GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Microsoft enters the Anti-Spyware Market

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4b

Option 1 - Research on Topics
in Information Security

Submitted by: Lilianne Choy

© SANS Institute 2005 Author retains full rights.

Table of Contents

© SANS Institute 2005, Author retains full rights.

Abstract

The pace at which spyware is evolving does not appear to be decreasing any time soon. It has captured the attention of users, business corporations, "government leaders, and consumer advocacy groups who identify spyware as a serious problem for the entire PC industry"[11]. According to an IDC study conducted in 2004, "67 percent of consumers PCs are infected with some form of spyware"[6] Spyware does not only impact the performance of a user's computing system, but it has the potential to steal important sensitive information, making the unauthorized use of personal information a significant legal issue.

This paper aims to provide a detailed overview of Microsoft's recent acquisition of the anti-spyware application from Giant Software Company. I will briefly examine Microsoft's strategy for entering the Anti-spyware market; review the features of Microsoft's AntiSpyware product (version beta1); and look at some preliminary tests performed between Microsoft's AntiSpyware product against other leading anti-spyware software.

Introduction

Microsoft recently released the Windows XP Service Pack 2 to address the growing number of security vulnerabilities in its operating system. This Service pack was designed to offer a myriad of security features which range from installing a new integrated personal firewall to hardening the configuration of its Internet Explorer browser to prevent malicious code exploits. This service pack, unfortunately, lacked any mechanism to effectively detect and remove spyware. So in mid-December 2004, Microsoft purchased Giant Software Company and its leading anti-spyware application. Only weeks later, Microsoft re-branded the software and released its own beta version of the product to the public for a free trial. It was apparent to Microsoft that the growing problem associated with spyware had to be mitigated, particularly since a growing number of spyware attacks were being written to target the vulnerabilities in its Internet Explorer browser and also, to exploit the architectural design flaws in its Windows Operating systems.

Microsoft retained most of the Giant AntiSpyware features and key support which include RealTime Detection, AutoUpdater, Spyware Scan and most importantly, the SpyNet Community network. "SpyNet is styled as a network of computer users who agree to forward information about spyware to help create and update spyware detection signatures. When the software's Security Agents are breached by unknown programs, the SpyNet servers are immediately updated to report the activity and check whether it is part of a spyware

© SANS Institute 2005 Author retains full rights.

outbreak."[2]

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Background

What is Spyware?

With the growth of e-commerce, Spyware has become a popular tool among advertisers and businesses to collect personal information about consumers without their knowledge or consent. The information that is gathered can be as simple as determining which websites a user has visited to extracting sensitive user information such as personal identification and passwords. Adware is similar to spyware in that is typically bundled and distributed with freeware or shareware software. The primary difference between Adware and Spyware is that Adware includes an 'End User License Agreement' in the downloaded software; albeit the "agreement is often very vague, is not complete, or is difficult to find"[10]. Throughout the remainder of this document, spyware will be used to refer to both adware and spyware programs.

Users are vulnerable to spyware if they download music from file-sharing programs, free games from un-trusted websites, or other software programs from unknown sources.[8] Spyware is often covertly installed in the background during the installation of the other software.

What are the signs of a spyware infection?

Typical signs of a Spyware infection include, but are not limited to the following:

1. Appearance of pop-up advertisements even when the web browser is not open.
2. Web browser home page and Search settings have been reconfigured. Cannot modify these settings as they reappear the next time the computer is restarted.
3. A new toolbar has been added to the web browser. Cannot remove the toolbar even after the computer has been restarted.
4. Increased latency is noticed on the computer. The spyware program may be consuming more resources on the computer system to track activities and deliver information to the host computer over the Internet.
5. The web browser frequently terminates while performing a search.

(Further details can be found at Microsoft Frequently Asked Questions on Spyware) [8].

© SANS Institute 2005 Author retains full rights.

The Microsoft Strategy on Spyware

For the past several years, the Microsoft Windows platform has been exposed to countless malicious attacks, hacking exploits, and vulnerability threats. In response to this, Microsoft is making a concerted effort to protect its users' security and privacy by integrating new security features into its operating system and applications. It has demonstrated this initiative by bundling a suite of security functions into the Windows XP Service Pack 2 and also in its launch of the AntiSpyware software. In its strategy on spyware, Microsoft quotes "The Microsoft anti-spyware vision is that PC users should be able to see and understand the software that is running on their PCs and have the power to prevent or remove software they do not want. This vision drove the acquisition of GIANT Company Software, and it will inform Microsoft's efforts in future versions of its products."[11] To this end, Microsoft is focusing its efforts in four principal areas:

Technology
Microsoft is combining the security enhancements in Windows XP Service Pack 2 with AntiSpyware to protect Windows users from spyware and unwanted software. Integrated functions in the AntiSpyware product will detect new variants of spyware by monitoring commonly known spyware entry points. The users' Internet browsing activities will be secured with new tools such as the Pop-Up Blocker and the Internet Explorer Information Bar which prevent the installation of unknown software. Details of the AntiSpyware features will be examined later.

Consumer Guidance & Engagement
Microsoft has dedicated a specific website http://www.microsoft.com/spyware on spyware. It contains articles on how to avoid and remove spyware. It has also launched a newsgroup on spyware, which is also accessible from this site.

Industry Collaboration
Microsoft endeavors to work with Industry partners to share best practices and to develop a solution in identifying and resolving spyware issues.

Legislation & Law Enforcement
Few laws exist today to prevent the development and spread of spyware. Microsoft plans to work with Law Enforcement agencies and Regulatory Agencies to enforce new legislation to reduce the distribution of spyware.

© SANS Institute 2005 Author retains full rights.

(Further details are available on the Microsoft website under “Microsoft’s Anti-Spyware Strategy”.) [11]

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

How does the Microsoft AntiSpyware Work?

The Microsoft AntiSpyware software is available as a free download from www.microsoft.com\spyware. It supports Windows 2000, Windows XP, and Windows Server 2003. There is one important caveat to note with Microsoft's AntiSpyware – it only protects Microsoft's Internet Explorer. Other competing web browsers such as Firefox, Netscape, and Opera are not protected by AntiSpyware. Also, there are no indications that the local desktop version of AntiSpyware – Beta1 will be expanded to a centralized Enterprise product, similar to current Antivirus Enterprise systems in the market.

After installing the AntiSpyware application, it will automatically run in real-time protection mode to detect unsolicited downloads and installations of unwanted software. When suspicious spyware is detected, a Pop-up message window will appear with details of the detected spyware. Information such as where the spyware files are located on the system, the risk rating applied to the spyware, and how to mitigate or remove the spyware infection are provided in this pop-up. Options are available to the user to either quarantine the detected spyware or to permanently remove it. The software interface is intuitively designed to allow any user to navigate and configure the software quickly.

The program is broken down into three main screens: Spyware Scan, Real-Time Protection, and Advanced Tools.

Spyware Scan

There are two different types of scans that can be performed to detect spyware:

- **Intelligent quick scan** - runs a scan on common entry points for spyware.
- **Full system scan -** performs a more in-depth customized scan of all files and folders. See Figure 1 – Spyware Scan.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

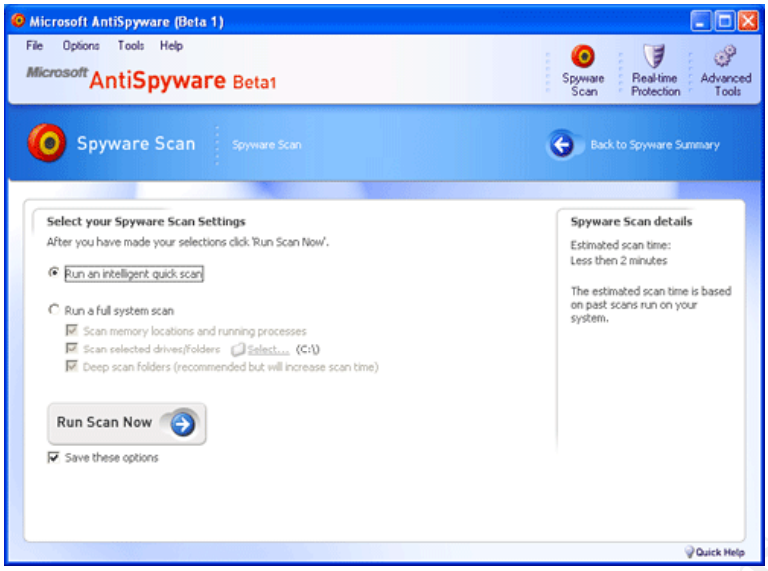

Figure 1 - Spyware Scan

After the scan is complete, a summary report is generated to show the spyware threats detected along with the number of files and registry keys scanned. See Figure 2 – Scan Summary.

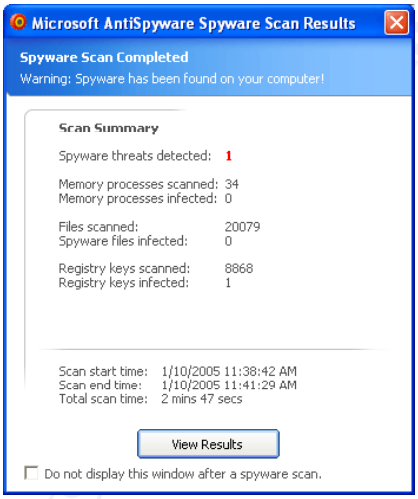

Figure 2 - Scan Summary

Specific actions can be taken against the identified threats which include removing the threat, quarantining it, or ignoring it. See Figure 3 – Spyware Threat Removal.

© SANS Institute 2005 Author retains full rights.

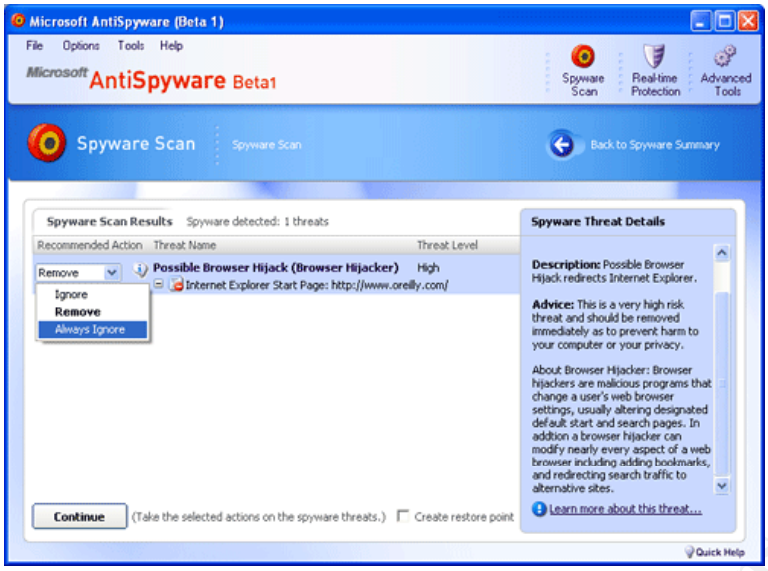

Figure 3 - Spyware Threat Removal

Threat Levels

The Microsoft AntiSpyware software assigns suspicious items a threat rating: Moderate, High, Elevated, or Severe along with a color-coded warning bar. Default actions are assigned to each of these threat rating levels: Ignore, Quarantine, or Remove. Users have the option to change the action associated with any of the threat items. For instance, if the "Always Ignore" is selected, the AntiSpyware software will stop notifying the user of that particular threat in the future. An Internet link is available to provide more information about each selected threat item.

The biggest drawback noticed on this page is the inability to sort the results by threat level. When the confirmation dialog reports that it will remove 50 spyware threats and ignore one, the program does not indicate which one will be ignored[1].

Real-time Protection

Microsoft's AntiSpyware offers continuous system protection by providing Real-time Protection to monitor and prevent specific security exploits from occurring. The Real-time Protection screen provides information on whether the real-time protection feature is active, and the status of three spyware detection agents: Internet, System, and Application. See Figure 4 – Security Agents Status.

© SANS Institute 2005 Author retains full rights.

Figure 4 – Security Agents Status

- **Internet Agents** - prevent applications from modifying Internet settings and making unauthorized connections to the Internet. Also prevents changes to a computer system's dial-up and wireless connection settings along with ensuring that spyware is not running on the system and recording network traffic. See Figure 5 - The Internet Agent and its checkpoints.
- **System Agents** - prevent threats that execute unauthorized changes to a computer system by monitoring key checkpoints for potential threats. For example, one of the important checkpoints that it monitors is system security permissions, and preventing alteration to these settings.
- **Application Agents** – prevents spyware threats from installing, deleting, or modifying Internet Explorer or downloading ActiveX controls. It also monitors the Microsoft Windows Startup files to ensure that new programs have not been loaded without the user's knowledge.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

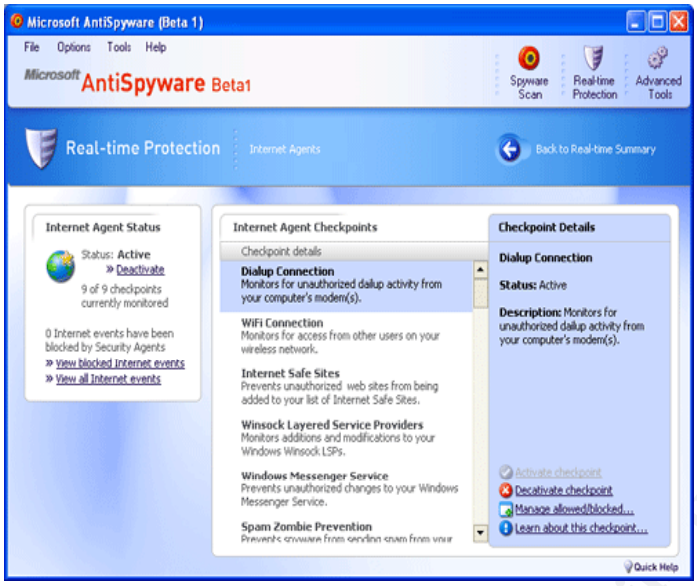

Figure 5 - The Internet Agent and its checkpoints

Based on Paul Thurrott's review of the AntiSpyware product, "these three agent types protect 58 so-called system checkpoints, entry-points in your system where malicious code can be inserted. For example, one typical checkpoint is called process execution. This checkpoint prevents spyware from executing processes (applications or services) on your PC. If an unknown process attempts to execute on your computer, the process will be blocked and you will receive an alert, which lets you remove the process. This is, possibly, the most critical function of this software: It blocks errant software from executing on your system, before it happens" [9]. Unauthorized scripts and hacker exploits, such as getting Windows to allow anonymous enumeration of user accounts or attempting Wireless access, are automatically blocked through real-time protection. See Figure 6 – Real-time Protection Settings

© SANS Institute 2005 Author retains full rights.

Figure 6 – Real-time Protection Settings

Advanced Tools

The Microsoft AntiSpyware includes a set of Advanced Tools for detecting and preventing spyware activities. See Figure 7 – Advanced Tools. These are divided into the following categories:

1. **System Explorers**
2. **Browser Hijack Restore**
3. **Tracks Eraser**

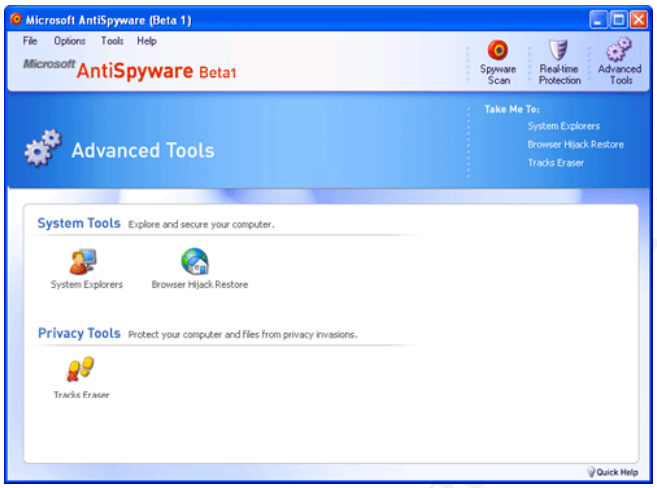

Figure 7 - Advanced Tools

System Explorers

System Explorers scan the system and detect hidden applications and application settings that may have been caused by a spyware infection. It also will determine which ActiveX components have been downloaded to the system; which applications are configured to run at Windows startup; and what processes are running at any given time. Options are available to allow the user to stop a particular running process and to configure specific applications to launch automatically when Windows starts. See Figure 8 – Startup Programs. Other features in System Explorer include the ability to explore ActiveX controls, Browser Helper Objects, and the Hosts file

© SANS Institute 2005 Author retains full rights.

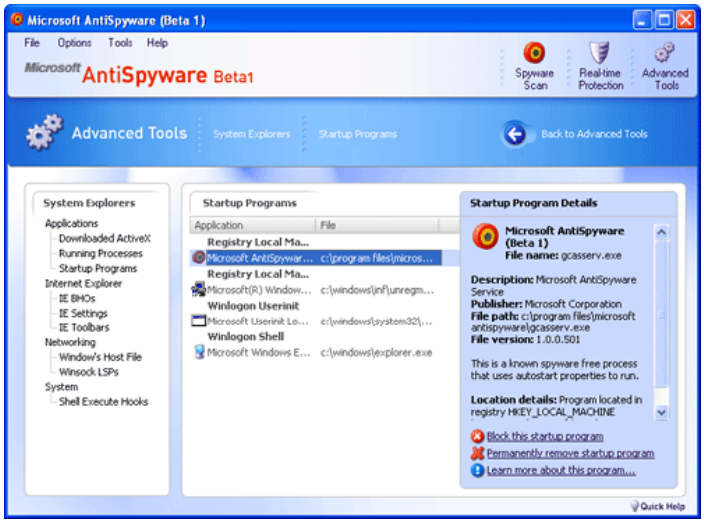

Figure 8 – Startup Programs

Browser Hijack Restore

The Browser Hijack Restore feature allows the user to restore Internet Explorer to its original settings after it has been infected with spyware. See Figure 9 – Restore Hijacked Internet Settings. It will reset about 20 Internet Explorer settings to its default values. This feature will only reset Internet Explorer to the Microsoft default settings - no support is available for competing web browsers such as FireFox, Opera, and Netscape.

Figure 9 - Restore Hijacked Internet Settings

Tracks Eraser

The Tracks Eraser helps to prevent web sites and advertisers from gathering information about the user by automatically deleting temporary files and cookies from Microsoft's Internet Explorer. This function also enables the user remove entries from the history list of such applications as Adobe Acrobat Reader,

© SANS Institute 2005 Author retains full rights.

Microsoft's Windows Media Player, and the Google toolbar. Again, there is no support for any of the competing Internet web browsers such as FireFox or Netscape. See Figure 10 – Tracks Eraser.

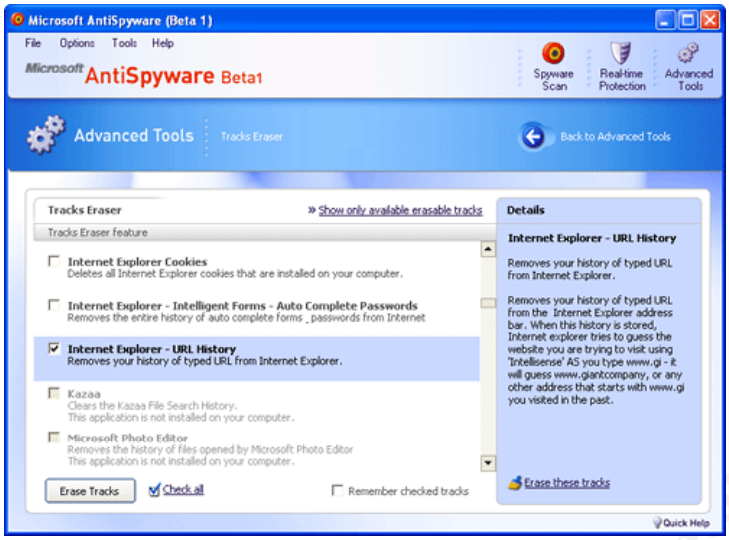

Figure 10 - Tracks Eraser

Automatic Pop-Ups

The Microsoft AntiSpyware software notifies users of suspicious spyware activity by launching a pop-up message window in the lower right-hand corner of the user's desktop. These Pop-up messages may even appear when installing or upgrading an application. If a malicious website is attempting to install spyware or if an application is attempting to make a configuration change, a pop-up message will appear prompting the user to Allow or Block the activity.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Spyware Definition Updates

The AntiSpyware can be configured to automatically check for new spyware definition files and updates from Microsoft AntiSpyware servers on a daily, weekly, or bi-weekly basis. It can even be configured to check for an update at Windows startup. The update will take a few minutes to install, and can be applied automatically. Update notifications can also be enabled. See Figure 11 – Automatic Definition File Updates.

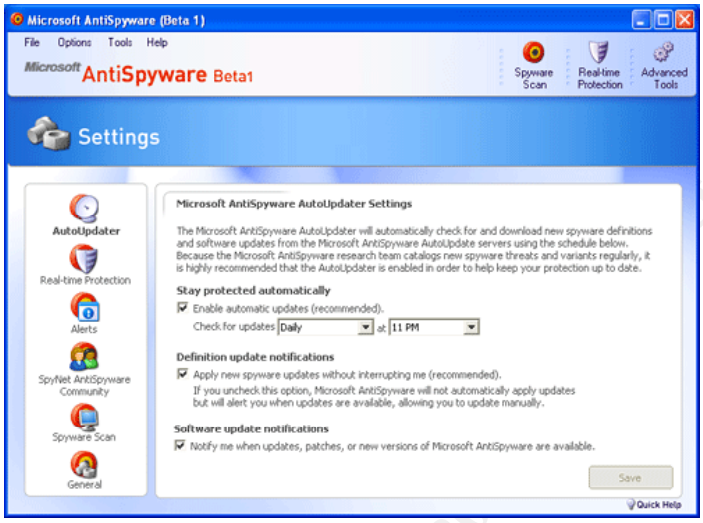

Figure 11 - Automatic Definition File Updates

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

How does it compare to other spyware products?

Based on early technical reviews, the Microsoft's AntiSpyware software is comparing favorably to its competitors' products. According to Wei-ming Lee of O'Reilly's Windows Development center, "the Microsoft AntiSpyware is off to a great start in that it already offers more features than the popular free versions of Ad-aware and Spybot Search & Destroy" [4]. Microsoft's AntiSpyware provides additional features such as Real-time protection against malicious spyware activities.

According to a test conducted by Tom Spring for PCWorld, "I found it able to identify the same three spyware threats that veteran spyware detectors Spybot Search and Destroy and Ad-Aware found on the system I used for testing. In fact, during my informal test, Microsoft AntiSpyware's scanning engine was able to scour my drive about twice as fast as Spybot Search and Destroy. Ad-Aware, however, was the fastest of the three." [5]

In a Spywarewarrior.com product test, the "AntiSpyware came out on top, detecting 111 of 138 possible spyware installs, compared to just 79 for Ad-aware (second place) and 69 for Spybot (fourth place). None of those programs reported any false positives, though another popular product, Pest Patrol, suffered a whopping 10 false positives and found just 55 real spyware installs." [9]

On the other hand, PC Magazine performed a test on the AntiSpyware product prior to Microsoft's purchase of Giant Software Company, and it published the following findings: "We compared its spyware removal and blocking abilities with those of nine other products for an upcoming article. Its performance wasn't outstanding. Overall, it removed about two-thirds of the adware, spyware, and keyloggers on our infested test system, and it blocked a little more than half of the threats we attempted to install on a clean system. An informal spyware removal test using the Microsoft's beta yielded similar results. It detected 51 threats and claimed to have removed them. But when we subsequently ran Webroot's Spy Sweeper 3.0 (our Editors' Choice for antispyware), we found almost 900 traces of 48 distinct threats still present, including two keyloggers and three Trojans. Some were merely leftover Registry entries or files in the browser's cache, but others were still active. With that, it looks like Microsoft still has work to do before they are on top of the market." [1]

© SANS Institute 2005 Author retains full rights.

Conclusion

The best defense against spyware is to understand how spyware is transmitted, and to prevent it from being downloaded in the first place. Other key considerations to preventing a spyware infection include downloading programs from trusted websites only; reading all security warnings, license agreements, and privacy statements before downloading any software; and finally, taking precautionary measures such as ensuring an antispyware program is loaded and running before downloading music or video files from peer to peer sites.

Many of the features in the Microsoft AntiSpyware software are customized to work only with the Internet Explorer browser. For instance, default settings can be restored to point the browser back to MSN as the home page, Internet Explorer as the default browser, and MSN Search as the default search engine. Further, removing history files only works with Microsoft programs, thus ignoring other products such as FireFox, Opera, and AOL software.[5] Designing the AntiSpyware tool to work only on the Windows platform and Internet Explorer browser may be a start for Microsoft. Hopefully, the AntiSpyware product will be expanded to detect spyware on other operating systems and competing web browsers.

The threat of spyware is unlikely to diminish in the near future. Adding AntiSpyware to today's growing suite of security tools - comprised of personal firewalls, host intrusion detection applications, antivirus software, vulnerability scanners, and security updates are viewed more to be a necessity, than a precautionary measure. But definitely, Microsoft has made a good choice in adding this AntiSpyware to its portfolio of security products.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

References

(1) Rubenking, Neil. "Microsoft AntiSpyware Beta 1" PC Magazine. 10 Jan. 2005 <http://www.pcmag.com/article2/0,1759,1749935,00.asp>

(2) Agarwal, Amit. "Spybot, Ad-aware face competition from Microsoft." The Indian Blogger 6 Jan. 2005 <http://labnol.blogspot.com/2005/01/spybot-ad-aware-face-competition-from.html>

(3) Kroll, David. "Microsoft AntiSpyware (Beta 1) – A Closer Look". ExtensionTech Net 10 Jan. 2005 <http://www.extensiontech.net/reviews/km/microsoft/asb1/2.shtml>

(4) Lee, Wei-Meng. "A First Look at Micrsoft's Anti-Spyware" O'Reilly Windows DevCenter.com 11 Jan. 2005 <http://www.windowsdevcenter.com/pub/a/windows/2005/01/11/antispyware.html>

(5) Spring, Tom. "First Look: Microsoft AntiSpyware". PCWorld.com 14 Jan. 2005 <http://www.pcworld.com/reviews/article/0,aid,119300,00.asp>

(6) "Spyware becoming a major threat to enterprise…" Continuity Central 1 Dec 2004 <http://www.continuitycentral.com/news01644.htm>

(7) Martin, Kelly. "Microsoft Anti-Spyware?" Security Focus 6 Jan. 2005 < http://www.securityfocus.com/columnists/289>

(8) "Frequently asked questions about Microsoft Windows AntiSpyware(Beta)" Microsoft Corporation 6 Jan. 2005 <http://www.microsoft.com/athome/security/spyware/software/faq.mspx>

(9) Thurrott, Paul. "Microsoft Anti-Spyware Preview" Paul Thurrot's Supersite for Windows 20 Dec. 2004 < http://www.winsupersite.com/reviews/ms_antispyware_preview.asp>

(10) Smith, Brian. "Defending against Spyware Invasion" SANS 28 Feb. 2004 <http://www.giac.org/practical/GSEC/Brian_Smith_GSEC.pdf>

(11) "Spyware Solutions – Technology and Leadership". Microsoft Corporation 17 Dec. 2004 <http://www.microsoft.com/athome/security/spyware/strategy.mspx>

(12) Preston, Gralla. "Microsoft Gets Anti-Spyware Right - Sort Of" O'Reilly Windows DevCenter.com 10 Jan. 2005

© SANS Institute 2005 Author retains full rights.

< http://www.oreillynet.com/pub/wlg/6177>

(13) "Microsoft Windows Antispyware" Microsoft Corporation 17 Dec. 2004 <http://www.microsoft.com/athome/security/spyware/software/default.mspx>

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.