

Forum:[Hack Forums](#)

Thread: [i would like to make on proper check up to see if my pc is rly clean!](#)

Jose"the real 1" - August 5, 2014, 2:51 am

I am about to do a lot of online banking and was not allways very carefull what i did download, can someone of the whitehat helper help me to check if my pc is clean or not and in case its not clean help to clean it!

what are the steps i have to do?

my privatepaste is following, i hope i did not forget anything!

<http://privatepaste.com/b4940fd826>

ven0m - August 8, 2014, 5:43 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 for 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

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.

Farbar Logs --FRST.txt

Addition.txt Regards,

ven0m

Jose"the real 1" - August 8, 2014, 9:41 am

hey, thank you very much for helping me!

[First.txt](#)
[addition.txt](#)

[Shortcut.txt](#)

ven0m - August 9, 2014, 7:47 am

Hi,

Step : 2

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

Hosts:

() C:\Windows\System32\PnkBstrA.exe

C:\Windows\System32\PnkBstrA.exe

SearchScopes: HKCU - {2E00D31D-D171-423D-836D-1A4D7EA7F1A9} URL =

http://astromenda.com/results.php?f=4&q={searchTerms}&a=ast_frg01_14_48_ff&cd=2XzuyEtN2Y1L1Qzu0DyEtA0DyB0EyC0CyCtC0EyBtAtA0EtCtN0D0Tzu0SzyyEtAtN1L2XzutBtFtBtCtFtCzztFtAtN1L1CzutCyEtBzytDyD1V1TtN1L1G1B1V1N2Y1L1Qzu2StB0A0DyEzz0E0C0AtGyB0CtA0EtG0ByCyDzytGtDtDyDyDtGtAtA0A0E0Bzy0EzzyCtAtC0B2QtN1M1F1B2Z1V1N2Y1L1Qzu2StCtD0F0DtDzztCyCtGzz0B0AzytG0EyCtBtDtGtD0CtB0AtGyDtDyDzzzy0CyByEzy0CtC0E2Q&cr=454746507&ir=CHR HomePage:

hxxp://astromenda.com/?f=1&a=ast_frg01_14_48_ff&cd=2XzuyEtN2Y1L1Qzu0DyEtA0DyB0EyC0CyCtC0EyBtAtA0EtCtN0D0Tzu0SzyyEtAtN1L2XzutBtFtBtCtFtCzztFtAtN1L1CzutCyEtBzytDyD1V1TtN1L1G1B1V1N2Y1L1Qzu2StB0A0DyEzz0E0C0AtGyB0CtA0EtG0ByCyDzytGtDtDyDyDtGtAtA0A0E0Bzy0EzzyCtAtC0B2QtN1M1F1B2Z1V1N2Y1L1Qzu2StCtD0F0DtDzztCyCtGzz0B0AzytG0EyCtBtDtGtD0CtB0AtGyDtDyDzzzy0CyByEzy0CtC0E2Q&cr=454746507&ir=

CHR StartupUrls:

"hxxp://astromenda.com/?f=7&a=ast_frg01_14_48_ff&cd=2XzuyEtN2Y1L1Qzu0DyEtA0DyB0EyC0CyCtC0EyBtAtA0EtCtN0D0Tzu0SzyyEtAtN1L2XzutBtFtBtCtFtCzztFtAtN1L1CzutCyEtBzytDyD1V1TtN1L1G1B1V1N2Y1L1Qzu2StB0A0DyEzz0E0C0AtGyB0CtA0EtG0ByCyDzytGtDtDyDyDtGtAtA0A0E0Bzy0EzzyCtAtC0B2QtN1M1F1B2Z1V1N2Y1L1Qzu2StCtD0F0DtDzztCyCtGzz0B0AzytG0EyCtBtDtGtD0CtB0AtGyDtDyDzzzy0CyByEzy0CtC0E2Q&cr=454746507&ir="

CHR DefaultSearchKeyword: Astromenda.com

R2 PnkBstrA; C:\WINDOWS\system32\PnkBstrA.exe [76152 2014-08-03] ()

R2 PnkBstrA; C:\WINDOWS\SysWOW64\PnkBstrA.exe [76888 2014-03-21] ()

C:\WINDOWS\SysWOW64\PnkBstrA.exe

2014-08-05 10:03 - 2014-08-05 10:30 - 000000 _____ () C:\end

2014-08-01 10:28 - 2014-07-16 16:43 - 00020280 _____ () C:\WINDOWS\system32\roboot64.exe

C:\Users\tobias\jagex_cl_runescape_LIVE.dat

C:\Users\tobias\random.dat

Reboot:

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.

Step : 3

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 : 4

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. 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
AdwCleaner Log
Junkware Removal Tool Log
Regards,
ven0m

Jose"the real 1" - August 9, 2014, 11:07 am

[jrt.txt](#)

[AdwCleaner\[S0\]](#)

[Fixlog](#)

it allready seems that my pc runs more smooth thanks for you help man!

ven0m - August 10, 2014, 7:47 am

Hi,
Step : 5
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 : 6
Run an online scan with ESET online scanner. Download and run the installer from [here](#).
Make sure than 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. 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
Regards,
ven0m

Jose"the real 1" - August 10, 2014, 11:45 am

[mbam logs](#)

[eset logs](#)

thanks for your help!!!

ven0m - August 11, 2014, 8:54 am

Hi,

Log looks good. How is your system as we speak. Please perform the following step.

Step : 7

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

C:\Games\Watch Dogs\bin\Watch_Dogs.exe

C:\Users\tobias\Desktop\Neuer Ordner\Sharp\lsharp.zip

C:\Users\tobias\Desktop\Neuer Ordner\Sharp\Assemblies\System\Leaguesharp.Core.dll

C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\IE\AskTo
olbarInstaller-AVIRA-V7[1].7z

C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\IE\AskTo
olbarInstaller-AVIRA-V7[2].7z

C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\IE\AskTo
olbarInstaller-AVIRA-V7[3].7z

C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\IE\Ask
ToolbarInstaller-AVIRA-V7[1].7z

C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\IE\Ask
ToolbarInstaller-AVIRA-V7[2].7z

C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\IE\Ask
ToolbarInstaller-AVIRA-V7[3].7z

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

Jose"the real 1" - August 11, 2014, 11:59 am

[FixlistLOg](#)

my pc runs more smooth, i hope we could clean all infections... was more then i thought.....

ven0m - August 12, 2014, 9:40 am

Hi,

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.

Jose"the real 1" - August 12, 2014, 1:06 pm

[del fix log](#)

thank you very much for your help and +3

ven0m - August 13, 2014, 6:34 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: