

## Forum: [Hack Forums](#)

Thread: [Infected\\$ 4000 PC totally unusable.](#)

**Viral Impact** - December 23, 2011, 1:39 am

1. My issues are:

I can't do anything on my PC I can't run 90% of the programs on my PC. I constantly got redirected all over the web for days previous while using google search. I get all these fake looking alerts telling me im infected with a bazillion different viruses and that i NEED TO PURCHASE some program but i never went to find out what it was as i new it was bullshit.

2. My MBAM log:

<http://pastebin.com/szeuhi5F>

3. My OTL log:

<http://pastebin.com/BiDDgehS>

<http://pastebin.com/yQXFeDTQ>

4. My GMER log:

<http://pastebin.com/DcGgMcBm>

Issues encountered:

I can't use any internet browser on my PC so i had to use my lappy to download the .exe's and write this thread

Thankyou for your help in advance.

**Deltron** - December 23, 2011, 12:19 pm

Do you still require assistance at this point in time?

**Viral Impact** - December 23, 2011, 2:50 pm

yes i do. Nothing has changed about my situation.

thanks :)

**Deltron** - December 23, 2011, 3:05 pm

Step 1

Run OTL.exe.

Copy and paste the following text written inside of the code box into the Custom Scans & Fixes box located at the bottom of OTL. Make sure you include everything in the code box.

Code :OTL

Hosts file not found

O2 - BHO: (ContributeBHO Class) - {074C1DC5-9320-4A9A-947D-C042949C6216} - E:\adobe CS5.5 Master Collection\Adobe Contribute CS5.1\Plugins\IEPlugin\contributeieplugin.dll File not

found

O2 - BHO: (uTorrentBar Toolbar) - {bf7380fa-e3b4-4db2-af3e-9d8783a45bfc} - C:\Program Files\uTorrentBar\prxtbuTor.dll (Conduit Ltd.)

O3 - HKLM\...\Toolbar: (Contribute Toolbar) - {517BDDE4-E3A7-4570-B21E-2B52B6139FC7} - E:\adobe CS5.5 Master Collection\Adobe Contribute CS5.1\Plugins\IEPlugin\contributeieplugin.dll  
File not found

O3 - HKLM\...\Toolbar: (uTorrentBar Toolbar) - {bf7380fa-e3b4-4db2-af3e-9d8783a45bfc} - C:\Program Files\uTorrentBar\prxtbuTor.dll (Conduit Ltd.)

O3 - HKCU\...\Toolbar\WebBrowser: (uTorrentBar Toolbar) - {BF7380FA-E3B4-4DB2-AF3E-9D8783A45BFC} - C:\Program Files\uTorrentBar\prxtbuTor.dll (Conduit Ltd.)

O16 - DPF: {8AD9C840-044E-11D1-B3E9-00805F499D93}

http://java.sun.com/update/1.6.0/jinstall-1\_6\_0\_27-windows-i586.cab (Java Plug-in 1.6.0\_27)

O16 - DPF: {CAFEEFAC-0016-0000-0027-ABCDEFFEDCBA}

http://java.sun.com/update/1.6.0/jinstall-1\_6\_0\_27-windows-i586.cab (Java Plug-in 1.6.0\_27)

O16 - DPF: {CAFEEFAC-FFFF-FFFF-FFFF-ABCDEFFEDCBA}

http://java.sun.com/update/1.6.0/jinstall-1\_6\_0\_27-windows-i586.cab (Java Plug-in 1.6.0\_27)

[2011/12/23 17:55:41 | 000,012,236 | -HS- | M] () --

C:\Users\Lochie\AppData\Local\d7co58k4xf3fqw

[2011/12/23 17:55:41 | 000,012,236 | -HS- | M] () -- C:\ProgramData\d7co58k4xf3fqw

[2011/12/23 10:48:57 | 000,010,512 | -HS- | M] () --

C:\Users\Lochie\AppData\Local\106834x4x200x010g827t1ajw4q6

[2011/12/23 10:48:57 | 000,010,512 | -HS- | M] () --

C:\ProgramData\106834x4x200x010g827t1ajw4q6

[2011/12/23 17:51:35 | 000,012,236 | -HS- | C] () --

C:\Users\Lochie\AppData\Local\d7co58k4xf3fqw

[2011/12/23 17:51:35 | 000,012,236 | -HS- | C] () -- C:\ProgramData\d7co58k4xf3fqw

[2011/12/23 10:43:54 | 000,010,512 | -HS- | C] () --

C:\Users\Lochie\AppData\Local\106834x4x200x010g827t1ajw4q6

[2011/12/23 10:43:54 | 000,010,512 | -HS- | C] () --

C:\ProgramData\106834x4x200x010g827t1ajw4q6

:Files

c:\Users\Lochie\AppData\Local\ddx.exe

C:\Users\Lochie\Desktop\gzy9ehvx.exe

:Commands

[PURITY]

[EMPTYTEMP]

Then click the Run Fix button at the top.

Let the program run unhindered; it will reboot when it is done. If it does not, please reboot your system.

Please include the log in your next post.

## Step 2

Please be aware that I am instructing you to use an extremely powerful removal tool. Following instructions is vital. Please read the instructions thoroughly and completely before you begin this process. Making a simple mistake may lead to problems with the normal functionality of your computer. Might you have any questions, please post on this thread before carrying out the below steps. If you are clear of what is expected, you may proceed.

### Notes:

Do not mouse-click ComboFix's window while it is running. That may cause it to stall.

Do not "re-run" ComboFix. If you have a problem, reply back for further instructions.

ComboFix may reset a number of Internet Explorer's settings, including making Internet Explorer the default browser.

ComboFix prevents auto run of ALL CD, floppy and USB devices to assist with malware removal & increase security. If this is an issue or makes it difficult for you, please tell your helper.

CombfoFix disconnects your machine from the internet. The connection is automatically restored before ComboFix completes its run. If ComboFix runs into difficulty and terminates prematurely, the connection can be manually restored by restarting your machine.

Please download ComboFix from [here](#). Save it to your desktop afterwards. Follow these next instructions carefully:

Disable your Antivirus and Antispyware applications, usually via a right click on the System Tray icon. They may otherwise interfere with our tools. (Click on [this link](#) to see a list of programs that should be disabled. The list is not all inclusive.)

Double-click on ComboFix.exe and follow the prompts.

Notes: Combfix will run without the Recovery Console installed. Skip the Recovery Console part if you're running Vista or Windows 7.

As part of it's process, ComboFix will check to see if the Microsoft Windows Recovery Console is installed. With malware infections being as they are today, it is strongly recommended to have this pre-installed on your machine before doing any malware removal. It will allow you to boot up into a special recovery/repair mode that will allow us to more easily help you should your computer have a problem after an attempted removal of malware.

Follow the prompts to allow ComboFix to download and install the Microsoft Windows Recovery Console, and when prompted, agree to the End-User License Agreement to install the Microsoft Windows Recovery Console.

If the Microsoft Windows Recovery Console is already installed, ComboFix will continue it's malware removal procedures.

[img]http://img.photobucket.com/albums/v706/ried7/RcAuto1.gif[/img]

Once the Microsoft Windows Recovery Console is installed using ComboFix, you should see the

following message:

[img]http://img.photobucket.com/albums/v706/ried7/whatnext.png[/img]

Click on Yes, to continue scanning for malware.

This scan in particular will take about thirty minutes. Please let it run until it is finished.

When finished, it shall produce a log for you. Please include the C:\ComboFix.txt in your next reply.

**Viral Impact** - December 23, 2011, 4:49 pm

Okay well i did have some trouble with OTL, it did not save any log's onto my desktop like last time, it did run and then reboot upon completion.

Then i went ahead with combo fix, it detected some rootkit activity made a loud beep then restarted itself several times and then compiled a log upon completion.

Now i was unable to open this log on my computer to even paste it to pastebin, as when ever i try to open any .txt file its says something about a registry key set for deletion, i can give you more details about that if you so wish.

However here is the one log from Combo fix. If you have any idea where the OTL log might be ill try find it for you.

<http://pastebin.com/83NpZ1BQ>

Once again thankyou for your help.

**Deltron** - December 23, 2011, 4:59 pm

The log should be located at C:\\_OTL.

**Viral Impact** - December 23, 2011, 5:24 pm

Thankyou found it, here is the log.

<http://pastebin.com/isxNaeqs>

I named the paste title exactly as the log was titled

**Deltron** - December 23, 2011, 5:34 pm

Step 3

Please download Malwarebytes' Anti-Malware from '[here](#)' and save it to your desktop. Double-click mbam-setup.exe to install the application.

Make sure a checkmark is placed next to Update Malwarebytes' Anti-Malware and Launch Malwarebytes' Anti-Malware, then click Finish.

If an update is found, it will download and install the latest version.

Once the program has loaded, select Perform Full Scan, then click Scan. The scan may take some

time to finish, so please be patient.

When the scan is complete, click OK, then Show Results to view the results.

Make sure that everything is checked, and click Remove Selected.

When disinfection is completed, a log will open in Notepad and you may be prompted to restart; reboot your computer if it requests to.

The log is automatically saved by the program and can be viewed by clicking the Logs tab.

Copy and paste the entire report in your next reply.

#### Step 4

Please run a free online scan with ESET Online Scanner by downloading it from ['here'](#). Save it to your desktop.

Please ensure that you're logged into an Administrator account before running the scanner. The ESET Online Scan will not work if you're on a limited account.

Double-click 'esetsmartinstaller\_enu.exe' to execute the program.

Check the box next to 'YES, I accept the Terms of Use'. Press 'Start'.

If this is your first time installing the scanner, allow the ActiveX Control to install.

Database download may take some time.

On the next page, ensure the box next to 'Remove found threats' has been checked. Also ensure that the box next to 'Scan unwanted applications' is checked. Proceed by clicking on 'Start'. The ESET Online Scanner will update the Virus Signature Database and begin the scan.

Please allow it to complete successfully and ensure that any current downloads are stopped.

Once the scan's completed, please open 'Notepad' by navigating to 'Start', then 'Run', and type in 'Notepad'. Open the file located at 'C:\Program Files\ESET\ESET Online Scanner\log.txt'.

Please copy and paste this log into your next reply. Press 'Finish'.

#### Step 5

Please provide me with a fresh OTL log. If the program is not already at your desktop, please

re-download it from '[here](#)'.

Double-click 'OTL.exe' to run the program.

When the window appears, underneath Output, change it to Minimal Output.

Check the boxes LOP Check and Purity Check.

Before running the scan, make sure to close all other windows so OTL runs without any interruptions.

Click the Run Scan button. Do not change any settings unless otherwise told to do so. The scan won't take long.

Once the scan has completed, it will open two Notepad windows. OTL.txt

Extras.txt

In case these logs failed to open automatically, you can find them at: C:\OTL\.

Copy (Right-click > Select All > Copy) all the contents of these files, one at a time, and include them separately in your next reply.

**Viral Impact** - December 23, 2011, 7:46 pm

here is the mbam-log: <http://pastebin.com/x9ja6fjV>

here is the est log: <http://pastebin.com/D4Yke8H2>

Here is the OTL log: <http://pastebin.com/vww6SLq6>

It has made it difficult to do this as i have to right click and run everything as administrator even though I'm on an admin account. Otherwise i get an error message that say's

(directory of what ever im trying to use)

Illegal operation on a registry key that has been marked for deletion.

**Deltron** - December 23, 2011, 8:59 pm

Step 6

Run OTL.exe.

Copy and paste the following text written inside of the code box into the Custom Scans & Fixes box located at the bottom of OTL. Make sure you include everything in the code box.

Code :Files

C:\Windows\System32\drivers\ldfsc.sys

:Commands  
[PURITY]  
[EMPTYTEMP]

Then click the Run Fix button at the top.

Let the program run unhindered; it will reboot when it is done. If it does not, please reboot your system.

Please include the log in your next post.

## Step 7

Please download Rooter from [here](#) and save it to your desktop.

Double-click on the Rooter.exe icon on your desktop to execute the application. If you are using Vista, right-click and Run as Administrator

Press the green Scan button to start the scanning.

Notepad will open with a file created called "Rooter#.txt" located at %systemdrive%\Rooter\$\Rooter#.txt. (# is the number assigned to the report).

Please copy and paste the contents of Rooter#.txt in you next reply.

Press the Close button, to close the Rooter window.

**Viral Impact** - December 23, 2011, 11:43 pm

Hello i have completed the latest OTL fix and here is the log.

<http://pastebin.com/SHaSG6Fk>

However i was unable to acess rooter through the link you provided me, if you have a mirror i could download from that would be great. I have not attempted to look for any program similar to this as i figured i would leave to to you.

**Deltron** - December 23, 2011, 11:45 pm

Right-click the Rooter link and copy and paste it directly into your address bar. Then press enter. Proceed with the listed instructions.

**Viral Impact** - December 24, 2011, 12:32 am

I downloaded it and ran it and then it keeps saying stopped working and closes shortly after starting the scan, i also tried to run it as administrator and the same problem

**Deltron** - December 24, 2011, 12:34 am

Would you mind re-uploading the OTL fix log to Tinypaste.com for me? Pastebin is unavliable at the moment.

**Viral Impact** - December 24, 2011, 12:47 am

no problem here you go, <http://tinypaste.com/7725424b>

**Deltron** - December 24, 2011, 3:34 pm

What issues are you currently experiencing?

**Viral Impact** - December 24, 2011, 11:21 pm

at the moment the computer seems back to normal. I cant notice anything out of the ordinary. Everything seems fine. but ill wait till you tell me im clean before i stop doing what you tell me.

Oh and i cant get rooter to scan, it keeps saying it has stopped working and needs to close.

**Deltron** - December 25, 2011, 12:14 am

## Step 8

Download [TDSSKiller](#) and save it to your desktop.

Make sure all other windows are closed and to let it run uninterrupted.

Extract the file and run it.

Once extracted, open the TDSSKiller folder and doubleclick on TDSSKiller.exe to run the application, then on Start Scan.

If an infected file is detected, the default action will be Cure, click on Continue.

If a suspicious file is detected, the default action will be Skip, click on Continue.

It may ask you to reboot the computer to complete the process. Click on Reboot Now.

## Step 9

Please provide me with a fresh OTL log. If the program is not already at your desktop, please re-download it from ['here'](#).

Double-click 'OTL.exe' to run the program.

When the window appears, underneath Output, change it to Minimal Output.

Check the boxes LOP Check and Purity Check.

Before running the scan, make sure to close all other windows so OTL runs without any interruptions.

Click the Run Scan button. Do not change any settings unless otherwise told to do so. The scan won't take long.

Once the scan has completed, it will open two Notepad windows. OTL.txt

Extras.txt

In case these logs failed to open automatically, you can find them at: C:\OTL\.

Copy (Right-click > Select All > Copy) all the contents of these files, one at a time, and include them separately in your next reply.

**Viral Impact** - December 25, 2011, 2:42 am

TDSSKiller found nothing at all, also here is the OTL log i still can find the Extra's log anywhere.

<http://pastebin.com/SuMHpXQh>

When we have finished all this do you mind telling me what actually was on my computer?

Thanks so much for your help i really do appreciate it :)

**Deltron** - December 25, 2011, 11:14 pm

(Dec 25, 2011 03:42 AM)Viral Impact Wrote: [\[CITE\]](#) When we have finished all this do you mind telling me what actually was on my computer?

Thanks so much for your help i really do appreciate it :)  
Looks like it was a Trojan Horse. And no problem at all. ?

## Step 10

Download SecurityCheck from ['here'](#) and save it to your desktop.

Double-click the icon to start the application.

A command prompt box will open, press any key to continue, and let it run.

After it completes, please copy and paste the contents of the log directly in your next post. No need to upload it to Pastebin/Tinypaste.

