STATE OF SPYWARE

Q1 2005

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

webroot
SOFTWARE, INC.

TABLE OF CONTENTS

webroot® Software, Inc.

FORWARD

FORWARD

In the late winter and early spring of 2004, a series of events hastened the public awareness of spyware as a clear and present danger to both consumers and enterprises. In February, the New York Times used its editorial page to call for legislation against an emerging software threat called spyware. In March, PC Magazine published the first comprehensive overview of anti-spyware software and featured the growing scourge on its cover, pulling this new security issue out of the chat rooms and into the bright light of mainstream technology media. Finally, in April the Federal Trade Commission hosted a workshop on spyware, attracting industry leaders, opinion makers and even apologists to Washington to debate the legislative implications of tiny pieces of software infiltrating unwitting computers and transmitting data to third parties without the consent of the information's owner.

Spyware had officially arrived.

By year's end, we knew that 90 percent of consumer computers had some form of spyware. Countless articles in countless newspapers and magazines had appeared bemoaning spyware and offering tips on how to get rid of it. Even the world's largest company had acquired a small company to develop its own spyware antidote. In general, the whole industry was now fueling a conflagration of attention about a threat that barely sparked anyone's curiosity nine months before.

It is hard to say whether the attention paid to spyware last year engendered the rash of spyware itself, or if we just finally came to notice a dormant infection that erupted into a plague. Whether you ascribe to the chicken or the egg theory, we can rest assured that, if 2004 was the year we discovered spyware, then in 2005 we are going to find out how hard it is to beat. But we can also be sure that the more we all know the better equipped we are to fight the fight we know we have ahead of us.

FORWARD

Webroot is proud to publish this inaugural edition of the State of Spyware report. This report, which we plan to publish quarterly going forward, is our attempt to share with the industry the data and background material we have developed to demonstrate the magnitude, breadth and overall impact of this problem. In so doing, we reveal the quantifiably frightening threat spyware represents. This report illustrates the problem from multiple angles and serves as a reference point as we all grapple with how to control and ultimately eradicate spyware. As you read the report, we hope it is elucidating and provides some context. The data in the report represents an heroic effort of both people and technology in tracking, identifying and categorizing myriad forms of spyware.

We are already anticipating next quarter's edition and so we invite you not to think of this as finite effort, but instead as a snapshot of an on-going conflict with a worthy adversary whose defeat requires us to know as much as we possibly can. We invite your feedback on the information presented, and the format we have chosen through a link at www.webroot.com/stateofspyware.

I would like to thank the Webroot professionals who compiled this data, analyzed it and have communicated in a way that is both compelling and educational. The rich information in this report can be daunting and it is their effort that makes it accessible and useful. We at Webroot hope you approach this data in the spirit in which it has been offered.

C. David Moll

CEO

Webroot Software, Inc.

HIGHLIGHTS

Enterprise, First Quarter 2005

In the first quarter of 2005, Webroot Corporate SpyAudit identified at least one form of unwanted program (Trojan, system monitor, cookie or adware) in 87 percent of the PCs it scanned. This number of infections remained relatively consistent to the 88 percent the SpyAudit found in Q4 of 2004. Excluding cookies, more than 55 percent of corporate PCs scanned were infected by the remaining spyware types.

By category, Trojan infections remained steady, both adware and system monitor instances declined, and the presence of cookies slightly decreased. Never the less, the problem of unknown monitoring technologies that put the security of corporate information at risk is still very real, as evidenced by the recent attempted bank robbery of Sumitomo Mitsui Bank of London using keylogger technology. – page 22

Consumer, First Quarter 2005

Results from the Webroot Consumer SpyAudit for the first quarter of 2005 indicate a slight decline in overall spyware penetrations. Whereas 92 percent of computers were infected with spyware in Q4 of 2004, the number in Q1 2005 dropped slightly to 88 percent. Within those infected machines, the SpyAudit found more than 25 instances of spyware. Excluding cookies, the number of infections averaged out at 7.2 per machine. — page 32

Breaking things down by spyware categories, the results were mixed with system monitors dropping, adware and cookies infections holding relatively steady, and Trojan penetrations actually on the increase.

Threats

CoolWebSearch (CWS) continues its reign as the most aggressive and prevalent threat on the Internet today. Its penetration onto PCs is nearly four times higher than its nearest competitor. Others notable names in top threats list include GAIN and 180search Assistant. — page 44

Contrary to common belief that the installation of spyware is only from visiting a few "alternate" sites, the Webroot proprietary research system, Phileas™, is quickly proving that spyware infections occur across a large number of sites. In March 2005 alone, Phileas identified 4,294 Web sites with 89,806 total associated Web pages containing some form of spyware — page 43

Legislation

Spyware is also making its way into state and federal legislation. At the state level, legislation to combat unwanted programs has been introduced in 27 states. At the federal level, both the House and the Senate are working through legislation that in all likelihood will supersede the legislative action being enacted at the state level.

While legislation is certainly a step in the right direction, we do not believe it will put an end to spyware, as spyware authors are likely to just move their operations outside of the US. — page 19

INTRODUCTION

INTRODUCTION

After a year of extraordinary growth in both the prevalence and the pervasiveness of spyware, it is valuable to examine this phenomenon and, at the same time, provide some thoughtful predictions for the coming months.

This report, the State of Spyware, seeks to provide data on the current levels and trends of spyware threats, and insightful analysis on what the data means to both consumers and businesses alike. In addition, the report tracks the legislative progress and provides a summary of incidents over the previous quarter where spyware played a part in the loss of information or direct financial loss. It's important to note that although it is somewhat US-centric, the results and implications may be applied globally.

For the purposes of this report, the definition of spyware is all programs installing themselves onto a user's computer by stealth, subterfuge, and/or social engineering and whose purpose is to redirect a user's activities or record those activities in a way that reduces a user's privacy, protection or peace of mind. Adware is often labeled as a subcategory of spyware, mainly due to the overt ways that adware vendors initially used to install their software on end user's machines with little regard for the user. As the spyware definition debate heats up, several industry groups, including one sponsored by the Center for Democracy and Technology, are forming to address this issue.

INTRODUCTION

The foundation for much of the analysis and trends in this report comes from the Webroot Consumer and Corporate SpyAudit tools*. Using these tools, Webroot can track four broad categories: system monitors, Trojan horses, adware, and cookies. Historically, Webroot and Earthlink published this data on the consumer side. The data* in this report is solely Webroot's, and not a combination of the data presented in the joint Consumer SpyAudit reports published by Earthlink and Webroot in 2004.

*see methodology

THE STATE of Spyware

2004 was the year that concerns over spyware began to exceed anxiety over any other cyber security threat. In the fourth quarter of 2004, more than 90 percent of the Consumer SpyAudit scans uncovered at least one instance of the four major categories for which it scans. For the first three months of this year, that number declined only slightly to 88 percent. However, when that statistic, coupled with the fact that the National Cyber Security Alliance and AOL found that 89 percent of participants had no idea that they had spyware on their PC, it is clear that the problem of spyware is neither abating nor is its impact well understood by PC users.

Throughout 2004 and the first quarter of 2005, stories of lost data and stolen accounts became more prevalent as more hackers sought quick profit. These events are not anomalies. The SpyAudit results reinforce the fact that many machines, both home and corporate, are infected with the malicious types of programs that often lead to theft of financial, personal, or public resources.

Incidents

The first quarter of 2005 saw an increase in high-severity security incidents involving spyware. Recently, headlines erupted around the globe with stories of spyware exploits, including the attempted theft of nearly $423 million from the Sumitomo Mitsui bank.

The spyware exploits are not isolated to high-profile corporations or financial institutions. Even crime fighters can fall victim to these threats. The Oklahoma sheriff's department was a victim of spyware, jeopardizing Homeland Security information. The Sheriff's department discovered surveillance spyware installed on computers in their office. The installed spyware allowed unauthorized access to sensitive information about prisoner transfers, personnel files and confidential Homeland Security information. Officials in Oklahoma have not determined who installed the software or how much information was compromised.

These incidents, in addition to the Kinko's case of 2003, where keylogging software was installed on computers at several locations in New York City, and the Valve Software Half Life source code loss, which was stolen using similar keylogging software highlight the risk that spyware is appearing in every sector of commerce, government and organizations.

Spyware Economics

Historically, adware was the primary category of software that created most of the problems for end users. Although other forms of spyware played their part, it was the flood of adware programs into the market that led to the creation of the anti-spyware market.

Adware is a constant and significant part of the overall spyware problem, and that is not expected to change in the near future. If there is one observation that stands out above all others regarding adware, it is the pecuniary motivations for creating and disseminating this form of spyware.

Only by looking at the actual data is the extent of the economics of the problem made obvious. The results reported here indicate that there is a market that derives more than $2 billion annually (see methodology) from pop-up ads, hijacking home pages, redirecting searches, and using hosts file and DNS poisoning. These numbers indicate that this previously unmeasured market may be approaching 25 percent of the already established market of online advertising as reported by the Internet Advertising Bureau.

Consumers and businesses alike have already begun to take steps to counter spyware. Webroot data suggests that spyware infection rates are dropping, probably due to increased awareness and the use of anti-spyware software. But while the numbers of infections may be on the decline, the ingenuity of spyware writers is increasing as they seek to protect and grow their business models, making protection that much more important.

DEBATING DEFINITIONS: Spyware vs. Adware

Since the development of the anti-spyware market, "spyware" has been the commonly accepted and used term to describe unwanted, unapproved, or malicious files and programs placed on a user's computer without the user's explicit consent. Although other terms like malware, scumware, PUPs (Potentially Unwanted Programs), and PUS (Potentially Unwanted Software) have been introduced over time, "spyware" seems to be fully engrained as a catch-all term, and the subtle distinctions between the various forms of spyware are lost on most consumers and businesses.

the subtle distinctions between the various forms of spyware are lost on most consumers and businesses.

At a time when many consumers and businesses struggle to understand the threat posed by spyware, trying to move away from the term “spyware” would serve only to confuse an already overwhelmed audience.

The term adware is a subcategory of the overarching “spyware” category, but may be slowly evolving into its own category. The challenge to the reclassification is caused by historical actions of adware vendors and those that use cross-domain cookies to track online behavior. While some organizations are rapidly adapting policies and practices to respect privacy regulations, many more adware distributors still violate the user’s right to privacy, and in many instances, still violate pending legislation and even break existing laws by exploiting vulnerabilities to install their adware. Over the next three to six months, the market can anticipate some clarification on these terms and topics as industry groups convene to debate the issues and arrive at a consensus on definitions.

System Monitors

This general category includes the greatest threats to a user’s privacy and to an enterprise’s proprietary information and trade secrets. System monitors may monitor a computer’s activity. They range in capabilities and may record some or all of the following: keystrokes, e-mails, chat room conversations, instant messages, Web sites visited, programs run, time spent on Web sites or using programs, and even usernames and passwords. The information is transmitted via remote access or sent by e-mail. Keyloggers are included in this category of spyware.

In the consumer world, the number of system monitor infections dropped to an all-time low of 7 percent of computers scanned. This represents a drop of more than 60 percent from the data collected in Q4 of 2004. While the drop is a move in the right direction, it is still unacceptable that one out of every fifteen computers is infected with a keylogger.

one out of every fifteen computers is infected with a keylogger.

In the business world, system monitors are running at the same rate of infection as consumers, 7 percent. Within specific enterprises, infection rates climbed as high as 12 infected machines per 100 scanned.

infection rates climbed as high as 12 infected machines per 100 scanned.

As the Sumitomo Mitsui bank exploit shows, any level of system monitor penetration represents a tremendous risk to corporate security, assets and intellectual property. Businesses are beginning to understand that while anti-virus and firewall protection are a must, they also need an anti-spyware solution to prevent these types of exposures.

Trojan Horses

A Trojan horse is a malicious program disguised as a harmless software program. Trojans do not replicate themselves like viruses, but spread through e-mail attachments and Web downloads. Once the file is opened, 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.

In the first quarter of 2005, Trojans were on 19 percent of consumer machines and 7 percent of enterprise machines. Corporate infection rates remained flat to Q4 2004, but the number of incidents per infected computer climbed 28 percent over the previous quarter. This jump represented the second quarter in a row where infection rates jumped by more than 25 percent.

Trojans were on 19 percent of consumer machines and 7 percent of enterprise machines.

While the original definition of a Trojan horse was an innocuous program that hid a more malicious program, it has become common to call the malicious component the Trojan horse as well.

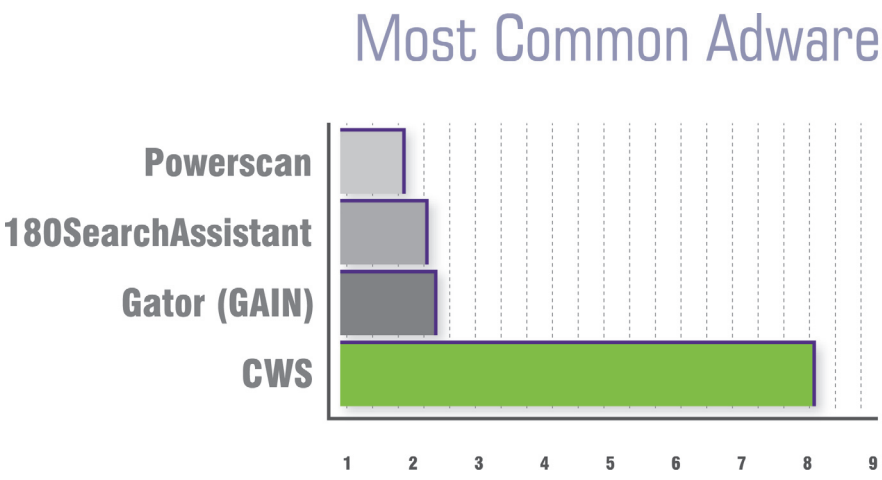
Adware

Data from the Webroot Consumer and Corporate SpyAudits clearly show that adware is the most dominant form of unwanted software on PCs today. Corporate PC infection rates topped more that 50 percent, whereas the number of consumer PCs found with adware were well over 60 percent. The Webroot Consumer SpyAudit identified an average of 7 pieces of adware on those machines containing adware infections. The most prevalent malicious adware is Cool Web Search (CWS) and its many variants. However, several dozen other entities produce and distribute adware with very significant penetration rates.

adware is the most dominant form of unwanted software on PCs today.

In Q1 of 2005, the SpyAudit scans found at least 17 variations of Cool Web Search, and over the last five quarters, the SpyAudit tracked 107 variants. These variants include the most nefarious versions such as CWS AboutBlank, CWS_NS3, and CoolWWW. CWS found in 8.2 percent of consumer scans.

The next most prevalent versions of adware were Gator (GAIN), 180SearchAssistant, and Powerscan registering 2.2 percent, 2 percent, and 1.7 percent penetration respectively.



Cookies

The Webroot Consumer SpyAudit identified more than 30 million instances of cookies over the last 15 months. The cookies with the greatest presence are from online ad server and tracking organizations such as Atlas DMT (a unit of aQuantive, Inc.), DoubleClick, Mediaplex, 2o7.net, and Atwalla.

Seventy-six percent of Consumer SpyAudit scans in Q1 of 2005 identified tracking cookies. The average cookie count was more than 20 on those machines and actually increased in the percentage of penetration during the last 15 months.

Anti-Spyware Legislation

Legislation relating to spyware or adware is being considered in 27 states. New states this quarter are: Alabama, Arkansas, Florida, Georgia, Iowa, Kansas, Maryland, Massachusetts, Missouri, New York, Pennsylvania, Rhode Island, Tennessee, Texas, and West Virginia.

These states passed bills in one or both of their houses: Arkansas, Georgia, Illinois, Iowa, Michigan, and Washington. The Governors of Arizona, Virginia, and Utah recently signed their respective measures into law.

The legislative activity is a response to the outpouring of concern from consumer groups, as well as individual constituents in each state over privacy. The measures working their way through both the US House and Senate are meant to head off and supersede state legislation.

For more detail about the state legislation, please see page 78.

Looking Forward

Based on the results from Webroot SpyAudit data for consumer and enterprise, and taking into consideration the rapid growth of Web sites that contain malware as derived from the Webroot Phileas malware crawler (see Phileas/Threat Research section), it is simple to see rough times ahead for those who seek to maintain the privacy of their computers or those who provide maintenance and support for corporate networks.

it is simple to see
rough times ahead

The amount of money to be earned by developing and propagating adware and by using spyware to steal identity and account information virtually guarantees that these issues are only going to grow over the next 12 to 18 months. Spyware writers continue to fill their bank accounts by using more ingenious methods to ensure the life and spread of their programs.

more ingenious methods to ensure the life and spread of their programs.

Malware techniques and methods for creating worms, viruses, and spam are being redirected towards generating revenue with next generation spyware. Because the spyware writer seeks to avoid detection and removal of the software, they employ more sophisticated techniques including changing security settings on Windows operating systems, file obfuscation using rootkit methods, and masquerading as legitimate software.

Legislation will probably pass at the federal level sometime in the next six months. It will curtail some of the more abusive activities of companies in the United States, but it will do nothing to stop invasions from offshore individuals or entities.

In 2005, we predict many more insider attacks, like the one that targeted Sumitomo Mitsui Bank of London, utilizing the widely available spy tools.

Overall, the rest of 2005 will be another bumpy ride.

CORPORATE
SpyAudit Results

CORPORATE SpyAudit Results

The Webroot Corporate SpyAudit was initiated in October 2004. The data presented below is for the last quarter of 2004 and the first quarter of 2005.

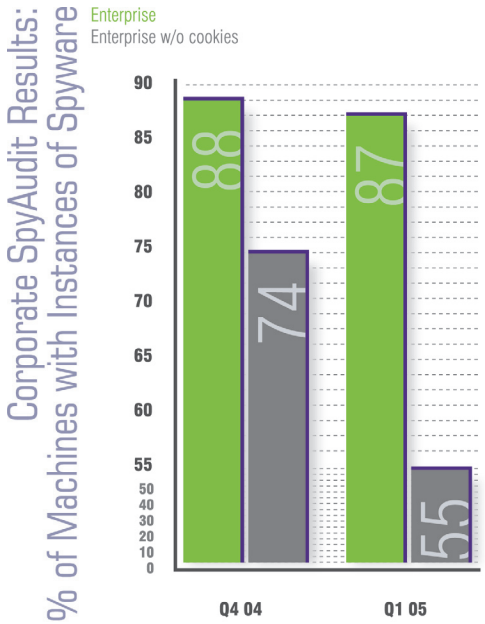
The Corporate SpyAudit operates in a slightly different manner than that of the Consumer SpyAudit. Unlike the Consumer SpyAudit, in which an individual runs the audit on a single machine, in the Corporate SpyAudit, a network administrator deploys the SpyAudit on a select number of PCs on a network, runs a scan, and collects the results.

Overall Findings

To date, the Webroot Corporate SpyAudit scanned more than 35,300 systems, representing more than 18,000 companies. The median number of PCs scanned using the Corporate SpyAudit is eight.

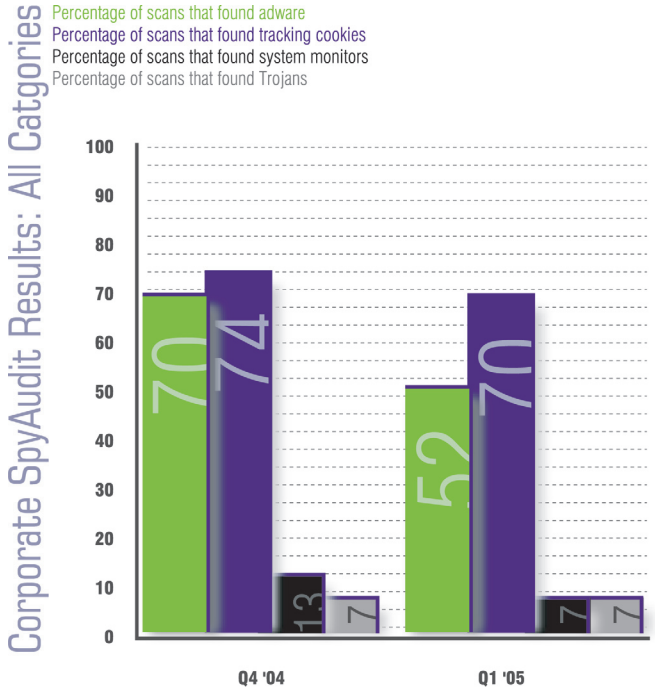
The good news is that the infection rate of machines in the corporate environment has dropped from Q404. The bad news is that the infection rate is still at 87 percent.

infection rate is still at 87 percent.



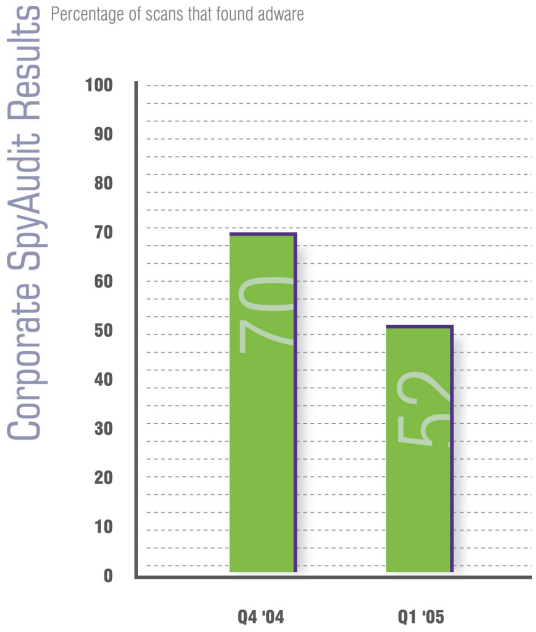
CORPORATE SpyAudit Results

Although cookies tend to make up the largest number of infections per corporate machine, the majority of scanned machines – more than 55 percent – are still infected with adware and the more malicious forms of spyware (system monitors and Trojans). Eliminating cookies from the audit, scans of the enterprise machines found an average of 3.8 instances of more malicious spyware – a very high number considering a single malicious program can compromise proprietary corporate information.



Adware

As of Q1 2005, adware was present on 52 percent of machines scanned within the enterprise.



The average infected machine had 3.6 instances of adware, equal to the previous quarter, but less than the 6.9 instances from the consumer scan results. However, even 3.6 instances per computer are too many for most companies, indicating why enterprises started to take such an interest in combating unwanted software on corporate machines.

CORPORATE SpyAudit Results

Multiple pieces of adware can lead to increased likelihood of system crashes and poor performance that ultimately lead to calls to the corporate help desk. Enterprise IT departments usually track help desk performance using such metrics as:

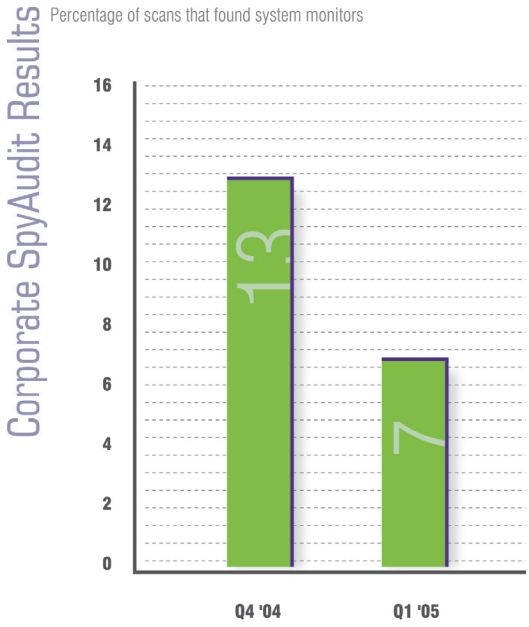
- Time to respond
- Time to close out trouble ticket
- Root cause

With spiraling helpdesk calls attributed to spyware, combating and removing spyware is becoming among the most pressing IT issues for enterprises.

System Monitors

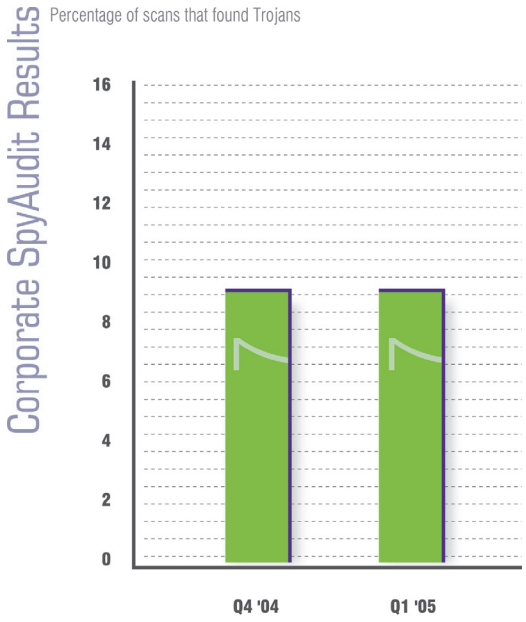
Just as in the Consumer SpyAudit results, system monitors decreased dramatically from the end of 2004 into the first quarter of 2005. System monitors found on corporate systems declined from 13 percent to 7 percent. However, the machine infected with this category had a higher frequency - the average instance went up from 1.1 to 1.2, meaning regardless of the number, system monitors signify a real and present danger to the enterprise.

machine infected with this category had **a higher frequency**



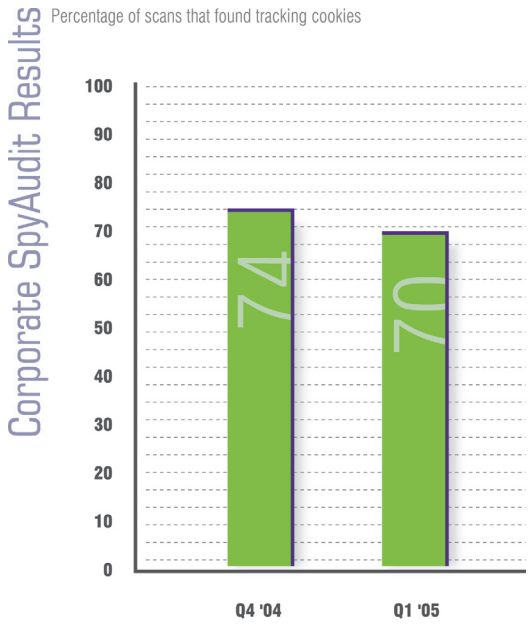
Trojan Horses

The presence of Trojan horses within enterprises is also surprisingly high at 7 percent, or 1.3 average instances per scanned PC infected with this type of program. While the Q1 2005 infection rates represent no significant change from Q1 2004, these programs present an ongoing danger to corporations.



Tracking cookies

While this particular area may be inconsequential to corporations, it's interesting to note that 70 percent of scanned computers had instances of cookies, not far from the 76 percent that the Consumer SpyAudit found in scans.



Corporate Compliance

Each State of Spyware report will have a section that focuses on compliance with government regulation, a particular concern to health care, financial services, and ecommerce vendors, as well as most publicly traded firms. While most federal regulations do not have explicit requirements for IT security, they imply that loss of information and failure to provide controls around that information may cause an organization to be out of compliance.

Gramm-Leach-Bliley (GLB) Compliance

The recent security issue at Sumitomo Mitsui's London bank underscores the daily exposure banks face from criminals, both cyber and traditional. Financial institutions have been the target of news making attacks. Cybercrime has taken the lead in all cyber threats. Phishing attacks, pharming, brute force attacks against online banking accounts, and the results of keystroke loggers embedded on Internet kiosks or spread via Trojan horses and worms represent evidence of a crime spree only imaginable in the digital age.

The implications of direct attacks on the assets of financial institutions dwarf the impact on personal privacy.

There are two primary regulatory statutes impacting financial institutions, and, in some cases, any organization that is responsible for financial data on consumers. The first is the Gramm-Leach-Bliley (GLB) Act, or the Financial Modernization Act of 1999. There are three major provisions of GLB. The first deals with how financial institutions handle consumer financial data, the Financial Privacy Rule. The biggest impact of this clause to date has been the requirement of a Privacy Notice, delivered to every customer of an financial institution. Customers of financial institutions are given the right to opt-out of any marketing activity that the financial institution may undertake using their information.

The other provisions of GLB are the Safeguards Rule and the Pretexting Rule. The Safeguards Rule requires all financial institutions to design, implement, and maintain safeguards to protect customer information. There is no mention at all within GLB of encryption, which, if properly implemented, would be a tremendous safeguard of customer information. The Pretexting provisions of GLB protect individuals from the misuse of their information when obtained under false pretenses.

The other law affecting financial institution concerns, those enterprises with operations in California, or California 1386. It requires financial institutions to immediately notify California residents if their information is lost or stolen. This law was invoked recently when ChoicePoint, the Georgia-based credit-reporting agency had to first notify California residents that their data was stolen by criminals that defrauded their way into ChoicePoint's service. ChoicePoint quickly succumbed to pressure from other states to notify their citizens as well.

There are no government rulings within GLB that advise or recommend particular measures to safeguard customer information. Nist.gov is one of the best resources for security practices. The security policies published there are becoming the de facto standard for state and federal government agencies. Nevertheless, new developments in the threat arena make most security guidelines outdated.

There is a rapid shift in the purpose and methods of creators of malware. Viruses, spam, worms, Trojan horses, and drive-by Web browser attacks all have one purpose: to generate revenue for the writers and distributors of spyware. Identity thieves are getting rich breaking into users' bank and trading accounts, and issuing new credit cards in the names of the victims. One of the tools in this new economy of larceny is the system monitor.

System monitors take several forms. Although audio and video snooping software exists, the most prevalent system monitor is a keystroke logger. These software programs record every keystroke made at a computer. The purpose is to harvest user names, passwords, and identities. A keystroke logger was the tool used in the case of Sumitomo Mitsui in London.

CORPORATE SpyAudit Results

The results of the most recent Webroot Corporate SpyAudit indicate that within the typical enterprise anywhere from 3 to 12 percent of machines are infected with system monitors. While no legislation dictates defensive or audit measures regarding keystroke loggers, it is imperative that auditors of financial institutions and their executives pose the question: "Are we in compliance with the Safeguards Rule of GLB if there are malicious keystroke loggers on internal computers?"

CONSUMER
SpyAudit Results

CONSUMER SpyAudit Results

Every quarter Webroot compiles the results from a continuous Consumer SpyAudit. This audit consists of the findings of voluntary sweeps of machines that belong to visitors to the www.webroot.com Web site and elsewhere. These results are anonymous, and are of machines that a computer owner chooses to sweep for spyware. See the methodology section for more detail.

Overall Results

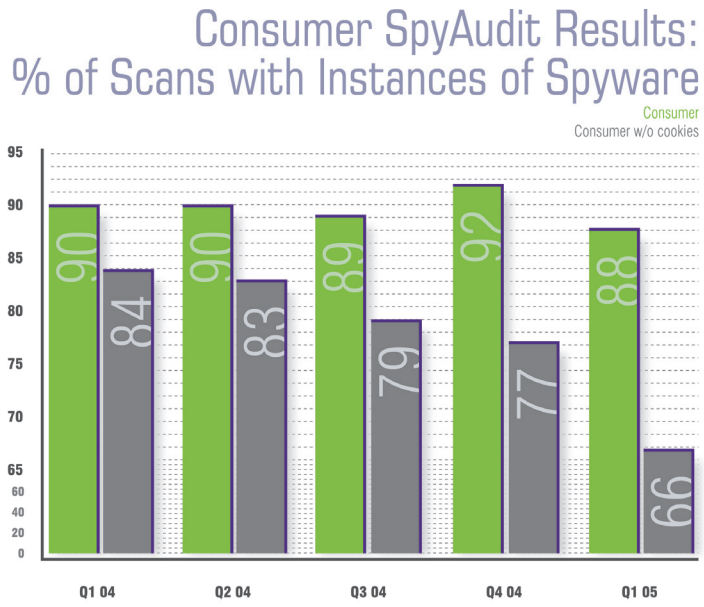
In Q4 of 2004, the Consumer SpyAudit saw a rise in the number of machines infected by spyware reach an all-time high of 92 percent, and perhaps even more alarming than the overall growth of the spyware plague was the dramatic rise in the most malicious forms of spyware – system monitors and Trojan horses. With these lofty infection rates, subsequent rates could only go down, potentially installing a false sense of security. The trends are definitely in consumers' favor, but the number and types of infections are staggering.

88 percent
of computers
scanned.

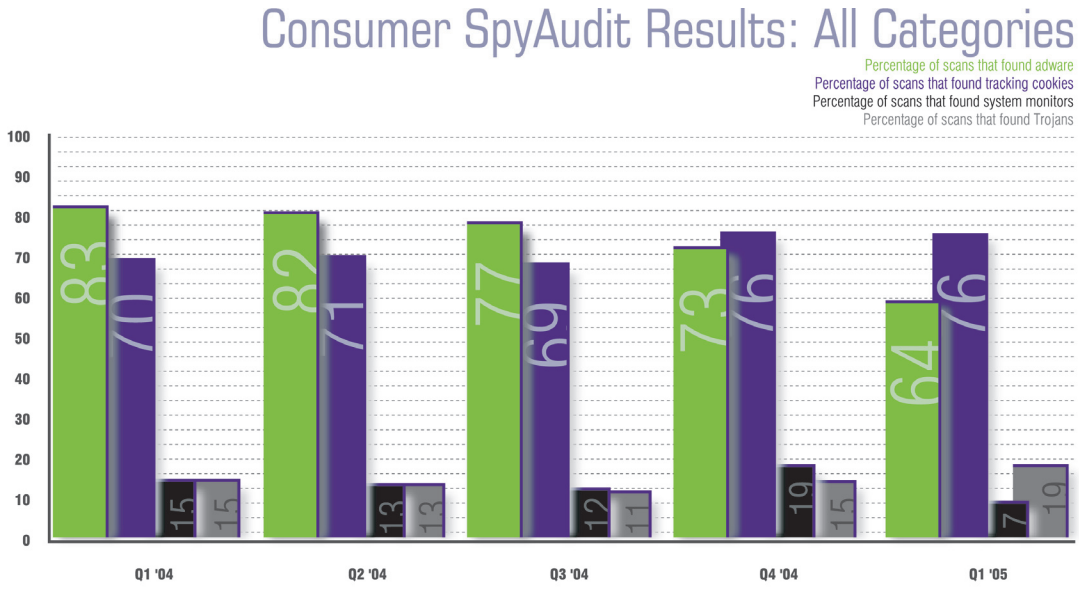
25 instances
per machine.

In the first quarter of this year, more than one million scans were performed using the Webroot Consumer SpyAudit tool, and the scans identified 26.2 million instances of unwanted software. The good news for consumers is that the infection rate of spyware dropped slightly from Q4 of 2004, down 4 percent from 92 to 88 percent of computers scanned. The bad news, however, is that for those which were infected, the number of overall category instances rose for the second quarter in a row to more

than 25 instances per machine. Not counting cookies, the average instance count stands at 7.2 Q1 of 2005, up slightly from 7.1 average instances for Q4 of 2004.

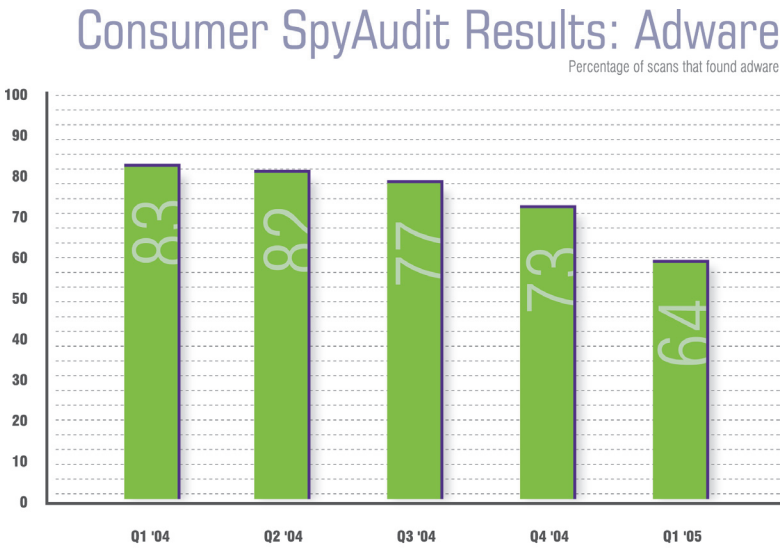


By category, adware, system monitors, and Trojan horses declined in penetration. Tracking cookies increased their percentage penetration slightly.



Adware

In the first three months of this year, 757,579 out of 1,185,032 scans indicated the presence of adware. On the average, one scan found 6.9 instances of adware. In the last quarter of 2004, 73 percent of scans identified adware compared to the 64 percent in the first quarter of 2005.



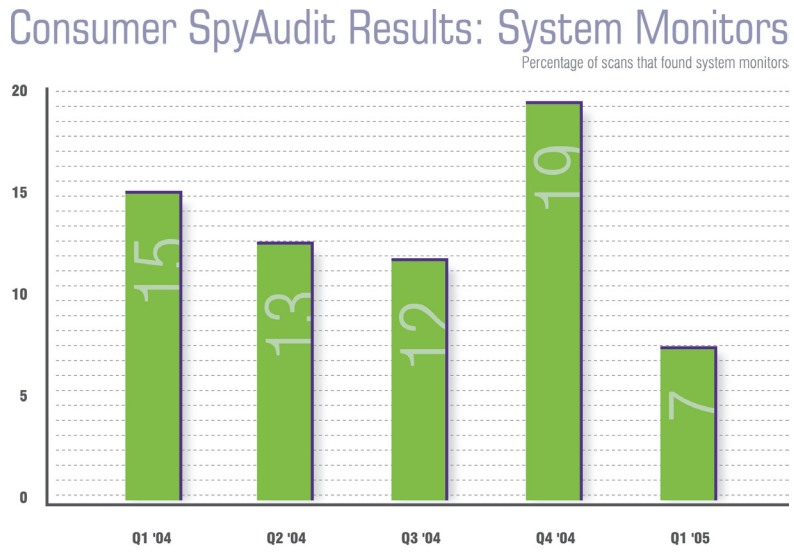
While the overall presence of adware on computers is a significantly large number, Webroot believes the reduction in percentages since the beginning of 2004 is indicative of the increased awareness that spyware and adware are threats. End users have begun to seek remedies and/or are less prone to install so-called "freeware" that often comes with adware or even system monitors. Microsoft's announcement of a free anti-spyware product contributed to the heightened awareness, as did the activity in 27 states to create anti-spyware laws while the US House and Senate re-introduced their legislation.

increased awareness that spyware and adware are threats.

At the same time, the average number of pieces of adware on an infected machine held constant at 6.9 for the last two quarters. Numbers this high indicate that unprotected machines are continually burdened with additional pieces of adware. Six or seven programs running in the background all trying to serve ads, redirect browsing, or search behavior inevitably leads to system slow downs and crashes.

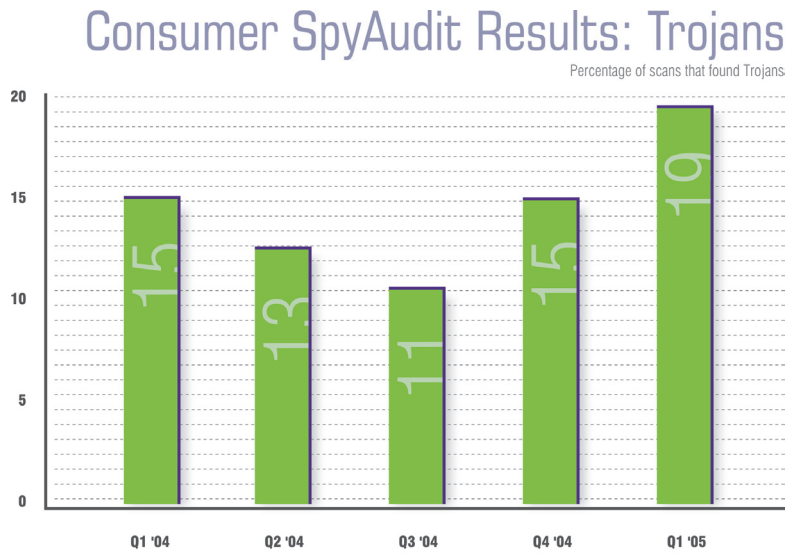
System Monitors

A dramatic drop in system monitors from Q4 2004 to Q1 2005 is also evident. The last month of 2004 saw a steep increase in system monitors. The Webroot Threat Research team is continuing to research the cause for that increase. In the meantime, the total percentage of machines with system monitors dropped from 19 to 7 percent. However, the average instances per scan with a system monitor present remained the same from quarter to quarter at a frequency of 1.2 instances per scan with a system monitor already present.



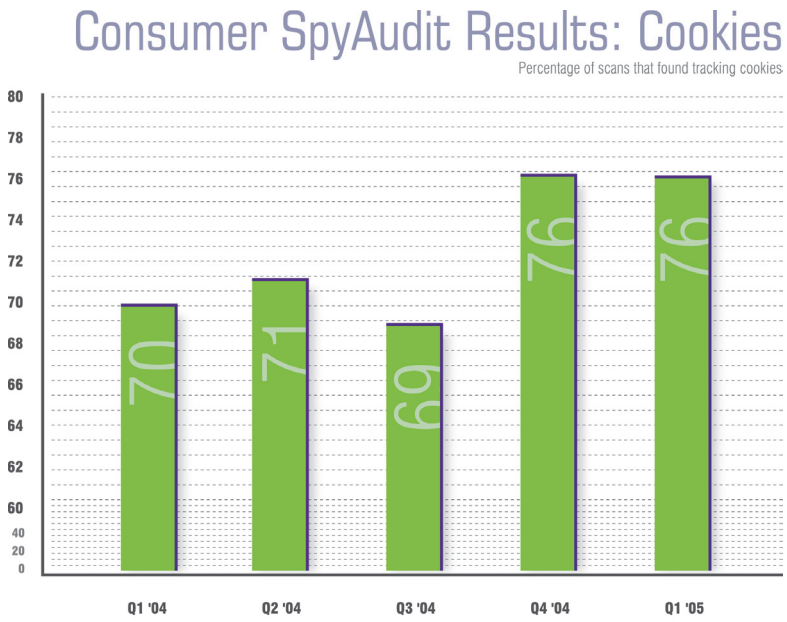
Trojan Horses

Although the percentage of spyware infections decreased in Q1 2005 from Q4 2004 overall, the percent of machines founds with Trojans increased almost 30 percent over the already-high Q4 2004 level. For those scans that identified Trojan horse infections, there was almost a 10 percent increase in the number of infections per scan – from 15 to 19 percent for frequency of instances by scan. This could indicate increased infection rates as Trojan horses used to recruit bots for armies for Denial of Service attacks.



Tracking Cookies

Much has been made of whether cookies really constitute spyware, and should be included in spyware counts. Interestingly enough, of those people infected with spyware, three out of every four are infected with non-cookie spyware traces. Tracking cookies overall are increasing their penetration into the consumer market with a gradual change from 70 percent at the beginning of 2004 to 76 percent in Q1 2005. Additionally, for scans that identify cookies, the number of infections per scan has grown by 10 percent over last quarter to more than 7.2 instances.



THREAT
Research/Phileas

Spyware research is significantly different, and far more challenging, than research methods used to identify viruses. While honeynets and user submissions are effective methods of research for the antivirus industry, the nature and complexity of spyware make those approaches ineffective in spyware research. Spyware researchers must instead rely on more active methods to identify new threats.

Keeping up with hundreds of adware companies and thousands of spyware writers is a daunting task. Currently, anti-spyware companies use three methods for finding spyware: manual, client automation, and Web crawling.

Manual Discovery

The earliest and still most prevalent method of spyware research is manual discovery, which involves researchers visiting known spyware Web sites and infecting machines with malicious code. This type of research is very time consuming and is not a scalable approach.

Some anti-spyware companies try to overcome the scalability issue by relying on volunteers to constantly scour the Internet for new spyware and report their findings to the product developers. However, this method is flawed as it relies on an unpredictable and unknown resource that can disappear at any time.

Client Automation

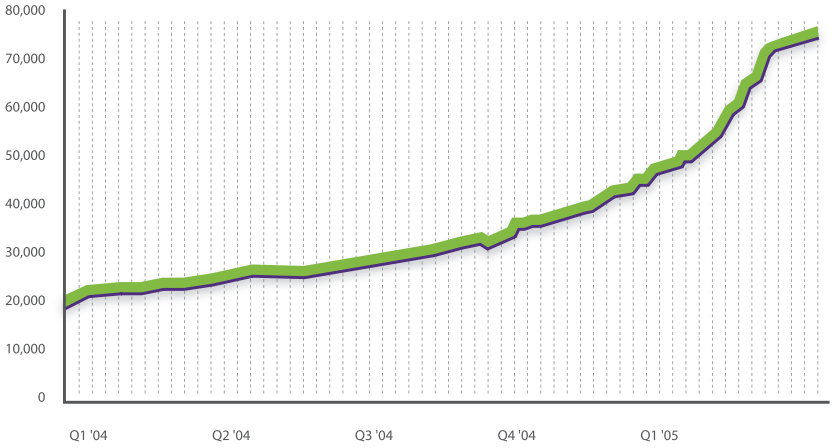
Another methodology used by some anti-spyware companies involves using a function of the anti-spyware software to collect and report potential spyware from end-user computers. These findings are sent to a central repository for further analysis. While this collection method is economical and scalable, it is reliant on end-user infection before protection is provided. The frequency of false positives is higher because the reports generated by the system do not provide enough data for deeper analysis before a definition is written.

Web Crawler Automation

The most effective and efficient means of identifying spyware in the wild is to employ webcrawler technology to find new threats before they can infect end-users. Phileas, Webroot's malware crawler, employs this methodology to populate its threat database, providing Webroot's anti-spyware products with the most up-to-date protection.

As of March 31, the Webroot Spy Sweeper product identifies **79,754 traces of unwanted programs.**

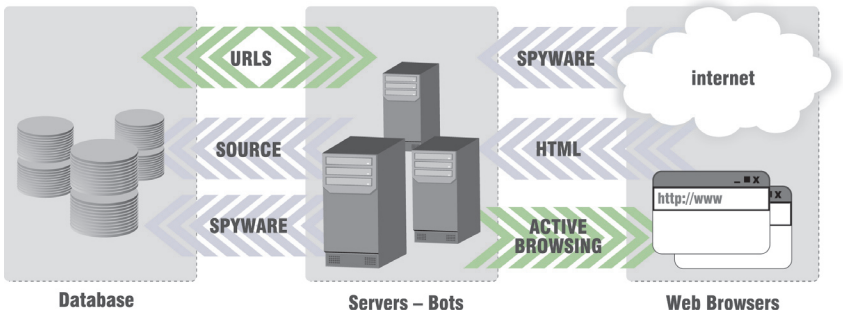
Spyware Trace Count



Using dozens of servers with high bandwidth Internet connections, Phileas controls an army of "bots" that scour the Web for sites containing malware. By using this system, Webroot is able to update its definition database with nearly 300 new definitions per week. As the problem scales, this architecture can adjust to keep pace. The graphic below depicts the process:

The Webroot Phileas malware crawler was developed to **automate the search and discovery of new spyware.**

Phileas Architecture



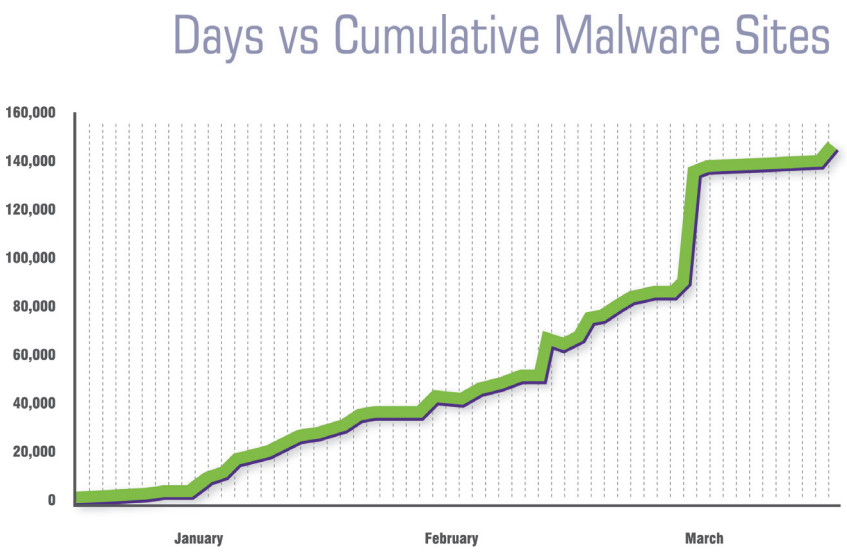
False Positives

Identification is just the first step in defeating spyware. Once a spy is identified, a definition must be written and tested to confirm that it not only correctly distinguishing the malicious code, but that it does NOT incorrectly identify, or interfere with, legitimate files in the process. This incorrect identification or false positive is often the hardest aspect of creating an effective anti-spyware application.

False positives can cause severe problems for application users. However, many anti-spyware providers do not take the additional steps in the quality assurance process to prevent false positives. In some cases, anti-spyware vendors purposefully create false positives to impress potential customers.

Consequently, the key to an effective anti-spyware product is both its ability to correctly identify and remove malicious files and its ability to avoid removing or corrupting legitimate files.

In the first quarter of 2005 Phileas returned results for close to 150,000 URLs and associated domain names.



In March alone, Phileas combed through 4,293 Web sites and found 89,806 associated Web pages classified as possible pages containing malware. It is a good measure of the increased distribution of spyware during the first quarter of 2005.

Phileas Research Results

Number of domains found and associated URLs

	Domains	URL's
January	3,205	29,745
February	3,775	37,295
March	4,293	82,806

An example of the kind of domain name that Phileas finds is http://www.search-and-more.com/249/clk. Warning! Do NOT look at this Web site unless you are fully protected with an anti-spyware solution. This URL uses an exploit (Microsoft Security Bulletin MS03-014) to install a toolbar.

Malware Sites Identified By Phileas

Domains	Number of Malicious URLís
www.smutserver.com	1,532
www.xtoplist.com	642
www.myfreeporn.com	598
hardcore.myfreephotos.com	326
www.sybianmoview.com	289

Other examples of sites discovered by Phileas include these listed in the above graph. The rapid rise in possible malware sites is the strongest indicator that the writers and distributors of malicious adware and other threats are expending considerable effort to infect users with their products. An automated tool such as Phileas is the only way to keep track of this magnitude of growth.

Top Threats

The chart below details the Webroot Top Threats for the first three months of 2005. Eight of these entries are adware, found on a large number of machines in both Q4 2004 and Q1 2005 as shown in the chart. These pieces of adware are found on a regular basis and rarely fall out of this list, although their positions vary, as distribution mechanisms are refined for each piece of software.

The listed adware vendors distributed their software successfully. CoolWebSearch is the most successful distributor in terms of number of infections. There are many Web sites affiliated with CoolWebSearch, and several use vulnerabilities in Microsoft Internet Explorer to automatically install. Additionally, many of these sites use social engineering or confusing forms to trick end users into accepting installation requests.

CoolWebSearch is the **most successful distributor**

Claria (GAIN) has seen wide distribution of their software by bundling with freeware products including popular peer-to-peer software such as Kazaa. 180SearchAssistant is also widely distributed through freeware products and other bundles, and is also installed through many Web sites using ActiveX installation methods as well as a search toolbar and from Zango.com.

Top Threats by Quarter

Percentage of scans that identified one or more of these threats

Threat	% Q4 04	%Q1 05
CWS (Cool Web Search)	8.2	8.2
Gator (GAIN)	2.6	2.2
180search Assistant	2.6	2.0
PowerScan	1.8	1.7
Altnet	1.7	1.7
WebSearch Toolbar	1.9	1.6
KeenValue	1.9	1.6
Hot as Hell	< 0.1	< 0.1
Advanced Keylogger	< 0.1	< 0.1
TIBS Dialer	< 0.1	< 0.1

CoolWebSearch (CWS) - several variants

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

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

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

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

GAIN-Supported Software

Short Description: GAIN-Supported Software is a group of adware programs that may display pop-up advertisements on your computer.

Characteristics: GAIN-Supported Software may track your Web surfing habits and display pop-up advertisements or results from a search provider in a separate window.

Method of Installation: By clicking an advertisement or visiting a Web site, a user may be prompted to install GAIN-Supported Software on their computer. GAIN-Supported software may also be bundled with various software programs.

Consequences: This program may send information about your Web surfing habits to centralized servers, which may slow your Web browser's performance.

180search Assistant

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

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

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

Consequences: 180search Assistant may open a new browser window displaying a sponsor's website, slowing your Web browser's performance.

PowerScan

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

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

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

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

Altnet

Short Description: Altnet is a program that is intended to keep track of uploads from Kazaa in order to reward people who are sharing content.

Characteristics: Altnet is a joint venture between Brilliant Digital and Sharman Networks, the makers of the peer-to-peer filesharing program Kazaa. Altnet is designed to allow users to purchase copyrighted material from other users. According to Altnet, it uses "Digital Rights Management (DRM) technologies to securely distribute and license" content. Members can host copyrighted files and get paid by Altnet for storing and sharing these files. This program is only supposed to track the uploads members make using Altnet, but it may track all the uploads a member makes using Kazaa. This tracking can be used to find people who are serving large amounts of illegal music to other users.

Method of Installation: Altnet is bundled with Kazaa software.

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

WebSearch Toolbar

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

Characteristics: WebSearch Toolbar may hijack your Internet Explorer settings and install a toolbar on your Web browser. This toolbar may also display advertisements

on your computer. It has the ability to run in the background, hiding its presence.

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

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

KeenValue

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

Characteristics: KeenValue displays targeted advertisements on your computer in the form of pop-up windows, pop-up slider windows, embedded advertisements, and Web links in the form of desktop icons and installation files. The adware program also collects personal information including your name, country, zip code, IP address, system settings, what software is on your computer, terms entered into search engines and Web surfing activities. In addition, KeenValue has an auto-update feature that allows the program to silently update itself and install other third-party software applications.

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

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

Hot as Hell

Short Description: Hot as Hell is a dialer that may hijack your modem and dial toll numbers that access paid, pornographic Web sites.

Long Description: Hot as Hell may disconnect your computer from your local Internet provider and reconnect you to the Internet using an expensive toll or international phone number. It does not spy on you, but it may accrue significant long distance phone charges. It may run in the background, hiding its presence.

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

Consequences: This dialer program may accrue significant long distance phone charges.

Recommendations: The Federal Trade Commission recommends that you dispute the charges from your telephone company and report the incident.

http://www.ftc.gov/bcp/conline/pubs/alerts/modmalrt.htm

Advanced Keylogger

Short Description: Advanced Keylogger may record keystrokes and take screenshots.

Long Description: Advanced Keylogger may monitor your computer activity. It may also capture almost everything you do on your computer including recording all keystrokes, e-mails, chat room dialogue, instant message dialogue, Web sites visited, usernames, passwords, and programs run. It may take screen shots of your desktop at scheduled intervals, and the information gathered may be stored on your computer in an encrypted log file for later retrieval. It may be capable of e-mailing the log files to a pre-defined e-mail address. It may run in the background, hiding its presence.

Method of Installation: Advanced Keylogger was likely installed by someone with administrative access to your computer, such as a system administrator or someone who shares your computer.

Consequences: This system monitor may allow an unauthorized third-party to view potentially sensitive information, such as passwords, e-mail, and chat room conversation.

TIBS Dialer

Short Description: TIBS Dialer is a dialer that may hijack your modem and dial toll numbers that access paid, pornographic Web sites.

Characteristics: TIBS Dialer may disconnect your computer from your local Internet provider and reconnect you to the Internet using an expensive toll or international phone number. It does not spy on you, but it may accrue significant long distance phone charges. It may run in the background, hiding its presence.

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

Consequences: This dialer program may accrue significant long distance phone charges.

Recommendations: The Federal Trade Commission recommends that you dispute the charges from your telephone company and report the incident.

http://www.ftc.gov/bcp/conline/pubs/alerts/modmalrt.htm

CONCLUSION

CONCLUSION

The four years since the advent of the Code Red and Nimda worms has seen a repetitive pattern in the ebb and flow of Internet security threats. This pattern can be largely attibuted to:

- the discovery of a vulnerability in a widely deployed application (usually belonging to Microsoft);
- the development of a new class of malware to exploit the vulnerability, and finally;
- the development of new defenses against the malware.

E-mail viruses, server-to-server worms, IM worms, Trojans, and denial of service attacks (DDOS) have all seen this pattern. The security industry has responded with more and more defenses that require continuous investment in security.

The first quarter of 2005, as measured by the Webroot Consumer and Corporate SpyAudit, demonstrated the prevalence of adware and cookies on a majority of computers. The slow decline in machines with adware and system monitors indicates that the attention paid to spyware in the press, legislative actions and online behavior has increased the awareness of the threat and that better educated users are taking steps to counter the threats. Simultaneously the dramatic climb in malware sites as discovered by Webroot's Phileas malware crawler provides early warning that the perpetrators of spyware are increasing their activity.

2004 marked a turning point for the entire Internet threat space. Cybercriminals morphed the capabilities of malware with the money-earning potential of spam. This is the new paradigm that will shape the future of Internet threats. Incidents of spyware being used to break into computer networks are on the rise and will continue to go up. 2005 will see more direct evidence of this as the publication of incidents of cybercrime jumps dramatically.

first quarter of 2005, as measured by the Webroot Consumer and Corporate SpyAudit, demonstrated the prevalence of adware and cookies

the dramatic climb in malware sites as discovered by Webroot's Phileas malware crawler provides early warning

CONCLUSION

Never has the need for vigilance been more imperative. Individuals and enterprises alike must begin to plan for the worst. Business processes that rely on trust, such as the ChoicePoint subscription model that allowed criminals to create accounts that gave them access to credit reports, must be re-evaluated. Defenses must be put in place to prevent identity theft, direct attacks against data repositories, and the corruption of business processes. Combating spyware at the desktop is only one element of a comprehensive, defensive posture, but it is an indispensable one.

CREDITS

CREDITS

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

Richard Stiennon, Vice President of Threat Research, Webroot Software Inc.

Paul Piccard, Director of Threat Research, Webroot Software Inc.

The Webroot Threat Research Team

Special thanks to Edward Halteman, PhD, Statistician, who acted as a statistical advisor to the report authors

APPENDIX

More on Categories

System Monitors

The wide availability of easy-to-install and easy-to-use software for monitoring purposes is also creating a dangerous environment both for personal computer use and for protecting corporate assets. Keystroke monitors have evolved rapidly. The primary reason is that hackers have begun to reap rich rewards from employing monitoring software.

A case in point is the situation in Istanbul, which is being mirrored in many places around the globe. There are dozens of Internet cafés in Istanbul, which is the result of a regulated telecom infrastructure. The citizens do not have broadband, so they do their browsing from cafés where the costs are a reasonable million lira per hour (less than a dollar US). The trouble with browsing from public computers, of course, is that you never know what evil lurks on that machine.

In Istanbul hackers installed keystroke loggers to steal online banking account information. Private interviews with five of the top banks in Istanbul revealed that security vulnerabilities were at the forefront of discussions and solutions to these issues was starting to take precedence. A first attempt was to modify the login process so that a virtual PIN pad is presented on the screen and a user has to click on the numbers to enter their PIN. It was only a matter of days until the system monitors captured screen images every time a user clicked the mouse.

A basic system monitor is one that records every keystroke entered at the keyboard. Keystroke loggers are available for purchase from many Web sites because there is a demand for this type of spyware. A parent may want to monitor his or her child's activity on the computer. An enterprise may install keystroke loggers to ensure proper use of computing resources. While these uses are legitimate, there is no way to discern the legitimacy of how a program is used so anti-spyware solutions must identify these legitimate monitoring tools along with the more nefarious products that may have been installed surreptitiously.

Enhancements to keystroke loggers are all about efficiency. In most cases, the criminal is after information like username/password pairs and credit card information. Simultaneously, criminals want to minimize the amount of data to be examined to find the compromising nuggets of information. Thus, system monitors exist that only capture information entered into Web forms or even look for particular matches with string length in the case of a social security number or credit card number. In the case of screen captures, the system monitors have evolved to the point where they only capture the segment of the screen immediately surrounding the cursor.

Spyware that uses a computer's microphone or video camera are in circulation as well. These pose a threat to privacy from targeted installations. In particular, co-workers, spouses, and roommates are likely culprits. A version of the Sub7 Trojan software can turn on a computer's microphone and send any recordings back to the hacker for instance.

Trojan Horses

Trojan horses have many purposes, but the most common is to provide remote control of a computer to a hacker. These computers can then be enlisted in an "army" that is used against targets such as an ecommerce site. Many times the purpose is extortion. If money is not paid, the attack is carried out.

A firewall is an excellent tool to battle Trojan horses. Properly configured, a firewall can prevent a Trojan horse from being effective. Network providers are also beginning to block Trojan horse activity. It is still critical however for end users to use tools to find and remove this type of software from their computers.

Adware

The goal of adware is to drive visitors to advertisers' Web sites. Adware writers and distributors earn revenue every time their adware redirects a browser, displays a pop-up advertisement for viewing, or results in a visited search result link. Using data from Claria's April 8, 2004 S1 filing as well as the reported numbers from a lawsuit filed against Direct Revenue (recently Direct Revenue went through yet another in a long series of name changes to A Better Internet, Inc.) by Avenue Media, it is possible to make some projections about the overall state of the adware business. Using the derived figure of $2.25/year/installation, it is possible to estimate that the adware business generates more than $2 billion a year in revenue.

Clearly, CoolWebSearch dominates the adware business. Little is known of their business operations and CWS is guilty of using some of the most destructive methodologies in their pursuit of infecting and staying on as many machines as possible. See the methodology section for details on this simple calculation.

Tracking Cookies

The question is asked often: Why are cookies included in a spyware audit? The answer draws more on historical perspective than on direct threats to privacy or security. Cookies are small data files generated by servers and downloaded to a directory on users' computers by their browsers.

Consequently, most anti-spyware program users choose to delete cookies. Users delete cookie even in cases where the cookies are benign and system and browser performance is not compromised. Market data organizations view deleted cookies as a threat to their ability to measure the services they offer, but there is no immediate solution that gives users control over their privacy while assuring accurate data for the marketing organizations.

In their most benign state, cookies contain the following characteristics:

- Cookies are anonymous; they contain no information that can identify the user.
- Cookies are encrypted; they cannot be read by third parties or modified effectively by the user.
- Cookies are associated with a single domain or Web site.
- Cookies are transient; they do not reside on a computer longer than the session in which they are used.

While many cookies exhibit these benign traits, even having certain cookies on a computer is objectionable to the average user. In the course of a day, a user may visit hundreds of Web sites. Many users prefer that no record of their online activity be available to the next person to sit down at that computer, so they erase the history of their activity. Yet, a simple investigation of the cookies on their computer reveals the Web sites they have visited and, by inference, their habits and interests.

The Platform for Privacy Preferences Project (P3P), developed by the World Wide Web Consortium (W3C), is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. Until the advent of the P3P initiative to offer best practices in cookie creation and delivery, there was no way to differentiate between cookies that stored personal information and those that respected a user's privacy. The P3P standards that have been developed allow a user to edit settings in their browser configuration to allow or block cookie deposits that comply with several levels of behavior. Unfortunately, most users do not change the default Internet Explorer settings and most creators of cookies disregard the true purpose of the P3P distinctions and simply set flags that attest to a cookie's relative safety with no regard for the actual care with which they treat a user's personal information. It is the historical misuse of cookies, including efforts on behalf of marketing data organizations to imbue cookies with useful data about the user that has led to the mistrust that most users have for cookies.

More on Anti-spyware Legislation

Increased consumer and business concerns about privacy and protection of their computer assets has generated concern and involvement on the part of elected officials at both the Federal and State levels.

As a result, the first part of 2005 has seen many legislative proposals surface. In addition to Federal legislation in both chambers of the U.S. Congress, there have been at least 43 bills introduced across 27 states since January 1, 2005 that specifically reference spyware.

Virginia became the most recent state, and the first in 2005, to enact an anti-spyware law. In March, Utah enacted amendments to their existing law. At the time of printing, bills in Arizona, Arkansas, Georgia, and Washington have passed the legislatures and are awaiting Governors' signatures. Any or all of these may become law by the time this report is issued.

In Michigan, three bills have been passed by the state Senate; and New Hampshire's bill has passed the state House of Representatives.

Meanwhile, in the nation's capital, there is a strong likelihood that Federal legislation will be passed before the end of 2005. US House of Representatives Bill H.R. 29 is awaiting floor consideration and may already be approved by the time this report is published. In the US Senate, S. 687 was introduced in March and will likely receive committee consideration before the summer. While the House and Senate bills differ in their approaches, both Federal bills include provisions that would preempt state legislation, and both would rely on the Federal Trade Commission to establish regulations and enforce the law. State Attorney Generals retain the ability to file suits in Federal Courts on behalf of their citizens.

Based on the legislative activities in the first part of 2005, we expect there will be more to report on this subject in future reports.

APPENDIX

State	Legislation	Summary	Status as of April 18, 2005
ALABAMA http://alisdb.legislature.state.al.us/acas	S.B. 122	Prohibits willfully using computer software to take control of another computer or otherwise attacking operation of another computer.	Introduced February 1, 2005. Referred to Judiciary
ALASKA http://w3.legis.state.ak.us	S.B. 140	Prohibits spyware and unsolicited Internet advertising, in particular "spyware pop-up advertisements".	Introduced March 10, 2005
ARIZONA http://www.azleg.state.az.us	H.B. 2414	Prohibits transmission of computer software, through intentionally deceptive means, that modifies settings, collects personally identifiable information, or takes control of the computer.	Governor signed April 18, 2005
ARKANSAS http://www.arkleg.state.ar.us	H.B. 2904	Prohibits unauthorized installation of computer software and numerous other deceptive practices as detailed in the bill. Violations are actionable as deceptive trade practices. Establishes a spyware monitoring fund.	Sent to Governor April 12, 2005 Passed Senate April 5, 2005 Passed House March 15, 2005
	H.B. 2261	Appropriates funds to cover expenses associated with spyware monitoring for the office of Attorney General.	Passed House April 12, 2005
	H.B. 2344	Appropriates funds to cover expenses associated with spyware monitoring for the Department of Information Systems.	Passed House April 12, 2005
CALIFORNIA http://www.leginfo.ca.gov	S.B. 92	Authorizes the recipient of spyware or software transmitted in violation of the prohibitions to recover damages, and also stipulates criminal penalties.	Passed Senate Judiciary. Committee April 5, 2005
FLORIDA http://www.flsenate.gov	S.B. 2162	Prohibits certain deceptive acts or practices that involve the computer; and prohibits the collection of certain information without notice and consent. Violations are considered deceptive and unfair trade practice and provides for civil action against violators.	Passed Senate Communications and Public Utilities Committee March 28, 2005.
GEORGIA http://www.legis.state.ga.us	S.B. 127	Prohibits deceptive acts and practices with regard to computers and requires notice be given prior the installation of software programs. Provides for civil and criminal penalties, and the recovery of certain damages.	Passed House March 29, 2005 Passed Senate March 11, 2005
ILLINOIS http://www.ilga.gov	H.B. 380	Prohibits unauthorized installation of programs that take control of the computer; modify settings; collect personally identifiable information through deceptive means, and other actions. Makes a violation of the Act a Class B misdemeanor.	Passed House February 8, 2005

APPENDIX

State	Legislation	Summary	Status as of April 18, 2005
INDIANA http://www.in.gov	H.B. 1714	Prohibits the installation of spyware, except when the computer owner consents after full disclosure. Provides for injunctive relief and the greater of actual damages or $10,000 per violation. Permits treble damages for intentional violations. Requires the consumer protection division of the attorney general's office to collect reports of spyware installations.	Passed House Technology, Research and Development Committee February 21, 2005
IOWA http://www.legis.state.ia.us	H.F. 614	Protects owners and operators of computers from the use of spyware and malware that is deceptively or surreptitiously installed on their computers.	Passed House March 30, 2005
	S.F. 465	Relates to the transmission, installation, and use of computer software through deceptive or unauthorized means.	Withdrawn March 30, 2005 (replaced by HF 614)
KANSAS http://www.kslegislature.org	H.B. 2343	Enacts the consumer protection against computer spyware act; prohibiting certain acts and providing penalties for violations.	Introduced February 8, 2005. Referred to Corrections and Justice.
MARYLAND http://mlis.state.md.us	H.B. 780	Prohibits unauthorized persons from modifying computer settings, collecting personally identifiable information, and other actions.	Introduced February 9, 2005 Referred to Economic Matters
	H.B. 945	Prohibits actions similar to H.B. 780, with the addition that such acts are undertaken with actual knowledge or conscious avoidance of actual knowledge.	Introduced February 10, 2005 Referred Economic Matters
	S.B. 492	Prohibits unauthorized persons from modifying computer settings, collecting personally identifiable information, and other actions.	Unfavorable report from Finance Committee March 31, 2005.
	S.B. 801	Prohibits unauthorized persons from modifying computer settings, collecting personally identifiable information, and other actions.	Withdrawn March 31, 2005.
MASSACHUSETTS http://www.mass.gov/legis	S.B. 273	Prohibits installation of spyware on another person's computer; or using a context based triggering mechanism to display an advertisement that interferes with a user's ability to view a website.	Introduced January 26, 2005 Referred to Economic Development and Emerging Technologies
	S.B. 286	Regulates "unconsented" Internet advertising, and requires a clear "opt-in" choice.	Introduced January 26, 2005 Referred to Economic Development and Emerging Technologies

APPENDIX

State	Legislation	Summary	Status as of April 18, 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 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.	
MISSOURI http://www.house.state.mo.us	H.B. 902	Prohibits the unauthorized installation of computer software on consumers' computers when there is actual knowledge or a conscious avoidance of actual knowledge.	Introduced March 31, 2005 Referred to Utilities
NEBRASKA http://www.unicam.state.ne.us	L.B. 316	Prohibits the unauthorized installation of computer software on consumers' computers when there is actual knowledge or a conscious avoidance of actual knowledge.	Introduced January 11, 2005 Referred to Judiciary
NEW HAMPSHIRE http://www.gencourt.state.nh.us	H.B. 47	Provides that using spyware or similar computer programs to knowingly alter, take control of, or damage a consumer's computer or Internet access will be a violation of the Consumer Protection Act.	Passed House February 23, 2005
NEW YORK http://assembly.state.ny.us	A.B. 549	Establishes the unlawful use of spyware and malware as a class A misdemeanor; and a class E felony for a person who has been previously convicted within the last five years of violating this section.	Introduced January 13, 2005 Referred to Codes
	A.B. 2682	Establishes the unlawful dissemination of spyware as a class A misdemeanor. Expands eavesdropping to include information intercepted by spyware. Requires an authorization agreement be provided to computer users prior to software downloads.	Introduced January 28, 2005 Referred to Codes
	S.B. 186	Same as A.B. 2682	Introduced January 10, 2005 Referred to Codes
	S.B. 3600	Same as A.B. 549	Introduced March 23, 2005 Referred to Codes
OREGON http://www.leg.state.or.us	H.B. 2302	Prohibits a person from installing or causing installation of spyware on a computer. Violations are an unlawful trade practice.	Introduced January 11, 2005 Referred to Information Management and Technology

APPENDIX

State	Legislation	Summary	Status as of April 18, 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.	Introduced February 16, 2005 Referred to Judiciary
RHODE ISLAND http://www.rilin.state.ri.us	H.B. 6211	Defines unlawful modification of computer settings, unlawful control of a computer and prohibits the deceptive sale of software.	Introduced March 10, 2005 Referred to House Corporations
TENNESSEE http://www.legislature.state.tn.us	H.B. 1742	Prohibits installation of certain "cookies" on another person's computer. Authorizes injunctive relief, civil damages and treble damages. Precludes class action suits against violators. Requires the establishment of reporting procedures.	Introduced February 16, 2005 Referred to Judiciary
	S.B. 2069	Same as H.B. 1742.	Introduced February 17, 2005 Referred to Commerce, Labor & Ag
TEXAS http://www.capitol.state.tx.us	H.B. 1351	Prohibits unauthorized copying of, or use of computer software for unauthorized purposes. Includes civil penalties.	Introduced February 21, 2005 Referred to Business & Industry
	H.B. 1430	Relates to the installation, copying, or use of computer software for unauthorized purposes; providing a penalty.	Passed Business and Industry Committee April 5, 2005
	S.B. 327	Prohibits unauthorized collection or transmission of personally identifiable data. Prohibits unauthorized installation or disabling of software. Includes civil penalties.	Passed Criminal Justice Committee April 11, 2005
	S.B. 958	Same as H.B. 1430	Introduced March 3, 2005 Referred to Jurisprudence
UTAH http://www.le.state.ut.us	H.B. 104	Amends the Spyware Control Act.	Governor signed March 17, 2005
VIRGINIA http://leg1.state.va.us	H.B. 2215	Amends the Virginia Computer Crimes Act to add unauthorized installation of software, disruption of another computer's ability to share or transfer information and maliciously obtaining computer information as crimes of computer trespass.	Governor signed March 26, 2005 Effective date July 1, 2005
WASHINGTON http://www1.leg.wa.gov/legislature	H.B. 1012	Prohibits unauthorized installation of software and other types of deceptive behavior.	Passed Senate April 11, 2005 Passed House March 9, 2005
WEST VIRGINIA http://www.legis.state.wv.us	H.B. 3246	Adds language regarding spyware to the West Virginia Computer Crime and Abuse Act; includes spyware definition, disclosure requirements and criminal penalties for failure to disclose.	Introduced March 25, 2005 Referred to Judiciary

Methodology

Data Collection

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

Data for the Corporate SpyAudit have been collected since October 2004. The Consumer SpyAudit has collected data since January 2004. Total number of machines scanned for both Consumer and Corporate SpyAudits are:

Consumer & Corporate SpyAudits

Total number of machines scanned

Period	Scans (Consumer)	Scans (Corporate)
Q1 04	345,248	N/A
Q2 04	510,802	N/A
Q3 04	501,162	N/A
Q4 04	977,776	23, 024
Q1 05	1,185,032	12,337

SpyAudit data is collected and aggregated anonymously. No personal or specific computer data is collected with the audit results.

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

Calculations and Formulae

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

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

The Webroot Consumer and Corporate SpyAudits can be accessed by visiting:

Corporate: http://www.webrootdisp.net/entaudit/start/php

Consumer: http://www.webroot.com/services/spyaudit/spyaudit_o3.htm

Calculating Adware Market size. Multiply the average number of pieces of adware times the number of active users on the Internet times the dollars earned per year per installed piece of adware.

- Average pieces of adware per machine = 4.38 (Consumer Spy Audit results, Q1 '05)
- Number of active users = 290 million (Nielsen Netratings)
- Dollars/installation/year derived from Claria S1 filing $90 million/40 million users = $2.25/install/year.
- 4.38 X 290,000,000 X $2.25 = $2.86 Billion

ABOUT
Webroot Software

ABOUT Webroot Software

Webroot Software, a privately held company based in Boulder, Colorado, creates innovative privacy, protection and performance products and services for millions of users around the world, ranging from enterprises, Internet service providers, government agencies and higher education institutions, to small businesses and individuals. The company provides easy-to-use anti-spyware software that guides and empowers computer users as they surf the Web, protecting sensitive information and returning control over computing environments. Webroot's software consistently receives top ratings and recommendations by respected third-party media and product reviewers. The company is backed by some of the industry's leading venture capital firms, including Technology Crossover Ventures, Accel Partners and Mayfield.

In addition to selling these products online at www.webroot.com. Webroot products are found on the shelves of leading retailers around the world, including: Best Buy, Circuit City, CompUSA, Fry's, MicroCenter, Office Depot, Staples, Target and Wal-Mart. Webroot products are also available as either branded solutions or on an OEM basis. To find out more about Webroot, visit www.webroot.com or call 1-800-772-9383.

Online Survey

Please tell us what you would like to see more of, less of and what you liked and didn't like about the State of Spyware report. Visit www.webroot.com/stateofspyware to participate in the survey.

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

Certain data is available upon request.

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

www.webroot.com

Corporate Sales & Support: (800) 870-8102
Consumer Sales & Support: www.webroot.com/support

Fax: (303) 442-3846
Outside of the USA: +1 (303) 442-3813