

Forum:[Hack Forums](#)

Thread: [Pretty sure I still have a virus](#)

+mK - November 29, 2015, 4:49 pm

Symantec keeps pushing tmp files as Trojan, while ESET finds nothing. Can someone help me out?

Below is my FSRT scans. I apologize for posting it in this format, I'm transferring the logs from my laptop to my phone.

Addition.txt - <http://www.pastebin.com/raw.php?i=NZa4BjFX>

FSRT.txt - <http://www.pastebin.com/raw.php?i=CZx2yvB7>

Knautschtabak - November 30, 2015, 12:43 am

Please read through the points below to ensure this process moves as quickly and efficiently as possible. Ensure you read through my instructions thoroughly, and carry out each step in the order specified.

Please do not run any tools or take any steps other than those I provide for you. Independent efforts may make matters worse, and will affect my ability in providing the best set of instructions for you.

Please backup important files before proceeding with my instructions. Malware removal can be unpredictable at times.

If you come across any issues whilst following my instructions, please stop and inform me of the issue in as much detail as possible. Please do not hesitate to ask before proceeding.

I will notify you when I believe your computer is free of malware. Please bear in mind, absence of symptoms does not necessarily correlate to absence of malware, so please wait until the "All Clean".

It is inadvisable to have more than one Anti-Virus installed on your computer at the same time. Doing so may cause conflicts, negatively impacting the effectiveness of each Anti-Virus installed.

Trigger [false-positives](#).

Trigger false-negatives, where neither programme detects malware.

Cause system instability/performance issues. Your system may lock up or slow down due to both software attempting to access the same file at the same time.

Please remove all but one Anti-Virus from your computer. Press the Windows Key + r on your keyboard at the same time.

Type appwiz.cpl and click OK.

Search for and uninstall all but one of the programmes listed below by right-clicking and clicking Uninstall. Symantec Endpoint Protection

ESET NOD32 Antivirus

Follow the prompts, and reboot your computer once uninstalled.

aswMBR Please download [aswMBR](#) and save the file to your Desktop.

Temporarily disable your anti-virus software. For instructions, please refer to the following [link](#).

Right-Click aswMBR.exe and select Run as administrator to run the program.

Click Yes when prompted to download avast! virus definitions. Wait until AVAST engine defs: ### appears.

If you are prompted to enable the use of "Virtualization Technology", click Yes.

Click the AV Scan: drop down box and click C:\.

Click Scan.

Upon completion, you will see Scan finished successfully. Click Save log. Save the log to your Desktop.

Re-enable your anti-virus software.

Copy the contents of the log to pastebin.com and paste the link in your next reply.

Note: Do NOT click Fix or FixMBR.

Note: A file (MBR.dat) will be created on your Desktop. Do NOT click or delete it.

In your next reply I get from you Did you successfully uninstall one of the AVs?

aswMBR log

+mK - November 30, 2015, 12:57 pm

Yes, I removed ESET.

Log: <http://pastebin.com/raw.php?i=04yGi8Qs>

Knautschtabak - December 1, 2015, 1:09 am

Step 1: Farbar Recovery Scan Tool (FRST) Script
Press the Windows Key + r on your keyboard at the same time. Type Notepad and click OK.

Copy the entire contents of the codebox below and paste into the Notepad document.

Code start

CreateRestorePoint:

CloseProcesses:

C:\Users\admin\AppData\Local\Temp\NETGEARGenieDaemon64.exe

C:\Users\PapaCraw\AppData\Local\Temp\chromeupdate.exe

C:\Users\PapaCraw\AppData\Local\Temp\DseShExt-x64.dll

C:\Users\PapaCraw\AppData\Local\Temp\DseShExt-x86.dll

C:\Users\PapaCraw\AppData\Local\Temp\dxdiag.exe

C:\Users\PapaCraw\AppData\Local\Temp\SDShelEx-win32.dll

C:\Users\PapaCraw\AppData\Local\Temp\SDShelEx-x64.dll

C:\Users\PapaCraw\AppData\Local\Temp\update.exe

C:\Users\PapaCraw\AppData\Local\Temp\xmlUpdater.exe

HKU\S-1-5-21-1322733642-1108219750-3070097398-1001\...\MountPoints2:

{0040eece-9461-11e4-82aa-f816543040bb} - "G:\VZW_Software_upgrade_assistant.exe"

HKU\S-1-5-21-1322733642-1108219750-3070097398-1001\...\MountPoints2:

{0040ef3a-9461-11e4-82aa-f816543040bb} - "G:\VZW_Software_upgrade_assistant.exe"

HKU\S-1-5-21-1322733642-1108219750-3070097398-1001\...\MountPoints2:

{56a9353a-de65-11e4-82df-f816543040bb} - "F:\LaunchU3.exe" -a

HKU\S-1-5-21-1322733642-1108219750-3070097398-1001\...\MountPoints2:

{59051c02-98f5-11e4-82ba-f816543040bb} - "G:\VZW_Software_upgrade_assistant.exe"

HKU\S-1-5-21-1322733642-1108219750-3070097398-1001\...\MountPoints2:

{d40539a0-db31-11e4-82db-f816543040bb} - "F:\WD Drive Unlock.exe" autoplay=true

SearchScopes: HKLM -> DefaultScope {0633EE93-D776-472f-A0FF-E1416B8B2E3A} URL =

SearchScopes: HKLM -> {0633EE93-D776-472f-A0FF-E1416B8B2E3A} URL =

SearchScopes: HKLM -> {DC91FAFB-6CEA-49E5-BB74-9CEE75D09B77} URL =

StartMenuInternet: IEXPLORE.EXE - iexplore.exe

URLSearchHook: [S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415]

ATTENTION => Default URLSearchHook is missing

Task: {29C80829-029F-4A92-845A-97D0175C508A} -

System32\Tasks\{55522518-D77C-4F0D-985F-868567C85590} => pcalua.exe -a

C:\Users\PapaCraw\Downloads\lfdshow-20041012.exe -d C:\Users\PapaCraw\Downloads

CHR StartupUrls: Default ->

"hxxp://Vosteran.com/?f=7&a=vst_dnlDstr_14_46_ch&cd=2XzuyEtN2Y1L1Qzu0FzztCyCyDyEtAtDyEtD0B0B0EtA0C0CtN0D0Tzu0StCtDyDtCtN1L2XzutAtFyCtFtBtFtDtN1L1CzutCyEtBzytDyD1V1TtN1L1G1B1V1N2Y1L1Qzu2SyBtDtAzy0F0BtB0EtG0DzzyEtAtG0FtCyDyEtGzzyEyCyCtGtDyD0CtBzztAyEyDyD0DyDtD2QtN1M1F1B2Z1V1N2Y1L1Qzu2SyCyD0B0D0CyByBtCtGyC0CzyyDtGyE0D0EzytG0AtDtCtCtGyCyC0AyEyE0BtDzztB0CtA0A2Q&cr=170225254&ir=", "hxxp://Vosteran.com/?f=7&a=vst_ggfc_15_01_ch&cd=2XzuyEtN2Y1L1Qzu0FzztCyCyDyEtAtDyEtD0B0B0EtA0C0CtN0D0Tzu0StCtDzyzytN1L2XzutAtFyCtFtCyCtFyCtN1L1CzutCyEtBzytDyD1V1StN1L1G1B1V1N2Y1L1Qzu2SyEyCtBtAtDyE0C0FtGtByByDyEtG0FzzyB0FtG0E0B0DyCtGyC0EtByD0E0CtC0DtD0A0D0A2QtN1M1F1B2Z1V1N2Y1L1Qzu2SyCyD0B0D0CyByBtCtGyC0CzyyDtGyE0D0EzytG0AtDtCtCtGyCyC0AyEyE0BtDzztB0CtA0A2Q&cr=1364942963&ir="

EmptyTemp:

end

Click File, Save As and type fixlist.txt as the File Name.

Important: The file must be saved in the same location as FRST.exe.

NOTICE: This script is intended for use on this particular machine. Do not use this script on any other machine; doing so may cause damage to your Operating System. Double-Click FRST.exe to run the program.

Click Fix.

A log (Fixlog.txt) will open on your desktop. Copy the contents of the log to pastebin.com and paste the link to it in your next reply.

Step 2: Junkware Removal Tool (JRT) Please download [Junkware Removal Tool](#) and save the file to your Desktop.

Temporarily disable your anti-virus software. For instructions, please refer to the following [link](#).

Right-Click JRT.exe and select Run as administrator to run the program.

Follow the prompts and allow the scan to run uninterrupted.

Upon completion, a log (JRT.txt) will open on your desktop.

Re-enable your anti-virus software

Copy the contents of JRT.txt to pastebin.com and paste the link in your next reply.

Step 3: AdwCleaner Please download [AdwCleaner](#) and save the file to your Desktop.

Right-Click AdwCleaner.exe and select Run as administrator to run the program.

Follow the prompts.

Click Scan.

Upon completion, click Logfile. A log (AdwCleaner[R0].txt) will open. Briefly check the log for anything you know to be legitimate.

Ensure anything you know to be legitimate does not have a checkmark, and click Clean.

Follow the prompts and allow your computer to reboot.

After rebooting, a log (AdwCleaner[S0].txt) will open. Copy the contents of the log to pastebin.com and paste the links in your next reply.

-- File and folder backups are made for items removed using this tool. Should a legitimate file or folder be removed (otherwise known as a 'false-positive'), simple steps can be taken to restore the item. Please do not overly concern yourself with the contents of AdwCleaner[R0].txt.

+mK - December 1, 2015, 11:58 am

Fixlog.txt - <http://pastebin.com/raw.php?i=0U8nfZQh>

JRT.txt - <http://pastebin.com/raw.php?i=7ENahB7F>
AdwCleaner.txt - <http://pastebin.com/raw.php?i=g04UEZKu>

Knautschtabak - December 3, 2015, 12:00 am

ESET Online Scan

Note: This scan may take a long time to complete. Please do not browse the Internet whilst your Anti-Virus is disabled. Please download [ESET Online Scan](#) and save the file to your Desktop.

Temporarily disable your anti-virus software. For instructions, please refer to the following [link](#).

Double-click esetsmartinstaller_enu.exe to run the programme.

Agree to the EULA by placing a checkmark next to Yes, I accept the Terms of Use. Then click Start.

Agree to the Terms of Use once more and click Start. Allow components to download.

Place a checkmark next to Enable detection of potentially unwanted applications.

Click Advanced settings. Place a checkmark next to: Scan archives

Scan for potentially unsafe applications

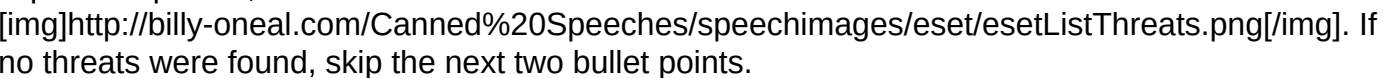
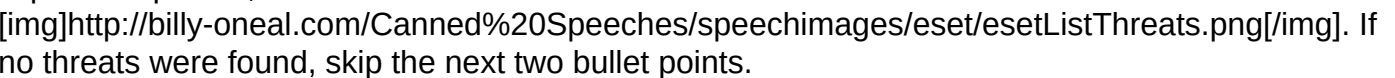
Enable Anti-Stealth technology

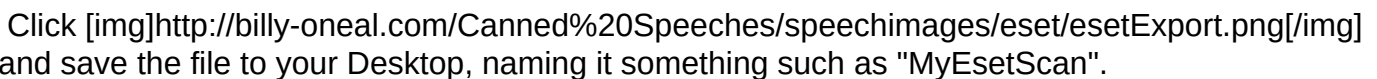
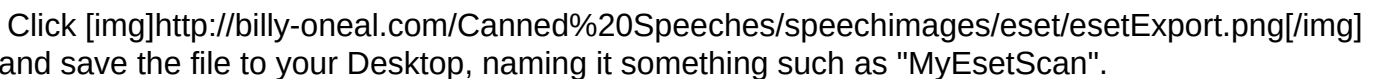
Ensure Remove found threats is unchecked.

Click Start.

Wait for the scan to finish. Please be patient as this can take some time.

Upon completion, click

http://billy-oneal.com/Canned%20Speeches/speechimages/eset/esetListThreats.png. If no threats were found, skip the next two bullet points.

Click http://billy-oneal.com/Canned%20Speeches/speechimages/eset/esetExport.png and save the file to your Desktop, naming it something such as "MyEsetScan".

Push the Back button.

Place a checkmark next to and click .

Re-enable your anti-virus software.

Copy the contents of the log and paste in your next reply.

Farbar Recovery Scan Tool (FRST) ScanDouble-Click FRST64.exe to run the programme

Click Yes to the disclaimer.

Ensure the Addition.txt box is checked.

Click the Scan button and let the program run.

Upon completion, click OK, then OK on the Addition.txt pop up screen.

Two logs (FRST.txt & Addition.txt) will now be open on your Desktop. Copy the contents of both logs and paste them to pastebin.com. Post the link here.