Symantec Security Response
http://www.symantec.com/security_response/index.jsp

Trojan.Vundo Removal Tool

Discovered: November 20, 2004
Updated: November 30, 2005 12:00:00 AM
Type: Removal Information

SUMMARY

This tool is designed to remove the infections of the following threats:

Trojan.Vundo
Trojan.Vundo.B

Important:
If you are on a network or have a full-time connection to the Internet, such as a DSL or cable modem, disconnect the computer from the network and Internet. Disable or password-protect file sharing, or set the shared files to Read Only, before reconnecting the computers to the network or to the Internet. Because this worm spreads by using shared folders on networked computers, to ensure that the worm does not reinfect the computer after it has been removed, Symantec suggests sharing with Read Only access or by using password protection.

For instructions on how to do this, refer to your Windows documentation, or the document: How to configure shared Windows folders for maximum network protection.
If you are removing an infection from a network, first make sure that all the shares are disabled or set to Read Only.
This tool is not designed to run on Novell NetWare servers. To remove this threat from a NetWare server, first make sure that you have the current virus definitions, and then run a full system scan with the Symantec antivirus product.

How to download and run the tool

Important: You must have administrative rights to run this tool on Windows NT 4.0, Windows 2000, or Windows XP.

Note for network administrators: If you are running MS Exchange 2000 Server, we recommend that you exclude the M drive from the scan by running the tool from a command line, with the Exclude switch. For more information, read the Microsoft knowledge base article: XADM: Do Not Back Up or Scan Exchange 2000 Drive M (Article 298924).

Follow these steps to download and run the tool:

Download the FixVundo.exe file from: http://www.symantec.com/content/en/us/global/removal_tool/threat_writeups/FixVundo.exe
Save the file to a convenient location, such as your Windows desktop.
Optional: To check the authenticity of the digital signature, refer to the "Digital signature" section later in this writeup.

Note: If you are sure that you are downloading this tool from the Security Response Web site, you can skip this step. If you are not sure, or are a network administrator and need to authenticate the files before deployment, follow the steps in the "Digital signature" section before proceeding with step 4.

Close all the running programs.
If you are on a network or if you have a full-time connection to the Internet, disconnect the computer from the network and the Internet.
If you are running Windows Me or XP, turn off System Restore. For instructions on how to turn off System Restore, read your Windows documentation, or one of the following articles:
Locate the file that you just downloaded.
Double-click the FixVundo.exe file to start the removal tool.
Click Start to begin the process, and then allow the tool to run.

Note: If you have any problems when you run the tool, or it does nor appear to remove the threat, restart the computer in Safe mode and run the tool again.

Restart the computer.
Run the removal tool again to ensure that the system is clean.
If you are running Windows Me/XP, then reenable System Restore.
If you are on a network or if you have a full-time connection to the Internet, reconnect the computer to the network or to the Internet connection.
Run LiveUpdate to make sure that you are using the most current virus definitions.

When the tool has finished running, you will see a message indicating whether the threat has infected the computer. The tool displays results similar to the following:
Total number of the scanned files
Number of deleted files
Number of repaired files
Number of terminated viral processes
Number of fixed registry entries

What the tool does
The Removal Tool does the following:
Terminates the associated processes
Deletes the associated files
Deletes the registry values added by the threat

Switches
The following switches are designed for use by network administrators:

Switch Description
/HELP, /H, /?
Displays the help message.

/NOFIXREG
Disables the registry repair (We do not recommend using this switch).

/SILENT, /S

/LOG=[PATH NAME]
Creates a log file where [PATH NAME] is the location in which to store the tool's output. By default, this switch creates the log file, FixVundo.log, in the same folder from which the removal tool was executed.

/MAPPED
Scans the mapped network drives. (We do not recommend using this switch. See the following Note.)
/START
Forces the tool to immediately start scanning.

/EXCLUDE=[PATH]
Excludes the specified [PATH] from scanning. (We do not recommend using this switch. See the following Note.)

/NOFILESCAN
Prevents the scanning of the file system.

Important: Using the /MAPPED switch does not ensure the complete removal of the virus on the remote computer, because:
The scanning of mapped drives scans only the mapped folders. This may not include all the folders on the remote computer, which can lead to missed detections.
If a viral file is detected on the mapped drive, the removal will fail if a program on the remote computer uses this file.
Therefore, you should run the tool on every computer.

The /EXCLUDE switch will only work with one path, not multiple. An alternative is the /NOFILESCAN switch followed by a manual scan with AntiVirus. This will let the tool alter the registry. Then, scan the computer with AntiVirus with current virus definitions. With these steps, you should be able to clean the file system.

The following is an example command line that can be used to exclude a single drive:

"C:\Documents and Settings\user1\Desktop\FixVundo.exe" /EXCLUDE=M:\ /LOG=c:\FixVundo.txt

Alternatively, the command line below will skip scanning the file system, but will repair the registry modifications. Then, run a regular scan of the system with proper exclusions:

"C:\Documents and Settings\user1\Desktop\FixVundo.exe" /NOFILESCAN /LOG=c:\FixVundo.txt

Note: You can give the log file any name and save it to any location.

Digital signature
For security purposes, the removal tool is digitally signed. Symantec recommends that you use only copies of the removal tool that have been directly downloaded from the Symantec Security Response Web site.

If you are not sure, or are a network administrator and need to authenticate files before deployment, you should check the authenticity of the digital signature.

Follow these steps:

Go to http://www.wmsoftware.com/free.htm.
Download and save the Chktrust.exe file to the same folder in which you saved the removal tool.

Note: Most of the following steps are done at a command prompt. If you downloaded the removal tool to the Windows desktop, it will be easier if you first move the tool to the root of the C drive. Then save the Chktrust.exe file to the root of C as well.

(Step 3 to assume that both the removal tool and Chktrust.exe are in the root of the C drive.)

Click Start > Run.
Type one of the following:

Windows 95/98/Me:
command

Windows NT/2000/XP:
cmd

Click OK.
In the command window, type the following, pressing Enter after typing each line:

cd\
cd downloads
chktrust -i FixVundo.exe

You should see one of the following messages, depending on your operating system:

Windows XP SP2:
The Trust Validation Utility window will appear.

Under Publisher, click the Symantec Corporation link. The Digital Signature Details appears.
Verify the contents of the following fields to ensure that the tool is authentic:

Name: Symantec Corporation
Signing Time: 04/2/2008 9:11:45 AM

All other operating systems:
You should see the following message:

Do you want to install and run "FixVundo Removal Tool" signed on Wednesday, April 02, 2008 9:11:45 AM and distributed by Symantec Corporation?

Notes:
The date and time in the digital signature above are based on Pacific time. They will be adjusted your computer's time zone and Regional Options settings.

If you are using Daylight Saving time, the displayed time will be exactly one hour earlier.

If this dialog box does not appear, there are two possible reasons:

The tool is not from Symantec: Unless you are sure that the tool is legitimate and that you downloaded it from the legitimate Symantec Web site, you should not run it.

The tool is from Symantec and is legitimate: However, your operating system was previously instructed to always trust content from Symantec. For information on this and on how to view the confirmation dialog again, read the document: How to restore the Publisher Authenticity confirmation dialog box.

Click Yes or Run to close the dialog box.
Type exit, and then press Enter. (This will close the MS-DOS session.)