

# Re: Black Worm Message?

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2006-03/msg00000.html>

---

- *From:* "David H. Lipman" <DLipman~nospam~@Verizon.Net>
  - *Date:* Tue, 28 Feb 2006 17:35:26 -0500
- 

From: "pc student" <pcstudent@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

| I am running this panda software right now and it shows that I have 87  
| possible problems. HELP!!! Ok and I have norton running ...

|  
| Potentially unwanted tool:application/winantivirus2006  
| Not disinfected C:\PROGRAM FILES\COMMON FILES\WinAntiVirus  
| Pro 2006

|  
| Adware:adware/savenow  
| Not disinfected Windows Registry

|  
| Potentially unwanted tool:application/myway  
| Not disinfected  
| HKEY\_CLASSES\_ROOT\MYWAYSEARCHASSISTANTDE.AUXILIARY

< snip >

|  
| Adware:Adware/ClockSync  
| Not disinfected C:\Documents and Settings\Dawn Baldwin\Local  
| Settings\Temp\VVSNIInst.exe

|  
| Potentially unwanted tool:Application/ErrorSafe  
| Not disinfected C:\Documents and Settings\Dawn Baldwin\Local  
| Settings\Temporary Internet  
| Files\Content.IE5\6KX37UAD\WinAntiVirusPro2006ScannerInstall[1].exe

|  
| Potentially unwanted tool:Application/Winfixer2005  
| Not disinfected C:\Documents and Settings\Dawn Baldwin\Local  
| Settings\Temporary Internet  
| Files\Content.IE5\WP2ZS1QZ\WinFixer2006FreeInstall[1].exe

|  
| Potentially unwanted tool:Application/Winantivirus2006  
| Not disinfected C:\Program Files\Common Files\WinAntiVirus  
| Pro 2006\WapCHK.dll

|  
| Potentially unwanted tool:Application/Winantivirus2006

## Re: Black Worm Message?

| Not disinfected C:\Program Files\Common Files\WinFixer 2006\pcheck.dll  
|  
| Spyware:Spyware/Virtumonde  
| Not disinfected C:\WINDOWS\system32\pmnkn.dll  
|

Most of what was found were cookies which are NOT a problem. However you did have "WinAntiVirus Pro" which is a Rogue anti spyware application and is NOT safe to use. Please check with Spyware Warrior when checking out any anti spyware applications. You will find WinAntiSpyware and WinAntiVirus listed as Rogues on Spyware Warrior.  
[http://www.spywarewarrior.com/rogue\\_anti-spyware.htm](http://www.spywarewarrior.com/rogue_anti-spyware.htm)

It should be removed ASAP !

It also shows the Winfixer and Vundo/Virtumonde. WinFixer is another rogue antospyware application on SyWare Warrior and is auto installed by certain downloader Trojans.

The following set of instructions can be used to clean your PC...

Two phase answer...

Perform Part 1 then perform Part 2

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, then you are strongly urged to remove any/all versions that are prior to JRE Version 5.0. There are vulnerabilities in them and they are actively being exploited. It is possible that is how you got infected with malware.

Therefore, it is highly suggested that if there are any prior versions of Sun Java to Version 5 on the PC that they be removed and Sun Java JRE Version 5.0 Update 6 be installed ASAP.

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

### 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 --

Re: Black Worm Message?

Re: Black Worm Message?

<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 }

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.

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>

.