webroot
SOFTWARE, INC.

Privacy. Protection. Peace of mind.

White Paper

The Unique Challenge of Spyware

Important Differences to Know About Spyware and Viruses

Webroot Software, Inc.
2560 55th Street, Boulder, CO 80301

Toll Free: 800.870.8102
Telephone: 303.442.3813
Facsimile: 303.442.3846

www.webroot.com

Index:

Introduction

At first comparison, spyware and computer viruses might appear to have more in common than not. They are both malicious programs, they both impact system stability, and the effects of both can range from being a nuisance to inflicting serious damage. They are also both programs that require specialized tools for their removal. And while these two different types of malicious programs might closely resemble each another at first glimpse, there are significant differences:

- Unlike viruses, the motivations behind spyware are financial, which has driven rapid technical innovation and broad distribution.
- Spyware is curiously difficult to locate for research, requiring specialized, proactive methods for discovery.
- Removing spyware is especially complicated and problematic because newer versions are highly adept at remaining on a system.
- The business impacts of spyware are greater, as it compromises privacy, threatens assets and affects productivity beyond even the damage caused by viruses.

The bottom line is that spyware presents a unique and serious problem that requires its own dedicated defenses. As spyware rapidly proliferates today, its well-funded developers are creating increasingly sophisticated versions, and it is clear that solutions devoted to handling the intricacies of spyware are necessary.

In this paper we will closely examine the differences between spyware and computer viruses. The first line of defense is education, and understanding the unique threat spyware poses is the first step in a practical plan for protection.

A Look at the Differences Between Spyware and Viruses

Designed to Hide

One important way spyware is distinguished from viruses is discoverability. Antivirus vendors are able to deploy passive techniques for identifying new viruses, such as "honey-nets" that capture the malicious programs as they replicate themselves across the Internet. Because antivirus vendors can rely on these more passive research methods, they have not been as prepared for the active approach necessary to combat the unique challenges of spyware detection.

In order to maintain a definitions database that will effectively defend its users from newly released forms of spyware, an anti-spyware provider must actively seek out new threats and their source location. Keeping up with hundreds of adware companies and thousands of spyware writers is a daunting task. Furthermore, it is becoming even more specialized as increasingly advanced forms of spyware morph into new variations requiring more sophisticated approaches.

There are several approaches to spyware research, but each is technically challenging and resource intensive. One of the more interesting approaches used involves using webcrawler technology to find new threats before they can infect end users. This automated scanning of the Internet to identify new forms of spyware involves proprietary technologies and a specific understanding of spyware and its unique properties.

Difficult to Remove

Once installed on a system, the presence of spyware on the PC can be insidious. While viruses typically take the form of a single executable and might affect a few registry entries, spyware typically impacts multiple registry entries and potentially leaves dozens of application files spread across the hard drive or deep within the hardware. Sophisticated techniques are required to locate and remove these many components created by spyware applications.

In addition, spyware is becoming increasingly sophisticated in its staying power. New spyware programs use complex approaches, such as running separate processes that monitor each other. These programs

are capable of reinstalling components and repopulating registry entries that have been removed. They are also capable of randomizing various elements of the program so that they leave a different footprint and are harder to track. To further complicate matters, if left unchecked many spyware applications are capable of downloading additional programs.

Consider for example the insidious spyware program called "Look2Me". This malicious application gets deep inside your system. It uses Internet Explorer as the launching point to insert another file into the Windows area that controls system start up processes. By hooking itself in this way, it tricks your computer into believing that it is a critical process that must not be removed. If attempts are made to remove the files or their registry entries, Look2Me can automatically reboot the computer to restore itself.

Compared to spyware, the newly identified virus W32.Mydoom.CF@mm is malicious, but much less difficult to remove. The W32.Mydoom.CF@mm virus is a mass-mailing worm that rapidly propagates by mailing itself to addresses gathered from the compromised computer. It copies itself to a Windows system folder and modifies up to three registry entries so it can load when Windows starts up, but removal is as simple as deleting its file and erasing the text strings that it has inserted in the registry. Antivirus programs are designed for this type of task.

When faced with more difficult removal efforts, antivirus programs are not sufficient. Even just to remove some viruses, leading anti-virus vendors have had to build completely separate custom removal tools. Removing aggressive spyware is even more difficult. To be effective, an anti-spyware program must engage in the complex, multi-step process of extracting the spyware components and removing the traces left behind throughout the system. Spyware removal requires highly specialized techniques that are different from the fundamental processes performed by antivirus software.

Different Impact

Another important difference between spyware and viruses is the impact they make on computers and their users. Viruses are developed to cause mischief by clogging networks, bringing down systems, or in some cases, deleting information. Spyware, however, is designed to execute even more malicious objectives. In the hands of cyber

criminals, spyware's impact can be devastating, enabling them to violate personal privacy, access proprietary information, and steal financial assets. This was the case in a recent headline-making cyber theft in which spyware was used to steal $423 million from Sumitomo Mitsui bank.

In addition, even "legitimate" adware programs make a significant negative impact on productivity. They often slow system performance, cause PC crashes, and result in lost time while infected systems are repaired. According to a Microsoft estimate, spyware causes more than half of Windows system crashes[1], and Dell announced in 2004 that a full 25% of the calls to its support staff were from users who had experienced degraded system performance caused by spyware[2].

Unique Distribution

The way in which spyware proliferates is also different from viruses. For one, there are often more variants. While viruses may have a few variants or encourage copycat efforts, spyware is often programmatically designed to spin off its own variations, which can lead to a substantially greater number of spyware programs to contend with.

In addition, while viruses are typically designed to spread themselves openly and obviously across networks, spyware is generally unwittingly downloaded and installed by computer users. Spyware's focus is on stealthy delivery, and thus it proliferates more "silently", which makes it more difficult to determine the scope of its dissemination. While antivirus solutions are focused on combating the more visible spread of viruses and worms, a spyware protection solution must be adept at exposing stealthy delivery methods.

Financially Motivated

Another important differentiator between spyware and viruses is the motivation for their creation in the first place. Viruses are often created by individuals or small groups with the intent of causing a nuisance, or testing their programming skills at the expense of others. Spyware, on the other hand, is financially motivated and represents a growing industry estimated at $2.5B.

[1] Brian Arbogast, Microsoft (corporate vice president of the Identity, Mobile and Partner Services Group within Microsoft's MSN and Personal Services Division), at a Federal Trade Commission spyware workshop, according to a Microsoft press release on April 20, 2004 (http://www.microsoft.com/presspass/features/2004/apr04/04-20Spyware.asp)

[2] Ed Maguire, Merrill Lynch comment, Security Software: Gartner Security Summit Highlights, June 10, 2004

Backed by legitimate organizations with substantial financial resources, spyware is becoming increasingly sophisticated, and increasingly more difficult and complex to manage. With a strong financial motivation behind its advancement, spyware protection will continue to require highly specialized techniques.

Conclusion

In summary, spyware is uniquely difficult to identify, and it becomes entangled in the systems it infects, making its removal extremely complicated. Spyware's impact can be dramatically different from that of viruses, resulting in significant loss to theft of assets and decreased productivity. Finally, because it is financially motivated and backed by increasing investment from a thriving industry, spyware is advancing rapidly and becoming progressively more complex.

When examined more closely, it is apparent that spyware has very different properties from viruses. Understanding the unique properties of spyware is the first defense against its dangers. Dealing with spyware is a complex challenge that requires specialized techniques. Today more than ever, computer users need to rely on a dedicated solution designed specifically to help navigate the unique threats of spyware.

Privacy. Protection. Peace of mind.

Webroot Software, Inc.
2560 55th Street, Boulder, CO 80301

Toll Free: 800.870.8102
Telephone: 303.442.3813
Facsimile: 303.442.3846

www.webroot.com