Global Information Assurance Certification Paper

Manual Spyware Removal

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

Option 1 – Research on Topics in Information Security

Submitted By: Jonathon Ross
Location: SANS Local Mentor Session in Columbia,MD

Table of Contents

Abstract

Spyware represents a wide spread, high risk threat to internet users. Systems infected with just one spyware program can quickly become overridden with malicious software that decreases productivity and compromises data integrity. An October 2004 study of internet users conducted by America Online and the National Cyber Security Alliance found eighty percent of the respondents had spyware on their computers[1]. While the popular belief is that spyware causes annoying pop-up windows, the reality of spyware expands beyond marketing to include data theft and system compromise.

To combat the threat posed by spyware users need an effective process to remove malicious software from their computers. Several programs now exist that were designed to remove spyware from compromised systems. While these spyware cleaners are useful tools, no one program proves effective against all spyware threats. Using a combination of freely available software and utilities included with Microsoft Windows operating systems users can attack spyware manually; find where spyware threats start, stop active spyware programs, and remove spyware files from their systems.

Introduction

In just a few years time spyware has grown from a minor nuisance to a large scale security threat to all internet users. While much spyware is used for arguably legitimate marketing purposes, much more is starting to track and communicate information beyond the websites users visit and the links they click. Spyware now captures keyboard input, installs more malicious software (such as backdoors and viruses), and in some cases redirects all network traffic to an intermediary internet site effectively wiretapping the user's internet activity.

A majority of systems attached to the internet run a Microsoft Windows operating system. Due to its popularity, the majority of spyware targets Windows operating systems and the Microsoft web browser, Internet Explorer. Windows users need effective procedures to quickly remove spyware from their computers. While many good free and commercial anti-spyware programs are available, none are one hundred percent effective at identifying or removing spyware threats. To successfully eliminate threats, users must find the registry entries and system files used to start spyware. Once found, users must stop any running programs associated with spyware and delete the spyware files from their system.

Roadblocks to Removal

Successful spyware removal is more complicated than the approach of

[1] AOL/NCSA Online Safety Study, p. 4.

'download or purchase a good anti-spyware tool'. Spyware cleaners such as Ad-Aware and Spybot Search and Destroy are able to remove the files and registry entries associated with many spyware threats. Automated cleaning tools regularly fail to handle four components of spyware: actively running executable files, ActiveX objects, Browser Helper Objects, and Winsock Layered Service Providers.

Like legitimate software, spyware makes use of the registry settings and configuration files processed by Windows operating systems as they start. Spyware will place entries in these locations for its own executable files and start running as soon as the victim's computer boots. While a program is executing in memory on a computer its file cannot be deleted. To remove these threats spyware cleaners must remove the registry entry, stop the program, and delete the file. This sounds easy in theory, but is more complicated in practice. Some spyware installs itself so that it is started by the system or as a user with administrative privileges. To have any chance at successful removal, anti-spyware programs must be run as an administrative user. Even then there are processes integral to Windows that no user can ever stop without shutting down the system, and unfortunately there is spyware that successfully targets these programs.

ActiveX object is a very generic term for a Windows operating system. Where spyware is concerned an ActiveX object represents a program downloaded from the internet, stored on a computer, and generally used by Internet Explorer. However, Windows Explorer, the process that provides the Windows graphical user interface, uses parts of Internet Explorer and may also use the ActiveX objects. Spyware cleaners that cannot stop Windows Explorer may not successfully remove a malicious ActiveX object.

Browser Helper Objects are designed to allow extra features to be added into Internet Explorer, and by extension the Microsoft Windows user interface. The registry entry and file associated with a BHO are easily removed if there are no programs active using the object. One of the programs that can use BHOs is Windows Explorer and, like ActiveX objects, it must be stopped before removing a BHO or the threat may not be removed from the hard drive.

The intended purpose of a Layered Service Provider is easy extensibility of Winsock, the IP protocol stack used by current versions of Microsoft Windows operating systems. Spyware that utilizes LSPs is typically used to implement a man in the middle attack, forcing all internet traffic to a third party system before being sent to its intended destination. This presents a large security problem as the integrity of all IP based network communications is lost. The user has no way of knowing if the data they send reaches its recipient unchanged. Additionally the user has no way of verifying the data they receive is returned from the location they were attempting to contact. It is very easy for a spyware cleaner to remove a LSP file. However, removing the LSP file does not remove

its reference from Winsock. As a consequence, IP networking usually fails on a computer after a LSP file is deleted. Repairing Winsock is possible, but is not usually done by spyware cleaning tools.

All of these problems can and will be addressed as anti-spyware software continues to develop. However, no matter how efficient anti-spyware software becomes it will always fail against 0-day spyware. A 0-day exploit is defined as malicious software that takes advantage of security vulnerabilities the same day they become generally known. Let us define 0-day spyware as any new or newly mutated spyware that the internet community does not generally know about. Like anti-virus programs, anti-spyware software is only as effective as the definitions used to identify threats. Spyware is constantly evolving in an attempt to avoid detection and removal. New spyware will continue to be seen, just as new viruses and new security vulnerabilities will continue to be discovered. Until their spyware definitions are updated, anti-spyware software will fail to detect 0-day spyware threats.

0-day spyware might not seem like a high risk threat, but consider the examples that Internet Storm Center Handler Tom Liston published on isc.sans.org site on 23 July 2004, 23 August 2004 and 4 November 2004.

> After installing the Google Toolbar, I did exactly what my "Joe Average" had done to get his machine compromised: Googled. Someone had told him about "Yahoo Games", and well, he wanted to check it out. I put "Yahoo games" into Google and then (for whatever reason... hey, it's what my "Joe Average" did) skipped several obvious links leading to Yahoo! and clicked instead on "www.yahoogamez.com" (NOTE: If you're running an unpatched machine, DO NOT GO THERE).[2]

Three lengthy diary entries follow tracing the malicious software that gets installed on his test system as a result of following one malicious link. At the end of his 4 November 2004 diary entry, Mr. Liston counts fifteen downloaded files weighing in over two megabytes. Any spyware program on a computer could act as an entry point for more malicious software. When cleaning spyware, the user must be as thorough as possible or they leave their system vulnerable to further attack. 0-day spyware, immune to automated cleaning tools, requires users to learn other methods to defend themselves.

Given the weaknesses of automated cleaning tools, users must take steps to find and remove some spyware manually. While current spyware may mutate, and new spyware will continue to emerge, the methods employed by spyware to execute once installed on a system do not change as often. Spyware uses the same registry entries and system files as legitimate software to start running just after system start up. Even when Microsoft changes their operating systems and adds a new path for automatic software execution, it is

[2] Liston http://isc.sans.org/diary.php?date=2004-07-23

documented as it becomes available.

The process of removing spyware manually is repetitive. Threatening files are identified through examination of Windows' registry and system files. The malicious start up entry must be removed to prevent future execution of the spyware file. Any program utilizing a threat is forcibly stopped and the malicious file removed. This process should be repeated until no malicious software is executing on the computer. All the necessary tools exist as part of Windows default installations, but using a combination of freely available tools in conjunction with Windows utilities offers a more expedient approach to successful removal.

Step 1: Prepare the User, the Tools, and the Computer

To find and remove spyware the user will look through Windows' registry and system files for start up entries that pertain to all the software on the computer, both legitimate and malicious. Successful removal depends on distinguishing good software from bad. Google searches for registry key names or filenames help, as do searches with security vendors such as Symantec's Security response site, http://securityresponse.symantec.com/, and UniBlue Systems Ltd WinTasks Process Library page located at http://www.liutilities.com/products/wintaskspro/processlibrary/. However, no amount of online intelligence gathering can replace a good working knowledge of the target system. The advice, 'Know thy system', is as applicable in hunting spyware as it is for any other system level security task.

A list of Windows automatic startup locations is available from the bleepingcomputer.com website at http://www.bleepingcomputer.com/forums/index.php?showtutorial=44. Microsoft's registry editing tools regedit.exe and regedt32.exe can be used to search through the registry for these entries. Windows 98, ME, and XP also offer the msconfig utility which displays some of these entries. For a more thorough display of startups, use a free tool called Autoruns that can be downloaded from http://www.sysinternals.com/ntw2k/freeware/autoruns.shtml.

Using a list of automatic startup programs, a user can find the executable spyware programs on their computer. However, spyware uses more than just programs to infect systems. ActiveX objects, Browser Helper Objects, and Layered Service Providers use other registry entries. Spyware will also attack browser settings for home page and search engine preference as well as modify the legacy name resolution hosts file. A free tool exists that performs a comprehensive search through the automatic startup entries as well as registry keys and files associated with other spyware threats.

Hijackthis, available from http://www.spywareinfo.com/~merijn, searches the operating system for changes known to be made by spyware, displays them,

and can attempt to remove any problems it finds. Since Hijackthis is looking for vectors of spyware infection it is not defeated by new or mutated spyware. However, Hijackthis is still susceptible to some 0-day spyware threats that make use of a previously unknown method of system infection. Users should check the website regularly for updated versions of Hijackthis that incorporate newly discovered infection methods. When run, Hijackthis displays all registry entries and modified files that it knows to be used by spyware. The display will also include legitimate programs; therefore, users should proceed cautiously when asking Hijackthis to modify their registry or system files.

After identifying spyware, the next task is to stop any software associated with it. Windows Task Manager (taskmgr.exe) can be used to forcibly stop software. Task Manager is especially useful for stopping explorer.exe and preventing it from starting again automatically. Users will also need to search for programs using dynamic link libraries that are associated with spyware. Process Explorer from Sysinternals will show the processes running on a system, and the files being used by each. Process Explorer can be downloaded from http://www.sysinternals.com/ntw2k/freeware/procexp.shtml.

Finally, Windows Command Prompt (cmd.exe or command.com depending on the Windows version) is needed to delete spyware files from a system. Since having Windows Explorer running while removing spyware can be detrimental, the file utilities available through the command prompt must be used. To remove individual files use *del <filename>* or *erase <filename>.* Some spyware will create a directory structure for its files. *rmdir /s <directory name>* will remove a directory and all of its files and subdirectories. Familiarity with the *attrib* command will also be necessary as some spyware will set file attribute flags to protect them from being deleted.

Before removing spyware it is helpful, but not required, to place the operating system in safe mode. With Windows running in safe mode many of the automatic start up files and registry entries are not processed. In safe mode many spyware programs will be laying dormant allowing easier removal. Spyware can be removed without running in safe mode, but many more programs will need to be stopped by Task Manager before their files can be deleted.

Whether in safe mode or not it is best to prepare the infected system for spyware removal by doing the following:

1. Log in as a user with administrative privilege. Use the administrator account if possible.
2. Start the Command Prompt by clicking ‘Start->Run’ and entering either *command.com* or *cmd.exe* in the dialog box before clicking ‘Ok’.
3. From the command prompt start Task Manager by entering *taskmgr.exe*.
4. Use the command prompt to start Hijackthis. Methods for starting will

depend on where the program is stored. Placing this tool on a recordable CD-Rom or write-protected removable storage is recommended.
5. Use Task Manager to stop any running web browsers. While Internet Explorer is the most used and most targeted browser available, browsers such as Firefox, Mozilla, and Netscape are targeted by spyware as well.
6. Finally, use Task Manager to stop *explorer.exe*. What will be left is the desktop background with three programs that will be used most during cleanup.

Step 2: Find the Spyware

With Hijackthis running, click the 'Scan' button to generate a list of system configuration entries associated with spyware. Hijackthis scans the registry entries and files used to start programs, load dynamic link libraries, modify browser settings, and extend Winsock with additional LSPs. After running a scan, a list of all items found is displayed. Hijackthis has a helpful 'Info on selected item' button that provides information associated with a highlighted result. A detailed listing of each result type is available at http://aumha.org/a/hjttutor.htm. As the goal of this process is to remove the hardest to delete spyware, focus on the following entries first:

1. F0, F1, F2, F3 and O4. These entries represent programs that are automatically started when the operating system boots.
2. O2 and O3. These headings are used for browser helper objects and Internet Explorer toolbars.
3. O16. These entries display ActiveX objects downloaded to the computer.
4. O10. These are issues related to Winsock layered service providers. This could be missing files still referenced by Winsock or display the locations of malicious LSPs.

Most of the items returned by Hijackthis are related to legitimate software. Knowledge of the computer's normal usage, examining the Add/Remove Programs tool in the Control Panel, browsing through the Start menu, and searching the internet are all helpful in differentiating good entries from bad. At this stage searching the internet is best done from a second system, if possible, as using web browsers can lead to more spyware infection if used before a system is clean.

Of the items that cannot be explained by installed software some will be easy to identify as hazardous. Consider the following entry taken from an infected system.

O4 - HKLM\..\Run: [dkmbscttjintb] C:\WINNT\system32\ibnktw.exe

A Google search for this executable does not return any results. Sometimes the lack of Google results should be as concerning as a result that links a program

to spyware. Unless the computer is used to develop new software it is probably not safe to have programs on it that are unrecognized. The registry key's name, dkmbscttjintb, and the executable program's name, ibnktw.exe, appear random. While legitimate executables may have names that appear like nonsense, the labels for their registry entries are usually meaningful. Also strange is the location of the executable, C:\WINNT\system32. This is a folder of system files used by the operating system. User installed software should rarely appear here. Given all this information, it is safe to presume that ibnktw.exe is a threat, or at least unnecessary, and should be removed. Before using Hijackthis to delete an entry, first identify associated processes and locate the file on the hard drive.

Step 3: Identify Running Processes

Some spyware identified by using Hijackthis will not be associated with any processes, nor related to Internet Explorer, which should not be running during the removal process. When removing ActiveX objects or BHOs it is sufficient to stop Internet Explorer and Windows Explorer. Checking for running processes is most important when attempting to remove spyware that is labeled with F0, F1, F2, F3 or O4 in Hijackthis. These labels represent automatically started programs, and if the file existed on the system at boot time it will probably still be running during clean up. When cleaning other types of spyware threats this step may not be necessary and can be skipped.

If the file referenced in the Hijackthis log is a dynamic link library, as is common with BHOs, Sysinternal's Process Explorer may be necessary to locate processes associated with the target. Another trick of spyware is to install itself as a system service. In this case, the guilty process may be *rundll32.exe* or *svchost.exe.* A normal Windows system may have multiple copies of *rundll32.exe* or *svchost.exe* running. Process Explorer can display the files in use by programs, and also includes a DLL search feature that displays all processes associated with a specified DLL file.

Process Explorer can also be used to stop programs, but Task Manager is more effective at doing so. Use Process Explorer to find the process identifier (PID) of the spyware program. Then configure Task Manager to display PIDs by clicking on 'View->Select Columns…' and checking the box next to PID. With the PID found in Process Explorer, Task Manager can be used to stop software even if multiple programs of the same name are executing concurrently.

In the Hijackthis example shown previously, an executable file listed in a registry entry is marked for removal. This registry entry causes a program to run at boot time and remain running as long as the system is up. Task Manager's 'Processes' tab should be used to see if the process is currently running on the computer. Make sure the option 'Show processes from all users' is selected if it appears in the lower left corner of the Task Manager window to insure all

programs are displayed. It is possible that no process will be found. The entry listed by Hijackthis may be related to a file that is no longer on the computer. If this is the case, move on to step 4 and continue the removal process. The example file, ibnktw.exe, was listed in Task Manager's process list at the time of clean up. Clicking once on the process name highlights the program, allowing it to be stopped by then clicking the 'End Process' button.

Stopping spyware software before using Hijackthis to also remove its startup entry may be counter productive as the program may start up again instantly. With a Hijackthis entry and any associated processes identified, the next step before removing any item is to locate the spyware file on the hard drive.

Step 4: Find the Spyware File on the Hard Drive

To find the targeted file first attempt to get a directory listing using *dir <full pathname>.* For our example file the syntax would be

dir c:\winnt\system32\ibnktw.exe

In most cases this will show the file's last modification time, size, and name. When searching for spyware the result might be 'File Not Found'. It is possible the file is already gone and the entry displayed in Hijackthis is an orphan. More likely, the file has some attributes set preventing *dir* from displaying the information. Whenever *dir* alone fails, try using *dir /ah <full pathname>* and *dir /as <full pathname>*. These switches will display files with hidden and system attributes set respectively. If *dir* still returns 'File Not Found' then it is safe to assume that the file does not exist on the system.

If a directory listing is achieved, the last modification time may offer more evidence that a file is associated with spyware. The example file had been modified in the last twenty-four hours. The user had done no system updates or software installs of any kind in months making an executable file stored in c:\winnt\system32 with a recent modification time very suspicious. At this point it is time to remove the threat from the system. Throughout cleanup no web browsers should be running on the system, but if any have been started to research Hijackthis entries, stop them before proceeding to the next step.

Step 5: Remove the Spyware

With spyware identified and located, removal is done in three steps. First, remove the spyware's start up entry by using Hijackthis. To remove an entry check the box to the left of the entry in Hijackthis and click 'Fix checked'. Hijackthis will remove the entry from the associated registry location or system file, and in some cases attempt to remove the file referenced by the entry from the hard drive. Removing the startup entry first is important; some entries will cause software to restart any time it is stopped, not just at system boot time.

Next, any processes using the spyware file must be stopped. Task Manager provides the best means of forcibly stopping programs. In Task Manager's processes tab click any entry previously identified as spyware to highlight the process then click the 'End Process' button at the lower right of the window. It is possible Task Manager will refuse to stop a process. In this case, confirm the login being used has administrative privilege and try again. Another possible problem, especially when stopping programs related to services such as *svchost.exe,* is the system requesting a reboot after the process stops. Should a popup appear requesting reboot, attempt to continue the process first and remove the files from the hard drive. If this not be possible restart the system in safe mode and try again.

Finally, use Windows command prompt to remove the spyware file from the hard drive. If either the hidden or system attributes were set, they will need to be removed using *attrib –h –s -r <filename>.* The *–h* switch removes the hidden attribute, the *-s* switch the system attribute, and the *–r* switch has been included to clear the read-only attribute. Read-only will not prevent the file from displaying under a normal *dir*, but it may be found on some spyware files as another attempt to prevent removal. If there is any question as to a file's attributes, running *attrib <filename>* will display the attributes without making any changes to them.

After clearing any attributes, remove the file with *del <filename>*. It is best to not use any wildcard characters in the filename during this process as spyware will exist in system directories with other legitimate and necessary applications. In the case where an entire directory is set aside for spyware such as C:\Program Files\Web Offers, use *rmdir /s <directory name>* to remove the directory and all files contained within it. Should an 'Access is denied' error be returned after attempting the delete, either an attribute is still set or there is an executable program still accessing the file. Use *attrib* to verify that file attributes are not still set, use Task Manager and Process Explorer to verify no programs are executing or using the file, and attempt to delete the file again.

Step 6: Repeat the Process

The first five steps should be repeated until no spyware is noted in the Hijackthis log. As a general rule, it is best to remove executable programs first. In addition to its nefarious activities, spyware executables will actively look to install new versions of themselves or other spyware programs. A user removing BHOs or an LSP might find that these same problems return even after deleting them several times. Some spyware executables are capable of downloading exploits from the internet, while other specimens create copies of their code on a hard drive under new names. As long as these programs are left running the computer is out of the user's control and no assumptions should be made as to what the software cannot do.

Once the system is no longer running any malicious programs, the next target should be ActiveX downloaded program files and Browser Helper Objects. Until these spyware threats are removed it is not safe to start Windows user interface or Internet Explorer. Just like spyware executable programs, the spyware DLLs associated with ActiveX objects and BHOs will do anything in the name of self preservation and can, under certain conditions, install more spyware on a system.

Next the user should remove any LSPs reported by Hijackthis. The file used by a LSP can be deleted at any time. The operating system makes no attempt to protect this file as it does for files in use by executable programs. However, Winsock will attempt to use the malicious file as a part of processing network traffic even after it has been removed. The result is impaired or inoperable networking functions. Two tools for repairing Winsock are LSPFix and WinsockXPFix. These tools are available from http://www.cexx.org/lspfix.htm and http://www.spychecker.com/program/winsockxpfix.html, respectively. Users of Windows XP Service Pack 2 can also use the following command, *netsh winsock reset catalog*, to reset Winsock to its default configuration.

At this point the most difficult to remove spyware threats have been removed from the system. Before continuing, scan the Hijackthis log one last time for any other abnormal entries. Spyware will also modify the hosts file, DNS settings, and browser settings (such as the home page and search engine). Any of these changes could redirect an innocent attempt to browse the web toward sites that will download and install more malicious software.

Step 7: Use an Automated Cleaning Tool

The previous steps focused on removing the registry entries and directly used by spyware to execute its malicious activities. These files represent the hardest items for an automated spyware scanner to remove. Spyware threats are rarely contained in just one registry entry or file. Finding and removing these registry entries and files is best done by an automated tool.

Numerous tools are available on the internet for scanning and removing spyware from a system. Each spyware removal program comes with its own set of definitions, and each has its own strengths and weaknesses against different spyware specimens. Therefore, the best results are obtained by using multiple programs to scan for files that the manual process did not remove.

When deciding which anti-spyware tools to use consult Eric L. Howes Anti-Spyware Test at http://spywarewarrior.com/asw-test-guide.htm, which also includes a page of suspected rogue anti-spyware products. Users should be careful selecting anti-spyware tools. Some tools turn out to be spyware that eliminates the competition on a system then installs its own malicious

programs. Ad-Aware and Spybot Search and Destroy are two popular, legitimate anti-spyware tools that work well.

Step 8: Repeat All Steps for Each User

At the beginning of the process it was advised to remove spyware while logged in as an administrative user, preferably administrator. On computers with multiple users the cleaning process should be applied once for each user. The first cleaning as an administrator will remove most spyware threats from a system, but there are some registry settings and files specific to each user account on a Windows system. The most likely place to find more spyware will be in the user profiles which contain Internet Explorer's cache and cookie files. Some data stored in a user's profile have strict permissions allowing access only by the owner. Spyware scans, even while logged in as administrator, will fail to detect spyware hiding in areas of the registry that are user specific, and in files they lack permission to access.

Summary

Spyware is the newest external threat to internet users' security and may be one of the most dangerous. Just one spyware program can provide a conduit for dozens of other malicious programs to infect a computer. The damage from spyware ranges from lost productivity to the loss of sensitive data. Many automated tools exist to remove spyware from computers, but these programs should not be considered a silver bullet. Spyware, like other malicious software, is adept at avoiding detection and preventing removal.

Effective and efficient spyware removal is a manual process that targets active spyware, and removes it clearing the way for anti-spyware software to complete the work. Hijackthis, Windows Task Manager, Windows Command Prompt, Sysinternal's Process Explorer, a Winsock repair utility, and two anti-spyware programs such as Lavasoft's Ad-Aware and Safer Networking Limited's Spybot Search and Destroy form a toolkit for spyware removal. By first eliminating threats found using Hijackthis, a system is left with only dormant spyware. Applying multiple anti-spyware programs to a system in this state will remove the remaining inactive threats, leaving behind a spyware free computer.

References

America Online and National Cyber Security Alliance. "AOL/NCSA Online Safety Study". 25 October 2004.
URL: http://www.staysafeonline.info/news/safety_study_v04.pdf

Bellekom, Merjin. Hijackthis. 2004.
URL: http://www.spywareinfo.com/~merijn/

Bellekom, Merijn and Eshelman, James A. "Hijackthis Log Tutorial". 2004.
URL: http://aumha.org/a/hjttutor.htm

Bleeping Computer. "Windows Program Automatic Startup Locations". 1 April 2004.
URL: http://www.bleepingcomputer.com/forums/index.php?showtutorial=44

Cexx.org. LSPFix. URL: http://www.cexx.org/lspfix.htm

Consortium of Anti-Spyware Technology Vendors. "Glossary". 2003.
URL: http://www.coast-info.org/glossary.htm

Healan, Mike. "Browser Hijacking". 23 March 2004.
URL: http://www.spywareinfo.com/articles/hijacked/

Healan, Mike. "Prevent Browser Hijacking". 7 May 2004.
URL: http://www.spywareinfo.com/articles/hijacked/prevent.php

Horowitz, Michael. "Removing Spyware". 31 October 2004.
URL: http://www.michaelhorowitz.com/removespyware.html

Howes, Eric L. "Anti-Spyware Test (Guide)". 15 October 2004.
URL: http://spywarewarrior.com/asw-test-guide.htm

Kolla, Patrick M. SpyBot Search and Destroy. 2004.
URL: http://www.safer-networking.org/en/index.html

Lavasoft Inc. Ad-Aware. 2004. URL: http://www.lavasoftusa.com

Liston, Tom. "Handlers Diary July 23rd 2004". 23 July 2004.
URL: http://isc.sans.org/diary.php?date=2004-07-23

Liston, Tom. "Handlers Diary August 23rd 2004". 23 August 2004.
URL: http://isc.sans.org/diary.php?date=2004-08-23

Liston, Tom. "Handlers Diary November 4th 2004". 4 November 2004.
URL: http://isc.sans.org/diary.php?date=2004-11-04

LIUtilities (Uniblue Systems LTD). "WinTasks Process Library". 2004.
URL: http://www.liutilities.com/products/wintaskspro/processlibrary/

Microsoft Corporation. "Command-line reference A-Z".
URL:
http://www.microsoft.com/windowsxp/home/using/productdoc/en/default.asp?url=/windowsxp/home/using/productdoc/en/ntcmds.asp

Microsoft Corporation. "Changes to Functionality in Microsoft Windows XP Service Pack 2: Part 2: Network Protection Technologies". 4 November 2004.
URL:
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx

Option Explicit. WinsockXPFix.
URL: http://www.spychecker.com/program/winsockxpfix.html

Pham, Theodore. "Spyware Removal & Prevention". 28 September 2004.
URL:
http://www.cmu.edu/computing/dept-computing/forums/2004-09/Spyware.ppt

Russinovich, Mark and Cogswell, Bryce. Sysinternals Autoruns.
URL: http://www.sysinternals.com/ntw2k/freeware/autoruns.shtml

Russinovich, Mark and Cogswell, Bryce. Sysinternals Process Explorer.
URL: http://www.sysinternals.com/ntw2k/freeware/procexp.shtml

Symantec Corporation. "Security Response".
URL: http://securityresponse.symantec.com