

Forum:[Hack Forums](#)

Thread: [\[INFECTED\]Member infected me\[INFECTED\]](#)

.Ganja - May 28, 2011, 10:08 pm

1.My issues are: This member infected me and its to much to explain, and I'm really really tired and trying to get these viruses off of my computer.

3.My MBAM logs: Forgot to save it, sorry. I had 12 infected files.

3.My OTL logs: <http://pastebin.com/L6KQpMvw>

3.My OTL logs(EXTRAS): <http://pastebin.com/8iVPwRUi>

4.My GMER log: <http://pastebin.com/1c148Usc>

Issues encountered: Keep getting these popups from AVG saying like random letters and things I never seen before.

T3h Hack3r - May 28, 2011, 10:14 pm

Step One

Run OTL.exeCopy/paste the following text written inside of the code box into the Custom Scans/Fixes box located at the bottom of OTL

Quote::OTL

O18:64bit: - Protocol\Handler\livecall {828030A1-22C1-4009-854F-8E305202313F} - Reg Error: Key error. File not found

O18:64bit: - Protocol\Handler\ms-help {314111c7-a502-11d2-bbca-00c04f8ec294} - Reg Error: Key error. File not found

O18:64bit: - Protocol\Handler\msnim {828030A1-22C1-4009-854F-8E305202313F} - Reg Error: Key error. File not found

O18:64bit: - Protocol\Handler\skype4com {FFC8B962-9B40-4DFF-9458-1830C7DD7F5D} - Reg Error: Key error. File not found

O18:64bit: - Protocol\Handler\skype-ie-addon-data {91774881-D725-4E58-B298-07617B9B86A8} - Reg Error: Key error. File not found

[2011/05/28 22:20:45 | 000,000,000 | -H-D | C] -- C:\Windupdt

[2011/05/28 21:52:15 | 000,000,000 | -HSD | C] -- C:\Users\Travis\AppData\Roaming\Windows DEP
1

@Alternate Data Stream - 138 bytes -> C:\ProgramData\TEMP:0B4227B4

:Files

C:\Users\Travis\AppData\Roaming\drvhost.exe

C:\Users\Travis\Desktop\b6ynhlz0.exe

:Commands

[purity]

[emptytemp]

[resethosts]

Then click the Run Fix button at the top

Let the program run unhindered, reboot when it is done

Then post the log from OTL presented after to Reboot.

Step Two

Please download Combofix from one of the following locations:

[LINK 1](#)

[LINK 2](#)

IMPORTANT! Save Combofix to your Desktop. Disable your AntiVirus and AntiSpyware applications, usually via a right click on the System Tray icon. They may otherwise interfere with our tools. If you have difficulty properly disabling your protective programs, refer to this link -->

<https://hackforums.net/showthread.php?tid=198032>

Double click on ComboFix.exe & follow the prompts.

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's 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. Please note: 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.

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

Notes:

1. Do not mouse-click Combofix's window while it is running. That may cause it to stall.
2. Do not "re-run" Combofix. If you have a problem, reply back for further instructions.
3. ComboFix may reset a number of Internet Explorer's settings, including making I-E the default browser.
4. Combofix prevents autorun 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.
5. CF disconnects your machine from the internet. The connection is automatically restored before CF completes its run. If CF runs into difficulty and terminates prematurely, the connection can be manually restored by restarting your machine.

.Ganja - May 28, 2011, 10:20 pm

1. OTL logs(UPDATED): <http://pastebin.com/XZ9sVxRE>
2. ComboFix logs: <http://pastebin.com/XfL7Nn6B>

T3h Hack3r - May 28, 2011, 10:46 pm

Please run a free online scan with the [ESET Online Scanner](#)

Note: You will need to use Internet Explorer for this scan. Tick the box next to Yes, I accept the Terms of Use.

Click Start

When asked, allow the ActiveX control to install
Click Start
Make sure that the options Remove found threats and the option Scan unwanted applications is checked
Click Scan
Wait for the scan to finish
Use Notepad to open the logfile located at C:\Program Files\EsetOnlineScanner\log.txt
Copy and paste that log as a reply to this topic

.Ganja - May 29, 2011, 7:25 am

1. ESET logs: <http://pastebin.com/9YLt6MaB>

T3h Hack3r - May 29, 2011, 2:14 pm

Download [SuperAntiSpyware](#) Load SuperAntiSpyware and click the Check for updates button.

Once the update is finished click the Scan your computer button.

Check Perform Complete Scan and then next.

SuperAntiSpyware will now scan your computer and when its finished it will list all the infections it has found.

Make sure that they all have a check next to them and press next.

Click finish and you will be taken back to the main interface.

Click Preferences and then click the statistics/logs tab. Click the dated log and press view log and a text file will appear.

Copy and paste the log onto the forum.