TREND MICRO

Defending Against **Spyware**

Spyware at Work: A Pervasive Threat

Standard Virus Protection Is Not Enough

A Trend Micro White Paper I July 2006

Ed English
Chief Technical Officer, Anti-Spyware

DEFENDING AGAINST SPYWARE

CONTENT

TREND MICRO™

DEFENDING AGAINST SPYWARE

I. INTRODUCTION

The startling growth and deceptive methods of spyware can be easily attributed to profit motives. Spyware developers make money from the information that their software silently collects from unsuspecting users. Companies that create spyware can be small or large. They do not require extensive resources to begin making money from the information they gather or steal. As long as there is a way to make money from it, spyware will continue to proliferate.

THE THREAT IS REAL

- According to FBI research, 80 percent of companies experience spyware problems.[1]
- Threats that contain spyware components more than doubled in 2005: 65 percent of the top 15 threats contained a spyware or grayware component.[2]
- IDC reports that their IT respondents now consider spyware the second worst threat, up from fourth place in 2004.[3]

II. NEITHER FREEWARE NOR REGULAR ONLINE SCANNING ALONE PROVIDE ENOUGH PROTECTION

Although there are numerous freeware programs and online scanning services that attempt to address the spyware threat, neither method alone offers sufficient protection

- Some free anti-spyware applications identify Microsoft operating system processes as spyware. Removing the identified process could damage the operating system
- Even freeware from a reputable vendor can have problems. The free Microsoft™ Windows™ Defender spyware removal tool misidentified Symantec's™ Norton Antivirus as a harmful program[4]
- Free anti-spyware applications can actually be spyware in disguise. These applications can cause new problems rather than solving them
- Using freeware in a business may violate end-user licensing agreements (EULAs)
- Support from freeware vendors is often inconsistent at best. A look at sample license agreements highlights the low level of support provided (see the sidebar for examples)

An antivirus vendor can make the lives of IT administrators easier by providing better interoperability and potential integration of security solutions. With an online scanning tool such as Trend Micro™ HouseCall™ (http://housecall.trendmicro.com), administrators can help clean up problems and evaluate the effectiveness of their current anti-spyware software. But even using HouseCall by itself is not a complete solution. Organizations need real-time protection to defend against spyware.

TREND MICRO™

SAMPLES OF FREEWARE END-USER LICENSE AGREEMENTS

Support from vendors that offer free anti-spyware applications is often inconsistent at best. The following excerpts from their license agreements suggest a poor level of support.

"I tried my very best to make the code of Spybot-S&D as stable as possible…"

"…You expressly agree that your use of the program(s) is at your sole risk."

"Spybot-S&D is dedicated to the most wonderful girl on earth."

"I cannot guarantee that your system will be running the same as before."

III. WHY CAN'T LAWS TAKE CARE OF SPYWARE?

- Laws that define the use of spam and spyware applications as a crime do not stop their development
- Laws help prosecute offenders, but they do not dissuade developers from creating spyware to make money
- Organizations that create and distribute the threats can be moved offshore, making it difficult for governments to find and prosecute the spyware developers

IV. HOW DOES SPYWARE DIFFER FROM VIRUSES?

In the age of broadband, wireless, and network interconnectivity, businesses benefit from faster and wider-ranging information exchange. Yet along with the high capacity and mobile connectivity comes numerous threats to computer productivity, data integrity, and confidentiality. In addition to hackers, computers can be attacked by malicious code.

The top two categories of malicious code computer threats rated by IDC respondents are now viruses and spyware.[5]

TREND MICRO™

Viruses Vs. Spyware

VIRUSES (INCLUDING WORMS AND TROJANS)	SPYWARE
THREAT SEVERITY	
• Ranked as top threat by IDC respondents[6]	• Ranked as second most significant threat by IDC repondents[6]
IMPACT	
• Immediate or delayed damage to computer systems • Downtime • Loss of data • Support costs • IT cleanup time	• Slowed productivity • Theft of confidential information • Invasion of privacy
PURPOSE	
• Damage—destruction of files or network connectivity • Rapid spread • Notoriety	• Profit—by collecting login information, passwords, personal information, Web surfing habits, and more, spyware can generate money for the companies that develop or distribute the malicious code
PROPAGATION METHOD	
• Infected files • Company or personal email • System vulnerabilities • Silent “drive-by” Web downloads	• User-permissioned installation of freeware, which might include a confusing EULA • Silent “drive-by” Web downloads and updating methods
CLEANUP	
• Antivirus software finds signatures files and identifies patches for vulnerabilities used to spread the virus	• Manual cleanup is difficult—spyware can update itself or reinstall itself if incompletely removed • Anti-spyware needs to identify suspect files and allow customization of whitelists and blacklists
PREVENTION	
• Keep systems patched • Do not open unknown emails • Use multi-layer antivirus protection for multiple entry points (desktop, Internet gateway, email server)	• Use anti-spyware that actively blocks installation, finds and completely eradicates spyware, and removes questionable cookies • Do not use freeware programs in general, and freeware anti-spyware in particular

FIGURE 1. Differences between viruses and spyware

TREND MICRO™

V. A BRIEF HISTORY OF THREATS

The first recorded widespread instance of a computer threat occurred in 1986 when a piece of code started to replicate itself to other floppy disks and files. Because of the code's ability to self-replicate and spread, the code was called a "virus." This was the first of many viruses, which are now a mature and continuously evolving threat. Viruses and their variations (including worms and Trojans) disrupt business by damaging computer systems and data. The proliferation of viruses has led to the creation of the antivirus industry, formed to protect business and consumer computers by battling viruses.

Spyware, first identified in 2002, was initially considered by antivirus companies to be another type of virus. Those antivirus companies believed they could cure spyware by simply adding to their antivirus pattern files. But, as antivirus companies eventually came to realize, spyware is not a virus. The defense against it requires new strategies.

Who Creates Viruses and Spyware?

Viruses are designed to propagate. They are written with the goal of generating notoriety and providing the coder with "fifteen minutes of fame." Most virus writers are:

- Experimental—they are trying to hone their programming skills
- Disgruntled—they often want to get back at someone in their organization for treating them badly
- Rebellious—they are frequently teens
- Seeking attention—they are trying to demonstrate how cool or smart they are

By spraying the world's computers with the equivalent of electronic graffiti, virus authors seek to achieve one or more of the following goals:

- Grabbing headlines
- Being popular in their underground communities
- Showing off their programming prowess
- Wreaking havoc in the digital world

Spyware programs, on the other hand, are written by software developers to support the goal of a company for which they work. The goal is normally commercial in nature: These companies want to generate revenue. Spyware is the equivalent of a cash register or ATM. Spyware authors have many ways of making money, and they invent new revenue schemes constantly.

To maximize revenue, spyware must be installed on many computers and communicate back to a mothership Web server. Most spyware is adware. Adware makes the writer's company money by displaying certain advertisements or by hijacking Web browsers, forcing users to pages that can generate revenue for the authors.

Spyware is not always developed or deployed by an organized group. Using open source programs, even some amateurs can create spyware. At the same time, however, some spyware is created by very skilled engineers.

Spyware at Work

GENERATION OF REVENUE	USER IMPACT	SYMPTOMS
SPYWARE		
• Registers with affiliates to major portals • Receives generous bounties per click or per unique user	• Degradation of systems • Loss of privacy and personal information • Denial of service • Fraudulent clicks for portals, causing inflated ad rates and bankrupting advertising	
KEYLOGGING		
• Build detailed profiles on everything you do • Lift credit card number to buy items • Gain access to financial accounts • Conduct corporate espionage	• Identity theft • Compromised IT security systems	None—the goal is to work transparently to keep collecting information
ADWARE		
• Inserting ads or forcing users to Web sites • Advertisers pay adware developers per click or unique visitor		An increase in the number of ads
GRAYWARE		
Same goals, but EULA may not have been read		

FIGURE 2. Spyware at work

TREND MICRO™

How Do Authors Learn to Create and Propagate Viruses, Spyware, and Their Variations?

Virus writers are often part of a group that exchanges information via the Internet to improve on their ability to develop viruses, propagate code, and damage computer networks, businesses, and systems. They create malicious code with the hope of gaining notoriety, not money. Of course, since many viruses are often produced by a one-person development team, those viruses frequently contain buggy and nonworking code.

Spyware authors, who are frequently backed by a revenue-generating company, often have more extensive resources at their disposal. Those resources are funded by their spyware "product" proceeds.

- Spyware authors can afford to have a development process, complete with labs and a testing environment, to apply quality assurance to the programs that they are developing.
- Some mainstream advertisers willingly provide revenue to spyware companies by paying for advertising.
- Most spyware authors have access to books on targeted systems and software development. They also have the ability to purchase legitimate software and take professional development training classes. Their companies apply proven, defined development, testing, and release cycles to their spyware "product." The authors are like typical software developers working in a corporation working toward revenue goals. The primary difference is the nature of the code they produce.

VI. AREN'T VIRUSES AND SPYWARE ILLEGAL?

Since viruses often lead to the loss of data or corruption of a computer system, they are viewed as malicious, and governments have made it illegal to create this type of code. Authorities tend to publicize the capture of virus authors to deter those aspiring to create new viruses. To avoid being arrested, charged, fined, or imprisoned, virus writers seek anonymity.

The spyware industry operates in a more gray legal area. Some freeware, such as an electronic wallet that keeps track of credit card numbers and passwords, might function as spyware and show ads based on a user's shopping habits. But a user may feel the functionality of the freeware is worth the invasion of privacy and the inconvenience of seeing some ads pop up.

Plenty of spyware looks like formal software, even offering an official EULA. The EULA lends legitimacy to the software, which users do not experience with viruses. But users should not equate the presence of a EULA with a legitimate product.

FIVE SIGNS THAT A EULA MAY BE FOR SPYWARE

1. The EULA openly states that it installs software that collects your personal information or Web surfing history.
2. The EULA is very long, perhaps more than 20 pages of legal language, which no average person can reasonably be expected to read or understand in its entirety.
3. The EULA is partly on a Web site (which can be easily changed) or requires you to check the Web site for any changes.
4. The EULA states that a user implicitly agrees to any and all changes by continuing to run the software.
5. The EULA includes double negative statements, such as "Do you want to discontinue the uninstallation?"

By providing a EULA that tells the user what the software does, companies hope to gain consent for their software. For companies that work against the spread of spyware, the presence of a EULA makes it more difficult to classify the software as malicious, since users may have agreed to the software's function.

TREND MICRO™

VII. HOW DO VIRUSES AND SPYWARE GET DISTRIBUTED?

A virus spreads without user permission and has multiple routes of infection. In the early days of viruses, computer systems contracted viruses when the user opened infected files on floppy disks, executed infected applications, or ran infected applications. Today, viruses are spread more frequently when a user opens an infected email attachment. Infections can also be introduced through system vulnerabilities—places where the operating system or an application allows a virus to run, take control of a system, or do whatever it is designed to do. Even surfing the Web can infect a computer. If a user has not patched system vulnerabilities, a simple Internet connection can infect a computer system.

By contrast, spyware is often installed by the user. Frequently, spyware is bundled with freeware that a user purposefully downloads. For example, a simple agreement to install a plug-in for a Web site a user visits can introduce spyware.

In some cases, the EULA may reveal with specificity the intent of software to monitor computer usage and transmit information to the Web for the spyware company's purposes. Spyware companies benefit from the low numbers of people that actually read EULAs in their entirety, especially when they are long. Most people just click "Yes, I Agree," without bothering to read the full agreement.

Spyware companies will pay a bounty for each installation of their spyware. Some freeware authors may be tempted to bundle spyware payloads in with their freeware as a way to generate revenue.

VIII. WHAT IS THE USER EXPERIENCE DURING INSTALLATION?

Viruses tend to hide their installation so they can avoid detection and continue to spread for as long as possible. Virus writers design viruses so that when an infected file or attachment is executed, system performance does not degrade and the user sees no error messages or notification. Viruses are also designed so that they will not interfere with common computing tasks. Since the goal is wide propagation and damage, the writers attempt to hide installation and propagation from the user as much as possible.

Spyware tends to be installed through a user's action and sometimes with the user's permission. But spyware frequently employs questionable means of obtaining that permission. The spyware EULAs may include confusing questions, messages, or links that attempt to trick the user into agreeing to something they do not fully understand. Some EULAs attempt to make the user agree without reading or understanding the consequences of the EULA.

Often spyware applications install additional spyware as well. The user may not understand that he or she gave permission for the bundled spyware.

IX. WHAT ARE THE SIGNS THAT A VIRUS OR SPYWARE IS ALREADY RUNNING IN THE BACKGROUND?

Because the virus author's intent is to spread the virus widely, virus writers hide both the installation and propagation process from the user. By avoiding detection, viruses can spread more widely. The user often has no indication, no notification, and no error messages to indicate a virus is present. The only sign is the damage done to the computer before the virus moves onto other computers.

Spyware also employs stealth techniques. Despite the presence of pop-up ads and freeware that constantly show colorful targeted information, spyware is designed to hide the fact that it is spying on the user. Spyware wants to stay unnoticed. It does not want to bring attention to itself, or it risks being uninstalled. The spyware itself, however, typically does not damage the computer—its goal is just to keep revenues coming in by operating silently.

X. HOW DIFFICULT IS IT TO GET RID OF THESE THREATS?

Viruses are designed to spread, not stay installed on a single computer.

- Traditional viruses that infect boot sectors and files can be addressed either by using an antivirus solution or by deleting infected files.
- Newer viruses infect systems in ways that render cleaning or deleting the main component ineffective. These viruses are tenacious and work against straightforward eradication. While this type of virus is resident in memory, it can restore a recently deleted physical file and then revive itself when the computer is rebooted or certain applications are opened. It may even attach to system files, making it necessary to reboot the system to completely remove the virus.

Spyware, on the other hand, is designed to remain installed in a single system. Because spyware companies want to retain their revenue stream, spyware is often written so its removal is very difficult.

- Using the computer's "Add/Remove Programs" utility may only remove only spyware's visible parts, while allowing the collection agent to remain.
- If a user attempts to remove the spyware, the application's components may reinstall the original spyware or ask the user a confusing question to trick him or her into allowing a reinstall.
- Frequently, spyware binds itself to the freeware it came with so that the freeware cannot be used unless the spyware is also installed. This forces the user into an all-or-nothing dilemma.
- Spyware exhibits a strong will to live—profitably—on one machine. It does not spread to other computers as viruses do. Spyware can function as a virtual ATM, generating cash for its creators, but only as long as it can keep running on a computer.
- Spyware programs often go to great lengths to stay alive or to reinstall themselves once they are detected.

XI. WHY CAN'T STANDARD ANTIVIRUS SOLUTIONS FIND AND ELIMINATE SPYWARE?

Antivirus companies protect against new viruses by updating the signatures, or earmarks, of viruses and by improving the methods of scanning for viruses.

Spyware is a relatively new threat, but it presents rapidly growing problems for all types of users, from consumers to small- and medium-size businesses to large enterprises. The damage caused by spyware is more subtle than that caused by viruses. Spyware causes greater damage the longer it remains installed.

Anti-spyware programs should identify spyware but allow an administrator to confirm which suspect software should be removed. They should also enable investigation of the source of the spyware and enable administrators to amend whitelists of allowed software and blacklists of software to be removed.

XII. CONTINUING THREATS

While viruses can cause significant damage to computer systems, the damage caused by spyware should not be underestimated. Spyware can rob users of privacy and drain their productivity, both by interrupting work with annoying pop-up ads and by running extra processes that slow down the computer.

The motivations behind the development of viruses and spyware are not likely to subside any time soon. Spurred by desire for revenue or renown, authors will develop new ways to spread their "product," add new functionality to the code, and resist attempts to remove the code. As a result, the need to combat viruses and spyware will remain strong in the foreseeable future.

For additional information, please visit our Web site at www.trendmicro.com.

TREND MICRO™

REFERENCE:

[1] Evers, Joris, "Computer crime costs $67 billion, FBI says," *CNET News.com*, January 19, 2006, http://news.com.com/Computer+crime+costs+67+billion,+FBI+says/2100-7349_3-6028946.html?tag=nefd.top.

[2] Trend Micro.

[3] IDC. *Worldwide Spyware 2004–2008 Forecast and Analysis: Security and System Management Sharing Nightmares, December 2004, and Worldwide IT Security Software, Hardware and Services 2005–2009 Forecast: The Big Picture*, December 2005.

[4] Seyfer, Jessie. "Microsoft Unveils New Security Tool," *San Jose Mercury News*, February 14, 2006, http://www.mercurynews.com/mld/mercurynews/13872691.htm.

[5] IDC, *Worldwide IT Security Software, Hardware and Services 2005–2009 Forecast: The Big Picture*, December 2005.

[6] Ibid.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014
USA toll free: 1+800-228-5651
phone: 1+408-257-1500
fax: 1+408-257-2003
www.trendmicro.com