

## Forum: [Hack Forums](#)

Thread: [Infected by a friend](#)

**Gokus\_Dog** - November 15, 2014, 7:23 am

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 Security Center service is not running! This report may not be accurate!

Windows Firewall Enabled!

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Java version out of Date!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 15.0.0.223

Adobe Reader XI

Mozilla Firefox 31.0 Firefox out of Date!

Google Chrome 38.0.2125.104

Google Chrome 38.0.2125.111

~~~~~Process Check: objlist.exe by Laurent~~~~~

Malwarebytes Anti-Malware mbamservice.exe

Malwarebytes Anti-Malware mbam.exe

Malwarebytes Anti-Malware mbamscheduler.exe

~~~~~System Health check~~~~~

Total Fragmentation on Drive C:

~~~~~End of Log~~~~~

<http://privatepaste.com/74cb5d9ac5> - FRST

<http://privatepaste.com/583915a092> - Additions

<http://privatepaste.com/f5906d2140> -MBAM Scan from when I was infected

The background of what happened is that a friend send me a link which auto downloaded a file, I didn't run it but it did save in my downloads folder.

**ven0m** - November 15, 2014, 9:51 pm

Delineate your current issue regarding your system.

**Gokus\_Dog** - November 16, 2014, 6:03 am

(Nov 15, 2014 10:51 PM)ven0m Wrote: [\[CITE\]](#) Delineate your current issue regarding your system.

So my friend send me a link of which to look at. After I clicked it the file automatically downloaded, suspecting it was a virus I didn't open it but MBAM picked it up as a trojan so I decided to come here.

**ven0m** - November 16, 2014, 7:33 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

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. Step : 2

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.

ESET Fiz Log

FRST Logs --FRST.txt

Addition.txt Regards,

ven0m

Gokus\_Dog - November 17, 2014, 5:11 pm

ESETSmartInstaller@High as downloader log:

all ok

ESETSmartInstaller@High as downloader log:

all ok

esets\_scanner\_update returned -1 esets\_gle=12

# product=EOS

# version=8

```
# OnlineScannerApp.exe=1.0.0.1
# OnlineScanner.ocx=1.0.0.7623
# api_version=3.0.2
# EOSSerial=2264d752b085ea4abde5f56db84c82e1
# engine=21134
# end=finished
# remove_checked=false
# archives_checked=true
# unwanted_checked=true
# unsafe_checked=true
# antistealth_checked=true
# utc_time=2014-11-18 12:22:36
# local_time=2014-11-17 07:22:36 (-0500, Eastern Standard Time)
# country="United States"
# lang=1033
# osver=6.1.7601 NT Service Pack 1
# scanned=568597
# found=0
# cleaned=0
# scan_time=9445
```

<http://privatepaste.com/4a3118de8a> - FRST

<http://privatepaste.com/983705a63e> - Additions

**ven0m** - November 17, 2014, 7:59 pm

Step : 3

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

Emptytemp:

Closeprocesses:

```
HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer: Policy restriction <===== ATTENTION
CHR StartupUrls: Default -> "", "hxxp://www.msn.com/?pc=UP97&ocid=UP97DHP",
"hxxp://rocket-find.com/?f=7&a=rckt_md_14_28_ch&cd=2XzuyEtN2Y1L1QzuyC0C0FtDyEzytDyEzy
0F0DtByCzytD0CtN0D0Tzu0SzytBtDtN1L2XzutBtFtBtCtFtCyEtFtDtN1L1CzutCyEtBzytDyD1V1TtN1
L1G1B1V1N2Y1L1Qzu2SyB0FzytA0E0E0D0DtGyCtDtDyEtGtB0DtBtAtG0B0EtCyDtGyDzztD0B0At
CzztA0C0FyE0C2QtN1M1F1B2Z1V1N2Y1L1Qzu2SyCtC0A0AtA0B0FtBtGyDyD0BtCtG0EzztByCt
GtDtAyB0DtGtAyCtAtA0EtC0CzyyDtAyByC2Q&cr=877554481&ir="
```

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

**Gokus\_Dog** - November 18, 2014, 6:51 pm

Fix result of Farbar Recovery Tool (FRST written by Farbar) (x64) Version: 17-11-2014

Ran by Administrator at 2014-11-18 20:45:10 Run:2

Running from C:\Users\Administrator\Desktop\FRST-OlderVersion  
Loaded Profile: Administrator (Available profiles: Administrator)  
Boot Mode: Normal  
=====

Content of fixlist: \*\*\*\*

Start

Emptytemp:

Closeprocesses:

HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer: Policy restriction <===== ATTENTION

CHR StartupUrls: Default -> "", "hxxp://www.msn.com/?pc=UP97&ocid=UP97DHP",

"hxxp://rocket-find.com/?f=7&a=rckt\_md\_14\_28\_ch&cd=2XzuyEtN2Y1L1QzuyC0C0FtDyEzytDyEzy  
0F0DtByCzytD0CtN0D0Tzu0SzytBtDtN1L2Xzut?BtFtBtCtFtCyEtFtDtN1L1CzutCyEtBzytDyD1V1TtN  
1L1G1B1V1N2Y1L1Qzu2SyB0FzytA0E0E0D0Dt?GyCtDtDyEtGtB0DtBtAtG0B0EtCyDtGyDzztD0B0  
AtCzztA0C0FyE0C2QtN1M1F1B2Z1V1N2Y1L1Qzu2?SyCtC0A0AtA0B0FtBtGyDyD0BtCtG0EzztBy  
CtGtDtAyB0DtGtAyCtAtA0EtC0CzyyDtAyByC2Q&cr=877554481&ir="

End \*\*\*\*

Processes closed successfully.

"HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer" => Key deleted successfully.

Chrome StartupUrls deleted successfully.

EmptyTemp: => Removed 665.4 MB temporary data.

The system needed a reboot.

==== End of Fixlog ====

**ven0m** - November 18, 2014, 8:52 pm

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.

**Gokus\_Dog** - November 19, 2014, 3:42 pm

# DelFix v10.8 - Logfile created 19/11/2014 at 18:42:15

# Updated 29/07/2014 by Xplode

# Username : Administrator - IK-PC

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

~ Activating UAC ... OK

~ Removing disinfection tools ...

Deleted : C:\\_OTL

Deleted : C:\FRST

Deleted : C:\AdwCleaner

Deleted : C:\Users\Administrator\Downloads\FRST-OlderVersion

Deleted : C:\Users\Administrator\Desktop\FRST-OlderVersion

Deleted : C:\TDSSKiller.2.8.16.0\_06.10.2013\_14.26.11\_log.txt

Deleted : C:\TDSSKiller.2.8.16.0\_06.10.2013\_14.26.58\_log.txt

Deleted : C:\Users\Administrator\Desktop\FRST64.exe

Deleted : C:\Users\Administrator\Desktop\scan.txt  
Deleted : C:\Users\Administrator\Downloads\Addition.txt  
Deleted : C:\Users\Administrator\Downloads\AdwCleaner.exe  
Deleted : C:\Users\Administrator\Downloads\esetsmartinstaller\_enu (1).exe  
Deleted : C:\Users\Administrator\Downloads\esetsmartinstaller\_enu (2).exe  
Deleted : C:\Users\Administrator\Downloads\esetsmartinstaller\_enu.exe  
Deleted : C:\Users\Administrator\Downloads\FRST.txt  
Deleted : C:\Users\Administrator\Downloads\FRST64.exe  
Deleted : C:\Users\Administrator\Downloads\JRT (1).exe  
Deleted : C:\Users\Administrator\Downloads\JRT.exe  
Deleted : C:\Users\Administrator\Downloads\SecurityCheck (1).exe  
Deleted : C:\Users\Administrator\Downloads\SecurityCheck.exe  
Deleted : C:\Users\Administrator\Downloads\Shortcut.txt  
Deleted : HKLM\SOFTWARE\OldTimer Tools  
Deleted : HKLM\SOFTWARE\AdwCleaner  
Deleted : HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY\_ASWMBR

~ Creating registry backup ... OK

~ Cleaning system restore ...

Deleted : RP #1979 [Windows Update | 11/17/2014 03:00:10]  
Deleted : RP #1981 [Windows Update | 11/17/2014 20:25:57]  
Deleted : RP #1982 [Windows Update | 11/18/2014 01:28:15]  
Deleted : RP #1983 [Windows Update | 11/19/2014 01:53:32]  
Deleted : RP #1984 [Windows Update | 11/19/2014 22:11:28]

New restore point created !

~ Resetting system settings ... OK

##### - EOF - #####

**ven0m** - November 19, 2014, 7:53 pm

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: