

Re: Winfixer

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-09/msg00064.html

- *From:* imhotep <imhotep@xxxxxxxxxxx>
 - *Date:* Sun, 03 Sep 2006 16:20:05 -0400
-

David H. Lipman wrote:

From: "johneboy" <johneboy@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

| My PC has picked up the Winfixer virus/malware and having trawled the
| forums there are endless suggestions about the best way to rid myself of
| this thing. I am running on OS Windows XP SP2, IE latest version, and
| have Norton Security Package which is unable to remedy it, in fact I
| think Winfixer came in when I renewed my Norton which had recently
| expired during a house move. I took on board one suggestion to get the
| latest version of Sun Java which I did, but I was unable to delete all
| the old program files, one remains in addition to the latest version.
| I've started down the road with some of the suggested fixes but always
| seem to reach a dead end.
| Can anyone give me the quickest solution please, bearing in mind I am
| not a PC expert but can get by... or should I just take my PC into the
| nearest shop and pay a man who can?
| Thanks in anticipation.

Two phase answer...

Perform Part 1 then perform Part 2

If the first two parts don't work, perform the alternate utility.

It is suggested that you execute each tool in Normal Mode then in Safe Mode.

If you are using any version of Sun Java that is prior to JRE Version 5.0 update 6, then you are strongly urged to remove any/all versions that are prior to JRE/JSE Version 5.0 update 6. There are vulnerabilities in them and they are actively being exploited. It is possible that is how you got infected with malware.

Re: Winfixer

Therefore, it is highly suggested that if there are any prior versions of Sun Java to Version 6 on the PC that they be removed ASAP.

The latest version is Sun Java JRE/JSE Version 5.0 Update 8

Simple check, look under...

C:\Program Files\Java

The only folder under that folder should be the latest version.

Such as...

C:\Program Files\Java\jre1.5.0_08

<http://www.java.com/en/download/manual.jsp>

or

<http://java.sun.com/javase/downloads/index.jsp>

FYI:

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102557-1>

Part 1

Download Adware-Virtumundo Removal Tool --

<http://secured2k.home.comcast.net/tools/VirtumundoBeGone.exe>

Information on the Adware-Virtumundo Removal Tool:

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

Part 2

Download WinFixerFix.exe from the URL --

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

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 }

Re: Winfixer

Re: Winfixer

A final report in HTML format called C:\mcafee\Normal_ScanReport.HTML or C:\mcafee\Safe_ScanReport.HTML will be generated. At the end of the scan, it will be displayed in your browser (Opera, FireFox or Internet Explorer). However, if you are using WinXP, Win2K or Win2003 your system will be left in a state where you will have to manually shutdown/reboot the PC. On Win9x/ME platforms the report will not be shown in your browser but your PC will automatically be shutdown. It is suggested that you move the report out of c:\mcafee before performing another scan.

It would be best to scan in both Safe Mode and in Normal Mode and save a copy of the HTML report for each session.

ALTERNATE:

Download Atribune's VUNDOFIX.EXE
<http://www.atribune.org/ccount/click.php?id=4>

Save VUNDOFIX.EXE to "C:\" (C:\VUNDOFIX.EXE) and execute it from there.

Please Copy and Paste the contents of the HTML Log files;
C:\mcafee\Normal_ScanReport.HTML & C:\mcafee\Safe_ScanReport.HTML in your reply.

* * * Please report back your results * * *

...of topic question. What is that graphic you have on your posts?

Imhotep

.