

Steve's Tech Resource

The Web Development, Internet, Software, Hardware, and Multimedia Resource

[HOME](#)[ABOUT](#)[WHAT'S NEW](#)[LOGIN](#)[JOIN](#)[SEARCH](#)[BY DATE](#)[ALL BOARDS](#)

On Windows 2000/XP/Vista/7 Processes And Identifying Malware Infection

80.2KB

For: [Windows 2000 Professional](#) | [Windows XP](#) | [Windows Vista](#) | [Windows 7](#)

Published: 08Dec03 | Last Updated: 29Jan11 | Status: To Be Continued

- [1. Introduction](#)
- [2. Accessing The Processes Tab](#)
 - [2.1. Accessing The Processes Tab: Windows 2000/XP](#)
 - [2.2. Accessing The Processes Tab: Windows Vista](#)
 - [2.3. Accessing The Processes Tab: Windows 7](#)
- [3. Establishing The Baseline Processes List](#)
 - [3.1. Establishing The Baseline Processes List: Clean Installation Of Windows 2000/XP/Vista/7](#)
 - [3.2. Establishing The Baseline Processes List: Existing Installation Of Windows 2000/XP/Vista/7](#)
- [4. On Identifying Malware Infection](#)
- [5. Identifying Malware Infection Example](#)
- [6. Additional Reading](#)

1. Introduction

Malware, short for **malicious software**, is a broad term that refers to viruses, worms, trojans, spyware, Browser hijackers, etc.. A computer that has contracted malware is known as being infected. Upon infection, the malware performs one or more actions on the infected computer. The actions are typically malicious in nature, hence the term, malware. The malicious actions may occur a single time, each time the computer is booted, or according to some other schedule prescribed by the malware. In some cases it is easy to suspect malware infection because one or more of the malicious actions are obvious. For example, the performance of the computer and/or the Internet seems markedly reduced, the computer automatically reboots itself, or pop-ups suddenly appear. In other cases it is difficult to suspect malware infection because the malicious actions are inconspicuous. For example, a listening port is opened, or some files are created, deleted, or patched that do not affect Windows or any application.

The action performing agent of software (including malware) is its executable(s). An executable is a file that can be run (i.e., executed) which, upon being run, performs some action. There are numerous executable file types. The principle executable file type for most software (including malware) is an .exe file. Accordingly, malware infection typically involves an .exe file being deposited on, and running on, the infected computer.

Note:

- Other executable file types include .bat, .com, .chm, .dll, .pif, and .shs files. For additional information, see [Program Executable Filename Extensions \(file-extensions.org\)](#).
- Some malware infections are the result of a non .exe executable file being deposited on, and running on, the infected computer. Further discussion of malware infection by a non .exe executable is beyond the scope of this page.

There is an unfortunate tendency for antivirus/antispyware/firewall software users to assume they are immune from malware infection. This is mistake for many reasons. First, there is always some lag time between the creation of a new piece of malware and the antivirus/antispyware/firewall software vendors detecting it in the wild and updating their software to protect against it. For this reason alone a user is always vulnerable to malware infection. Second, to detect the latest malware, the user must update their antivirus/antispyware/firewall software on a regular basis. Many users, and dial-up users in particular, do not have the patience or discipline for this. Third, antivirus/antispyware/firewall software is not fail-safe on at least two levels: 1.) antivirus/antispyware/firewall software is only as good as person using/configuring it, and 2.) antivirus/antispyware/firewall software is not 100% effective in detecting the malware it should detect. Lastly, some malware has the ability to disable antivirus/antispyware/firewall software, thereby rendering it partially or completely ineffective.

For these reasons, and others, it is strongly recommended that a security conscious user employs an antivirus/antispyware/firewall

software **independent** method for identifying malware infection. And not only should the method be employed when malware infection is suspected, but periodically even when malware infection is not suspected so as to identify malware infection in those cases where the malicious action is inconspicuous. One such antivirus/antispysware/firewall software independent method for identifying malware infection that is available to all Windows 2000 Professional, Windows XP, Windows Vista, and Windows 7 (Windows 2000/XP/Vista/7) users involves monitoring the Windows 2000/XP/Vista/7 Processes tab.

In short, a process is a running .exe file. The Windows 2000/XP/Vista/7 Task Manager includes a Processes tab which lists the currently running processes (i.e., the currently running .exe files). Since malware infection typically involves an .exe file being deposited on, and running on, the infected computer, monitoring the Processes tab so as to distinguish legitimate Windows and application processes from illegitimate malware affiliated processes is an extremely powerful antivirus/antispysware/firewall software independent method for identifying malware infection.

Important Note: For screen shots of the Processes tab after clean installations of Windows 2000/XP/Vista/7 at various Service Pack levels see [Windows 2000/XP/Vista/7 Default Processes \(stevetechresource.com\)](http://www.stevetechresource.com). Each line in the Processes tab is a process, and the running .exe file for each process is listed.

Anytime malware infection is suspected, to stop the malware from possibly spreading to other computers on the network (i.e., an Intranet and/or the Internet), the suspect computer must be taken offline until it is determined whether or not the computer is infected, and, if the computer is infected, until the malware infection is confirmed removed. Depending upon the version of Windows and how many applications are installed and configured to run at startup, the Processes tab can list anywhere from 15 to 50+ processes. The larger the number of processes the more tedious and time consuming it is to investigate each and every processes as possibly being malware affiliated. And if the computer performs a mission critical function, investigating each and every process as possibly being malware affiliated is simply not practical.

The procedure for identifying malware infection described in this page aims to reduce the amount of time it takes to identify malware infection, and, therefore, to reduce computer downtime, by making use of a so-called Baseline Processes List. The Baseline Processes List is the list of legitimate Windows and application processes that appear in the Processes tab upon starting the computer. With the Baseline Processes List in hand, checking the Processes tab for a possible malware affiliated process is simply a matter of comparing the Baseline Processes List to computer's current processes and crossing off the processes that appear in both. Then, rather than having to investigate each and every one of the computer's current processes, only the newly listed, uncrossed off processes need to be investigated as possibly being affiliated.

The Baseline Processes List is easier to establish with a clean installation of Windows 2000/XP/Vista/7 than with an existing installation of Windows 2000/XP/Vista/7. With a clean installation of Windows 2000/XP/Vista/7, since it is possible to install Windows and one's applications free from malware infection, the Windows 2000/XP/Vista/7 Processes tab lists only legitimate Windows and application processes and, therefore, immediately qualifies as the Baseline Processes List. With an existing installation of Windows, on the other hand, first it must be determined whether or not the computer is malware infected, and, if the computer is malware infected, the malware must be removed. Only after the computer is confirmed malware free is it trusted that the Processes tab lists only legitimate Windows and application processes and, therefore, qualify as the Baseline Processes List.

2. Accessing The Processes Tab

The Processes tab lists the currently running processes (i.e., the currently running .exe files). Accessing the Processes tab is required to establish the Baseline Processes List and to check the computer for possible malware affiliated processes.

2.1. Accessing The Processes Tab: Windows 2000/XP

- From The Desktop: Right click the **taskbar** and then click **Task Manager | Processes**.
- Keyboard Shortcut Ctrl+Shift+Esc: Press **Ctrl+Shift+Esc** and then click **Processes**.
- Keyboard Shortcut Ctrl+Alt+Del: Press **Ctrl+Alt+Del** and then click **Processes**.

2.2. Accessing The Processes Tab: Windows Vista

- From The Desktop: Right click the **taskbar** and then click **Task Manager | Processes**.
- Keyboard Shortcut Ctrl+Shift+Esc: Press **Ctrl+Shift+Esc** and then click **Processes**.
- Keyboard Shortcut Ctrl+Alt+Del: Press **Ctrl+Alt+Del** and then click **Start Task Manager | Processes**.

2.3. Accessing The Processes Tab: Windows 7

- From The Desktop: Right click the **taskbar** and then click **Start Task Manager | Processes**.
- Keyboard Shortcut Ctrl+Shift+Esc: Press **Ctrl+Shift+Esc** and then click **Processes**.
- Keyboard Shortcut Ctrl+Alt+Del: Press **Ctrl+Alt+Del** and then click **Start Task Manager | Processes**.

3. Establishing The Baseline Processes List

3.1. Establishing The Baseline Processes List: Clean Installation Of Windows 2000/XP/Vista/7

1. Perform a clean installation of Windows 2000/XP/Vista/7 according to [Securing A Clean Installation Of Windows XP/Vista/7 \(stevestechresource.com\)](http://www.stevestechresource.com).
2. Install all reputable, known malware-free applications that you use and, if applicable, connect to the manufacturer's Web sites to download/install any updates.
3. Restart the computer
4. Take a screen shot of, or write down the complete contents of the Windows 2000/XP/Vista/7 Processes tab. This list of processes is the Baseline Processes List.
5. Anytime something is installed or uninstalled (be it a Windows Component, a Windows or Office Service Pack, a Windows/Microsoft Update, an application, etc.) restart the computer and take a screen shot of, or write down the complete contents of the Windows 2000/XP/Vista/7 Processes tab. This list of processes is the updated Baseline Processes List.

3.2. Establishing The Baseline Processes List: Existing Installation Of Windows 2000/XP/Vista/7

1. Restart the computer.
2. Take a screen shot of, or write down the complete contents of the Windows 2000/XP/Vista/7 Processes tab. This list of processes is the Starting Processes List.
3. The processes associated with a clean installation of Windows 2000/XP/Vista/7 are legitimate and can be crossed off from the Starting Processes List. From the starting processes list, cross off the processes associated with a clean installation of your version of Windows as shown in [Windows 2000/XP/Vista/7 Default Processes \(stevestechresource.com\)](http://www.stevestechresource.com).
4. The processes associated with reputable, known malware-free, applications that you install are legitimate and can be crossed off from the starting processes list. For the remaining, uncrossed off processes in the Starting Processes List, search your computer for each processes' .exe file. If the path to the .exe file corresponds to installation directory for the application, cross off the process from the Starting Processes List.
5. For the remaining, uncrossed off processes in the Starting Processes List, search Google for each processes' .exe file. If the .exe file appears to be malware affiliated, read the available literature for instructions on how to positively identify malware infection. Some common ways in which malware infection is positively identified include: 1.) The presence of a file with a filename unique to malware infection, 2.) The presence of a file with a Windows or application filename but being the wrong size and/or in the wrong location unique to malware infection, 3.) The absence of a Windows or application file unique to malware infection, 4.) A non-traditional .exe file being run as a Service or on computer startup via the Windows Startup menu or some other method unique to malware infection, and 5.) An entry added to or deleted from the registry unique to malware infection.
6. If the .exe file cannot be positively identified with malware infection and/or appears to be a legitimate Windows or application file, cross it off from the Starting Processes List. If the .exe file is positively identified with malware infection, read the available literature for instructions on how to remove the malware. Then either manually remove the malware or employ some software solution to remove the malware. Restart the computer and confirm that the malware is removed, including that the malware process is no longer listed in the Windows 2000/XP/Vista/7 Processes tab. Once the malware is confirmed removed, cross of the malware process from the Starting Processes List.
7. Once all processes in the Starting Processes List are crossed off (i.e., are accounted for either as legitimate Windows or application processes, or as illegitimate malware processes that have been removed) restart the computer and take a screen shot of, or write down the complete contents of the Windows 2000/XP/Vista/7 Processes tab. This list of processes is the Baseline Processes List.
8. Anytime something is installed or uninstalled (i.e., a Windows Component, a Windows or Office Service Pack, a Windows/Microsoft Update, an application, etc.) restart the computer and take a screen shot of, or write down the complete contents of the Windows 2000/XP/Vista/7 Processes tab. This list of processes is the updated Baseline Processes List.

4. On Identifying Malware Infection

Note: The following assumes the user has established the Baseline Processes List described in [Establishing The Baseline Processes List \(above\)](#).

1. Anytime malware infection is suspected, or approximately once a month even when malware infection is not suspected, take a screen shot of, or write down the complete contents of the Windows 2000/XP/Vista/7 Processes tab. This list of processes is the Current Processes List.
2. From the Current Processes List, cross off the processes that appear in the Baseline Processes List.
3. For the remaining, uncrossed off processes in the Current Processes List, search Google for each processes' .exe file. If the .exe file appears to be malware affiliated, read the available literature for instructions on how to positively identify malware infection. Some common ways in which malware infection is positively identified include: 1.) The presence of a file

- with a filename unique to malware infection, 2.) The presence of a file with a Windows or application filename but being the wrong size and/or in the wrong location unique to malware infection, 3.) The absence of a Windows or application file unique to malware infection, 4.) A non-traditional .exe file being run as a Service or on computer startup via the Windows Startup menu or some other method unique to malware infection, and 5.) An entry added to or deleted from the registry unique to malware infection.
4. If the .exe file cannot be positively identified with malware infection and/or appears to be a legitimate Windows or application file, cross it off from the Current Processes List. If the .exe file is positively identified with malware infection, read the available literature for instructions on how to remove the malware. Then either manually remove the malware or employ some software solution to remove the malware. Restart the computer and confirm that the malware is removed, including that the malware process is no longer listed in the Windows 2000/XP/Vista/7 Processes tab. Once the malware is confirmed removed, crossed off the malware process from the Current Processes List.
 5. Once all processes in the Current Processes List are crossed off (i.e., are accounted for either as legitimate Windows or application processes, or as illegitimate malware processes that have been removed) restart the computer and take a screen shot of, or write down the complete contents of the Windows 2000/XP/Vista/7 Processes tab. This list of processes is the updated Baseline Processes List.
 6. Repeat steps 1-5 above as needed.

5. Identifying Malware Infection Example

The following is a real-world example of the power and utility of monitoring the Processes tab for possible malware affiliated processes. In short, a Web server of dubious history running Windows 2000 was configured for a network, attached to that network, and powered on. When the desktop appeared I suggested placing the Local Area Connection (LAC) icon in the system tray. The LAC icon was lit solid, which I pointed out was odd for the amount of traffic that server typically received. I then suggested running NETSTAT, to which we both noticed traffic on ports not associated with the server's Web host function. The person sitting at the computer expressed the concern that the computer might be infected with malware, to which I agreed. Knowing the computer did not have any antivirus/antispyware/firewall software installed and, therefore, that the person sitting at the computer was at a loss for quickly identifying malware infection, I suggested opening the Processes tab. Immediately understanding where I was coming from, the person sitting at the computer opened the Processes tab, we both noted a suspicious process, and, without saying a word, I disconnected the ethernet cable, and we both went to our computer's to investigate the suspicious processes' .exe file, DLLHOST.EXE.

A search at Google for DLLHOST.EXE returns, amongst other things, that DLLHOST.EXE is a legitimate Windows 2000/XP file located at C:\Winnt\System32\ in Windows 2000 and C:\Windows\System32\ in Windows XP. Many users reading this are likely to conclude this means the appearance of DLLHOST.EXE in the Processes tab is normal, and, therefore, not indicative of malware infection. This, however, is a mistake on two fronts. First, some malware creators, knowing that many users coming across files with legitimate Windows 2000/XP/Vista/7 (and/or application) filenames automatically deem them legitimate, use legitimate Windows 2000/XP/Vista/7 (and/or application) filenames for the names of their malware files to deliberately trick people. In other words, when it come to malware, a file having a Windows 2000/XP/Vista/7 (and/or application) filename could be the legitimate Windows 2000/XP/Vista/7 file (and/or application) or an illegitimate malware file. Second, a Windows 2000/XP/Vista/7 user having a Baseline Process List in front of them (or in their head as the case might be) should know that a typical Windows 2000/XP/Vista/7 computer does not list DLLHOST.EXE in the Windows 2000/XP/Vista/7 Processes tab. In other words, whether DLLHOST.EXE is the legitimate Windows 2000/XP/Vista/7 file or an illegitimate malware file is a matter of profound indifference because no matter the case it should not be listed in the Windows 2000/XP/Vista/7 Processes tab. Hence, when it come to malware, do not be fooled by appearances: one suspicious characteristic outweighs one hundred apparently normal characteristics. And always be suspicious until proven one way or the other (i.e., as a legitimate Windows 2000/XP/Vista/7 (and/or application) file running as expected or as an illegitimate malware file which may or may not be mimicking a legitimate Windows 2000/XP/Vista/7 (and/or application) file).

Note: About the only time a Windows 2000/XP computer should list DLLHOST.EXE in the Processes tab apart from malware infection is if: 1.) the user accessed Windows 2000 Component Services (Control Panel | Administrative Tools | Component Services | Component Services); 2.) the user accessed Windows XP Component Services (Control Panel | Performance and Maintenance | Administrative Tools | Component Services | Component Services); or 3.) the Windows XP COM+ System Application Service or MS Software Shadow Copy Provider Service is started. Since users rarely access Windows 2000/XP Component Services, and since the Windows XP COM+ System Application Service and MS Software Shadow Copy Provider Service default Startup Type is manual, indeed, a typical Windows 2000/XP computer should not list DLLHOST.EXE in the Processes tab.

Continuing to read the Google search returns for DLLHOST.EXE, it became apparent that there is also an illegitimate DLLHOST.EXE file affiliated with W32.Welchia.Worm (a.k.a., Nachi Worm) (symantec.com) infection. W32.Welchia.Worm infection on Windows 2000/XP initiates a handful of actions including most notably:

1. The copying and deleting of a small number of files. One of the files copied is DLLHOST.EXE, the Worm itself, which is copied to C:\Winnt\System32\Wins\ in Windows 2000 and C:\Windows\System32\Wins\ in Windows XP.

2. The creation of two Services. One of the Services, with Startup Type set to automatic, runs the Worm's DLLHOST.EXE file. This explains the appearance of the process running DLLHOST.EXE in the Processes tab.
3. The worm sends itself to vulnerable computers on the network (i.e., an Intranet and/or the Internet). This explains the LAC icon being lit solid and the NETSTAT results.

At this point everything pointed to W32.Welchia.Worm infection. The only remaining was to positively identify W32.Welchia.Worm infection, of which there were several choices, perhaps the easiest being to look for the presence of DLLHOST.EXE at C:\Winnt\System32\Wins\ in Windows 2000 or C:\Windows\System32\Wins\ in Windows XP. Needless to say, DLLHOST.EXE was found in the wrong location.

The moral of the story? It is possible to rapidly suspect and identify malware infection armed apart from antivirus/antispyware/firewall software armed solely with a knowledge of should appear in the Windows 2000/XP/Vista/7 Processes tab.

6. Additional Reading

- [Program Executable Filename Extensions \(file-extensions.org\)](http://file-extensions.org)
- [Windows 2000/XP/Vista/7 Default Processes \(stevestechresource.com\)](http://stevestechresource.com)
- [Securing A Clean Installation Of Windows XP/Vista/7 \(stevestechresource.com\)](http://stevestechresource.com)
- [NETSTAT \(technet.microsoft.com\)](http://technet.microsoft.com)
- [W32.Welchia.Worm \(a.k.a., Nachi Worm\) \(symantec.com\)](http://symantec.com)

Steve's Tech Resource

The Web Development, Internet, Software, Hardware, and Multimedia Resource



Copyright © 2000-2011 Steve's Tech Resource