STATE OF SPYWARE

Q1 2009

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

webroot
SOFTWARE, INC.

TABLE OF CONTENTS

Foreword	1
Threat Research/Phileas™	2
Enterprise	6
Consumer	9
Legislation	14
Conclusion	15
About Webroot Software	16

webroot
SOFTWARE, INC.

F O R E W O R D

Spyware's Second Act

The concept of one-hit wonders is well known in modern life. Andy Warhol once posited that everyone will be famous for 15 minutes. F. Scott Fitzgerald offered that there are no second acts in life. Each seemed to imply there is a single chance to attract meaningful attention and then it's time to fade into obscurity again.

If only it were true for spyware.

Webroot has been tracking the proliferation of spyware since 2003. What began as a slow, yet steady, spread of spies across consumer and corporate landscapes quickly erupted into a mushroom cloud of malware infections. Unprotected users scrambled to safeguard their PCs and networks while anti-spyware software developers like Webroot doubled and then tripled their education, research and development efforts. Like any outburst, the rampant destruction eventually began to wane and during the past few quarters, we have witnessed infection rates begin to slow and even decline for the more common and more benign -- albeit annoying and interruptive -- adware.

Unfortunately, while we live in a land that disdains and creates has-beens all at the same time, we also love a good sequel. The obvious idea is that if it worked once, then it's bound to be successful again. Spyware writers must ascribe to this maxim, because just as we began to feel like the tide may be turning, we experienced the most substantial increase of spyware in months. Welcome to Spyware 2.

Our research this quarter reports a significant up-tick in adware and overall infection rates along with steady growth in other more malicious and threatening malware. We have speculated that a number of reasons could be behind this dramatic comeback – new distribution methods, renewed efforts by criminals to take advantage of the opportunities posed by the adware industries, or new, advanced research technologies – but whatever the reason, the results remain the same: this is simply another battle in a war that has no foreseeable end. And in this current battle, as documented by this quarter's State of Spyware Report, adware is on the offensive.

The tagline to one of the Jaws sequels was "Just when you thought it was safe to go back in the water...." We may all be able to relate to that after reading this quarter's report. In a memorable line from that Jaws sequel, the police chief, contemplating another eventful summer, says "I'm not going through that again!" We probably all wish spyware was a flash in the pan and had no second act, but like Chief Brody, we know the threat is out there and no matter how much we wish it would go away, there's a shark in the water and we had better be prepared.

C. David Moll
CEO
Webroot Software, Inc.

THREAT RESEARCH/PHILEAS™

Spyware companies and spyware writers continue to refine their malicious programs to evade detection and removal. This refinement includes using new, advanced techniques to infect as many machines as possible while continuing to operate under the radar.

One trend that became apparent in 2005 and continues today involves the implementation of auto-updating technology embedded in spyware programs to avoid detection. This sophisticated skill serves as a reminder that the constant changing of threats requires the anti-spyware industry's undivided attention.

New Distribution and Obfuscation Methods

Trojan and viral procedures in spyware continue their reinvention and implementation. Advanced obfuscation procedures like rotating encryption and compression algorithms are still used by spyware writers on an almost daily basis. Rootkit-like behavior is growing by attempting to hide files from core Windows Application Programming Interfaces (the most direct way for software programs to interact with a Windows system) and detection processes.

Some of the more malicious spyware writers include code to stop detection services for popular virus scanning software. Known spyware is blocking outbound Internet connections from detecting update services for popular scanning engines. By reusing code from viruses and Trojans, spyware has become increasingly difficult to detect.

Phishing Trojans

Phishing Trojans have garnered much press coverage since their inception in the late 1990s. A large amount of the initially released phishing Trojans attempted to steal passwords and serial numbers for commonly used applications and games. Phishing Trojans gradually declined as transport procedures and installation techniques became stale. Now there is a re-emergence of phishing Trojans in the last year, but even more so during the past six months.

Security insiders attribute this spike in phishing Trojans to the released source code for common Trojan downloads and new Trojan phishers. These new phishing Trojans include code updates implementing rootkit-like functionality and advanced obfuscation procedures. The implementation of these new obfuscation procedures makes the collection of secure information (credit card numbers, bank account information, social security numbers, etc.) much easier.

Phishing Trojans are now changing weekly.

Currently reusing common code between Trojan phishers makes the variants harder to track. Phishing Trojans are now changing weekly, and targeting common financial, auction and popular Web sites for the broadest infection rate.

Keylogger Advances

As in 2005, keyloggers continue to use kernel-level drivers, not only making them more robust and stable, but also extremely difficult to detect. In fact, some keyloggers use process blocking techniques to actively stop anti-spyware programs from running.

Keyloggers are becoming **more aggressive.**

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

Throughout the range of commercial and non-commercial system monitors, keyloggers are becoming more aggressive and are no longer content to merely evade a computer's operating system.

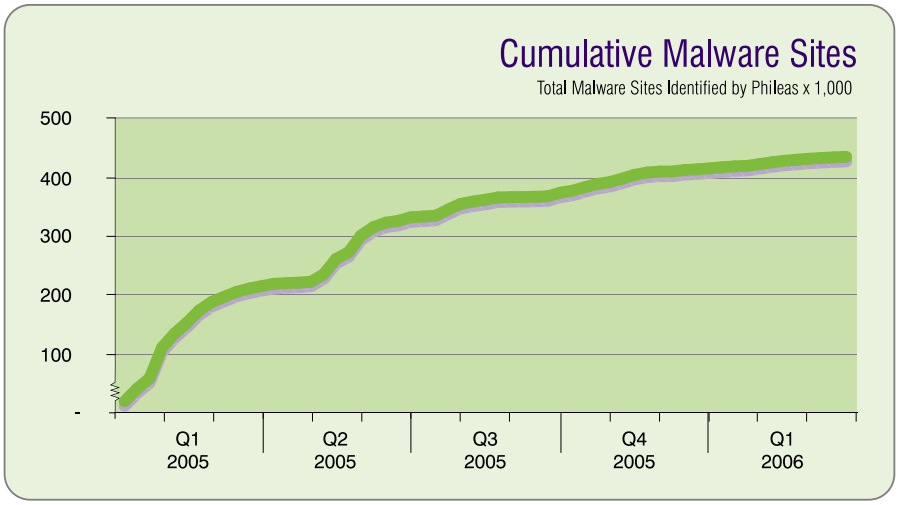
Changes in Adware

As more and more computer users and companies adopt anti-spyware tools, many adware companies revised their use of spyware tactics. Some adware companies continue to use malicious techniques to increase their user base by adopting sophisticated techniques used by malicious spyware writers to evade detection and removal. Many of these programs continue to download adware programs onto a machine without the user's consent. Frequently, adware will download a toolbar without consent, but also serves advertisements and hijacks browser settings.

Web Crawler Automation

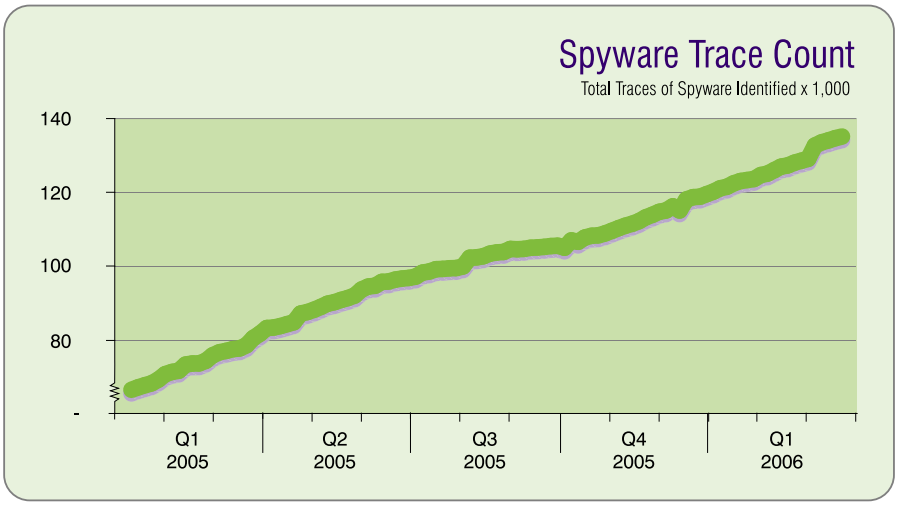
During the first quarter of 2006, Webroot identified more than 24,000 sites hosting spyware, bringing the total number of sites identified to nearly 427,000. Webroot uses Phileas, a patented technology to search for threats before they affect users.

An automated tool such as Phileas is the best way to track the rapid growth of spyware. The Webroot Threat Research team identified a trend that indicates that there are at least 10 variants for each spyware program identified.



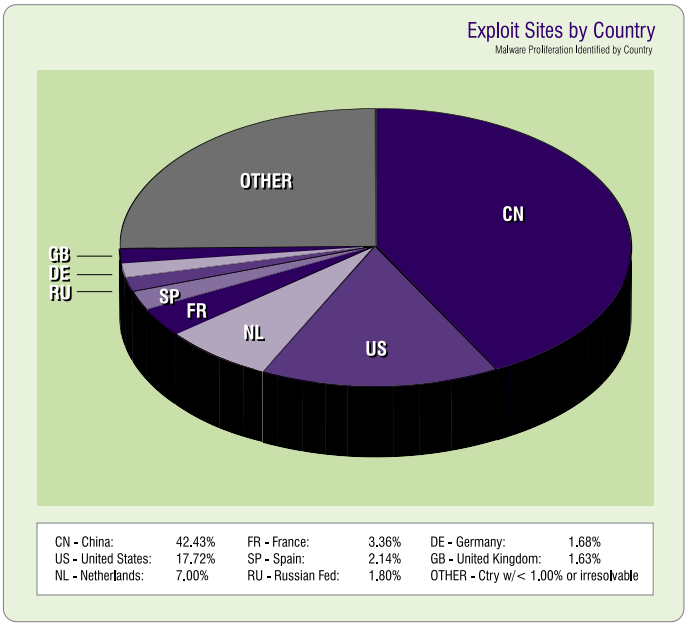
As spyware purveyors continue to modify their programs to evade detection, each program becomes more and more complicated with supplementary associated traces. In other words, a single spyware program has more traces associated with it than the earlier generation of less sophisticated programs.

Last quarter, Webroot identified more than 14,000 traces of spyware. The current total number of spyware traces identified by Spy Sweeper is more than 135,000.



Top Countries Hosting Spyware

According to recent Phileas statistics, more than 42 percent of the spyware exploits originate from China, followed by the United States with more than 17 percent. China and United States have switched positions from Q4 2005, when the United States hosted the largest number of spyware sites, followed by China.



One reason for China's hosting growth could be due to pending anti-spyware legislation in the United States driving spyware writers to less monitored and regulated countries. In addition, the proliferation and attainability for wireless Internet-enabled devices may be responsible for these increasing high numbers.

Top Spyware Threats

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

It is important to note that four of the top 10 threats are Trojans, which further illustrates the rise of malicious spyware.

Trojan-Downloader-Zlob: Trojan-Downloader-Zlob is a common downloader that may download other threats on your computer.

Perfect Keylogger: Perfect Keylogger is a monitoring tool that records all visited Web sites, keystrokes and mouse clicks.

HotBar: HotBar is a toolbar that comes in two versions: a free version that is adware-supported and may display pop-up advertisements and a paid version. The paid version does not include adware or display pop-up advertisements.

Trojan-Backdoor-us15info: Trojan-Backdoor-us15info is a Trojan which runs in the background and may collect information about your computer and DNS packet information. Once collected, this information can be sent to a destination specified by the author.

Trojan-Backdoor-SecureMulti: Trojan-Backdoor-SecureMulti is a Trojan horse that may allow a hacker to gain unrestricted access to your computer when you are online.

Trojan Downloader Matcash: Trojan Downloader Matcash is a downloader that may download other threats on your computer.

Virtumonde: Virtumonde may display advertisements on your computer.

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

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

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

E N T E R P R I S E

During Q1 2006, enterprises continued to confront a high number of complex spyware programs, such as system monitors and Trojan horses.

To stay ahead of the spyware offensive, many of these enterprises have adopted anti-spyware tools. In fact, the IDC and other industry analysts declare that roughly 70 percent of corporations have deployed an anti-spyware solution.

To maintain compliance with federal regulatory initiatives, such as FDIC, HIPAA, Gramm-Leach-Bliley Act and Section 5 of the FTC Act, corporations have been forced to rethink their data security measures.

The looming question of how spyware may jeopardize compliance with these regulations has compelled many companies to incorporate anti-spyware solutions as part of their overall security plan.

Webroot spyware scans continue to detect **a high number of spyware programs.**

Unfortunately, Webroot spyware scans continue to detect a high number of spyware programs. This may indicate that enterprises are relying on inadequate anti-spyware programs, such as freeware.

Other enterprises may expect their anti-virus solution to detect and remove these dangerous programs, without realizing that most anti-virus programs can't detect extremely sophisticated spyware programs.

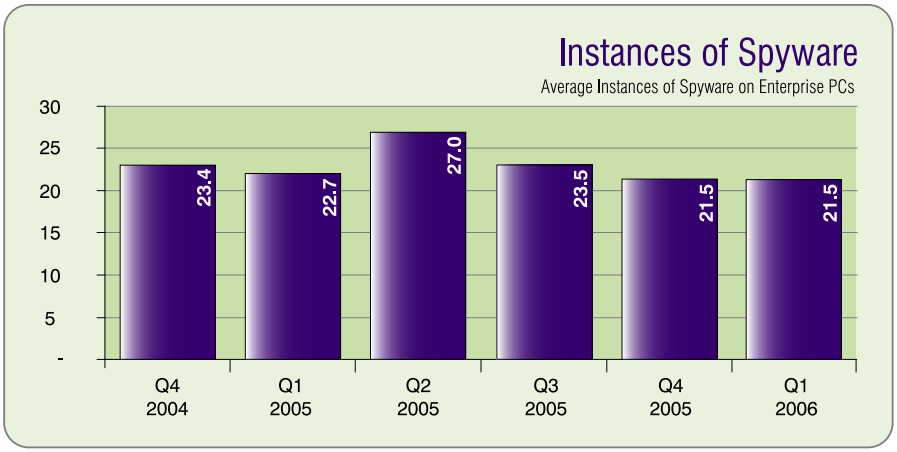
Another area of concern is related to small business. Small businesses are especially attractive to spyware criminals due to their often limited IT resources and lack of network security. According to a survey of small businesses conducted by Webroot, more than 50 percent of small and medium-sized businesses experienced a spyware attack during the first quarter of 2006.

The ramifications of these spyware attacks on the businesses themselves were particularly disturbing. Sixty-five percent experienced slowed system performance, 58 percent reported a reduction in employee productivity, 35 percent experienced a negative impact on their bottom line and 20 percent reported a loss in sales.

Fifty percent of small and medium-sized businesses **experienced a spyware attack during the first quarter of 2006.**

Overall Findings

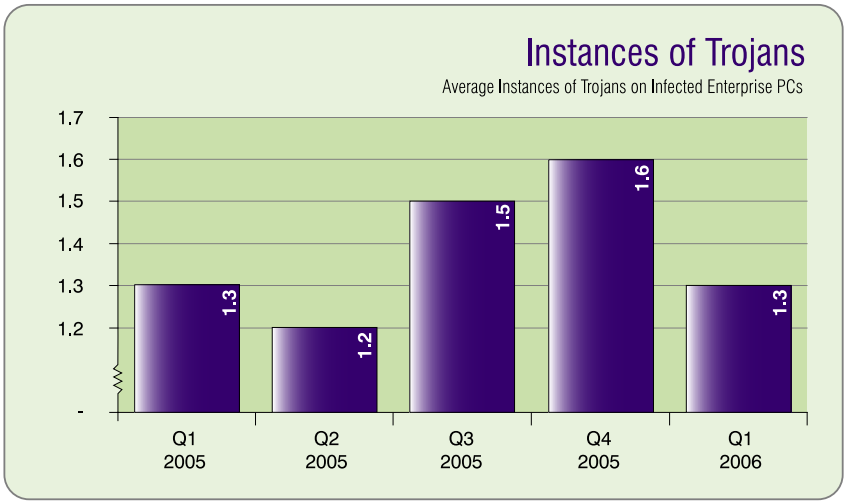
In Q1 2006, Spy Audit was run on 19,480 enterprise PCs in 71 countries. The majority of PCs scanned were in the United States (59 percent), Italy (12 percent), the United Kingdom (7 percent) and Belgium (4 percent). On infected enterprise PCs, the average instances of spyware held steady at 21.5.



Additional Enterprise Findings

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 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.

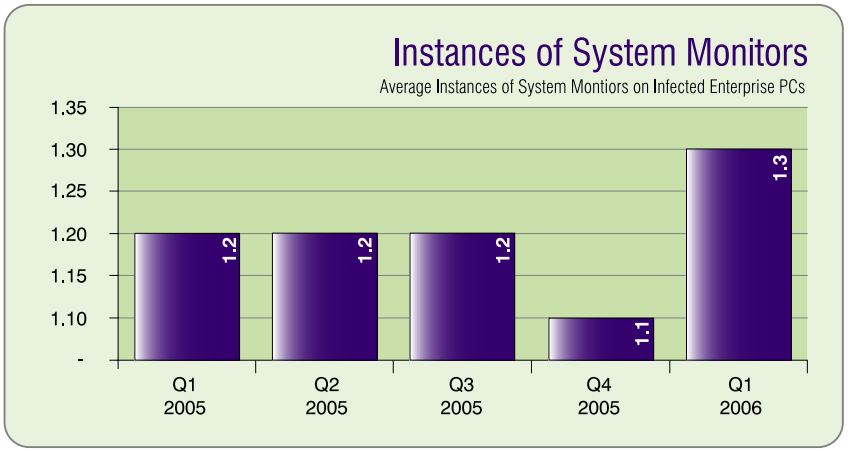
The average instances of Trojan horses within enterprises decreased slightly during Q1 2006 from 1.6 instances per infected PC in Q4 2005 to 1.3 in Q1 2006.



System Monitors

Seeking a way to gain access to networks, online criminals use sophisticated system monitors to capture personal logins and other passwords.

On PCs with system monitors, the average number of instances increased this quarter to 1.3 from 1.1 instances of system monitors per infected PC in Q4 2005.



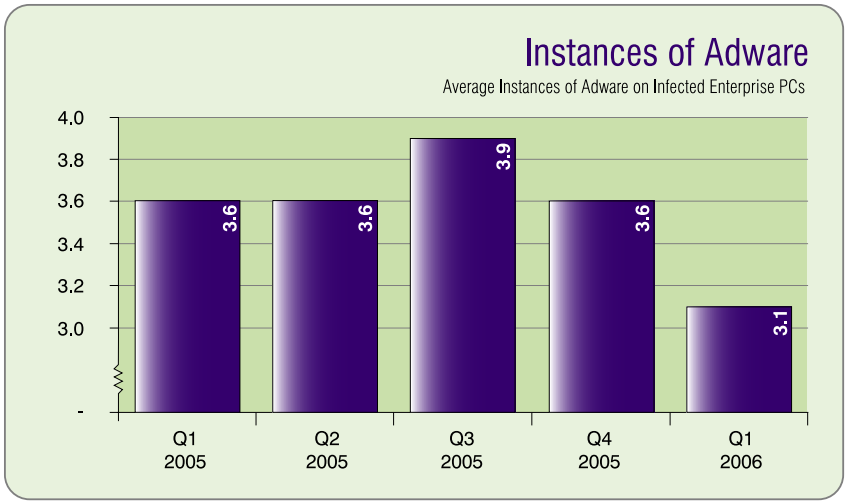
On PCs with system monitors, the **average number of instances increased.**

Adware

More and more enterprises have adopted anti-spyware solutions to protect against spyware. Simple spyware programs are easy to detect, even for antiquated anti-virus solutions or freeware solutions.

As a result adware rates declined somewhat on enterprise PCs. PCs with adware had an average of 3.1 adware infections in the Q1 2006, down from 3.6 in the fourth quarter of 2005.

However, because adware infections can lead to a high number of help desk calls, removing adware is a key concern for enterprises.



Adware infections can lead to **a high number of help desk calls.**

Worldwide Problem

A growing number of home computer users have heeded the warnings about spyware infections and the risks it poses by adopting anti-spyware technology as part of their computer security plan.

Even in the face of this high awareness level, malicious spyware programs such as Trojan horses and system monitors continue to infect more and more home computer users.

U.S. home computer users are infected with an average of thirty-four pieces of spyware.

Webroot spyware scan data shows that 87 percent of consumer PCs are infected with spyware. In fact, U.S. home computer users are infected with an average of 34 pieces of spyware on their PCs.

Security analysts blame this increasing infection rate on the adoption of free anti-spyware programs that use outdated technology and don't provide immediate threat definitions to combat against new and emerging threats.

In other words, spyware writers frequently modify their programs to avoid detection. Moreover, spyware authors use rootkits and driver-level technology on a growing basis to avoid detection and removal. To guard against new spyware programs, home computer users must use an anti-spyware program with frequent definition updates and engines that are capable of removing the toughest spyware from deep within the operating system. Unfortunately, users who only install free anti-spyware programs do not get access to frequently updated definitions and versions.

Other consumers turn to anti-virus products to protect against spyware. Most anti-virus programs can't effectively detect and remove spyware, especially programs using advanced obfuscation procedures like rotating encryption and compression algorithms.

A man in Washington state was ordered to pay $84,000 in victim restitution.

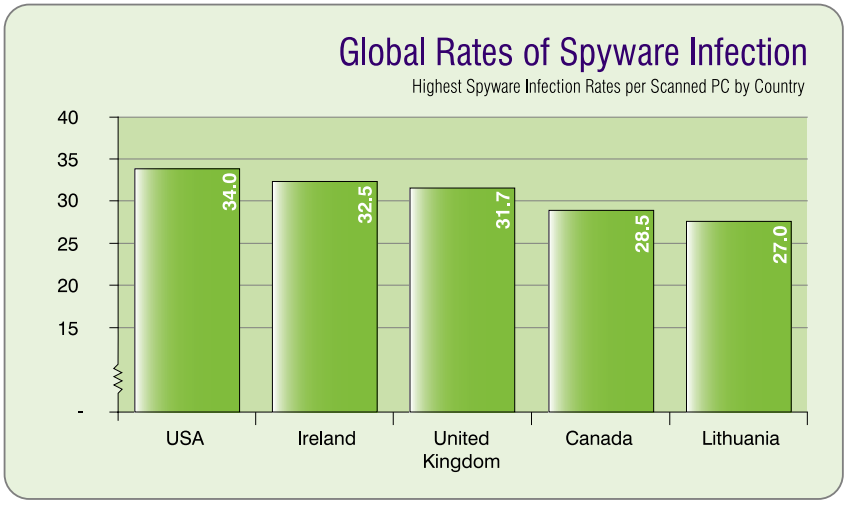
To make matters worse, scam artists are cashing in on this heightened awareness by offering bogus, or "rogue" anti-spyware products. Some of these rogue anti-spyware products are associated with known distributors of spyware and have been known to install spyware themselves.

Police and government officials are starting to take notice of this real threat. A man in Washington state was ordered to pay $84,000 in victim restitution for his part in selling fake anti-spyware programs.

Global Infection Rates

Consumers from 115 countries ran scans for spyware in Q1 2006. The United States had the highest average number of spies detected: 34 per scanned PC. Ireland and the United Kingdom had similar infection rates, with 32.5 per scanned PC and 31.7, respectively.

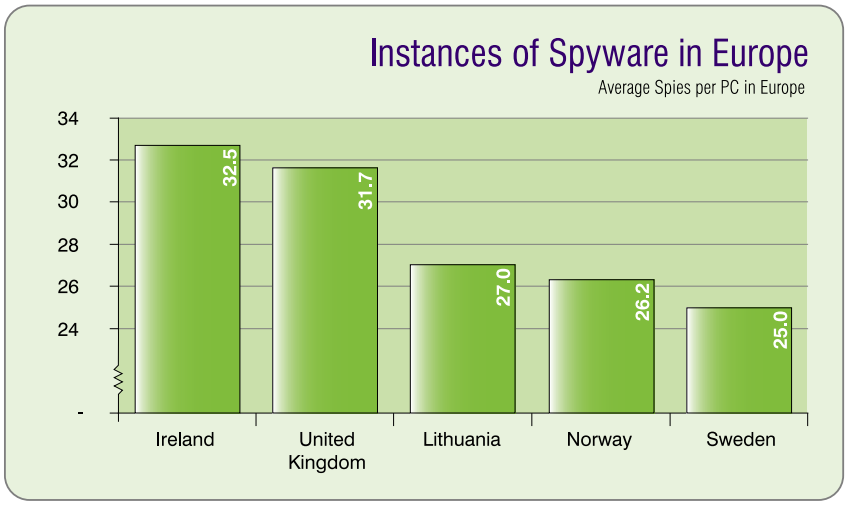
Looking at the 47 countries with 500 or more PC scans in Q1 2006, the average number of spyware traces found was 21.5.



European

Internet usage continues to increase throughout the European Union. In fact, statistics indicate that nearly half of the EU population (49.8 percent) use the Internet at home, work or school. It's easy to connect the dots. As the number of home computers rises, spyware sources have more users to target.

Ireland still records the highest number of spies per PC in Europe. The United Kingdom replaces Norway for second place, followed by Lithuania.



Asia Pacific & Australia

Consumer PCs in Australia and Hong Kong have the highest average number of spies: 26.3 and 23.1 respectively. Internet use throughout Asia accounts for just over 35 percent of the entire world's Internet usage, more than any other region. Europe comes in second at 28.5 percent, followed by North America at 23.1 percent.

PCs in Australia and Hong Kong have the **highest average number of spies.**

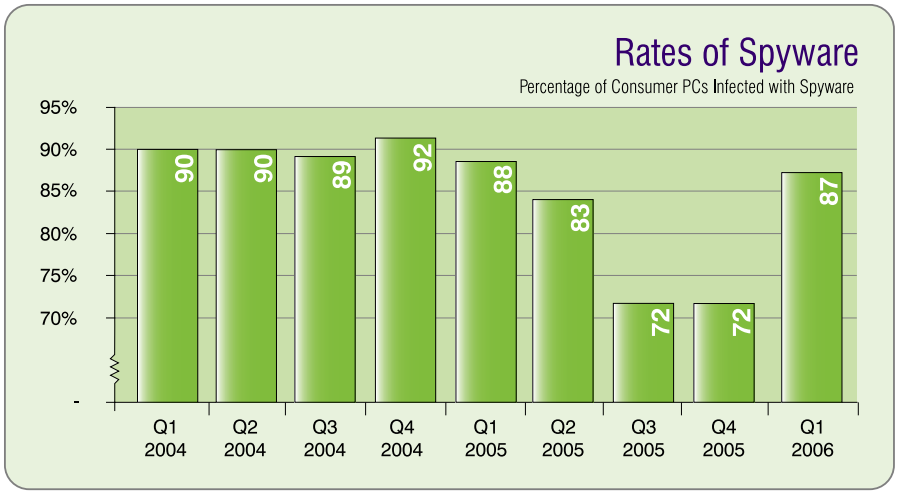
Global Rates of Spyware

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

Q1 2006 Rank	Country	Quantity
1	Australia	26.3
2	Hong Kong	23.1
3	New Zealand	22.7
4	Thailand	22.4
5	Korea	19.2

Q1 2006 Overall Findings

The first quarter of 2006 saw a 15 percentage point jump in the share of consumer PCs infected with spyware: from 72 percent in Q4 2005 to 87 percent.



Despite higher adoption rates of anti-spyware software by home computer users, Q1 2006 showed an increase in spyware infections. This increase demonstrates that although people are using anti-spyware tools, they aren't using the best tools available. Home computer users need to evaluate an anti-spyware program's ability to detect and remove all types of spyware, especially malicious programs.

In the first quarter of 2006, the average instances of spyware increased 18 percent from Q4 2005. Infected PCs had an average of 29.5 instances of spyware in the first quarter of this year, an increase from 24.9 instances in the last quarter of 2005.

Trojan Horses

In Q1 2006, Trojan horse infection rates increased to 29 percent, up from 24 percent in Q4 2005. The instances of Trojan horses on infected PCs increased in the first quarter. Trojans increased from 1.9 instances on infected PCs to 2.0 instances.

The most common Trojan horse detected was Trojan-Downloader-Zlob (TDzlb1). The overall incidence of Trojan-Downloader-Zlob more than doubled from 3.2 percent of computers scanned in Q4 to 6.7 percent in Q1.

Global Trojan Horse Rates

In the first quarter of 2006, Poland continues to report the highest incidence of Trojan horses, jumping from 863 in Q4 2005 to 1,064 in Q1 2006.

Global Rates of Trojan Horses

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

Q1 2006 Rank	Country	Quantity
1	Poland	1064
2	Croatia/Hrvatska	783
3	Slovenia	726
4	Mexico	682
5	Turkey	660

System Monitors

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

Webroot spyware scans revealed that system monitors, which also fall under the umbrella of malicious spyware, are present on 6 percent of infected machines, a slight increase from the 5 percent reported in Q4 2005.

Global System Monitors

In the first quarter of 2006, Iran had the highest incidence of system monitors with 198 per 1000 PCs scanned. Bulgaria followed right behind with 197 incidences.

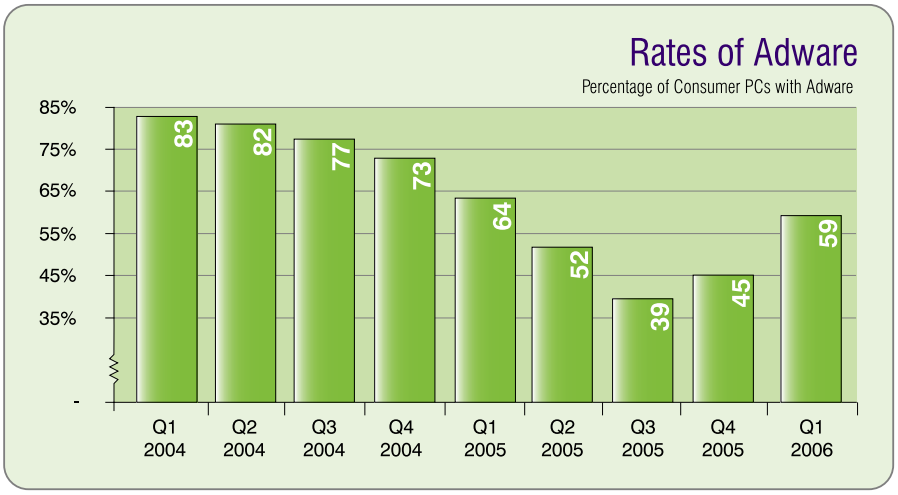
Global Rates of System Monitors

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

Q1 2006 Rank	Country	Quantity
1	Iran	198
2	Bulgaria	197
3	Peru	170
4	Egypt	152
5	Brazil	135

Adware

The prevalence of adware is on the rise, an indication that some adware vendors have found new ways to infect PCs. Spyware scans conducted in Q1 2006 found that the percentage of PCs with adware increased to 59 percent, up from 45 percent in the last quarter of 2005.



Not only is adware more prevalent, but the infections are worse. The average instances of adware on infected PCs increased from 6.1 in Q4 2005 to 6.7 in Q1 2006.

As adware vendors adopt and deploy malicious spyware techniques to increase their install base, adware infection rates may continue to rise.

L E G I S L A T I O N

Federal Legislative Update

In March, the U.S. Senate passed S.1608, the U.S. Safe Web Act. The bill, introduced by Senator Gordon Smith (R-OR), gives the Federal Trade Commission greater authority to collaborate with international law enforcement agencies to investigate cases involving illegal spam, spyware and cross-border fraud and deception.

State Legislative Update

State legislatures continue to work to enact new spyware laws. Since 2004, 12 U.S. states have enacted legislation, and as of April 15, 2006, spyware bills are currently pending in 17 additional states.

C O N C L U S I O N

As the Q1 2006 State of Spyware reveals, spyware continues to plague Internet users – both home computer users and enterprises – and shows no signs of letting up. Spyware writers constantly develop new techniques and advanced distribution methods to infect users to steal information for financial gain.

It's important to recognize that consumers and enterprises have taken steps to protect their information by adopting anti-spyware tools and other Internet security measures. However, it now comes down to having the right protection.

Meanwhile, the effects of passing state and federal legislation to protect computer users and corporations alike from the threat of spyware are beginning to take hold. Washington state's attorney general recently charged a man under Washington's 2005 Computer Spyware Act for selling fake anti-spyware tools.

But the coast is far from clear. Webroot Threat Research team reports that spyware writers will refine their sophisticated tools and techniques, such as using rootkits, to insidiously install their spyware. Strategic use of a desktop anti-spyware is a necessary measure to protect personal information and corporate data.

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.

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