

Forum: [Hack Forums](#)

Thread: [Probably Ratted might solved it](#)

Xero666 - October 28, 2014, 10:35 am

Here is the context of my Checkup.txt:

```
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:~~~~~
avast! Antivirus
Antivirus up to date!
~~~~~Anti-malware/Other Utilities Check:~~~~~
Java 7 Update 55
Java version out of Date!
Adobe Flash Player 12.0.0.77 Flash Player out of Date!
Adobe Reader 10.0.1 Adobe Reader out of Date!
Google Chrome 38.0.2125.104
Google Chrome 38.0.2125.111
~~~~~Process Check: objlist.exe by Laurent~~~~~
AVAST Software Avast AvastSvc.exe
AVAST Software Avast AvastUI.exe
~~~~~System Health check~~~~~
Total Fragmentation on Drive C:
~~~~~End of Log~~~~~
```

And here are the two Pastebin Logs of Addition.txt and FRST.txt

FRST.txt: <http://pastebin.com/NHyTZJ2z>

Addition.txt: <http://pastebin.com/esBUAmDH>

I also noticed that i have an Windows Testbuild V.7601.

It happened some time ago but im not sure how could i remove that and because i got now negative effects from it i didnt cared that much.

For now i use a Keyscrambler because im not totally sure if im RAT free.

The reason i think i got ratted is all my pws got changed in no time even when i changed them to something very hard to bruteforce and i never used them before.

ven0m - November 2, 2014, 12:50 pm

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

You currently have following out-dated program(s) in your system which (if left alone) may cause system vulnerability. I urge you to un-install the program(s) completely and download their updated version from their official sites and install them.

Java 7 Update 55

Adobe Flash Player

Adobe Reader

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

Closeprocesses:

Emptytemp:

HKLM-x32\...\Run: [] => [X]

HKU\S-1-5-21-1011809894-3870464874-3822914839-1000\...\Run: [ASRockXTU] => [X]

HKU\S-1-5-21-1011809894-3870464874-3822914839-1000\...\Run: [zASRockInstantBoot] => [X]

FF Plugin-x32: @pandonetworks.com/PandoWebPlugin -> C:\Program Files (x86)\Pando Networks\Media Booster\npPandoWebPlugin.dll No File

C:\Program Files (x86)\Pando Networks\

testsigning: ==> Check for possible unsigned rootkit driver <===== 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.

Step : 3

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 : 4

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.

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

MBAM Log

ESET Log

Regards,
ven0m

Xero666 - November 2, 2014, 10:41 pm

Eset Results:

C:\Documents and Settings\Vincent\AppData\Local\Google\Chrome\User Data\Default\File System\002\t\00\000000 a variant of Win32/DomaIQ.BB potentially unwanted application

C:\Documents and Settings\Vincent\AppData\Local\Google\Chrome\User Data\Default\File System\003\t\00\000000 a variant of Win32/DomaIQ.BG potentially unwanted application

C:\Documents and Settings\Vincent\Lokale Einstellungen\Google\Chrome\User Data\Default\File System\002\t\00\000000 a variant of Win32/DomaIQ.BB potentially unwanted application

C:\Documents and Settings\Vincent\Lokale Einstellungen\Google\Chrome\User Data\Default\File System\003\t\00\000000 a variant of Win32/DomaIQ.BG potentially unwanted application

C:\Dokumente und Einstellungen\Vincent\AppData\Local\Anwendungsdaten\Google\Chrome\User Data\Default\File System\002\t\00\000000 a variant of Win32/DomaIQ.BB potentially unwanted application

C:\Dokumente und Einstellungen\Vincent\AppData\Local\Anwendungsdaten\Google\Chrome\User Data\Default\File System\003\t\00\000000 a variant of Win32/DomaIQ.BG potentially unwanted application

C:\Dokumente und Einstellungen\Vincent\AppData\Local\Google\Chrome\User Data\Default\File System\002\t\00\000000 a variant of Win32/DomaIQ.BB potentially unwanted application

C:\Dokumente und Einstellungen\Vincent\AppData\Local\Google\Chrome\User Data\Default\File System\003\t\00\000000 a variant of Win32/DomaIQ.BG potentially unwanted application

C:\Dokumente und Einstellungen\Vincent\Desktop\hacks\High Minded\High Minded.exe a variant of Win32/Packed.VMProtect.ABD trojan

C:\Dokumente und Einstellungen\Vincent\Desktop\hacks\League of Legends\Bot\Scripts\Common\Evadeeee.dll a variant of Win32/Packed.VMProtect.ABD trojan

C:\Dokumente und Einstellungen\Vincent\Desktop\hacks\Payday 2\PDAY2+17Tr-LNG_v39.0.exe a variant of Win32/Packed.VMProtect.ABD trojan

C:\Dokumente und Einstellungen\Vincent\Lokale Einstellungen\Google\Chrome\User Data\Default\File System\002\t\00\000000 a variant of Win32/DomaIQ.BB potentially unwanted application
C:\Dokumente und Einstellungen\Vincent\Lokale Einstellungen\Google\Chrome\User Data\Default\File System\003\t\00\000000 a variant of Win32/DomaIQ.BG potentially unwanted application
C:\Users\Vincent\AppData\Local\Google\Chrome\User Data\Default\File System\002\t\00\000000 a variant of Win32/DomaIQ.BB potentially unwanted application
C:\Users\Vincent\AppData\Local\Google\Chrome\User Data\Default\File System\003\t\00\000000 a variant of Win32/DomaIQ.BG potentially unwanted application
C:\Users\Vincent\Desktop\hacks\High Minded\High Minded.exe a variant of Win32/Packed.VMProtect.ABD trojan
C:\Users\Vincent\Desktop\hacks\League of Legends\Bot\Scripts\Common\Evadeeee.dll a variant of Win32/Packed.VMProtect.ABD trojan
C:\Users\Vincent\Desktop\hacks\Payday 2\PDAY2+17Tr-LNG_v39.0.exe a variant of Win32/Packed.VMProtect.ABD trojan
C:\Users\Vincent\Lokale Einstellungen\Google\Chrome\User Data\Default\File System\002\t\00\000000 a variant of Win32/DomaIQ.BB potentially unwanted application
C:\Users\Vincent\Lokale Einstellungen\Google\Chrome\User Data\Default\File System\003\t\00\000000 a variant of Win32/DomaIQ.BG potentially unwanted application
C:\Documents and Settings\Vincent\AppData\Local\Anwendungsdaten\Google\Chrome\User Data\Default\File System\002\t\00\000000 a variant of Win32/DomaIQ.BB potentially unwanted application deleted - quarantined
C:\Documents and Settings\Vincent\AppData\Local\Anwendungsdaten\Google\Chrome\User Data\Default\File System\003\t\00\000000 a variant of Win32/DomaIQ.BG potentially unwanted application deleted - quarantined
C:\Documents and Settings\Vincent\Desktop\hacks\High Minded\High Minded.exe a variant of Win32/Packed.VMProtect.ABD trojan cleaned by deleting - quarantined
C:\Documents and Settings\Vincent\Desktop\hacks\League of Legends\Bot\Scripts\Common\Evadeeee.dll a variant of Win32/Packed.VMProtect.ABD trojan cleaned by deleting - quarantined
C:\Documents and Settings\Vincent\Desktop\hacks\Payday 2\PDAY2+17Tr-LNG_v39.0.exe a variant of Win32/Packed.VMProtect.ABD trojan cleaned by deleting - quarantined

MBAM:

Malwarebytes Anti-Malware
www.malwarebytes.org

Scan Date: 03.11.2014
Scan Time: 07:33:12
Logfile: MBAMlog.txt
Administrator: Yes

Version: 2.00.3.1025
Malware Database: v2014.11.03.03
Rootkit Database: v2014.11.01.02
License: Free
Malware Protection: Disabled
Malicious Website Protection: Disabled
Self-protection: Disabled

OS: Windows 7 Service Pack 1

CPU: x64
File System: NTFS
User: Vincent

Scan Type: Threat Scan
Result: Completed
Objects Scanned: 346992
Time Elapsed: 5 min, 58 sec

Memory: Enabled
Startup: Enabled
Filesystem: Enabled
Archives: Enabled
Rootkits: Enabled
Heuristics: Enabled
PUP: Enabled
PUM: Enabled

Processes: 0
(No malicious items detected)

Modules: 0
(No malicious items detected)

Registry Keys: 0
(No malicious items detected)

Registry Values: 0
(No malicious items detected)

Registry Data: 0
(No malicious items detected)

Folders: 0
(No malicious items detected)

Files: 1
Trojan.MSIL, C:\Users\Vincent\Desktop\hacks\ArtificialAiming\AA (26).exe, Quarantined,
[4754b086ee8e3303ac53396fa25e47b9],

Physical Sectors: 0
(No malicious items detected)

(end)

FRST:

Fix result of Farbar Recovery Tool (FRST written by Farbar) (x64) Version: 02-11-2014
Ran by Vincent at 2014-11-02 23:09:47 Run:1
Running from C:\Users\Vincent\Desktop\FRST
Loaded Profile: Vincent (Available profiles: Vincent)
Boot Mode: Normal

=====

Content of fixlist: ****

Start

Closeprocesses:

Emptytemp:

HKLM-x32\...\Run: [] => [X]

HKU\S-1-5-21-1011809894-3870464874-3822914839-1000\...\Run: [ASRockXTU] => [X]

HKU\S-1-5-21-1011809894-3870464874-3822914839-1000\...\Run: [zASRockInstantBoot] => [X]

FF Plugin-x32: @pandonetworks.com/PandoWebPlugin -> C:\Program Files (x86)\Pando

Networks\Media Booster\npPandoWebPlugin.dll No File

C:\Program Files (x86)\Pando Networks\

testsigning: ==> Check for possible unsigned rootkit driver <===== ATTENTION!

End ****

Processes closed successfully.

HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Run\ => value deleted successfully.

HKU\S-1-5-21-1011809894-3870464874-3822914839-1000\Software\Microsoft\Windows\CurrentVersion\Run\ASRockXTU => value deleted successfully.

HKU\S-1-5-21-1011809894-3870464874-3822914839-1000\Software\Microsoft\Windows\CurrentVersion\Run\zASRockInstantBoot => value deleted successfully.

"HKLM\Software\Wow6432Node\MozillaPlugins\@pandonetworks.com/PandoWebPlugin" => Key deleted successfully.

"C:\Program Files (x86)\Pando Networks" => File/Directory not found.

Der Vorgang wurde erfolgreich beendet.

EmptyTemp: => Removed 761.7 MB temporary data.

The system needed a reboot.

==== End of Fixlog ====

ven0m - November 3, 2014, 12:22 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.

Xero666 - November 3, 2014, 12:32 am

DelFix:

DelFix v10.8 - Datei am 03/11/2014 um 09:31:09 erstellt

Aktualisiert am 29/07/2014 von Xplode

Benutzer : Vincent - VINCENT-PC

Betriebssystem : Windows 7 Home Premium Service Pack 1 (64 bits)

~ Aktiviere die Benutzerkontensteuerung ... OK

~ Entferne die Bereinigungsprogramme ...

Gelöscht : C:\FRST

Gelöscht : C:\TDSSKiller.3.0.0.34_02.11.2014_23.37.30_log.txt

Gelöscht : C:\TDSSKiller.3.0.0.41_02.11.2014_23.38.01_log.txt

Gelöscht : C:\Users\Vincent\Desktop\Fixlog.txt

Gelöscht : C:\Users\Vincent\Desktop\RKreport_DEL_10232014_005218.log

Gelöscht : C:\Users\Vincent\Desktop\RogueKillerX64.exe

~ Erstelle ein Backup der Registrierungsdatenbank ... OK

~ Lösche die Wiederherstellungspunkte ...

Gelöscht : RP #135 [avast! antivirus system restore point | 11/03/2014 07:25:51]

Ein neuer Wiederherstellungspunkt wurde erstellt !

~ Stelle die Systemeinstellungen wieder her ... OK

- EOF -

ven0m - November 3, 2014, 12:33 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: