PROCESS™
SOFTWARE

How to Win the Battle Against Spyware with Next Generation Technology

White Paper

Table Of Contents

Overview

In the past year there have been many real life examples of what can happen if sensitive data has not been secured properly. Data security breaches have been reported at many high profile companies including TJX, Disney, Western Union, Fidelity, Monster.com and TD Ameritrade. Data breaches have also occurred at many smaller organizations, yet they are often not made public. The FBI estimates that spyware and other computer-related crimes cost US businesses $67 billion per year.[1] The damage to a company's brand is immeasurable.

Spyware is on the rise and has been the cause of many data breaches. The reason for this is that unlike virus writers, the motive of its perpetrators is financial gains. Unprotected data that once had a low risk of being stolen now has a greater chance of being exploited. Sophisticated spying techniques are being used to steal data, such as key logging (an application that records keystrokes), or modifying host files to redirect an IP address from a trusted website to another untrustworthy site. There are many tools freely available on the Internet to aid with this data theft, and to complicate the situation even further there is often legitimate software that can be used for illicit means. For example, remote control software used by technical support to troubleshoot employees' computers can be used to obtain unauthorized access to a system containing confidential information such as social security numbers or bank accounts.

Not only is there a sinister motive by spyware developers and distributors, but spyware has exhibited more complex multifaceted behaviors making detection and removal more difficult. Microsoft reports that in the first half of 2007 there was a 500 percent increase in trojan downloaders and droppers (malicious code used to install files such as trojans, password stealers, key loggers and other malware on users' systems) as compared to the previous six months.[2] Spyware is pervasive on the Internet and it can be difficult to pinpoint where a user may download spyware. Since it can be invisible to users, the longer the spyware is running undetected on a system, the greater chance a data theft may occur. Usually there is only a hint that spyware is present when computer or network performance degrades, users report more display ads, and/or users report their browser home page has been redirected.

Even in the face of escalating data security breaches, many administrators are not using a solution that specifically addresses the spyware threat. In a survey of 479 US corporations, the Poneman Institute cited that 62% of IT security professionals rate spyware as the number one threat to the integrity of intellectual property and customer personal identifiable information, yet 98% of them rely on firewalls to protect them against spyware. [3]

[1] Joris Evers. Computer crime costs $67 billion, FBI says. http://www.news.com/Computer-crime-costs-67-billion,-FBI-says/2100-7349_3-6028946.html

[2] Microsoft. October 23, 2007. http://www.microsoft.com/presspass/press/2007/oct07/10-23IAPPRSAPR.mspx?rss_fdn=Press%20Releases

[3] Poneman Institute. November 13, 2006.
http://www.ponemon.org/press/Ponemon_Mi5%20Spyware%20Study_Final.pdf

Signature-Based Solution Limitations

There is a great temptation to use anti-virus and/or firewall solutions already installed in an organization for spyware protection. Because these products are already in place, there is virtually no effort required to add anti-spyware on the part of overtaxed administrators. Some vendors will claim in their literature that one solution will protect you from many potential data breaches that can occur through viruses, spyware, spam, and DOS attacks. These “all-in-one” security solutions are helpful when IT departments are understaffed and have a long list of requirements that need to be implemented to comply with their data security goals. However, upon further examination of the technology used in these solutions to prevent spyware, one would conclude that they are greatly limited and leave an organization’s data open to potential theft.

Anti-virus vendors’ primary means of detecting and stopping viruses is by using a database of virus signatures. This works by examining the content of the computer's memory and the files stored on fixed or removable drives, and comparing those files against their signature database. In recent years, anti-virus vendors have extended their signature database to include spyware applications. Some vendors have assembled a vast list of spyware signatures for their products, erroneously believing that the biggest list could provide the best protection. In reality, signature-based solutions are inherently limited because they are a reactive security solution. Spyware detection occurs only after a particular piece of spyware has been identified. While signature-based solutions are useful for stopping known threats, they are powerless to stop new threats.

Gateway firewalls have added some anti-spyware capabilities by monitoring web traffic and blocking potentially harmful applications from being downloaded from certain websites. These solutions rely on signature matching only and provide protection at the network level, but not at the individual client level. This means that they are unable to protect mobile devices, such as laptops, which leaves a substantial gap in any data security policy. In addition, spyware detection performed at that level could cause performance issues for the whole network. A few gateway firewall solutions have extended their protection to the client side. However, they offer limited anti-spyware protection with the use of signature-based detection.

Behavior-Based Solutions

Presently, some anti-spyware vendors have introduced behavioral analysis as a means of detecting spyware proactively. These first-generation solutions are limited by not being precise enough to differentiate between destructive and constructive behaviors. Not all software that performs a suspicious behavior (such as key logging) is spyware. More advanced behavioral detection solutions should be able to identify all the pertinent information about the applications and computers performing the suspicious behavior. This way, administrators can make an informed decision on what is and is not spyware. For example, Google Desktop exhibits several behaviors including keystroke monitoring, hijacking an application and changing IE settings. These behaviors are performed by components of that application and if only the name of the component that performed the behavior is reported then administrators might not know whether the component is part of a legitimate application. SpyCatcher uses advanced behavioral analysis for proactive protection, which can trace back these behaviors from the component to the originating application. As a result, administrators would know that Google Desktop is running and they can decide if it should be allowed to run across their entire organization or just select computers.

SpyCatcher Enterprise monitors a broad-range of behaviors that are pervasive in spyware, particularly those involved in data theft. By analyzing and correlating a combination of suspicious behaviors so that they are put into proper context, SpyCatcher achieves a higher accuracy rate at identifying spyware. This functionality is not available in first generation behavior-based solutions. For example, when the software called "All In One Keylogger" is installed, SpyCatcher reports a number of behaviors including taking screenshots, hijacking an application, and overwriting the memory of other applications. Since SpyCatcher includes the call trace information for each behavior, administrators can see the name of the originating application. Because this particular application uses very cryptic names for its executables, administrators would be suspicious of the legitimacy of this application.

Advanced behavioral detection can identify and prevent legitimate applications from being corrupted. Another benefit of advanced behavioral analysis is that it can be used by IT departments to enforce policies so that even legitimate applications can be prevented from being used for illicit purposed. For example, an IT department may be allowed to use specific remote control applications to assist in diagnosing employee system issues across many locations. If they fall into the wrong hands, legitimate remote control tools can also be used for data theft. SpyCatcher’s application policy enforcement provides administrators with the capability to block remote control applications from being used by anyone outside their department. SpyCatcher will alert administrators if anyone else outside their department tries to download and use remote control software.

Benefits of
Advanced Behavioral Detection

- **Identifies unknown emerging threats**
- **Distinguishes between legitimate and suspicious applications to avoid false positives**
- **Allows granular controls - administrators can add customer signatures to the signature database**
- **Enables application policy enforcement**
- **Preserves the integrity of existing applications**

Profiling Behaviors

It is important to monitor a broad range of behaviors in order to provide administrators with a complete picture of application activity. This allows policy decisions to be made quickly and easily since some behaviors may not be regarded as harmful as others. For example, changing the default home page in Internet Explorer or altering a tool bar are behaviors most likely to be performed by applications trying to sell products rather than steal data.

SpyCatcher monitors a wide variety of behaviors, which help to identify all types of spyware (See Appendix I). The top five behaviors associated with data theft are described in the following sections.

Key Logging

Key logging is the recording of all keystrokes on a system. Applications that perform this function are often marketed as legitimate applications. For example, some organizations install them on computers belonging to employees suspected of theft or other unethical activities. Many parents also use these programs to track their children’s online activities with the intent of ensuring that they’re not visiting inappropriate Web sites or engaging in other dangerous activities. However, a much larger percentage of programs that include an element of key logging are found in spyware and used for criminal activity. Designed to steal usernames, passwords, and even your identity, these programs are typically installed without your knowledge, often in conjunction with another legitimate program. As a result of the multiple uses, it is difficult in practice to discover that key logging is occurring without raising some false alarms. It is important to put key logging in context by seeing what other behaviors are occurring with a given application and what its purpose is.

Register System Driver

System drivers have full access to your entire system, thus they should only be allowed to install when you completely trust the product. Malware applications known as kernel rootkits are implemented as drivers, and once installed they can make themselves invisible to security software and can gain complete control over your system. A rootkit's purpose is typically to hide files, network connections, memory addresses, or registry entries from other programs used by administrators to detect intended or unintended special privilege accesses to the computer resources. A rootkit may be incorporated with other files which have other purposes, such as key logging.[4]

Hijacking Applications

Once installed, some malware will inject itself into other applications running on the computer so that it can transparently intercept any operating system calls made by those applications. Calls made by applications to save files to disk or to send data over the network can provide the malware with opportunities to collect sensitive information without anyone knowing it is happening. Many of the techniques used to perform this hijacking were originally supported by Windows to allow the deployment of 'hot fixes', which enabled a software fix to be applied to a system without requiring a reboot. However, as with many such features, malware developers have seized upon this as a way to steal valuable data.

Screenshots

A screenshot is an image that shows everything visible on the computer monitor at the time the screenshot is taken. It is used for a number of legitimate purposes such as demonstrations, documentation, or debugging a software problem. Spyware will take screenshots at various intervals and send those images to a remote server with the hope that they will show some critical data, which can be used for financial gain. For example, critical data includes a list of employees with their social security numbers or a company financial statement showing bank account information. Passwords are not usually displayed while being entered so they are not vulnerable to screenshots, but account numbers, usernames, and answers to security questions are vulnerable and could be used by someone to obtain passwords.

Modify the Hosts File

The hosts file on a computer is used to translate the host name part of a URL into an IP address. If no match is found for the host name in that file then the computer will use external DNS systems to resolve the name. Adding entries to a computer's hosts file is a simple way of redirecting requests from the intended site to one which may extract data from the request and then potentially forward the request to the legitimate, making it appear to the user that everything is working correctly. In some cases, spyware has been known to add entries for the hosts of popular anti-spyware software vendors to a

[4] http://en.wikipedia.org/wiki/Rootkit

computer's hosts file so that those requests are redirected to an invalid IP address. This would make it difficult for the user to get to any of those sites, which has the side effect of making it impossible for anti-spyware software installed on the user’s system to retrieve signature updates from the vendor's site.

Conclusion

Stopping spyware needs to be a strategic part of an organization’s overall security plan. Reactive signature-based anti-virus and firewall technology is not a complete solution to stopping spyware. Because there is a high risk that data leakage can occur when spyware infiltrates a company’s network, it is essential that administrators evaluate anti-spyware solutions that are designed to address this issue.

The better anti-spyware solutions use a mix of different technologies to identify and eliminate spyware. A layered approach to stopping spyware has proven to be more accurate at identifying potentially unwanted software rather than relying on a single technology to stop a complex problem. The mix must include a proactive technological component to insure effective data protection.

SpyCatcher Enterprise’s Profiling Engine™ uses multiple layers of technology to prevent both known and emerging spyware threats. SpyCatcher includes advanced behavioral analysis for proactive protection. It is complemented by other technologies, such as analyzing applications against an extensive database of legitimate applications, and against a database of spyware producing vendors that have digitally signed their software. Often spyware vendors sign their software in order to appear legitimate. SpyCatcher also includes a signature database, which is coupled with DeepDefense™, an application-intercepting technology. This feature blocks known spyware from executing by intercepting the operating system calls that launch these applications. DeepDefense stops known spyware from executing even without scanning. Most anti-spyware solutions leave PCs vulnerable to problems by allowing malware to run in memory before being detected and cleaned.

Appendix I – SpyCatcher's Advanced Behavioral Detection

Key Logging

Key logging is the recording of all keystrokes on a system. Applications that perform this function are often marketed as legitimate applications.

Take Screenshots

Applications that take screenshots repeatedly capture what is being displayed on the monitor. These images are stored on a remote system for later review, and can reveal computer activity (e.g. visited web sites) as well as the content of sensitive documents.

Modify the Hosts File

The hosts file maps host names to IP addresses. Malware can edit this file to redirect requests to a trusted web site to any site of its choice.

Register System Driver

System drivers have full access to your entire system, thus they should only be allowed to install when you completely trust the product. Malware applications called rootkits are implemented as drivers, and once installed they are invisible and can gain complete control over your system.

Hijack Application

Some malware attempts to gain complete control over your system by silently attaching itself to other innocent applications. While "inside" these applications, malware can intercept requests made of the operating system in order to spy on your activities or modify the behavior of the applications in which it resides.

Run Custom Code within Winlogon

Winlogon is responsible for managing the sequence of events that occur when a user logs into Windows. If malware inserts itself into Winlogon it will be able to steal passwords and, since Winlogon runs at the System level, the malware will have unrestricted access to all areas of the system. Note that in Windows Vista Winlogon's roles and responsibilities have changed which has significantly reduced this security threat.

Overwrite Application Memory

Some malware modifies the memory contents of innocent applications in order to change their behavior or to open up a security breach.

Install a Browser Helper Object

Browser Helper Objects (BHOs) run within Internet Explorer. Spyware is often written in the form of a BHO because BHOs can monitor surfing habits and even control much of Internet Explorer's behavior.

Change an Internet Explorer Setting

Some undesirable programs, adware in particular, change Internet Explorer settings in order to customize your browsing experience to suit their tastes rather than your own.

Change the Internet Explorer Home Page

Some malware attempts to change your home page, typically in order to lure you into buying products.

Change the Internet Explorer Default Page

The default Internet Explorer page is accessible by clicking on the "Use Default" button in the Internet Options dialog box.

Change the Internet Explorer Local Page

Internet Explorer loads this page at startup if you have no home page set. Typically the local page is set to about:blank.

Change the Internet Explorer Search Bar

The search bar value defines the search page that is accessed when you click “Search” on the Internet Explorer toolbar.

Change the Internet Explorer Search Page

The search page value defines the search page that is accessed when you click “Start”, point to “Find”, and then click “On The Internet”, or when you click “Search The Web” on the Go menu in Internet Explorer 4.

Register for One Time Automatic Launch

Windows allows applications to be automatically launched after the next reboot via the RunOnce registry setting. Malware applications often take advantage of this configuration to ensure that their applications run at system startup.

Register For Automatic Launch

Windows allows applications to be automatically launched after each reboot via the Run registry setting. Malware applications often take advantage of this configuration to ensure that their applications run at system startup.

Disable Windows Task Manager

This highly suspect action causes Windows Task Manager to no longer function. Task Manager is a system utility used to see all processes in memory and terminate undesirable applications. A primary reason for disabling Task Manager would be to effectively hide an application or make it difficult to terminate.

Change the Desktop Wallpaper

Some undesirable applications change the background image on the Windows desktop (i.e. the wallpaper) without the end user's permission. The replacement image may be offensive or it may be a product advertisement.

Create Shortcut on Desktop to Website

During installation, undesirable applications such as adware often create a shortcut link on the Windows desktop that point to a location on the web. This web site usually contains nothing but advertisements.

About Process Software

Process Software is a premier supplier of communications software solutions to mission critical environments. Since the company was founded in 1984, Process Software has grown its customer base to over 3,000 organizations, including Global 2000 and Fortune 1000 companies. Process Software has earned a strong reputation for meeting the stringent reliability and performance requirements of enterprise networks. The Tenebril division of Process Software delivers award-winning security solutions for home and enterprise customers. The products include SpyCatcher, a leading antispyware solutions for enterprise and consumer markets and GhostSurf, an Internet privacy and anonymous surfing software for consumers.

PROCESS™
SOFTWARE

U.S.A.: (800)722-7770 • International: (508)879-6994 • Fax: (508)879-0042
E-mail: info@process.com • Web: http://www.process.com