spyware installation, the Spyware Assassin Web site offered to scan consumers' computers at no cost to determine the extent of spyware infection. According to the FTC, the "scan" always resulted in notification of spyware detection, even on computers where there was no spyware installed. Although the scan was free, consumers were asked to purchase software that would remove all "spyware" – software that the FTC claims failed to remove any spyware.

The settlement, announced on January 5, 2006 in tandem with the Trustsoft settlement, requires the defendants to pay $76,000, which was the full amount of consumer injury, and bars defendants from future sales or marketing of any anti-spyware product or service. It further prohibits defendants from downloading or installing spyware on consumers' computers, from assisting others in downloading or installing spyware, and from making future misrepresentations in connection with the sale or marketing of any good or service. The settlement provides for certain record-keeping and reporting provisions that allow the FTC to monitor compliance.

FTC v. Trustsoft, Inc. et al.

FTC File No. 052 3059 – Settlement Announced January 5, 2006

In May 2005, the FTC filed an action against Trustsoft claiming that Trustsoft used deceptive marketing practices, such as bogus "scans" and illegal spam, to market its anti-spyware program, SpyKiller. According to the FTC, Trustsoft sent pop-up and e-mail messages informing consumers that their computers had been "scanned" and that spyware had been "detected" even though Trustsoft had not actually performed any scans. After a consumer accessed the SpyKiller Web site to get a "free" computer scan, the program displayed a status report that the FTC claimed deceptively identified anti-virus programs, word processing programs, and processes running on the consumer's computer system as spyware. Although the scan itself was free, consumers had to pay a fee to enable SpyKiller's "removal" capabilities, which, according to the FTC, failed to remove significant amounts of spyware.

The settlement, announced on January 5, 2006 in tandem with the MaxTheater settlement, requires the defendants to pay $13.5 million (of which approximately $12 million was suspended) – the total amount of consumer injury that the FTC claimed the defendants caused. The settlement also prohibits the making of deceptive claims in the sale, marketing, advertising or promotion of any goods or services, and prohibits the specific misrepresentations used in promoting SpyKiller. Further, defendants are prohibited from delivering ads using the spyware that their "anti-spyware software" supposedly detected and destroyed. The settlement provides for certain record-keeping and reporting provisions that allow the FTC to monitor compliance.

Instead of uninstalling the software, the tool triggered additional installations.

FTC vs. Odysseus Marketing, Inc. et al.

FTC File No. 042 3205 – Pending

In October 2005, the FTC filed an action against alleged spyware operator Odysseus Marketing. In its complaint, the FTC requested that the court halt the unfair and deceptive operations of Odysseus Marketing, Inc. and its founder, Walter Rines. Odysseus offered a freely downloadable software product that Odysseus claimed would allow users to engage in peer-to-peer file sharing anonymously. The FTC alleged, however, that Odysseus' software did not allow for anonymous file sharing because the

peer-to-peer software is bundled with spyware, called "Clientman," that installed on users' computers without their consent. Clientman, according to the FTC, secretly downloaded dozens of other software programs, generated pop-up ads that degraded computer performance and consumed memory and corrupted users' search results.

The FTC claimed that Odysseus deliberately made its software difficult to detect and impossible to remove using standard software utilities. Although Odysseus offered its own "uninstall" tool, the FTC alleged that, instead of uninstalling the software, the tool triggered additional installations of unwanted software that also captured and transmitted information from the users' computers to servers controlled by Odysseus. Lastly, the FTC argued that Odysseus has an obligation to disclose that its "free" software download is not without cost given that it causes spyware to be installed on users' computers. According to the FTC, the consequences of downloading Odysseus' free software are disclosed only in the middle of a two-page end user license agreement buried in the "Terms and Conditions" section of their Web site.

FTC v. Enternet Media Inc. et al.
FTC File No. 052 3135 – Pending
The FTC rounded out 2005 by filing a complaint in October against several defendants including Enternet Media Inc., the company that distributes EliteBar.

The complaint alleged that defendants' Web sites caused "installation boxes" offering "freeware" and "security updates" to pop-up on consumers' computer screens. The FTC claimed that consumers who elected to install the downloads on their computers did not receive what they were promised – instead, the consumers' computers were infected with spyware. According to the FTC, the defendants' software tracked consumers' Internet traffic, changed consumers' preferred home page settings, inserted new toolbars onto consumers' Internet browsers, inserted a window on consumers' Internet browsers that displayed ads, and displayed pop-up ads on consumers' computers, even when the Internet browsers are not active. Further, the FTC claimed that once the software was installed on consumers' computers, it interfered with computer function and was difficult for consumers to uninstall or remove.

Shortly after the FTC filed the action, the court ordered the defendants and an affiliate of the defendants to halt their downloads and froze the defendants' assets pending a further hearing. The FTC seeks to enjoin this activity permanently and force the defendants to surrender their profits.

Negligence

In addition to the cases that specifically dealt with reportedly deceptive practices tied to the distribution of spyware, the FTC also brought enforcement actions against companies believed to be negligent in protecting their customers' data from security threats. In 2005, settlements were reached in four such cases.

The FTC brought actions against companies believed to be negligent.

In the Matter of Vision I Properties, LLC, d/b/a CartManager Int'l
FTC File No. 042 3068 – Settlement Announced March 10, 2005

Vision I Properties d/b/a CartManager International, an Internet company that provides shopping cart software to online merchants, agreed to settle FTC charges that it rented personal information about merchants' customers to marketers while knowing that such disclosure contradicted the merchants' privacy policies. The settlement bars use of the personal data the company has already collected, as well as future misrepresentations about the collection, use, or disclosure of personally identifiable information, and requires the company to ensure that consumers receive a clear and conspicuous notice before their personal information is disclosed to other companies for marketing purposes. The settlement also requires that the company give up the $9,101.63 it made from selling the consumer information and includes several record-keeping provisions designed to allow the FTC to monitor CartManager's compliance.

In the Matter of BJ's Wholesale Club, Inc.
FTC File No. 042 3160 – Settlement Announced June 16, 2005

BJ's Wholesale Club, Inc. agreed to settle FTC 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, BJ's collects information from credit and debit cards, such as name, card number and

expiration date, and transmits that information on its computer network to obtain bank authorization. The FTC charged that BJ's engaged in several practices that did not provide reasonable security for this sensitive information, including BJ's failure to encrypt consumer information in transmission or storage, storage of the information for up to 30 days in violation of bank security rules, storage of information in files that could be accessed using commonly known default user IDs and passwords, and failure to use readily available security measures to prevent unauthorized access to its networks. The FTC claimed that unauthorized persons exploited these practices and used counterfeit copies of the cards containing the consumer information to make millions of dollars of fraudulent purchases.

The settlement requires BJ's to implement a comprehensive information security program that includes administrative, technical and physical safeguards, and also requires BJ's to obtain audits by an independent third-party security professional every other year for 20 years. Several banks and credit unions have also filed lawsuits against BJ's and pursued bank procedures seeking the return of millions of dollars in fraudulent purchases and operating expenses. The bank actions are pending.

In the Matter of Superior Mortgage Corp.
FTC File No. 052 3136 – Settlement Announced September 28, 2005
The FTC filed an action against Superior Mortgage Corp., a lender with 40 branch offices in 10 states and multiple Web sites, for its alleged violation of the FTC's Safeguards Rule, which requires financial institutions to implement reasonable policies and procedures to ensure the security and confidentiality of sensitive customer information.

The FTC claimed that several of Superior's practices violated the Safeguards Rule, including its failure to implement appropriate password policies to limit access to company systems and documents containing sensitive customer information, failure to encrypt or otherwise protect sensitive customer information before sending it by e-mail and failure to fully encrypt sensitive personal information collected at its Web site.

The settlement bars Superior from misrepresenting the extent to which it maintains and protects the privacy, confidentiality or security of any personal information collected from or about consumers and prohibits violations of the Safeguards Rule. The settlement also contains a periodic auditing provision that requires Superior to engage an independent third-party auditor to assess its security procedures every two years for the next 10 years and certify that these procedures meet or exceed the protections required by the Safeguards Rule. To enable the FTC to monitor compliance with the settlement agreement, Superior must abide by certain record-keeping requirements.

In the Matter of DSW, Inc.

FTC File No. 052 3096 – Settlement Announced December 1, 2005

The FTC's complaint alleged that DSW's data security failure allowed hackers to gain access to the sensitive credit card, debit card and checking account information of more than 1.4 million customers. According to the FTC, DSW collects credit, debit and checking account information and transmits the information via computer networks to obtain authorization. The FTC charged that DSW engaged in a number of practices that failed to provide reasonable and appropriate security for sensitive customer information, including DSW's storage of information in multiple files when it no longer had a business need to keep the information, failure to use readily available security measures to limit access to its computer networks, storage of information in unencrypted files that could be easily accessed using a commonly known user ID and password, and failure to employ sufficient measures to detect unauthorized access. The FTC charged that, because of these practices, approximately 1.4 million credit and debit cards and 96,000 checking accounts were compromised.

The FTC charged that DSW failed to provide reasonable security for its customers.

The settlement requires DSW to implement a comprehensive information-security program that includes administrative, technical and physical safeguards. The settlement also contains a periodic auditing provision that requires DSW to engage a qualified, independent, third-party professional every two years for the next 20 years to assure that its security program meets the standards of the order. To enable the FTC to monitor compliance with the settlement agreement, DSW must abide by certain record-keeping and reporting requirements.

In the Matter of Integrated Search Technologies et al.

Pending

In November 2005, the U.S. Center for Democracy & Technology (CDT) and the Canadian Internet Policy and Public Interest Clinic (CIPPIC) tried a novel approach to enforcement actions against alleged spyware purveyors. The CDT and the CIPPIC filed joint complaints requesting investigations and cooperation between United States and Canadian regulatory authorities. The complaints asked the FTC and its Canadian equivalent, the Canadian Competition Bureau, to investigate the business practices of Montreal-based software distributor Integrated Search Technologies (IST) and several of its business partners. The CDT and CIPPIC alleged that IST engaged in a widespread campaign of installing unwanted software on consumers' computers and did so using unfair and deceptive practices, including enticing Internet users into downloading software they did not ask to receive and downloading software without notice to or consent from consumers.

State Actions

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

Settlement Announced October 20, 2005

As part of a consent agreement and settlement with the Attorney General's office, Intermix Media, a leading Internet marketing company accused of secretly installing adware and spyware on millions of home computers, agreed to pay $7.5 million in penalties and accepted a ban on its future distribution of adware programs.

Intermix Media agreed to pay $7.5 million in penalties.

In addition, Brad Greenspan, the founder and former CEO of Intermix, agreed to pay $750,000 in penalties. The consent agreement describes how Greenspan directed Intermix's employees to bundle adware programs with other free software programs to avoid informing consumers of the adware's existence and to make the adware difficult to uninstall.

Intermix affiliate Acez Software also resolved an investigation by the Attorney General's office of its bundling of Intermix adware with free Acez screensavers without providing notice to consumers. Acez agreed to pay $35,000 in penalties and to adhere to fair notice and disclosure standards in the future.

United States v. Ancheta

Case No. 2:05-CR-01060 (C.D. Cal. Nov. 2, 2005) (Los Angeles) – Pending

On November 2, 2005, police in California arrested Jeanson Ancheta, 20, for taking control of approximately 400,000 computers through pop-up adware and renting computer time on the commandeered computers to other hackers. Ancheta faces a 17-count federal indictment, which includes allegations that he accessed a protected computer to commit fraud, attempted transmission of code to a protected computer and transmission of code to a government computer located at the Weapons Division of the U.S. Naval Air Warfare Center in China Lake, California. Federal prosecutors allege Ancheta was an affiliate of several different advertising service companies, which paid him commissions based on how many computers he infected with the alleged adware.

SONY BMG

In 2005, Sony BMG introduced CDs containing its "copy-protection" software. If the owners of these CDs want to play or copy a CD on a computer, the user must first install software intended to restrict the number and kind of copies the computer can make. In November 2005, computer security professionals discovered that the copy-protection software reportedly creates serious security risks. The feature of the software creating the most serious security risk was the "rootkit." A rootkit permits software to render itself invisible to a computer's operating system, anti-virus programs and anti-spyware software, cloaking itself from discovery by the computer user. The Sony BMG rootkit posed a serious security risk because, once installed on a computer, third parties could use it to hide their own malicious software.

Amid consumer and community outcry, Sony BMG released several patches designed to uninstall the software and remedy the security risks it created. However, despite these efforts, consumers filed several class action lawsuits in various courts across the country and one state, Texas, filed an action against Sony BMG.

Consumer Class Actions

The numerous consumer class action lawsuits filed against Sony BMG contained several claims. One set of claims relied on federal statutes forbidding consumer intrusion, such as the federal Computer Fraud and Abuse Act (CFAA), which forbids accessing a computer without, or in excess of, the authority of the owner of the computer. Private civil litigants are entitled to bring suit where the prohibited computer intrusion causes losses exceeding $5,000, threatens public health or safety, or damages a computer system used by government entities for judicial, national security or defense functions. Several plaintiffs invoked similar state laws.

Recently enacted state laws aimed at spyware and adware provided another basis for legal claims against Sony BMG. Class action lawsuits in California, for example, alleged violations of the state Consumer Protection Against Spyware Act, which prohibits deceptively taking control of a user's computer, modifying computer settings, or preventing users from uninstalling software.

The Sony BMG rootkit posed a serious security risk.

Some of the complaints included common law trespass to chattels claims, alleging that Sony BMG's software constitutes unauthorized interference with the property interests of computer owners, resulting in damage to their computers. Many of the complaints also alleged that Sony BMG's conduct amounts to an unfair or deceptive trade practice, fraud or false advertising under applicable state statutes.

At the end of December 2005, Sony BMG agreed to settle several of the class action lawsuits, which will end many of the cases filed by consumers against Sony. The settlement requires Sony BMG to stop making CDs with the copy-protection software, recall the CDs containing the software, ensure that fixes are readily available, provide updates to help consumers uninstall the software, and provide free music downloads and replacement CDs without the copy-protection software.

State Actions

Texas was the first state to bring an action against Sony BMG, alleging that Sony BMG's conduct violates the state Consumer Protection Against Computer Spyware Act, which prohibits manipulating software in order to prevent the computer user from detecting, locating and removing the software, and also prohibits intentionally misrepresenting that the installation of the software is necessary for security or privacy reasons.
The class action settlement will not affect the Texas action.

No other state regulatory actions have been filed, however, other states are reportedly reviewing the case.

Consumer Class Actions

In 2005, several computer users took matters into their own hands, filing class action lawsuits against companies that allegedly deceptively promote spyware. Given the relative novelty of this approach, the industry is watching these suits closely to see whether they open the floodgates of litigation.

Sony agreed to settle several of its class action lawsuits.

Sotelo v. DirectRevenue LLC
No. 05 C 2562 (N.D. Ill. Aug. 29, 2005) (Chicago) – Pending

At the end of August 2005, Stephen Sotelo brought a class action lawsuit against a group of defendants, including DirectRevenue LLC. Filed in federal court in northern Illinois, the complaint included, among other allegations, trespass to personal property, fraud, negligence and computer tampering.

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

The defendants filed a motion to dismiss the case on several grounds, but the court issued a ruling in September allowing the case to proceed. The court refused to enforce an arbitration clause contained in the end-user license agreement (EULA) because there was a factual dispute between the parties over whether users consent to the license agreement prior to installation of the software. The court also refused to dismiss the claim of trespass to personal property, which requires that the plaintiffs' personal property be lost or damaged, because the court deemed the plaintiffs' demonstration that the software caused "interference" with a users' computer to be sufficient to maintain the claim.

Simios v. 180Solutions, Inc.
No. 05 C 5235 (N.D. Ill. Sept. 13, 2005) (Chicago) – Pending
In September 2005, Logan Simios brought a class action lawsuit against a group of defendants, including 180Solutions.

Computer users took matters into their own hands.

In language similar to that used in the Sotelo v. DirectRevenue lawsuit, the plaintiffs claimed that the defendants deceptively caused spyware to be installed on the plaintiffs' computers by installing the software without users' consent, by bundling spyware with legitimate software available for free download over the Internet, or by bundling their software with other spyware, including software distributed by DirectRevenue.

The plaintiffs alleged that the software tracked the plaintiffs' browsing habits, sent intrusive pop-up ads, compromised computer performance by consuming bandwidth and memory, and was difficult to remove.

Michaeli v. eXact Advertising, LLC
No. 05 CV 8331 (S.D.N.Y. Sept. 27, 2005) (New York) – Pending
The third suit in a flurry of class action activity in late 2005, Yehuda Michaeli filed this class action lawsuit against eXact Advertising, LLC. The plaintiffs' complaint included claims similar to the other two previously discussed class actions, including trespass to chattels, deceptive consumer acts under state law, false advertising under New York state law, common law negligence and unjust enrichment.

The plaintiffs alleged that eXact infected their computers with spyware by deceptively bundling the software with a variety of free games, cursors, screensavers and other small software programs. Once installed, the plaintiffs claimed that the programs secretly tracked their Internet use and bombarded their computers with adware, which caused the computer to slow down, consume excessive bandwidth, monopolize computer resources, and disable or destroy user-installed computer software.

Legislative Actions

State Actions

By the end of 2005, twelve U.S. states have passed spyware laws – eleven of which are already in effect, and one, Nevada, will go into effect January 1, 2007. Enforcement of these new laws in Alaska, Arizona, Arkansas, California, Georgia, Iowa, New Hampshire, Texas, Utah, Virginia and Washington, over the coming months and years will be an indication of their effectiveness.

As the state legislatures reconvene for the 2006 session, it is likely that additional states will consider spyware bills over the coming months.

It's likely that additional states will consider spyware bills.

Congressional Actions

The U.S. House of Representatives completed their actions on spyware legislation with the passage of the SPY Act (H.R. 29) and the I-SPY Act (H.R. 744) on May 23, 2005. The U.S. Senate Committee on Commerce, Transportation and Science worked on spyware legislation throughout the year, passing two bills by the end of 2005.

The Senate Committee actions included two hearings. The first was held on May 11, 2005. Three witnesses testified in May: David Moll, Webroot CEO; Trevor Hughes, Executive Director, Network Advertising Initiative; and, Ari Schwartz, Associate Director, Center for Democracy and Technology. The Committee held a second hearing on October 5, 2005 at which the only witness was Deborah Majoras, Chairwoman of the Federal Trade Commission.

The SPY BLOCK bill (S. 687), sponsored by Senator Conrad Burns (R-MT) was approved by the Senate Commerce committee on November 17, 2005. The U.S. SAFE WEB Act (S. 1608) sponsored by Sen. Gordon Smith (R-OR) passed the committee December 15, 2005.

These bills are now pending Senate floor action in 2006.

A company's consent agreement with the FTC is for settlement purposes only and does not constitute an admission of guilt.

CONCLUSION

With the accelerating threat in the spyware space, what does 2006 hold for those attempting to defend their systems from this scourge?

Spyware continues to grow more complex and more harmful. As a result, corporations are overhauling their security plans to protect their desktops from these malicious while maintaining compliance with HIPAA, Gramm-Leach-Bliley and the FTC.

While Congress is getting closer to passing an anti-spyware bill, it is unlikely to have any conclusive impact on the prevalence of spyware in 2006, due to slow implementation and enforcement of new laws.

Spyware writers are taking note of the pending legislation and are routinely routing their malicious programs through other countries like China or Romania where prosecution is difficult. By using advanced encryption techniques along with rootkit technology, the more malicious forms of unwanted software will continue to proliferate.

As the Internet grows beyond a billion users, there are more and more targets for criminals to attack in an attempt to garner revenue through adware click-throughs. More malicious programs are targeting this expanded user group to steal credit card and bank information.

During 2005, consumers and enterprises became more aware of spyware and its growing impact and many users adopted anti-spyware programs as part of their online arsenal of tools. However, the next step is to ensure that the protection they have adopted is indeed solving their problem, and that they continue to keep their protection software up to date at all times.

It is not hard to predict that there will continue to be day zero attacks against Windows, such as the WMF vulnerability, that cannot be blocked by legacy anti-virus products. Hackers will continue to target new products introduced by Microsoft, such as Windows Vista, new versions of Internet Explorer or Microsoft's pending anti-spyware program.

As the State of Spyware Report for 2005 documents, the overall threat of online security is rising dramatically as spyware continues target more and more users.

APPENDIX

Federal Legislation

Bill Title & Number	Primary Supporters	Summary	Status as of 12.31.05
"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 • Introduced January 01, 2005
"I-SPY Act" Internet Spyware Prevention Act of 2005 US House Bill HR 744	Rep. Bob Goodlatte (R-VA) Rep. Lamar Smith (R-TX) Rep. Zoe Lofgren (D-CA)	• Criminal penalties (up to 5 years jail time) for the unauthorized access or download to a computer. • Expresses the sense of Congress that the Department of Justice should vigorously prosecute those who use spyware to commit crimes and those that conduct phishing scams. • Preempts state laws. • Authorizes $10 million for the U.S. Attorney General for prosecutions and enforcement activities.	• Sent to Senate May 24, 2005 referred to Commerce Committee • Approved by the House with a vote of 395-1 May 23, 2005 • Passed Judiciary committee by voice vote May 18, 2005 • Introduced February 10, 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	• Passed Commerce Committee November 17, 2005 • Commerce Committee hearing October 05, 2005 • Commerce Committee Spyware hearing May 11, 2005 • Introduced March 20, 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 that the FTC has authority over these cases, and allows for them to triple the regular fines allowed by existing law. • No private right of action, 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.	• Commerce Committee hearing October 05, 2005 • Commerce Committee Spyware hearing May 11, 2005 • Introduced May 11, 2005

State Legislation

State & URL	Legislation	Summary	Status as of 12.31.05
California http://www.leginfo.ca.gov	S.B. 92	• Authorizes the recipient of spyware or software transmitted in violation of the prohibitions to recover damages, and also stipulates criminal penalties.	• Placed on inactive file.
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, and makes a violation of the Act a Class B misdemeanor.	• Passed House February 8, 2005 • Pending Senate floor action
Massachusetts http://www.mass.gov	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.	• Referred to Economic Development and Emerging Technologies Hearing October 25, 2005 • Introduced January 26, 2005
	S.B. 286	• Regulates "unconsented" Internet advertising, and requires a clear "opt-in" choice.	• Referred to Economic Development and Emerging Technologies Hearing October 25, 2005 • Introduced January 26, 2005
Michigan http://www.legislature.mi.gov	S.B. 53	• Provides sentencing guidelines for the crime of installing spyware on another person's computer without consent.	• Passed Senate March 9, 2005
	S.B. 54	• Prohibits accessing computers, computer systems, and computer networks for fraudulent purposes. • Prohibits intentional and unauthorized access, alteration, damage, and destruction of computers, networks, computer software, or data. • Prescribes criminal penalties.	• Passed Senate March 9, 2005
	S.B. 151	• Prohibits and provides civil remedies for installing spyware or adware onto another individual's computer without consent.	• Passed Senate March 9, 2005
New York http://assembly.state.ny.us	A.B. 549	• Establishes the unlawful use of spyware and malware as a class A misdemeanor; and a class E felony for a person who has been previously convicted within the last five years of violating this section.	• Referred to Codes • Introduced January 13, 2005
	A.B. 2682	• Establishes the unlawful dissemination of spyware as a class A misdemeanor. • Expands eavesdropping to include information intercepted by spyware. • Requires an authorization agreement be provided to computer users prior to software downloads.	• Referred to Codes • Introduced January 28, 2005
	S.B. 186	• Same as A.B. 2682	• Passed Senate June 23, 2005
	S.B. 3600	• Same as A.B. 549	• Referred to Codes • Introduced March 23, 2005
Pennsylvania http://www.legis.state.pa.us	H.B. 574	• Prohibits the misuse of adware or spyware and defines what actions would constitute misuse.	• Referred to Judiciary • Introduced February 16, 2005
	H.B. 1697	• Prohibits the unauthorized transmission of computer software, adware or spyware to a computer owned by another person.	• Passed House December 6, 2005
	S.B. 711	• Prohibits deceptive installation of spyware and provides for enforcement and for civil relief.	• Referred to House Consumer Affairs September 28, 2005 • Passed Senate September 27, 2005
Rhode Island http://www.rilin.state.ri.us	H.B. 6211	• Defines unlawful modification of computer settings and unlawful control of a computer. • Prohibits the deceptive sale of software.	• Referred to Senate Judiciary May 18, 2005 • Passed House May 12, 2005

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 file-sharing 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 message, 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

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

Data from the Enterprise SpyAudit have been collected since October 2004. The Consumer SpyAudit has collected data since January 2004. Spy Sweeper Scan tool began collecting data in November 2005. All scan results collected are anonymous and no personal or computer data is gathered with the scan results.

Instances of spyware detected are collected from each scan and grouped into one of four categories (adware, cookie, system monitor, Trojan horse). 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 were 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 the 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/land/freescan.php

CREDITS

Credits

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

- Threat Research Team, Webroot Software
- Legal Team, Webroot Software
- Christine Owens, Amplify Communications

ABOUT
Webroot Software

Webroot Software, Inc. is the creator and publisher of the award-winning Spy Sweeper line of anti-spyware products for consumers, small businesses and enterprises worldwide. Based in Boulder, Colo., the company is privately held and backed by some of the industry's leading venture capital firms, including Technology Crossover Ventures, Accel Partners and Mayfield. Webroot's software consistently receives top ratings and recommendations by respected third-party media and product reviews, and has been adopted by millions globally. Spy Sweeper and other Webroot products can be found online at www.webroot.com and on the shelves of leading retailers throughout the United States, Europe and Japan. 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 1-866-612-4227.

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.

Editor's Note: Beginning in 2006, the State of Spyware report will be released every six months, with updates every quarter.