

Forum:[Hack Forums](#)

Thread: [\[Hijackthis Logs Included\] suspect i'm being infected.. \[Hijackthis Logs Included\]](#)

Stenography - August 31, 2011, 5:51 am

Ok so idk why but i susspect i'm being infected ..

Please tell me if you see something in my logs:Spoiler [\(Click to View\)](#)

Quote:Logfile of Trend Micro HijackThis v2.0.4

Scan saved at 3:45:45 PM, on 8/31/2011

Platform: Windows 7 SP1 (WinNT 6.00.3505)

MSIE: Internet Explorer v9.00 (9.00.8112.16421)

Boot mode: Normal

Running processes:

C:\Windows\system32\taskhost.exe

C:\Windows\system32\Dwm.exe

C:\Windows\Explorer.EXE

C:\Windows\system32\cmd.exe

C:\Windows\system32\conhost.exe

C:\Windows\system32\notepad.exe

C:\Users\ILANA\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\ILANA\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Program Files\Trend Micro\HiJackThis\HiJackThis.exe

C:\Users\ILANA\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Users\ILANA\AppData\Local\Google\Chrome\Application\chrome.exe

C:\Windows\system32\taskeng.exe

C:\Windows\system32\DllHost.exe

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = <http://www.google.co.il/>

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL =
<http://go.microsoft.com/fwlink/?LinkId=69157>

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL =
<http://go.microsoft.com/fwlink/?LinkId=54896>

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page =
<http://go.microsoft.com/fwlink/?LinkId=54896>

R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page =

R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant =

R0 - HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =

R1 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyServer =
83.216.184.132:8080

R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =

R3 - URLSearchHook: (no name) - {67aa0145-a051-4660-a910-22da3bab1fa5} - (no file)

R3 - URLSearchHook: (no name) - {f228c6a4-a593-4017-944c-4e7958fb3177} - (no file)

O2 - BHO: IDM Helper - {0055C089-8582-441B-A0BF-17B458C2A3A8} - C:\Program Files\Internet
Download Manager\IDMIECC.dll

O2 - BHO: AcroIEHelperStub - {18DF081C-E8AD-4283-A596-FA578C2EBDC3} - C:\Program
Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll

O2 - BHO: Groove GFS Browser Helper - {72853161-30C5-4D22-B7F9-0BBC1D38A37E} -
C:\Program Files\Microsoft Office\Office12\GrooveShellExtensions.dll

O2 - BHO: Windows Live ID Sign-in Helper - {9030D464-4C02-4ABF-8ECC-5164760863C6} - C:\Program Files\Common Files\Microsoft Shared\Windows Live\WindowsLiveLogin.dll

O2 - BHO: Windows Live Messenger Companion Helper - {9FDDE16B-836F-4806-AB1F-1455CBEFF289} - C:\Program Files\Windows Live\Companion\companioncore.dll

O2 - BHO: Java™ Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-9C25C1C588A9} - C:\Program Files\Java\jre6\bin\jp2ssv.dll

O2 - BHO: Microsoft Web Test Recorder 10.0 Helper - {DDA57003-0068-4ed2-9D32-4D1EC707D94D} - c:\Program Files\Microsoft Visual Studio 10.0\Common7\IDE\PrivateAssemblies\Microsoft.VisualStudio.QualityTools.RecorderBarBHO100.dll

O4 - HKLM\..\Run: [lgfxTray] C:\Windows\system32\lgfxtray.exe

O4 - HKLM\..\Run: [HotKeysCmds] C:\Windows\system32\hkcmd.exe

O4 - HKLM\..\Run: [Persistence] C:\Windows\system32\igfxpers.exe

O4 - HKLM\..\RunOnce: [AvgUninstallURL] cmd.exe /c start <http://www.avg.com/www.special-uninstallation-feedback-app?lic=OQBBAFYARgBSAEUARQAtAFYATgBKADMAMgAtAEcAMwBMAEEAQQAtAEEANAA4ADkAUgAtADkAVQBKAESARgAtAEUASwBLADMAWAA>

"&"inst=NwA3AC0ANAA0ADMAMgAyADMAMwA5ADcALQBCAEEAUgA5AEcAKwAxAC0AVABCA DkAKwAyAC0ARgBMACsAQQAtAFgATwAzADYAKwAxAC0AWABPADkAKwAxAC0ARABEAFQA KwAwAA"&"prod=90"&"ver=9.0.894

O4 - HKUS\S-1-5-19\..\Run: [Sidebar] %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun (User 'LOCAL SERVICE')

O4 - HKUS\S-1-5-19\..\RunOnce: [mctadmin] C:\Windows\System32\mctadmin.exe (User 'LOCAL SERVICE')

O4 - HKUS\S-1-5-20\..\Run: [Sidebar] %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun (User 'NETWORK SERVICE')

O4 - HKUS\S-1-5-20\..\RunOnce: [mctadmin] C:\Windows\System32\mctadmin.exe (User 'NETWORK SERVICE')

O8 - Extra context menu item: &????? ?? Microsoft Excel - res://C:\PROGRA~1\MICROS~2\Office12\EXCEL.EXE/3000

O8 - Extra context menu item: Download all links with IDM - C:\Program Files\Internet Download Manager\IEGetAll.htm

O8 - Extra context menu item: Download with IDM - C:\Program Files\Internet Download Manager\IEExt.htm

O8 - Extra context menu item: Google Sidewiki... - res://C:\Program Files\Google\Google Toolbar\Component\GoogleToolbarDynamic_mui_en_70C5B381380DB17F.dll/cmsidewiki.html

O8 - Extra context menu item: Sothink SWF Catcher - C:\Program Files\Common Files\SourceTec\SWF Catcher\InternetExplorer.htm

O9 - Extra button: @C:\Program Files\Windows Live\Companion\companionlang.dll,-600 - {0000036B-C524-4050-81A0-243669A86B9F} - C:\Program Files\Windows Live\Companion\companioncore.dll

O9 - Extra button: @C:\Program Files\Windows Live\Writer\WindowsLiveWriterShortcuts.dll,-1004 - {219C3416-8CB2-491a-A3C7-D9FCDDC9D600} - C:\Program Files\Windows Live\Writer\WriterBrowserExtension.dll

O9 - Extra 'Tools' menuitem: @C:\Program Files\Windows Live\Writer\WindowsLiveWriterShortcuts.dll,-1003 - {219C3416-8CB2-491a-A3C7-D9FCDDC9D600} - C:\Program Files\Windows Live\Writer\WriterBrowserExtension.dll

O9 - Extra button: ??? ?? OneNote - {2670000A-7350-4f3c-8081-5663EE0C6C49} - C:\PROGRA~1\MICROS~2\Office12\ONBttNIE.dll

O9 - Extra 'Tools' menuitem: ?&?? ?? OneNote - {2670000A-7350-4f3c-8081-5663EE0C6C49} - C:\PROGRA~1\MICROS~2\Office12\ONBttNIE.dll

O9 - Extra button: Research - {92780B25-18CC-41C8-B9BE-3C9C571A8263} - C:\PROGRA~1\MICROS~2\Office12\REFIEBAR.DLL

O9 - Extra button: Fiddler2 - {CF819DA3-9882-4944-ADF5-6EF17ECF3C6E} - "C:\Program Files\Fiddler2\Fiddler.exe" (file missing)
O9 - Extra 'Tools' menuitem: Fiddler2 - {CF819DA3-9882-4944-ADF5-6EF17ECF3C6E} - "C:\Program Files\Fiddler2\Fiddler.exe" (file missing)
O9 - Extra button: Sothink SWF Catcher - {E19ADC6E-3909-43E4-9A89-B7B676377EE3} - C:\Program Files\Common Files\SourceTec\SWF Catcher\InternetExplorer.htm
O9 - Extra 'Tools' menuitem: Sothink SWF Catcher - {E19ADC6E-3909-43E4-9A89-B7B676377EE3} - C:\Program Files\Common Files\SourceTec\SWF Catcher\InternetExplorer.htm
O10 - Unknown file in Winsock LSP: c:\program files\common files\microsoft shared\windows live\wlidnsp.dll
O10 - Unknown file in Winsock LSP: c:\program files\common files\microsoft shared\windows live\wlidnsp.dll
O11 - Options group: [ACCELERATED_GRAPHICS] Accelerated graphics
O16 - DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} (Shockwave Flash Object) - <http://fpdownload2.macromedia.com/get/shockwave/cabs/flash/swflash.cab>
O16 - DPF: {F6ACF75C-C32C-447B-9BEF-46B766368D29} (Creative Software AutoUpdate Support Package) - <http://ccfiles.creative.com/Web/softwareupdate/su2/ocx/15112/CTPID.cab>
O16 - DPF: {FD0B6769-6490-4A91-AA0A-B5AE0DC75AC9} (Performance Viewer Activex Control) - <https://secure.logmein.com/activex/ractrl.cab?lmi=100>
O18 - Protocol: grooveLocalGWS - {88FED34C-F0CA-4636-A375-3CB6248B04CD} - C:\Program Files\Microsoft Office\Office12\GrooveSystemServices.dll
O18 - Protocol: wpg - {E43EF6CD-A37A-4A9B-9E6F-83F89B8E6324} - C:\Program Files\Windows Live\Photo Gallery\AlbumDownloadProtocolHandler.dll
O23 - Service: AMD External Events Utility - AMD - C:\Windows\system32\atiesrxx.exe
O23 - Service: FLEXnet Licensing Service - Macrovision Europe Ltd. - C:\Program Files\Common Files\Macrovision Shared\FLEXnet Publisher\FNPLicensingService.exe
O23 - Service: ????? Google Update (gupdate) (gupdate) - Google Inc. - C:\Program Files\Google\Update\GoogleUpdate.exe
O23 - Service: ????? Google (gupdatem) (gupdatem) - Google Inc. - C:\Program Files\Google\Update\GoogleUpdate.exe
O23 - Service: MBAMService - Malwarebytes Corporation - C:\Program Files\Malwarebytes' Anti-Malware\mbamservice.exe
O23 - Service: Nero BackItUp Scheduler 3 - Nero AG - C:\Program Files\Nero\Nero8\Nero BackItUp\NBService.exe
O23 - Service: NMIndexingService - Nero AG - C:\Program Files\Common Files\Nero\Lib\NMIndexingService.exe
O23 - Service: PLFlash DeviceIoControl Service - Prolific Technology Inc. - C:\Windows\system32\IoctlSvc.exe
O23 - Service: Sandboxie Service (SbieSvc) - SANDBOXIE L.T.D - C:\Program Files\Sandboxie\SbieSvc.exe
O23 - Service: SwitchBoard - Adobe Systems Incorporated - C:\Program Files\Common Files\Adobe\SwitchBoard\SwitchBoard.exe
O23 - Service: TeamViewer 6 (TeamViewer6) - TeamViewer GmbH - C:\Program Files\TeamViewer\Version6\TeamViewer_Service.exe

--

End of file - 8407 bytes

Thanks in advance.

Greetings,

Whilst I am in the process of scrutinizing your complete set of provided logs for any possible infections or problems, I ask for your forbearance. Understand that the process of analysis requires time and careful examination hence the need for a cautious response. Accuracy is of the essence. Once I come across infections, I shall present the finest methods of removal for your convenience.

In return for this service, I propose to you two conditions:

You are not to create any new threads regarding the similar topic as it will waste another helper's time.

You are not to install any new software in your system, as it may hinder our process thus making this futile.

In accordance to my terms, I also ask of you six things, stated below:

You are not to modify the logs in any way. Failure to do so will instantly deprive you of this service.

You are to paste each log separately at '[Pastebin](#)' as it is. That is correct, no syntax highlighting, no editing - just the log purely. Post back the links for each log. You shall not hide them under spoiler codes.

You are to provide the complete set of requested logs.

You are to keep all your trusted tools that the scanners may detect in a password protected archive. This is to prevent them from being deleted as we've had complaints or refusal to use the scanner for this reason.

You are to respond to every step I ask you to do using the format provided at the end of my post.

You agree that I have the right to discontinue the analysis at any time, upon a violation of a single rule.

Provided that you will continue with this service, you hereby agree to the above statements. If you deem the conditions are portraying equality, I will willingly perform the analysis without further delay. Should you have any concerns or problems with the above conditions, or if you feel that I have overlooked your log, do inform me through a Private Message.

Thank you.

Genuinely yours,
Paradoxum
Optional Pre-Step

With regard to my fourth condition, here are the steps on how to password protect your trusted tools momentarily. Do note that I would advise you to remove all the infections present in your system as I am not certain of the sources of these programs thereby I will not be able to verify whether they are backdoored or not.

You are doing this at your own risk.

Create a new folder with the name of your choice.

Gather all of your tools into that folder.

If you do not have a file compressor, download '[7-Zip](#)' and install it.

After doing so, navigate to the said folder and right-click. You are now presented with options.

Please chose 7-Zip > Add to Archive.

Under the Archive Name, enter any name you wish.

Set the Archive Format to 7z.

Set the Compression Level to Ultra.

Under Encryption fill in the Password field twice. You can tick Show Password if you desire.

When everything is done, click OK.

Wait for some time. The waiting time is determined by the size of your files.

7-Zip will have produced the file for you.

Now we test the file by Right-click > 7-Zip > Extract Here.

A prompt asking you for the password should appear.

Select Cancel as this is for testing purposes only.

Now delete the other folder, empty your Recycle Bin and proceed with the instructions.

Note: After I have declared you ALL CLEAN, you may extract your files and dispose of the protected archive.

Pre-Step I

Click '[here](#)' to download Temp File Cleaner by OldTimer. Save it to your desktop.

Close any open windows.

Double-click TFC.exe and select Run when prompted to execute the program. It will close all open programs itself in order to run.

Click the Start button to begin the cleaning process.

Please let the program run uninterruptedly.

Once the cleaning has been done, your computer should automatically reboot. Otherwise, please do so when it does not.

Pre-Step II

Download Security Check by screen317 from ['here'](#) or ['here'](#).

Save it to your desktop.

Double-click SecurityCheck.exe and follow the instructions inside of the black box.

A Notepad document called Checkup.txt should automatically open; please post the contents of that document.

Pre-Step III

Download ['aswMBR.exe'](#) to your desktop.

Double-click aswMBR.exe to run it. Windows Vista and Windows 7 users should run it as an administrator.

Click the Scan button to start the scan.

Upon the completion of the scan, click Save Log, and save it to your desktop. Post it in your next reply.

Prerequisite

If you are having a problem running HijackThis as an administrator (Windows Vista and Windows 7), please follow the steps below.

On your desktop, right-click the HijackThis icon and select Properties.

Navigate to the Compatibility tab and put a check on the Run this program as an administrator box.

Click Apply > OK.

HijackThis should prompt you to run it as an administrator every time you open it.

Step 1

Please run HijackThis as an administrator. Click Do a system scan only and place a check next to the following line(s) if present:

R3 - URLSearchHook: (no name) - {67aa0145-a051-4660-a910-22da3bab1fa5} - (no file)

R3 - URLSearchHook: (no name) - {f228c6a4-a593-4017-944c-4e7958fb3177} - (no file)

Then, close all other open windows and click Fix Checked. You are to reboot your system

afterwards.

Step 2

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

Double-click esetsmartinstaller_enu.exe to execute the program.

Tick Yes, I accept the Terms of Use.

Click Start.

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

Database download may take some time.

When done, make sure that the option Remove found threats is ticked. Under the and Advanced Settings, please put a check on the following options: Scan for potentially unwanted applications

Enable Anti-Stealth Technology

Click Start.

Wait for the scan to finish.

Once it is finished, use Notepad to open the log file located at C:\Program Files\ESET\ESET Online Scanner\log.txt.

Copy and paste that log as a reply to this topic.

Step 3

Please download Malwarebytes' Anti-Malware ['here'](#). This is a scanner which I will ask you to use.

Double-click mbam-setup.exe to install the application.

Make sure a check mark is placed next to 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.

Restart if it tells you to.

The log is automatically saved by Malwarebytes' Anti-Malware and can be viewed by clicking the Logs tab in the interface.

Copy and paste the entire report in your next reply.

Step 4

Download DDS.scr by SUBs from one of the following links and save it to your desktop.

['Link 1'](#)

['Link 2'](#)

Double-click on DDS.scr and a command window will appear. This is normal.

Shortly after two logs will appear, DDS.txt and Attach.txt.

A window will open instructing you save and post the logs.

Save the logs to a convenient place such as your desktop.

Copy the contents of both logs and post them at ['Pastebin'](#) separately and post the links in your next reply.

In your next post, please provide the following: A Fresh HijackThis (HJT) Log

aswMBR Log

Doesn't Do Squat (DDS) Logs DDS.txt

Attach.txt

ESET Scan Log

Malwarebytes' Anti-Malware Scan Log

Security Check Log

Format of Response

As part of my service terms, you are to fill this up every time you respond to your log. Copy and paste the content inside the code box and write directly after the closing tags.

Example: [\(Click to View\)](#) Step # 1

Problems Encountered: N/A

Step # 2

Problems Encountered: N/A

Step # 3

Problems Encountered: The scan did not finish.

Step # 4

Problems Encountered: N/A

Link To Requested Logs:

<http://pastebin.com/example>
<http://pastebin.com/example>
<http://pastebin.com/example>
<http://pastebin.com/example>

Code [b]Step # [/b]

[b]Problems Encountered: [/b]

[b]Step # [/b]

[b]Problems Encountered: [/b]

[b]Step # [/b]

[b]Problems Encountered: [/b]

[b]Step # [/b]

[b]Problems Encountered: [/b]

[b]Link To Requested Logs: [/b]

Stenography - September 2, 2011, 2:09 pm

(Sep 2, 2011 06:06 AM)Paradoxum Wrote: [\[CITE\]](#) Greetings,

Whilst I am in the process of scrutinizing your complete set of provided logs for any possible infections or problems, I ask for your forbearance. Understand that the process of analysis requires time and careful examination hence the need for a cautious response. Accuracy is of the essence. Once I come across infections, I shall present the finest methods of removal for your convenience.

In return for this service, I propose to you two conditions:

You are not to create any new threads regarding the similar topic as it will waste another helper's time.

You are not to install any new software in your system, as it may hinder our process thus making this futile.

In accordance to my terms, I also ask of you six things, stated below:

You are not to modify the logs in any way. Failure to oodo so will instantly deprive you of this service.

You are to paste each log separately at '[Pastebin](#)' as it is. That is correct, no syntax highlighting, no editing - just the log purely. Post back the links for each log. You shall not hide them under spoiler codes.

You are to provide the complete set of requested logs.

You are to keep all your trusted tools that the scanners may detect in a password protected archive. This is to prevent them from being deleted as we've had complaints or refusal to use the scanner for this reason.

You are to respond to every step I ask you to do using the format provided at the end of my post.

You agree that I have the right to discontinue the analysis at any time, upon a violation of a single rule.

Provided that you will continue with this service, you hereby agree to the above statements. If you deem the conditions are portraying equality, I will willingly perform the analysis without further delay. Should you have any concerns or problems with the above conditions, or if you feel that I have overlooked your log, do inform me through a Private Message.

Thank you.

Genuinely yours,
Paradoxum
Optional Pre-Step

With regard to my fourth condition, here are the steps on how to password protect your trusted tools momentarily. Do note that I would advise you to remove all the infections present in your system as I am not certain of the sources of these programs thereby I will not be able to verify whether they are backdoored or not.

You are doing this at your own risk.

Create a new folder with the name of your choice.

Gather all of your tools into that folder.

If you do not have a file compressor, download '[7-Zip](#)' and install it.

After doing so, navigate to the said folder and right-click. You are now presented with options.

Please chose 7-Zip > Add to Archive.

Under the Archive Name, enter any name you wish.

Set the Archive Format to 7z.

Set the Compression Level to Ultra.

Under Encryption fill in the Password field twice. You can tick Show Password if you desire.

When everything is done, click OK.

Wait for some time. The waiting time is determined by the size of your files.

7-Zip will have produced the file for you.

Now we test the file by Right-click > 7-Zip > Extract Here.

A prompt asking you for the password should appear.

Select Cancel as this is for testing purposes only.

Now delete the other folder, empty your Recycle Bin and proceed with the instructions.

Note: After I have declared you ALL CLEAN, you may extract your files and dispose of the protected archive.

Pre-Step I

Click ['here'](#) to download Temp File Cleaner by OldTimer. Save it to your desktop.

Close any open windows.

Double-click TFC.exe and select Run when prompted to execute the program. It will close all open programs itself in order to run.

Click the Start button to begin the cleaning process.

Please let the program run uninterrupted.

Once the cleaning has been done, your computer should automatically reboot. Otherwise, please do so when it does not.

Pre-Step II

Download Security Check by screen317 from ['here'](#) or ['here'](#).

Save it to your desktop.

Double-click SecurityCheck.exe and follow the instructions inside of the black box.

A Notepad document called Checkup.txt should automatically open; please post the contents of that document.

Pre-Step III

Download ['aswMBR.exe'](#) to your desktop.

Double-click aswMBR.exe to run it. Windows Vista and Windows 7 users should run it as an administrator.

Click the Scan button to start the scan.

Upon the completion of the scan, click Save Log, and save it to your desktop. Post it in your next reply.

Prerequisite

If you are having a problem running HijackThis as an administrator (Windows Vista and Windows 7), please follow the steps below.

On your desktop, right-click the HijackThis icon and select Properties.

Navigate to the Compatibility tab and put a check on the Run this program as an administrator box.

Click Apply > OK.

HijackThis should prompt you to run it as an administrator every time you open it.

Step 1

Please run HijackThis as an administrator. Click Do a system scan only and place a check next to the following line(s) if present:

R3 - URLSearchHook: (no name) - {67aa0145-a051-4660-a910-22da3bab1fa5} - (no file)

R3 - URLSearchHook: (no name) - {f228c6a4-a593-4017-944c-4e7958fb3177} - (no file)

Then, close all other open windows and click Fix Checked. You are to reboot your system afterwards.

Step 2

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

Double-click esetsmartinstaller_enu.exe to execute the program.

Tick Yes, I accept the Terms of Use.

Click Start.

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

Database download may take some time.

When done, make sure that the option Remove found threats is ticked. Under the and Advanced

Settings, please put a check on the following options: Scan for potentially unwanted applications

Enable Anti-Stealth Technology

Click Start.

Wait for the scan to finish.

Once it is finished, use Notepad to open the log file located at C:\Program Files\ESET\ESET Online Scanner\log.txt.

Copy and paste that log as a reply to this topic.

Step 3

Please download Malwarebytes' Anti-Malware ['here'](#). This is a scanner which I will ask you to use.

Double-click mbam-setup.exe to install the application.

Make sure a check mark is placed next to 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. Restart if it tells you to.

The log is automatically saved by Malwarebytes' Anti-Malware and can be viewed by clicking the Logs tab in the interface.

Copy and paste the entire report in your next reply.

Step 4

Download DDS.scr by sUBs from one of the following links and save it to your desktop.

['Link 1'](#)

['Link 2'](#)

Double-click on DDS.scr and a command window will appear. This is normal.

Shortly after two logs will appear, DDS.txt and Attach.txt.

A window will open instructing you save and post the logs.

Save the logs to a convenient place such as your desktop.

Copy the contents of both logs and post them at '[Pastebin](#)' separately and post the links in your next reply.

In your next post, please provide the following:

- A Fresh HijackThis (HJT) Log

- aswMBR Log

- Doesn't Do Squat (DDS) Logs

- DDS.txt

- ESET Scan Log

- Malwarebytes' Anti-Malware Scan Log

- Security Check Log

Format of Response

As part of my service terms, you are to fill this up every time you respond to your log. Copy and paste the content inside the code box and write directly after the closing tags.

Example: [\(Click to View\)](#)

Step # 1

Problems Encountered: N/A

Step # 2

Problems Encountered: N/A

Step # 3

Problems Encountered: The scan did not finish.

Step # 4

Problems Encountered: N/A

Link To Requested Logs:

<http://pastebin.com/example>
<http://pastebin.com/example>
<http://pastebin.com/example>
<http://pastebin.com/example>

Code [b]Step # [/b]
[b]Problems Encountered: [/b]

[b]Step # [/b]
[b]Problems Encountered: [/b]

[b]Step # [/b]
[b]Problems Encountered: [/b]

[b]Step # [/b]
[b]Problems Encountered: [/b]

[b]Link To Requested Logs: [/b]

Gosh,i cleared temp and cleaned verything else with ATF cleaner CCleaner.
You just posted something that was saved in notepad and didn't analysed the logs

Paradoxum - September 2, 2011, 10:16 pm

(Sep 2, 2011 02:09 PM)PolarX Wrote: [\[CITE\]](#) Gosh,i cleared temp and cleaned verything else with ATF cleaner CCleaner.

Gosh, implying you think the rest of the steps are void? Forgive me when I say this, but you are an idiot. Do you think any helper will be able to determine that you used ATF-Cleaner or CCleaner? Just wow. I commend you for being able to read logs (oh wait, I only see one log) and not knowing the fact that the log above does not display whether or not you used such programs or any other log for this matter. Also, I hate to break it to you, but ATF-Cleaner is not for your operating system. Props to you. Also, I would like to say that your argument is invalid. What is the big deal if I ask you to clean your temporary files again? Will it make your computer explode? Oh joy, the hazards and difficulty of cleaning one's temporary files that one must never do it again for the sake of everyone's sanity.

Quote:You just posted something that was saved in notepad and didn't analysed the logs

I beg your pardon but my speeches aren't saved in Notepad for one. I did not analyse the log? Perhaps you should look at the first step? Or you should tell me how analysis is done, yes? I looked at your log for less than a minute. It's that easy and practically tells nothing in-depth of your system. If you have a problem with my asking for more logs to properly analyse your system (seeing as you can't read that you must post OTL logs instead of HijackThis then you have the guts to complain when the obvious problem is your reading capability) then I suggest you get out of this section. Also, I would like to enlighten you that helpers cannot and do not copy and paste similar instructions for everyone (except when certain idiots such as yourself forget the basics of scanning or attaching the log proving that they did scan and not assume helpers are magical people who can predict such a scan has been done) unless we want your system to crash. Which in all honesty, I wish to happen. TL;DR? Every log is different. It's not fucking rocket science.

So much for being a person asking for help that later complains when help is given. If you know what steps you should be doing then do it yourself. Do not post here and waste my time.