

Re: Pop Up MALWARE: winfixer2005, winantivirus etc.

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-11/0583.html>

From: Jim Byrd (jrbyrd_at_spamlessadelphia.net)

Date: 11/28/05

Date: Sun, 27 Nov 2005 22:53:57 -0800

Hi Xlurker – Six approaches to removing Winfixer (Vundo). Not all will work on all variants. It's suggested that you try them in this order.

1 – Symantec has a new Vundo remover:

<http://securityresponse.symantec.com/avcenter/FixVundo.exe>

<http://securityresponse.symantec.com/avcenter/venc/data/trojan.vundo.removal.tool.html>

<http://securityresponse.symantec.com/avcenter/venc/data/adware.virtumonde.html#removalinstructions>

2 – Courtesy of Dave Lipman:

"Download WinFixerFix.exe from the URL ---

<http://www.ik-cs.com/programs/virtools/WinFixerFix.exe>

On the infected PC...

Execute; WinFixerFix.exe { Note: You must accept the default of

C:\McAfee }

Choose; Unzip

Choose; Close

NOTE: You may have to disable your software FireWall or allow WGET.EXE to go through your FireWall to enable WGET.EXE to download the needed McAfee related files.

Execute; c:\mcafee\clean.bat { or Double-click on 'Clean Link' in c:\mcafee }

A final report in HTML format called C:\mcafee\ScanReport.HTML will be generated. At the end of the scan, it will be displayed in your browser (Opera, FireFox or Internet Explorer). It is suggested that you move the report out of c:\mcafee before performing another scan. It would be a good idea to scan in Safe Mode and in Normal Mode and save a copy of the HTML report for each session."

3 – McAfee has a combined automated/manual removal procedure here:

http://vil.nai.com/vil/content/v_127690.htm

microsoft.public.security.virus: Re: Pop Up MALWARE: winfixer2005, winantivirus etc.

4 – It's been reported that the Removal Tool here is worthwhile:

<http://forums.mcafeehelp.com/viewtopic.php?t=57049>

5 – Then, courtesy of MVP Suzi Turner and Mosaic1:

"Atribune, a guy in the forums, has a Vundo fix tool as well:

Instructions for use by user as posted in the SpywareWarrior forum:

'Please download VundoFix.exe to your desktop. Here's a link:

<http://www.atribune.org/downloads/VundoFix.exe>

Double-click VundoFix.exe to extract the files

This will create a VundoFix folder on your desktop.

After the files are extracted, please restart your computer into Safe Mode.

Once in safe mode open the VundoFix folder and double-click on KillVundo.bat

A command window will open and it should look like this:

VundoFix V2.1 by Atri

By pressing enter you agree that you are using this at your own risk

At this point press enter one time.

Next you will see:

Type in the filepath as instructed by the forum staff

Then Press Enter, to continue with the fix.

At this point please type the following file path (make sure to enter it exactly as below!):

C:\WINDOWS\system32\geeby.dll

Press Enter.

Next you will see:

Please type in the second filepath as instructed by the forum staff

At this point please type the following file path (make sure to enter it exactly as below!):

C:\WINDOWS\system32\ybeeg.*

Press Enter to continue.

The fix will run then HijackThis will open.

In HijackThis, please place a check next to the following items and click

FIX CHECKED:

Re: Pop Up MALWARE: winfixer2005, winantivirus etc.

microsoft.public.security.virus: Re: Pop Up MALWARE: winfixer2005, winantivirus etc.

O2 – BHO: MSEvents Object – {52B1DFC7-AAFC-4362-B103-868B0683C697} –
C:\WINDOWS\system32\geeby.dll
O20 – Winlogon Notify: geeby – C:\WINDOWS\system32\geeby.dll

After you have fixed these items, close Hijackthis.

The fix will tell you to shutdown using the Power button. Hold in your power button until the computer shuts down. Wait about 15 seconds and then restart the computer into regular windows.

Chkdsk will run. This is normal. It will take a few minutes and is checking your file system because of the Bad Shutdown we caused.

Go for free online Virus scans here:

http://housecall.trendmicro.com/housecall/start_corp.asp
<http://www.pandasoftware.com/activescan/>

Allow them to clean

Panda will have the option to create a log after the scan has finished. Click the See Report button. Then click the save Report button. It will be saved under the name activescan.txt Do that and post that log into your next reply here.

Run hijackthis and post the new log and the vundofix.txt file from the vundofix folder into as well.'

The forum helpers have reported this fix from Atribune works. I don't know about the Symantec tool.

If you'd like to join Spyware Warrior, you could see the thread where the helpers are discussing this.

Suzi"

Note: Here's some added info relative to the above courtesy of MVP Steve Wechsler (akaMowGreen):

"the .dll's file name :

C:\WINDOWS\system32\geeby.dll

will be different on different systems. What you can do to identify it is to scan the system with HijackThis and look at the O2 BHO and/or O20 Winlogon entries to find out it's name. Close all other programs and browsers prior to scanning with HJT. REMEMBER that there is a hidden file that will have the name of the .dll spelled backwards. Enter that name when the VundoFix requests the path to the second file.

Re: Pop Up MALWARE: winfixer2005, winantivirus etc.

microsoft.public.security.virus: Re: Pop Up MALWARE: winfixer2005, winantivirus etc.

6 – Grinler, (Lawrence Abrams, a Security MVP), has another removal method that can be used if the recommended method fails :

<http://www.bleepingcomputer.com/forums/topic18610.html>"

Here's the HijackThis info you may need:

Download HijackThis, free, here:

<http://209.133.47.200/~merijn/files/HijackThis.exe> (Always download a new fresh copy of HijackThis [and CWShredder also] – It's UPDATED frequently.)

You may also get it here if that link is blocked:

<http://www.majorgeeks.com/downloadget.php?id=3155&file=3&evp=3304750663b552982a8baee6434cfc13>

There's a good "How-to-Use" tutorial here:

<http://computercops.biz/HijackThis.html>

In Windows Explorer, click on Tools\Folder Options\View and check "Show hidden files and folders" and uncheck "Hide protected operating system files". (You may want to restore these when you're all finished with HijackThis.)

Place HijackThis.exe or unzip HijackThis.zip into its own dedicated folder at the root level such as C:\HijackThis (NOT in a Temp folder or on your Desktop), reboot to Safe mode, start HT then press Scan. Click on SaveLog when it's finished which will create hijackthis.log. Now click the Config button, then Misc Tools and click on Generate StartupList.log which will create Startuplist.txt

Then go to one of the following forums:

Spyware and Hijackware Removal Support, here:

<http://forums.spywareinfo.com/>

or Jim Eshelman's site here: <http://forum.aumha.org/>

or Bleepingcomputer here: <http://www.bleepingcomputer.com/>

or Computer Cops here: <http://www.computercops.biz/forums.html>

or Tom Coyote here: <http://forums.tomcoyote.org/index.php?act=idx>

or Net-Integration here: <http://net-integration.us/forums/index.php>

Register if necessary, then sign in and READ THE DIRECTIONS at the beginning of the particular site's HiJackThis forum, then copy and paste both files into a message asking for assistance, Someone will answer with detailed instructions for the removal of your parasite(s). Be sure you include at the beginning of your post a description of "What specific problem(s)/symptoms you're trying to solve" and "What steps you've already taken."

ONLY IF you've successfully eliminated the malware, you can now make a new, clean Restore Point and delete any previously saved (possibly infected) ones. The following suggested approach is courtesy of Gary Woodruff: For XP you can run a Disk Cleanup cycle and then look in the More Options tab. The System Restore option removes all but the latest Restore Point. If there

Re: Pop Up MALWARE: winfixer2005, winantivirus etc.

microsoft.public.security.virus: Re: Pop Up MALWARE: winfixer2005, winantivirus etc.

hasn't been one made since the system was cleaned you should manually create one before dumping the old possibly infected ones.

You probably should consider switching to Sun Java J2SE 5.0 JRE or later here: <http://java.sun.com/j2se/1.5.0/download.jsp> (What I use, BTW), especially since MS will apparently no longer be distributing Java or providing any support for Java including security fixes after Dec 31, 2007. BE SURE that you uninstall any prior versions of Sun Java as some, specifically JRE v. 1.4.2_03, contain a security bug which certain malware, notably Winfixer/Vundo, are suspected of exploiting. If you did have this version of Sun Java, JRE v. 1.4.2-03, installed, please post back and tell us.

When you get things cleaned up, take a look at my Blog, Defending Your Machine, addy in my Signature below, for some additional curative and preventive measures you might want to implement to help prevent this type of thing in the future.

--

Regards, Jim Byrd, MS-MVP/DTS/AH-VSOP

My Blog, Defending Your Machine, here:

<http://DefendingYourMachine.blogspot.com/>

<xlurker@lycos.com> wrote in message

news:1133153859.258769.120390@g14g2000cwa.googlegroups.com

> All of these fixes may be a very long trip to what should be a very
> short and quick solution. I have an application which overwrites files
> with random numbers. I would use it on the file with the virus if
> access to that file were not denied.

>

> Does that infected file generate this problem? Why are Symantec and I
> denied access to it? How can we dissolve that denial? Why could Symantec
> not quarantine that file so that no code from it could ever run?

>

> Anyhow, I ran Spybot and the Symantec FixVundo utility on 11/27/2005.
> FixVundo created a log which includes:

>

> "Trojan.Vundo has been successfully removed from your computer!

> Here is the report:

> The total number of the scanned files: 183114

> The number of deleted files: 0

> The number of viral processes terminated: 3

> The number of viral processes suspended: 3

> The number of viral threads terminated: 7

> The number of registry entries fixed: 2"

>

> When I next rebooted after running FixVundo, the virus alert
> immediately appeared as it had before.

>

> The Spybot search and destroy function delivered a list of what it
> thought were suspicious cookies. All of those looked innocuous to me
> except some in a folder with WinFix in its folder name. I let Spybot
> kill the cookies in that folder. However, I do not intuit that cookies
> can execute a pop up intrusion.