

Re: Thanks! David

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-04/msg00155.html>

- *From:* Jani <Jani@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 11 Apr 2006 07:28:02 -0700
-

David thank you for your quick response. Both my daughter and I are at our wits end with this. We have spent lots of time and staying up late etc. Just another question so that I fully understand....

When I did a search to learn more on this blackworm, winfixer etc. I kept getting ads for spyware removal, that's why I thought it might be easier at this point to just spend the money. I also read that there were some download tools from MS, Bitdefender and a couple of others that would remove it. So what you are telling me is that even all those don't do the job either? I just want to be able to tell my daughter that this is the only way. She did try Vundo but it didn't work.

"David H. Lipman" wrote:

From: "Jani" <Jani@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

| David, My daughter is being plagued with the same worm, all the same symptoms
| etc. I have read all the instructions you gave Karen, some I am a little
| unclear of. Still a novice I'm afraid...anyway, my question is, would it be
| easier for someone like me to just buy a spyware program online and let it do
| it or won't those work? Will we still have to follow all the instructions?
| Please help!
|

I wish it was that easy. It isn't and that is why I wrote the WinFixerFix utility.

You need to make sure that the old and very vulnerable version of Sun Java is removed and the latest version is installed.

Looking 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_06

If there are older versions they must be removed via the control panel applet; "Add/Remove programs" and the newest version will need to be installed.

Re: Thanks! David

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

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.

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/virtools/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 }

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.

Re: Thanks! David

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 * * *

Dave

<http://www.claymania.com/removal-trojan-adware.html>

<http://www.ik-cs.com/got-a-virus.htm>