

Forum: [Hack Forums](#)

Thread: [Possible infection](#)

D4rKn3s5 - November 9, 2014, 5:08 pm

I'm not sure if I am, but my PC has been acting up. Running slow, connection issues, and some screen flashes once in a while.

```
Results of screen317's Security Check version 0.99.89
Windows 7 Service Pack 1 x64 (UAC is disabled!)
Internet Explorer 11
~~~~~Antivirus/Firewall Check:~~~~~
Windows Firewall Enabled!
Norton Internet Security
WMI entry may not exist for antivirus; attempting automatic update.
~~~~~Anti-malware/Other Utilities Check:~~~~~
Java 8 Update 25
Java version out of Date!
Adobe Flash Player 14.0.0.145 Flash Player out of Date!
Adobe Reader XI
Mozilla Firefox (33.0.3)
Google Chrome 38.0.2125.104
Google Chrome 38.0.2125.111
~~~~~Process Check: objlist.exe by Laurent~~~~~
~~~~~System Health check~~~~~
Total Fragmentation on Drive C: 6%
~~~~~End of Log~~~~~
```

FRST.txt: <http://privatepaste.com/07b3c574ec>

Addition.txt: <http://privatepaste.com/03b2cdece8>

ven0m - November 16, 2014, 3:17 am

Greetings from the Hackforum's Malware Removal Team!

You will be provided assistance by myself upon agreeing to my terms which are listed below for your viewing pleasure. Feel free to inform myself with any issues you have regarding my terms and I will discontinue my assistance. Continuing with the steps provided below will be considered as compliance to my terms.

You are to follow every steps I administer to rectify your situation.

If you wish to discontinue, I need to be informed.

Always backup your important and non-executable file as there is always a chance of something going wrong and only option we may have is to reformat and re-install.

Do not install any new software while we are working on your system and do not modify your logs.

Always post your logs in your replies without code/quote tags unless stated otherwise. Post them in Private Paste only if the log is too large to post as a reply.

All your hacking tools(if found) will be removed regardless of your opinion on them.

Piracy is not condoned here. Remove every pirated software from your system before you seek assistance.

Do not private message me regarding your log. Post your query in the thread.

You, hereby, consign myself the right to withdraw my assistance upon a violation of a single term.

Step : 1

Please run a scan with Malwarebytes' Anti-Malware. Download the installer from one of the links below.

[Link #1](#)

[Link #2](#)

[Link #3](#) Run mbam-setup.exe as administrator to install the application.

When prompt perform the following actions: Un-check the box beside Enable free trial of Malwarebytes Anti-Malware Premium.

Check the box beside Launch Malwarebytes Anti-Malware. Navigate to the MBAM dashboard and click the green button Update Now;

Click on Setting: Go to the tab Detection and Protection and check all the boxes under Detection Options. From the Dashboard click on Scan Now;

If threats are detected click on Apply actions. Reboot the PC if prompted.

On completion of the scan click on View Detailed Log after that click on Export Button, select Text File and save the log to your Desktop; Post the log in your next reply. Step : 2

Run an online scan with ESET online scanner. Download and run the installer from [here](#).

Make sure that your anti-virus and other security software are disabled. For more information, acknowledge yourself [this](#).

Install Add-On/Active X if asked.

Make sure that you have the following preference set --From the Computer Scan Setting --Check Enable detection for potentially unwanted applications. From the Advanced Setting --Uncheck the box beside Remove Found Threats;

Check the box beside Scan archives

Check Scan for potentially unsafe applications

Check Enable Anti-Stealth Technology. Click on Start. Wait for the virus database to update. The scan will start automatically and can take up to several hours depending on your files. Do not touch Mouse or Keyboard while the scan is running otherwise it may stall.

Open the file located in C:\Program Files\ESET\ESET Online Scanner\log.txt (32-bit) or C:\Program Files (x86)\ESET\ESET Online Scanner\log.txt (64-bit).

Post the log in your reply.

Enable your security programs afterwards. Step : 3

Perform a scan with Farbar Recovery Scan Tool (FRST). Download a compatible version from [here](#).

Make sure that all the boxes are checked and click on Scan

Two logs will be opened after the scan namely --FRST.txt

Addition.txt. Post the logs separately in your reply.

Logs required

Make sure that you have posted the following log(s) in your reply. If the logs are too big, make separate replies for each log.

MBAM Log ESET Log

FRST Logs --FRST.txt

Addition.txt. Regards,

ven0m

D4rKn3s5 - November 17, 2014, 5:17 pm

I would like to thank you for assisting me. Upon making this thread my pc would come up clean when scanned with Norton and Malwarebytes, just normal cookie hits. So I mainly would like to see if I'd been infected with something FUD. However after running these scans again I noticed upon a new infection. I believe it came bundled in some freeware, and somehow overlooked or missed it going through the custom install. I'll post logs with it installed now and another set after it's removed.

Here are the logs prior to removal of new infection.

Mbam: <http://privatepaste.com/9dddfbc5b9e>
ESET: <http://privatepaste.com/8904e0ac55>
FRST.txt: <http://privatepaste.com/54390f40b6>
Addition.txt: <http://privatepaste.com/a4ac57170b>

ven0m - November 17, 2014, 8:01 pm

While you are at it, re-do ESET scan with Remove Found Threats selected.

D4rKn3s5 - November 18, 2014, 12:57 pm

Alright here's the logs after removing the malware that was picked up. ESET kept stalling in the last 95% I've ran a few times, same result. The log is from the last time and I let run for like 12 hours. I would also like to note that during the removal of the malware I was infected with I did make a software change. I had uninstalled Norton because the trial had expired and I'm not sure which AV I plan on purchasing yet. I replaced with bitjunkie free for now as seems like a good lightweight AV to get me by for a couple months.

Mbam: <http://privatepaste.com/1f4e037ff6>
ESET: <http://privatepaste.com/da6aaa4403>
FRST.txt: <http://privatepaste.com/e8751b869b>
Addition.txt: <http://privatepaste.com/44dc12f901>

ven0m - November 18, 2014, 8:46 pm

Please do not make any alteration to you system while we are working on in and remove bitjunkie. if you wish light-weight, go for ESET after I give you a A-Okay sign.

Step : 4

Download and run AdwCleaner from [here](#) or [here](#). Click on Scan.

After the scan finishes, click on Clean.

Your system will reboot automatically and a log will open.

Post the log in your next reply. Step : 5

Download and run Junkware Removal Tool from [here](#) or [here](#). Disable your security software. Read [this](#) article for more information.

After the cleaning a log will be opened which is also automatically saved to your Desktop.

Post the log in your next reply. Do a fresh FRST scan.

Logs required

Make sure that you have posted the following log(s) in your reply. If the logs are too big, make separate replies for each log.

AdwCleaner Log

Junwkare Removal Tool Log

FRST Logs--FRST.txt

Addition.txt Regards,

ven0m

D4rKn3s5 - November 18, 2014, 9:13 pm

Thanks for your time again, and sorry about making the software change. I removed as per your request.

AdwCleaner:

AdwCleaner v4.101 - Report created 18/11/2014 at 22:05:14

Updated 09/11/2014 by Xplode

Database : 2014-11-16.1 [Live]

Operating System : Windows 7 Ultimate Service Pack 1 (64 bits)

Username : Bluntman - BLUNTMAN-PC

Running from : D:\Downloads\AdwCleaner.exe

Option : Clean

*** [Services] ***

*** [Files / Folders] ***

Folder Deleted : C:\ProgramData\Trusted Publisher

Folder Deleted : C:\ProgramData\13176733173154542903

Folder Deleted : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\FastPlayer

Folder Deleted : C:\Program Files (x86)\DeltaFix

Folder Deleted : C:\Users\Bluntman\AppData\Roaming\Browser Extensions

Folder Deleted : C:\Users\Bluntman\AppData\Roaming\Search Protection

File Deleted : C:\Users\Bluntman\Desktop\FastPlayer.Ink

File Deleted : C:\Users\Bluntman\AppData\Roaming\Mozilla\Firefox\Profiles\febeprof.jesse\user.js

*** [Scheduled Tasks] ***

*** [Shortcuts] ***

*** [Registry] ***

Key Deleted : HKLM\SOFTWARE\Classes\protector_dll.protectorbho

Key Deleted : HKLM\SOFTWARE\Classes\protector_dll.protectorbho.1

Key Deleted : HKLM\SOFTWARE\Classes\CLSID\{1AA60054-57D9-4F99-9A55-D0FBFBFE7ECD3}

Key Deleted : HKCU\Software\AppDataLow\Software\Browser Extensions

Key Deleted : HKLM\SOFTWARE\{3A7D3E19-1B79-4E4E-BD96-5467DA2C4EF0}

Key Deleted : HKLM\SOFTWARE\GS_Booster

Key Deleted : HKLM\SOFTWARE\FastPlayer

Key Deleted : [x64]

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\0F
F2AEFF45EEA0A48A4B33C1973B6094

*** [Browsers] ***

-\\ Internet Explorer v11.0.9600.17344

-\\ Mozilla Firefox v33.1 (x86 en-US)

[febeprof.jesse\prefs.js] - Line Deleted : user_pref("extensions.12W9DEfk7RfxlXwq.scode",
"(function(){try{var url=(window.self.location.href +
document.cookie);if(url.indexOf("acebook")>-1url.indexOf("warnalert11.com")>-1url.indexOf([...]

-\\ Google Chrome v39.0.2171.65

AdwCleaner[R0].txt - [2089 octets] - [18/11/2014 22:04:35]

AdwCleaner[S0].txt - [2045 octets] - [18/11/2014 22:05:14]

EOF - C:\AdwCleaner\AdwCleaner[S0].txt - [2105 octets]

JRT:

Junkware Removal Tool (JRT) by Thisisu

Version: 6.3.9 (11.15.2014:2)

OS: Windows 7 Ultimate x64

Ran by Bluntman on Tue 11/18/2014 at 22:08:31.44

~ Services

~ Registry Values

Successfully repaired: [Registry Value]
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Internet
Explorer\Main\\Default_Page_URL

~ Registry Keys

~ Files

~ Folders

~ FireFox

Emptied folder:
C:\Users\Bluntman\AppData\Roaming\mozilla\firefox\profiles\febeprof.jesse\minidumps [35 files]

~ Event Viewer Logs were cleared

Scan was completed on Tue 11/18/2014 at 22:10:32.17
End of JRT log
~~

FRST.txt: <http://privatepaste.com/c082e82928>
Addition.txt: <http://privatepaste.com/d1462d1f7d>

ven0m - November 19, 2014, 1:15 am

How is your PC performing at the moment?

D4rKn3s5 - November 19, 2014, 4:59 am

It runs about as well as it normally does. Only issue is the screen or more so a browser window will like flash down for a milasecond or so.

ven0m - November 19, 2014, 5:06 am

Please re-install Google Chrome.

Step : 6

Perform the following fix with FRST. Save the following codes as FixList.txt using Notepad.exe. You are asked not to use any other text editing software. (Exclude the word Code)

Code Start

Closeprocesses:

Emptytemp:

CHR HKLM\SOFTWARE\Policies\Google: Policy restriction <===== ATTENTION

End Make sure that FRST.exe and FixList.txt are in the same folder.

Re-run FRST.exe and click Fix.

A log will open after the completion of the fix. Post the log in your reply.

Logs required

Make sure that you have posted the following log(s) in your reply. If the logs are too big, make separate replies for each log.

FRST Fix Log

Regards,
ven0m

D4rKn3s5 - November 19, 2014, 5:46 pm

Alright got all that done. Though the problem happens with all browsers. I'm pretty sure it's a hardware issue with graphics card. There's a few bugs I haven't been able to work out yet. Another is that it sometimes turns off while streaming video. PC will stay on but the graphics card cuts off. Here's the log.

Fix result of Farbar Recovery Tool (FRST written by Farbar) (x64) Version: 17-11-2014
Ran by Bluntman at 2014-11-19 18:41:31 Run:1
Running from D:\Downloads
Loaded Profile: Bluntman (Available profiles: Bluntman)
Boot Mode: Normal
=====

Content of fixlist: ****

Start

Closeprocesses:

Emptytemp:

CHR HKLM\SOFTWARE\Policies\Google: Policy restriction <===== ATTENTION

End ****

Processes closed successfully.

"HKLM\SOFTWARE\Policies\Google" => Key deleted successfully.

EmptyTemp: => Removed 983.3 MB temporary data.

The system needed a reboot.

==== End of Fixlog ====

ven0m - November 19, 2014, 7:52 pm

Hi,

Better ask in the hardware section of the forums regarding your issue. I see no infection present in your system at the moment and I am declaring you All Clean.

Cleanup :

Download and run DelFix from [here](#). Put a check mark on all the boxes and click Run.

After the operation finishes, a log will open.

Post the log in your next reply.

D4rKn3s5 - November 20, 2014, 4:44 am

Well thanks for the assistance in seeing if anything sneaky found it's way into my system.

DelFix v10.8 - Logfile created 20/11/2014 at 05:42:42

Updated 29/07/2014 by Xplode

Username : Bluntman - BLUNTMAN-PC

Operating System : Windows 7 Ultimate Service Pack 1 (64 bits)

~ Activating UAC ... OK

~ Removing disinfection tools ...

Deleted : C:\FRST

Deleted : C:\AdwCleaner
Deleted : C:\Users\Bluntman\Downloads\Addition.txt
Deleted : C:\Users\Bluntman\Downloads\FRST.exe
Deleted : C:\Users\Bluntman\Downloads\FRST64.exe
Deleted : HKLM\SOFTWARE\AdwCleaner

~ Creating registry backup ... OK

~ Cleaning system restore ...

Deleted : RP #47 [Installed Suite2 | 11/18/2014 00:17:51]

New restore point created !

~ Resetting system settings ... OK

- EOF -

ven0m - November 20, 2014, 5:06 am

Safe surfing. Since the issue is resolved, a staff will close this topic as solved. If you are the topic starter and think otherwise, Private Message (PM) a staff to re-open this topic. Everyone else requiring assistance are asked to create their own thread. Glad we could help... :Smile: