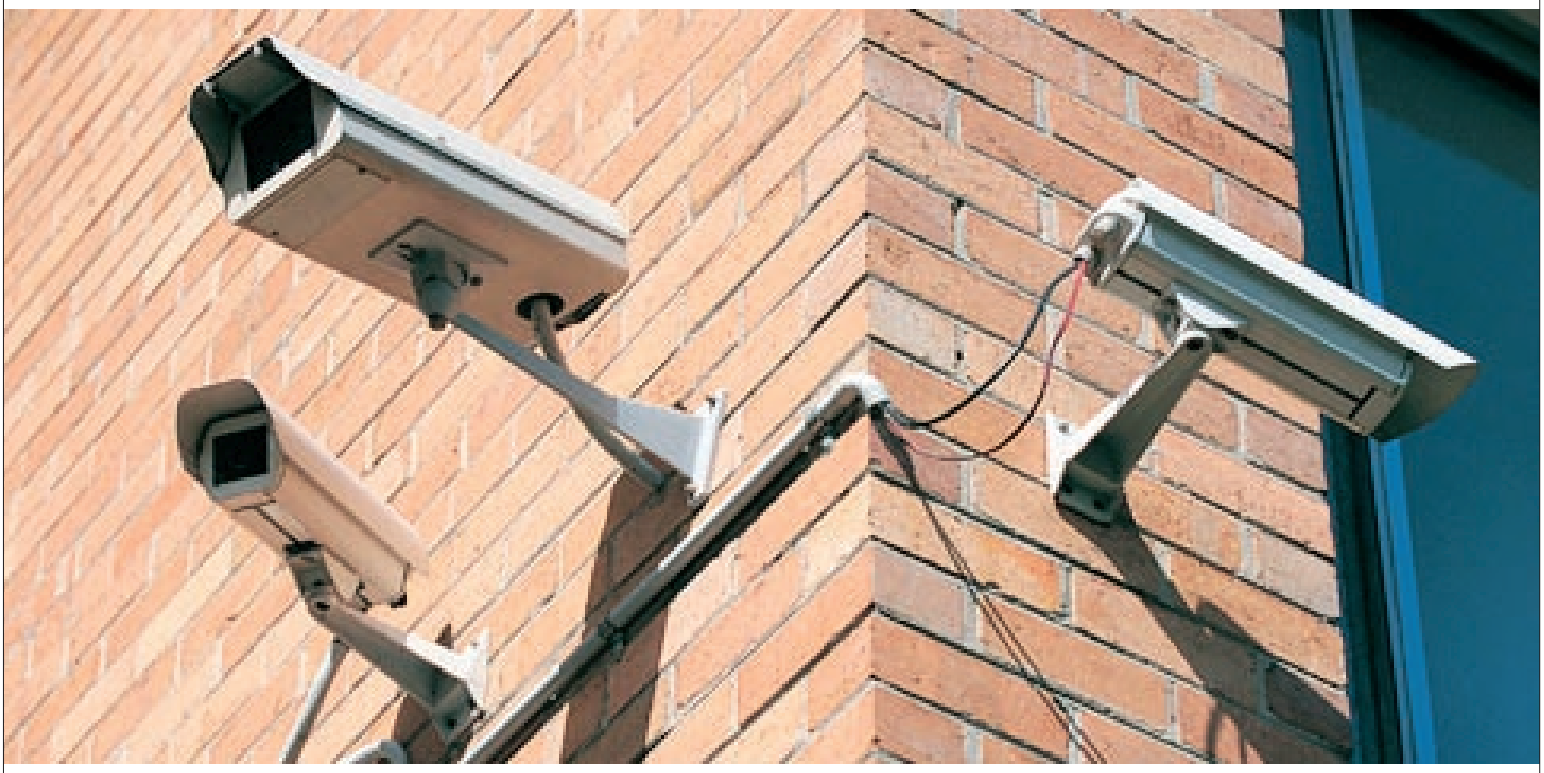
SPYWARE vs. VIRUSES



webroot SOFTWARE

Contents

Introduction

At first glance, spyware and viruses appear to have more in common than not. Both are malicious programs that impact system stability and the effects from both can range from a minor annoyance to major system failures. Both types of malware require specialized tools for removal. While these two types of malware closely resemble one another, there are significant differences:

→ Unlike viruses, the motivations behind spyware are financial, which has driven rapid technical innovation and broad distribution.

→ Spyware is remarkably difficult to locate for research, requiring specialized, proactive methods for discovery.

→ Removing spyware is especially complicated and problematic because spyware morphs frequently and new versions are highly adept at remaining on a system.

→ The business impacts of spyware are greater than viruses, as spyware can compromise private data, threaten corporate assets (both financial and proprietary) and affect business productivity to the point where networks shut down.

VIRUSES

→ replicates by attaching to files
→ spreads quickly
→ visible damage
→ inconvenient

SPYWARE

→ monitors/controls/records keystrokes
→ steals passwords and personal data
→ hidden damage
→ financially motivated

The bottom line is that spyware is a unique challenge that requires a specialized solution. As spyware proliferates, its well-funded developers are creating increasingly sophisticated versions that require dedicated solutions. This paper will closely examine the differences between spyware and 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

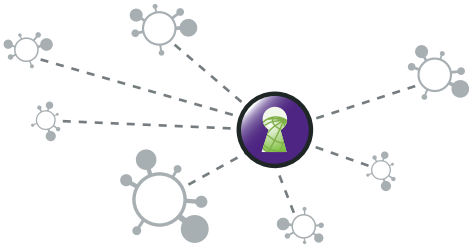
Designed to Hide

A critical way that spyware is distinguished from viruses is discoverability. Antivirus vendors are able to deploy passive research techniques to identify new viruses, such as "honey pots" that capture the malicious programs as they replicate themselves across the Internet. Because antivirus vendors can rely on these more passive research methods, they are not 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 users from newly released spyware variants, an antispyware vendor must actively seek out new threats and their source location. This is a daunting task considering there are thousands of adware companies and spyware writers. Furthermore, increasingly complex forms of spyware are making the discovery method more difficult, which has lead to the creation of more sophisticated research methods. One of these methods involves using webcrawler technology, which automatically scours the internet looking for 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.

COMPEDITORS LAY TRAPS
A PASSIVE TECHNIQUE

WEBROOT HUNTS PROACTIVELY
USING WEBCRAWLER TECHNOLOGY



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 impacts multiple registry entries and potentially leaves dozens of application files spread across the hard drive or deep within the operating system. 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, many spyware applications are capable of downloading additional malicious programs.

Consider for example the spyware program called "Look2Me". This application positions itself deep inside your system and uses Internet Explorer as the launching point to insert another file into your system start up process. By doing this, Look2Me effectively tricks your computer into believing that Look2Me is a critical process that must not be removed. If attempts are made to remove files or registry entries, Look2Me can automatically reboot the computer and restore any deleted components.

When you compare Look2Me to a virus like W32.Mydoom. CF@mm (Mydoom), it's clear that both are malicious, but Mydoom is much less difficult to remove than Look2Me. Essentially, Mydoom infects a machine by copying itself to a Windows system folder and modifying up to three registry entries – this makes it so Mydoom loads when Windows starts up. Removal of this type of infection is as simple as deleting the file in the Windows system folder and erasing the text strings that were inserted into the registry. Antivirus programs are designed for this type of task and are very effective at doing it.

When faced with a more advanced threat like spyware, antivirus programs are not sufficient. Spyware removal requires highly specialized techniques that are different from the fundamental processes performed by antivirus software Removing aggressive spyware requires an antispyware program to engage in a complex, multi-step process of extracting spyware components and removing the traces left throughout the system.

Different Impact

Another important difference between spyware and viruses is the impact they have 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 upon more malicious objectives. In the hands of a criminal, the impact of spyware can be devastating. With the use of spyware, a criminal can violate personal privacy, access proprietary information, and steal financial assets. This was the case in a recent headline in which 46 million customer credit card numbers were stolen from the networks of retail giant TJX.

Additionally, "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 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 a stealth 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, an antispyware solution must be adept at exposing stealthy delivery methods.

[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

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 $2.5 billion a year.

Backed by legitimate organizations with substantial financial resources, spyware is becoming increasingly sophisticated and 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 its removal is extremely complicated. The impact of spyware can be dramatically different from that of a virus and can result in decreased productivity and stolen assets, both financial and proprietary. Finally, because spyware is financially motivated it is advancing rapidly and becoming progressively more complex. When examined closely, it is apparent that spyware has very different properties from viruses. Dealing with spyware is a unique 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 threat and rapidly morphing landscape of spyware.

About Webroot

Webroot Software, Inc. provides industry leading security software for consumers, enterprises and small and medium-sized businesses worldwide. Globally recognized for its award-winning Spy Sweeper® line of antispyware and antivirus products, Webroot security software consistently receives top ratings by respected third-party media and has been adopted by millions globally. Webroot® AntiSpyware Corporate Edition (formerly Spy Sweeper Enterprise) is a comprehensive, centrally managed enterprise solution that aggressively blocks, detects and eradicates spyware on desktops across the network. Webroot® AntiSpyware Corporate Edition with AntiVirus offers combined protection for spyware and viruses. Available either as branded solutions or on an OEM basis, Webroot products can be found online at http://www.webroot.com.