STATE OF SPYWARE

Q2 2006

A review and analysis of the impact of spyware on consumers and corporations.

webroot
SOFTWARE, INC.

TABLE OF CONTENTS

webroot
SOFTWARE, INC.

F O R E W O R D

Hysterical Blindness

In times of extreme stress, people have been known to experience spontaneous and complete blindness. The condition is unpredictable and untreatable. It simply shows up and goes away with the same mystery. Sometimes I wonder if many spyware sufferers are afflicted by hysterical blindness when it comes to protecting themselves and their information.

We have published the State of Spyware report for over a year now. We originally embarked on the project to provide some perspective on this issue. I remember in 2003 when we first began talking about spyware, we would literally hear people ask "Spy what?" There were few other evangelists in those days and mostly freeware solutions that have since been eclipsed by a threat that simply outpaced their ability to stay in the fight. Without commercial resources to support new research and new methodologies, it was only a matter of time.

The story hit a fever pitch in 2004 when incidents of spyware seemed to be peaking. Many cried over-hype. Many claimed the problem was not that pervasive and even if it were, it wasn't that serious. And maybe they were on to something; the incidents of spyware in 2005 seemed to drop. The most serious flavors of spyware still thrived, but adware was falling and some even predicted it was the beginning of the end. As if spyware had flared dramatically, like a match, but now was burning out.

So this is where the blindness seems to have set in. Even though we at Webroot proffered that spyware was a criminal enterprise and therefore would not go quietly; even though we demonstrated that the incidents of Trojans and system monitors were not waning, people still turned a blind eye to the threat. It was now an old story.

Well, everything old can be new again.

The numbers in this quarter's State of Spyware Report show that spyware is officially back to the same levels it was in 2004 when it hit its supposed peak. For consumers, that is across the board in adware, Trojans and system monitors, which is pretty scary since there are a lot more computers in the world than there were 2004. For enterprises, it's slightly different. IT organizations have done a good job in fighting adware, but the number of much more serious threats – like Trojans and system monitors – remains virtually unchanged since 2004. During the past year, the number and availability of anti-spyware programs on the market have dramatically increased.

Maybe people have decided that spyware is a tolerable condition, like some ailment that is never cured, just contained. Or maybe people think if they just don't pay attention, it will somehow slip back into the shadows from which it first emerged in 2003. That seems pretty blind to me and makes me a bit hysterical.

The good thing about hysterical blindness is that it is temporary. The bad thing is no one is really sure when it wears off. With spyware getting stronger when some think it's getting weaker, we can only hope our collective eyesight comes back sooner than later.

C. David Moll
CEO
Webroot Software, Inc.

THREAT RESEARCH/PHILEAS™

Spyware distributors and spyware writers are hitting home computer users harder than ever before. A number of news stories tell of spyware installing from banner ads on MySpace.com and from popular photo-sharing Web sites, hitting millions of computer users, especially those with unpatched Internet Explorer browsers. Windows Genuine Advantage has made the vulnerability of spyware threats to unpatched systems even more pronounced.

This ambush upon home computer users illustrates that spyware isn't going away and it's leaving a path of victims in its wake. Webroot threat research data suggests that spyware infection rates increase every day as more and more spyware programs are launched across the Internet.

Spyware isn't going away, and it's leaving a path of victims in its wake.

The force behind this continual rise is simple economics. Spyware is highly profitable for spyware villains, who steal billions of dollars every year from unsuspecting computer users and corporations. Considering that Phileas, the Webroot automated threat research tool, has identified more than half a million different potential malware sites since its inception in January 2005, the possibility of infection seems more and more likely.

Consider the story of Tom Stevens:*

Tom only used his computer for reading e-mail, surfing the Web occasionally, and checking his bank account. On a Wednesday night after reading his e-mail, Tom wanted to find the name of a song he heard that day on the radio. He typed the lyrics he could remember into the search engine and numerous lyrics sites appeared. Upon entering the first Web site, Tom's machine froze for a second and then his browser closed; he thought nothing of it and restarted his browser. Tom attempted the search again and this time found the name of the song.

Unbeknownst to Tom, when he re-started his Internet browser, a Trojan horse downloader installed through an Internet browser exploit from the lyric Web site and started downloading other pieces of malware.

As Tom continued to browse the Web, the Trojan horse downloader installed a Trojan called Rebery. The Rebery Trojan remains dormant on a user's machine until they type certain keywords that activate the Trojans logging capability. After browsing the Web, Tom decided to check his bank account before he went to bed. He logged into his bank's Web site, checked his account, and went to bed.

The moment Tom completed typing his bank's URL into the address bar, Trojan Rebery activated its logging feature and logged Tom's username and password for his bank account. Within a few short hours, Trojan Rebery connected to a secret Internet Relay Chat server somewhere in the Czech Republic and uploaded his login information to a bot host machine connected to the server.

Two days later, when Tom logged onto his computer to read his e-mail and browse the Web, Trojan Rebery's logging feature was activated once again and captured Tom's e-mail username and password. After browsing the Web, Tom decided to check his bank

** Fictional user account of common spyware infection method*

account, once again activating Rebery's logging feature. Upon checking his account, Tom noticed that nearly all of his savings were gone; presuming it was a mistake with his bank's Web site, he called customer service. He discovered that an unknown thief transferred the majority of his savings to a number of offshore casino accounts. Tom isn't sure how this happened. After talking with someone at his bank who suspects spyware, Tom takes his PC to a PC repair shop to figure out the problem.

This story isn't unique. Joe Lopez, a Miami businessman, sued Bank of America after $90,000 was stolen from his bank account following a Trojan horse attack. Bank of America denied responsibility in the attack and refused to reimburse Lopez for his losses. Lopez claims that Bank of America failed to protect his account from known risks, such as spyware.

A growing number of threats can attack a computer and steal information.

Detailed Examples of Top Spyware Threats

The user story of Tom Stevens points out the growing number of threats that can attack a computer and steal information. The Webroot threat research team compiled a list of common spyware programs accompanied by an explanation of their characteristics and activities.

Trojan-Downloader-Zlob: Trojan-Downloader-Zlob is a malware downloader that usually masquerades as a free media-codec update for the Windows Media Player. A video code allows users to view different types of streaming media, mostly associated with streaming video clips. Trojan-Downloader-Zlob uses the popularity of these streaming video clips to trick users into installing the Trojan.

A basic example of Zlob's installation technique is a user who comes across a video on the Internet that they would like to watch, but when they attempt to view the video the media player displays an error such as "Media Player is unable to play this video. Please click here to download a new version of codec." The user's browser then redirects to a Web site where they are able to download and install the media-codec. More often than not, users end up downloading this codec, which includes Trojan-Downloader-Zlob. Once executed, Zlob downloads a number of other malware applications onto the computer such as rogue anti-spyware applications, spyware and adware.

180 SearchAssistant: 180 SearchAssistant is an adware program typically bundled with other free software and automatically runs in the background of a user's computer and monitors a user's surfing habits. This program monitors search keywords and Web sites to determine the type of pop-up advertisement or site redirection.

Makers of free software such as some peer-to-peer and toolbar applications occasionally bundle adware programs such as 180 SearchAssistant so they can generate ad revenue from the users installing their software. Usually as a prerequisite to installation, the user must agree with the additional install of 180 SearchAssistant.

Apropos: Apropos is an adware program that can display pop-up advertisements and send information about a user's surfing habits back to their databases. Apropos is one of the more aggressive adware programs on the Internet. Apropos uses techniques of social engineering by way of misleading ActiveX prompts or exploit driven drive-by download sites to have the user inadvertently install their adware. The Apropos program also incorporates rootkit techniques to hide its application files. Apropos does not come with an uninstall feature, and its files are usually obfuscated from users, making removal difficult. Apropos has proven to be one of the more persistent adware applications available on the Internet.

Elite and Perfect Keyloggers: Elite and Perfect Keyloggers are system monitors that allow an attacker to create an installer bundled with a benign application. The attacker can then use social engineering techniques such as e-mailing a Windows update bundled with the keylogger to the victim. The keylogger installs on the victim's computer along with the legitimate application. In the case of Elite Keylogger the system monitor process is concealed completely from the victim and is able to bypass firewall software by injecting its code into Internet Explorer. This allows Elite Keylogger to begin e-mailing usernames, financial information and passwords to the attacker without any indication to the victim.

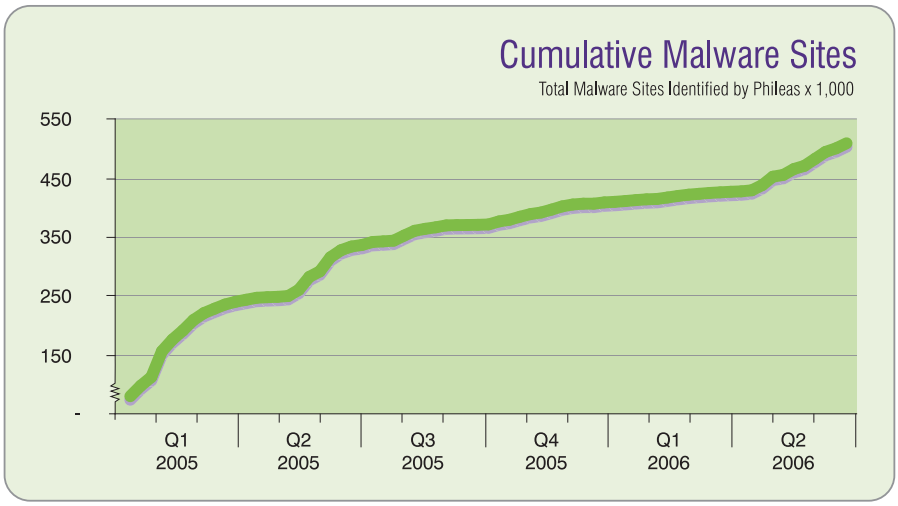
Additional Spyware Threats

- **WebSearch Toolbar**: An Internet Explorer toolbar that may hijack your Web searches.
- **Lopdotcom**: A pay-per-click search portal that places numerous Web site shortcuts on your desktop, adds Web sites to your Favorites folder, and changes your default search engine pages.
- **Trojan-Backdoor-SecureMulti11**: A Trojan horse that may allow a hacker to gain unrestricted access to your computer when you are online.
- **Virtumonde**: May display advertisements on your computer.
- **ISTbar**: A toolbar that may be used for searching pornographic Web sites, which display pornographic pop-ups and hijack user homepages and Internet searches.
- **SurfSideKick**: May display advertisements on your computer.
- **DirectRevenue-ABetterInternet**: Commonly known as VX2 or Transponder, is an adware program that may display pop-up advertisements on your computer.
- **DollarRevenue**: An adware bundler that may install other adware programs on your computer.
- **CoolWebSearch**: CoolWebSearch (CWS) may hijack any of the following: Web searches, home page and other Internet Explorer settings.
- **PurityScan**: PurityScan is an adware program that may display pop-up advertisements on your computer. This program has been downloaded repeatedly by users of MySpace.com.

Web Crawler Automation

Using Web crawler automation, a crucial form of technology that searches for threats before they affect users, Phileas has identified 527,136 potentially malicious sites to date.

As new discovery techniques develop, Phileas is updated, ensuring detection of the latest threats. To accomplish this, dozens of servers with high bandwidth Internet connections control an army of "bots" that scour the Web for sites containing malware.

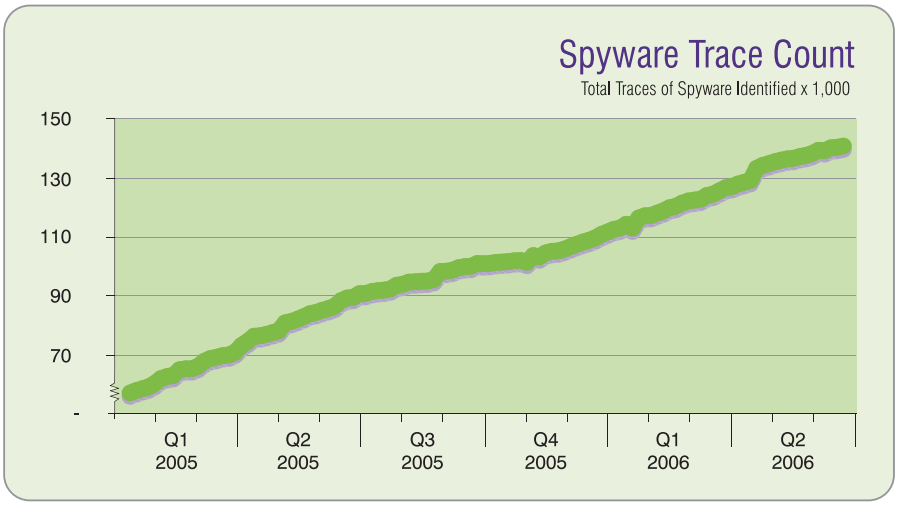


The increase in the number of identified potentially malicious Web sites is bolstered by the launch of Phileas V – the next generation of Webroot's automated spyware research system designed to proactively seek out the most malicious types of spyware and malware. Phileas debuted in January 2005 as the first automated anti-spyware research system and dramatically enhances Webroot's anti-spyware definition database and detection capabilities.

Phileas V builds upon the phenomenal success of the original system with several technical enhancements to more effectively fight the spyware plague, including a multi-tiered bot network that employs advanced research techniques, like deep packet sniffing. This and other advanced technologies ultimately improve Phileas' ability to discover new threats more quickly, accurately and efficiently than ever before.

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

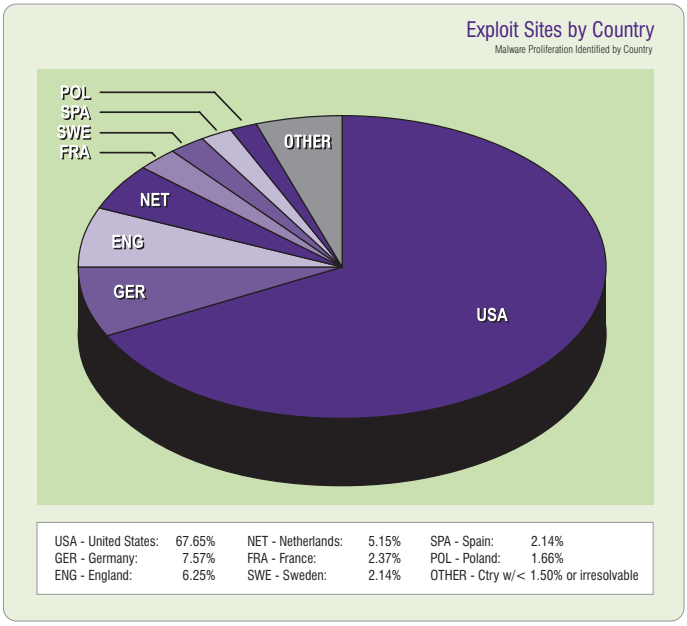
Last quarter, Webroot identified more than 10,000 traces of spyware. The current total number of spyware traces identified by Phileas is over 144,000.



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

Top Countries Hosting Spyware

According to recent Phileas statistics, more than 67 percent of the spyware exploits originate from the United States, followed by Germany with more than 7 percent, and the United Kingdom with just over 6 percent.



The proliferation and attainability of various Internet connections in the United States may be the cause for this continuing high percentage. Security analysts suggest that the increasing proliferation and attainability for Internet-enabled devices may also be responsible for the high numbers in the European Union.

E N T E R P R I S E

During Q2 2006, enterprises continue to confront spyware programs on a number of fronts. Motivated by regulatory compliance and protecting intellectual property, many corporations have turned to anti-spyware tools to stay ahead of the spyware offensive.

Unfortunately, not all corporations have dodged the bullet when it comes to spyware infection. More than 40 companies reported security breaches during the past quarter. 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. Recently, a number of Internet blogs reported that hackers hit Flagship Studios to steal the source code for Hellgate: London. Company officials aren't admitting the theft, but some industry analysts point to a keylogger as the culprit. According to blog postings, losing this intellectual property may delay the release of the game.

More than 40 companies **reported security breaches during the last quarter.**

Infection rates remain high despite the fact that many corporations have deployed an anti-spyware tool. IDC estimates that only 30 percent of corporations haven't added an anti-spyware program to their security arsenal.

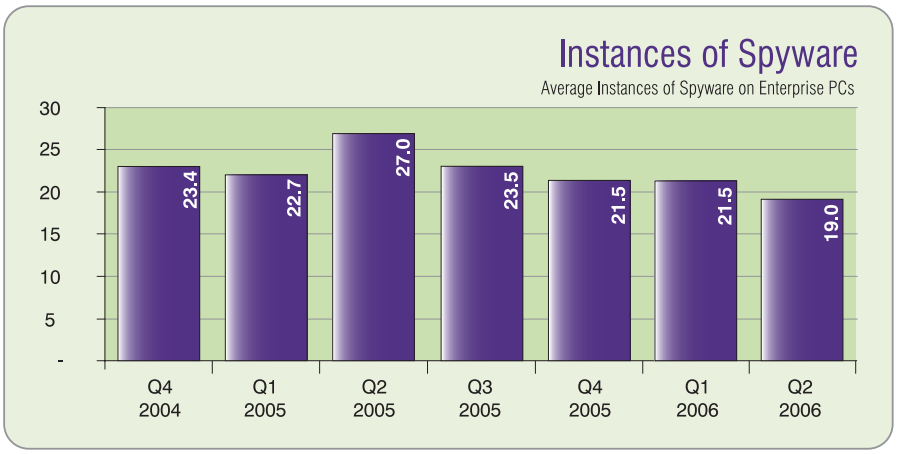
The steady spyware infection rates in corporations suggest that enterprises may be relying on inadequate anti-spyware programs, such as suites or freeware, to protect their networks. These solutions have the capabilities to detect and remove the most primitive programs, but leave malicious programs behind. Sophisticated Trojan horses and system monitors can easily avoid detection by anti-virus and freeware programs.

Surprisingly, larger technology companies tend to **lag behind most other industries in adopting security technologies.**

As seen in the Flagship Studios example, security incidents at corporations can take a heavy toll and the ramifications of spyware attacks on the businesses themselves are particularly disturbing.

Overall Findings

In Q2 2006, Spy Audit was run on 19,480 enterprise PCs in 71 countries. The majority of PCs scanned were in the United States (59 percent), Italy (12 percent), the United Kingdom (7 percent) and Belgium (4 percent). On infected enterprise PCs, the average instances of spyware declined slightly to 19 from 21.5.

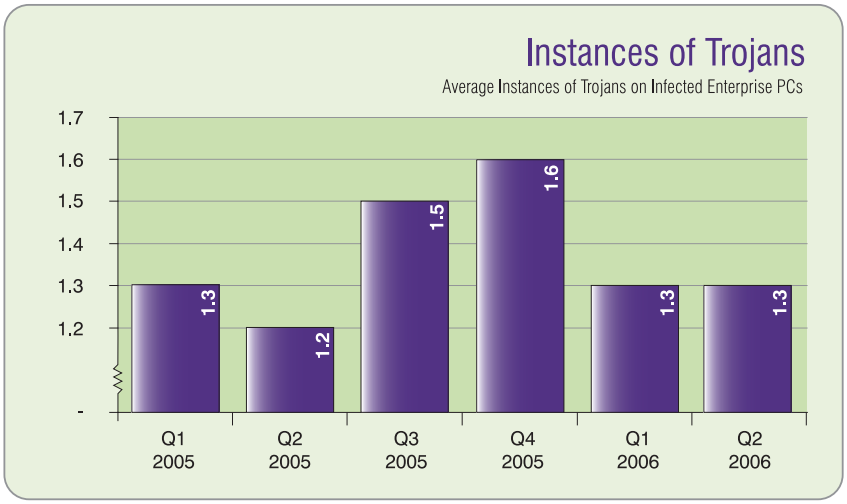


Global Infection Rates

Of the 70 countries that performed Spy Audit scans, 18 of these countries had more than 1,000 scans performed in Q2. Australia had the highest average number of spies detected for enterprise PCs: 37.7. Mexico and Switzerland also had high infection rates with 29.4 and 21.4, respectively.

Trojan Horses

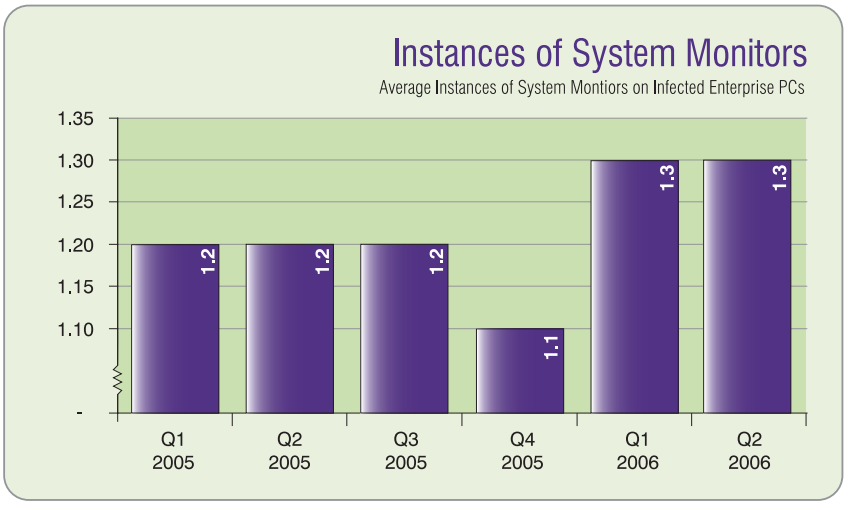
The consistent number of Trojans indicates that enterprises are relying on legacy anti-virus programs or have deployed perimeter anti-spyware solutions to protect their networks. Unfortunately, because sophisticated spyware acts at the desktop level, rather than the network level, spyware writers intentionally write programs that can avoid detection at the perimeter. Enterprises that solely rely on this defense are using just one layer of defense. The average instances of Trojan horses within enterprises held steady at 1.3 instances per infected PC in Q2 2006.



The most common Trojan horse detected on enterprise PCs was RASDialer, which is a Trojan dialer that is capable of hijacking modems to dial toll numbers that access paid Web sites. Mexico, Poland and Brazil had the highest infection rates of Trojans on enterprise PCs in Q2 2006.

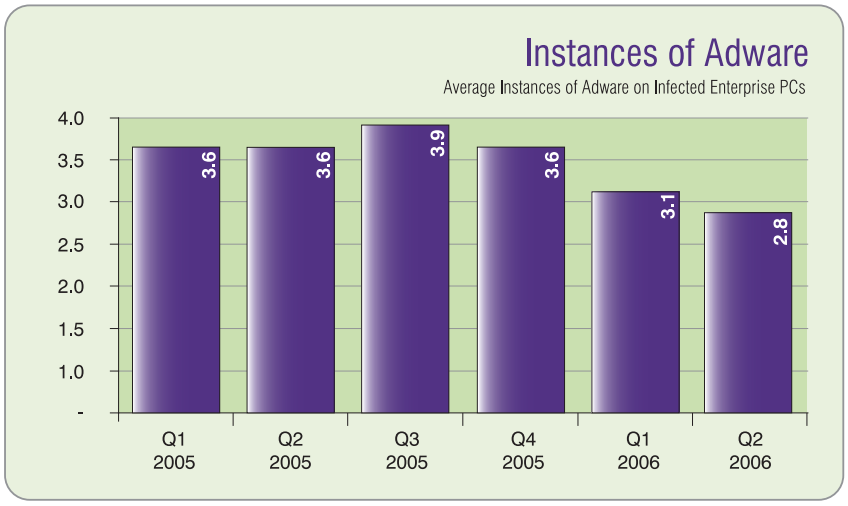
System Monitors

As we've seen quarter over quarter, online criminals continue to use sophisticated system monitors to capture information, such as personal logins and other passwords. On PCs with system monitors, the average number of instances held steady at 1.3 instances of system monitors per infected PC. Enterprise PCs in Mexico, Spain and China had the highest infection rates of system monitors.



Adware

Adware rates declined on enterprise PCs. PCs with adware had an average of 2.8 adware infections in Q2 2006, down from 3.1 in the first quarter. More and more enterprises have adopted anti-spyware solutions to protect against spyware. The simple versions of adware are typically detected by anti-virus solutions or freeware solutions.



C O N S U M E R

Spyware incidents continue to make headlines around the globe. As spyware writers become more sophisticated and more cutthroat, home computer users are paying the price.

Security analysts report that spyware writers are stooping to all-time lows when it comes to targeting consumers. Spammers now use spyware to make their e-mail campaigns more successful. There have been reports of crafty spyware writers creating false profiles on MySpace to target the large install base of teenagers and young adults using the popular Web site.

As spyware becomes more sophisticated and cutthroat, computer users are paying the price.

Despite the publicity about the dangers of spyware, infection rates are on the rise. Webroot spyware scan data shows that 89 percent of consumer PCs are infected with spyware. U.S. home computer users are infected with an average of 30 pieces of spyware on their PCs.

Spyware writers are constantly modifying their programs and installation methods to avoid detection. They are using rootkits and driver-level technology to hide from anti-spyware programs. Many free anti-spyware programs simply aren't capable of finding these sophisticated spyware programs.

As the Webroot Threat Research team discovered with a particularly malicious program, "Trojan-Phisher-Rebery," online criminals use malicious Web sites, common software vulnerabilities, and keylogging software to harvest information from unsuspecting Web surfers.

Not only do free anti-spyware programs offer a false sense of security, so do anti-virus products. Most anti-virus programs do not effectively detect and remove malicious spyware and the more complex adware threats, especially spyware programs that use advanced obfuscation procedures like rotating encryption and compressed algorithms.

To make matters worse, as spyware writers find a way to access a home computer, it's the home computer user who is left holding the bag – financially, that is. In many cases, spyware infection can result in identity theft, which can take time and money to recover. Individuals hit with spyware can lose thousands of dollars as their bank accounts and credit cards are pillaged by these online criminals. A Bank of America customer lost almost $90,000 when a Trojan horse captured his password and login information. Bank of America denied responsibility and has refused to reimburse the customer for his loss.

Most anti-virus programs do not effectively detect and remove malicious spyware.

Q2 2006 Overall Findings

Overall spyware infection rates continue to rise for the third straight quarter. The second quarter of 2006 saw an increase in the share of consumer PCs infected with spyware: from 87 percent in Q1 2006 to 89 percent.

This increase in spyware infections suggests that although home computer users are adopting anti-spyware programs, they are choosing inadequate programs to protect their computers or not keeping their programs up-to-date.

Before installing an anti-spyware program, home computer users should evaluate the program's ability to detect and remove all types of spyware, especially malicious programs. In addition, given how quickly spyware programs morph and evolve, the best anti-spyware programs should offer daily defensive definition updates.

Global Infection Rates

During the second quarter of 2006, Puerto Rico had the highest average number of spies detected: 42.6 per scanned PC. Algeria and Bahrain also had high infection rates with 38.4 per scanned PC and 35.7, respectively.

Global Rates of Spyware

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

Q2 2006 Rank	Country	Quantity
1	Puerto Rico	42.6
2	Algeria	38.4
3	Bahrain	35.7
4	Dominican Republic	35.1
5	Trinidad & Tobago	33.8

Looking at the 95 countries with 500 or more PCs scanned in Q2 2006, the average number of spyware traces found was 24.5 spies. The United States was above average with 30 spies detected.

European Infection Rates

Internet use continues to increase throughout the European Union, with nearly half of the EU population using the Internet at home or on mobile devices. Spyware sources have targeted this growing population as a new market for their malicious programs.

The United Kingdom, Ireland and Lithuania still have the highest infection rates in European countries. Ireland and the United Kingdom swapped places since Q1 2006. Now the United Kingdom records the highest number of spies per PC in Europe, while Ireland comes in second, followed by Lithuania.

European Rates of Spyware

Highest Number of Spyware per 1,000 PCs Scanned in Europe

Q2 2006 Rank	Country	Quantity
1	United Kingdom	30.5
2	Ireland	30.3
3	Lithuania	29.3
4	Latvia	26.5
5	Norway	26.1

Asia Pacific

Consumer PCs in Singapore have the highest number of spies in Asia at 31.5. Australia was second with 25.6 spies per PC, followed by New Zealand with 25.3 spies per PC. Internet use throughout Asia has grown more than 200 percent since 2002 and now accounts for just over 35 percent of the entire world's Internet use, more than any other region. In Singapore alone, more than two-thirds of the population uses the Internet at home or work. As access to the Internet rises, spyware writers have more users to target.

Asia Pacific Rates of Spyware

Highest Number of Spyware per 1,000 PCs Scanned in Asia Pacific

Q2 2006 Rank	Country	Quantity
1	Singapore	31.5
2	Australia	25.6
3	New Zealand	25.3
4	Thailand	22.7
5	Hong Kong	22.4

Malicious Spyware

In the second quarter of 2006, Trojan horse infection rates increased to 31 percent, up from 29 percent in Q1. Trojans increased from 1.9 instances on infected PCs to 2.0 instances.

The most common Trojan horse detected was Trojan-Downloader-Zlob, which is a Trojan downloader that may download other threats onto user's computers. According to Webroot spyware scan data, there were more than 1 million counts of this Trojan horse on consumer PCs during Q2 2006.

Global Trojan Horses

During Q2 2006, Dominican Republic had the highest infection rates for Trojans at 1,099 per 1,000 PCs scanned, compared with the worldwide average of 504 Trojan horses.

Global Rates of Trojan Horses

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

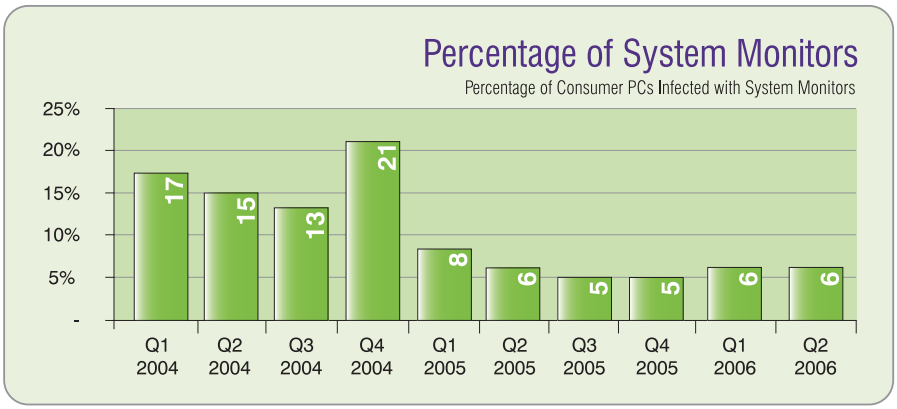
Q2 2006 Rank	Country	Quantity
1	Dominican Republic	1099
2	Algeria	1023
3	Trinidad & Tobago	1010
4	Monaco	1000
5	Iceland	991

System Monitors

Frequently, spyware purveyors rely on Trojans to install sophisticated system monitors to capture personal information, like bank account information or credit card numbers.

Webroot spyware scans revealed that system monitors are present on 6 percent of infected machines during Q2 2006, the same percentage as last quarter. This steady rate may indicate that malicious spyware, like system monitors, remains the modus operandi for a majority of online criminals.

The most common system monitor detected was Perfect Keylogger. Perfect Keylogger is a monitoring tool that records all visited Web sites, keystrokes and mouse clicks. According to Webroot spyware scan data, there were more 43,000 counts of this system monitor during Q2 2006.



Global System Monitors

In the second quarter of 2006, Yemen had the highest infection rates of system monitors with 426 per 1,000 PCs scanned, followed by Vietnam with 356 instances. The world average was 61 system monitors per 1,000 PCs scanned.

Global Rates of System Monitors

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

Q2 2006 Rank	Country	Quantity
1	Yemen	426
2	Vietnam	356
3	Zimbabwe	236
4	Libya	220
5	Qatar	207

Adware

Adware continues to be a burden to home computer users. Webroot spyware scans show a steady infection rate of 59 percent. This stable infection rate is yet another indication that home computer users aren't using the best anti-spyware tool available.

Federal Trade Commission Actions

Previous State of Spyware reports have provided information about the spyware enforcement actions brought by the Federal Trade Commission (FTC). While the FTC has not filed any new cases in the first half of 2006, actions in two of the previously filed cases were announced. These include:

Federal Trade Commission v. Seismic Entertainment Productions, Inc., SmartBot.net, Inc., and Sanford Wallace

United States District Court, District of New Hampshire – FTC File No. 042 3125

The Court issued a default judgment against Wallace and Smartbot.Net that ordered them to give up $4,089,500 in ill-gotten gains. The order also barred them from downloading spyware onto consumers' computers; from downloading any software without consumers' consent; from redirecting consumers' computers to sites or servers other than those the consumers selected to visit; from changing any Web browser's default home page; and from modifying or replacing the search features or functions of any search engine. A settlement with defendants OptinTrade and Jared Lansky bars the same practices that are barred in the Wallace and Smartbot.Net judgment. Lansky, an ad broker who disseminated ads containing Wallace's spyware, will give up $227,000 in ill-gotten gains.

Federal Trade Commission v. Odysseus Marketing, Inc., and Walter Rines

United States District Court, District of New Hampshire – FTC File No. 042 3205

The Court issued a revised preliminary injunction against Odysseus and Rines. It bars them from downloading spyware without consumers' consent, and from disclosing, using or further obtaining consumers' personal information, pending trial.

The Webroot report "State of Spyware 2005: The Year in Review," issued earlier this year, provided information about the actions taken in the other three spyware cases filed by the FTC to date, including:

Federal Trade Commission v. Max Theater, Inc, and Thomas L. Delanoy

United States District Court, Eastern District of Washington

Federal Trade Commission v. Trustsoft, Inc. (doing business as Swanksoft and Spykiller), and Danilo Ladendorf

United States District Court for the Southern District of Texas – FTC File No. 052 3059

Federal Trade Commission v. Enternet Media, Inc., Lida Rohbani; Conspy & Co., Inc.; Nima Hakimi, Baback (Babak) Hakimi; and Nicholas C. Albert

United States District Court, Central District of California – FTC File No. 052 3135

U.S. Federal Legislation

While both the House and Senate have passed spyware legislation, no action has been taken to reconcile differences between the bills as needed to produce a final piece of legislation to send to President Bush.

U.S. State Legislative Actions

In the first half of 2006, Louisiana, Rhode Island and Tennessee enacted new spyware laws, bringing the total number of states with specific spyware laws in effect to 15. Oklahoma also passed a spyware bill, HB 2083, however, the text of the bill was completely changed during the conference committee. As a result, the final version of HB 2083 that was vetoed by the Oklahoma Governor did not contain any spyware-related provisions.

As of July 20, 2006, spyware bills are still pending in California (as amendments to the existing spyware law), Illinois, Massachusetts, Michigan, New York, North Carolina and Pennsylvania.

Over the past couple years, another dozen states have had spyware bills pending, however these legislatures have all adjourned for the year, curtailing any additional activity on their bills.

IT Security under Basel II – New Challenges in the War against Spyware

Basel II is a collaborative effort by the 13 countries that comprise the Basel Committee on Banking Supervision to revise international standards for measuring the adequacy of a bank's capital. Basel II has become a common term in the European Union to refer to bank's IT security and how to best manage security risks.

In short, Basel II aims to improve risk sensitivity and measurement for the three major risks a bank faces:

- Credit risk
- Operational risk
- Market risk

Operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events."

It's no secret that modern information technology creates vulnerabilities that can affect companies and enterprises worldwide. For businesses that rely on electronic data to be readily accessible and accurate, such vulnerabilities can have serious economic consequences. Spyware has become one of the pre-eminent security threats to today's computer systems. The use of spyware to engage in information theft, data robbery, external fraud and fraudulent misrepresentation makes it a particularly important threat to businesses. In addition, the loss of data due to spyware attacks may itself result in considerable financial losses if, for example, development or research data is compromised. Spyware can also jeopardize a bank's compliance status, implicate data protection laws, and compromise bank managers. Reasonable investments in anti-spyware solutions can, therefore, improve technical security and lead to direct financial benefits.

C O N C L U S I O N

As the Q2 2006 State of Spyware reveals, spyware continues to beat computer users – both at home and at work. In the end, spyware victims are left with financial damage as the dangerous threats show no signs of letting up.

It's no secret that spyware is costly for home computer users – wiping out savings accounts, stealing identities and damaging computers. But, it's even more frightening that home computer users become infected by visiting mainstream Web sites, such as MySpace.

Enterprises have realized the threat, but are taking inadequate action against the dangers of spyware. As the enterprise Spy Audit data revealed, a number of enterprises still have spyware infections, despite adopting some type of anti-spyware software. As the spyware scourge continues to grow, it comes down to having the right protection.

ABOUT WEBROOT

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 1-800-870-8102.

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

Certain data is available upon request.

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

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