Forum:Hack Forums

Thread: Avira uninstall issue.

roto25 - *March 7, 2018, 6:56 am*

I had Avira antivirus for few years now and i decided that it would be time to try avast free antivirus and see if its better or worse.
My issue here is that i can not delete Avira fully.
There is one file left named "AntiVir Desktop". I tried googling for answers i found people saying that you should try to use the "avira registry tool" while running the system in safe mode. It did not work, i tried deleting the antivirus using Install/uninstall section that windows 10 have where you can see the programs that you have on your system i saw it there i tried uninstalling it said it has done so successfully. When i went to check if it was really gone i saw that i still had the folder "Avira" on my pc inside the folder was 2 more files the first file was deleted without any issues, however when i tried to uninstall the second file named "AntiVir Desktop" it would say that File is open in another program. Even though i checked all programs that were running on my system and i could not find anything that i could connect with Avira.

I hope someone will find a way to delete this program fully.

Thanks in advance!!

Sigma - *March 7, 2018, 10:06 am*

I'm Sigma, I'm one of the leaders of the Security Malware Removal Team and will be assisting you throughout this thread. Before we start just take a second to read through these few requests - these are to ensure we can help you quickly and safely:Only use this thread for help. Please don't create multiple threads, accounts, PM me or post on other forums - if you do just let me know.

Only follow my guidance.

Don't run tools I haven't asked you to run. If you do just let me know so I can take that into consideration when viewing logs.

DO NOT install any other software while we are attempting to clean your machine. It can get quite confusing especially if you are downloading questionable tools.

Please be prompt in responding. I'll do my best to do so. If >48hrs has passed, please either PM me or ask "Are you there, I still need help" in this thread.

Please stick with me until I give you the 'All Clean'. I'll help you cleanup quickly and offer some tips to make you more secure and get your system running faster.

Your malware related tools will be removed. I don't support the tools often distributed on these forums. Scanners will generally remove these - I take no responsibility for any malicious software that is lost.

I (nor does the forum) support pirated software.

If you don't understand something, don't be afraid to ask - I'm here to help. ?

You'll notice the logs are pretty big and you won't be able to post a reply containing it all. Please use ONLY either:https://hastebin.com - here you can upload the .txt file directly. <- I prefer this.

http://pasted.co/ - here you can set a password if you wish to protect your data. Just PM me the password.

And paste the link to the logs in your reply. Post each log separately (each with a separate link). If you're a new member and can't paste links you can fool the forums system by removing the beginning of the link.

e.g.If you can't post this: https://hastebin.com/raw/epaduvuyic

Post: I used hastebin, here is the ending /raw/epaduvuyic

If I request you to post an image please use a service like https://imgur.com

Download the right version of FRST for your system:FRST 32-bit

FRST 64-bit
Note: Only the right version will run on your system, the other will throw an error message. So if you don't know what your system's version is, simply download both of them, and the one that works is the one you should be using.

Move the executable (FRST.exe or FRST64.exe) on your Desktop

Right-click on the executable and select Run as Administrator (for Windows Vista, 7, 8, 8.1 and 10 users)

Accept the disclaimer by clicking on Yes, and FRST will then do a back-up of your Registry which should take a few seconds

Make sure the Addition.txt box is checked

Click on the Scan button

On completion, two message box will open, saying that the results were saved to FRST.txt and Addition.txt, then open two Notepad files

Copy and paste the content of both FRST.txt and Addition.txt in your next reply

Please read the guide AsSaSs@iN constructed here before continuing:
https://hackforums.net/showthread.php?tid=5772641

Post the logs in THIS THREAD

Let's get to it!

roto25 - *March 7, 2018, 2:10 pm*
Addition: https://hastebin.com/ujalojavud.tex
FRST: https://hastebin.com/gijeruyeri.tex

Aura - *March 7, 2018, 6:27 pm*
This is the article you followed, right?

https://www.avira.com/en/support-for-home-knowledgebase-detail/kbid/902

roto25 - *March 8, 2018, 10:20 am*
(Mar 7, 2018 07:27 PM)Aur? Wrote: *[CITE]* This is the article you followed, right?

https://www.avira.com/en/support-for-home-knowledgebase-detail/kbid/902
Yea that's the one i followed.

Sigma - *March 8, 2018, 11:15 am*
Farbar Recovery Scan Tool (FRST) - Fix

Follow the instructions below to execute a fix on your system using FRST, and provide the log in your next reply.Open Notepad and copy/paste the following into notepad:

Code CreateRestorePoint:
CloseProcesses:
HKLM-x32\...\Run: [] => [X]
FF Plugin-x32: @esn/npbattlelog,version=2.7.1 -> C:\Program Files (x86)\Battlelog Web Plugins\2.7.1\npbattlelog.dll [No File]
FF HKLM\...\Thunderbird\Extensions: [eplgTb@eset.com] - C:\Program Files\ESET\ESET NOD32 Antivirus\Mozilla Thunderbird => not found
FF HKLM-x32\...\Thunderbird\Extensions: [msktbird@mcafee.com] - C:\Program Files\McAfee\MSK => not found
FF HKLM-x32\...\Thunderbird\Extensions: [eplgTb@eset.com] - C:\Program Files\ESET\ESET NOD32 Antivirus\Mozilla Thunderbird => not found
FF Plugin: @esn/npbattlelog,version=2.7.1 -> C:\Program Files (x86)\Battlelog Web Plugins\2.7.1\npbattlelogx64.dll [No File]
U3 aswbdisk; no ImagePath
2018-03-07 05:34 - 2018-03-07 05:34 - 000003208 _____ C:\WINDOWS\System32\Tasks\Avira SystrayStartTrigger
2018-03-06 21:33 - 2018-03-06 21:33 - 000008212 _____ C:\WINDOWS\system32\.crusader
2018-02-09 20:22 - 2018-02-16 15:48 - 008083703 _____ C:\WINDOWS\system32\nvcoproc.bin
2018-02-09 20:21 - 2018-02-23 21:01 - 000001951 _____ C:\WINDOWS\NvContainerRecovery.bat
2018-03-07 05:33 - 2014-10-03 17:57 - 000000000 ____D C:\ProgramData\Avira
2018-03-07 05:34 - 2014-10-03 17:57 - 000000000 ____D C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Avira
2018-02-09 22:20 - 2012-12-26 02:00 - 000000000 ____D C:\Users\roto25\AppData\Local\ElevatedDiagnostics
ShellIconOverlayIdentifiers: [GDriveSharedOverlay] -> {81539FE6-33C7-4CE7-90C7-1C7B8F2F2D44} => -> No File

Task: {156647E6-3B54-41E8-AE27-3BFD82BC7019} - \Microsoft\Windows\Setup\GWXTriggers\ScheduleUpgradeReminderTime -> No File <==== ATTENTION
Task: {199E3C49-A86E-4C2D-A264-71FF1207D35B} - \Microsoft\Windows\Setup\GWXTriggers\refreshgwxconfig-B -> No File <==== ATTENTION
Task: {1BB2E287-0A5B-4A9A-A6F5-E682C82942D7} - \Microsoft\Windows\Setup\GWXTriggers\Time-5d -> No File <==== ATTENTION
Task: {24FE8471-B41E-40FB-A4C1-7165C2610444} - \Microsoft\Windows\Setup\GWXTriggers\MachineUnlock-5d -> No File <==== ATTENTION
Task: {2581376E-8A07-4AFE-B578-0713FB01B490} - \Microsoft\Windows\Setup\gwx\refreshgwxconfigandcontent -> No File <==== ATTENTION
Task: {431B41D6-A518-44BF-9778-F58BCC9EE118} - \Microsoft\Windows\Setup\GWXTriggers\OutOfSleep-5d -> No File <==== ATTENTION
Task: {4A9F7712-2151-4745-84CA-E878086E8DDE} - \Microsoft\Windows\Setup\GWXTriggers\Logon-5d -> No File <==== ATTENTION
Task: {5A0F9BAD-6A27-4B5E-A933-B930FB25B602} - \Microsoft\Windows\Setup\GWXTriggers\ScheduleUpgradeTime -> No File <==== ATTENTION
Task: {688D93AE-92BE-4516-B754-89E636031116} - \Microsoft\Windows\UNP\RunCampaignManager -> No File <==== ATTENTION
Task: {701BADEF-67BD-4BD9-B8AC-8F919FA59978} - \Microsoft\Windows\Setup\gwx\refreshgwxcontent -> No File <==== ATTENTION
Task: {7B9E3946-7E55-48FB-97F5-238808D882A8} - \WPD\SqmUpload_S-1-5-21-2861178066-1603776425-4246682640-1001 -> No File <==== ATTENTION
Task: {9DD17375-B141-415C-B270-48692AED3720} - \Microsoft\Windows\Setup\gwx\launchtrayprocess -> No File <==== ATTENTION
Task: {B8F4B566-1C36-48B5-9640-3CE26F1162EA} - \Microsoft\Windows\Setup\gwx\refreshgwxconfig -> No File <==== ATTENTION
Task: {F22E2C05-1EF3-47ED-99AF-94674874F638} - \Microsoft\Windows\Setup\GWXTriggers\OutOfIdle-5d -> No File <==== ATTENTION
EmptyTemp:

Save the file as fixlist.txt, and save it on your Desktop (or wherever your FRST.exe/FRST64.exe executable is located)

Right-click on the FRST executable and select Run as Administrator (for Windows Vista, 7, 8, 8.1 and 10 users)

Click on the Fix button

On completion, a message will come up saying that the fix has been completed and it'll open a log in Notepad

Copy and paste its content into your next reply

roto25 - *March 8, 2018, 11:48 am*

Fixlog: https://hastebin.com/uzenuwutus.tex

Edit: After i ran the fix my pc crashed shortly after. On restart it said i had to use boot system, So i did a force restart since all it gave me was black screen with white text and nothing else.
Edit2: Now i am getting adds from Avira once again.

Sigma - *March 8, 2018, 11:59 am*
Malwarebytes - Clean ModeDownload and install the free version of Malwarebytes
Note: If you have Malwarebytes already installed, you don't need to install it again. Simply start from the next bullet point

Once Malwarebytes is installed, launch it and let it update his database. You might have to click on the little arrow by Scan Status in the middle right pane for it to do so

Once the database update is complete, click on the Scan tab, then select the Threat Scan button and click on Start Scan

Let the scan run, the time required to complete the scan depends of your system and computer specs

Once the scan is complete, make sure that the first checkbox at the top is checked (which will automatically check every detected item), then click on the Quarantine Selected buttonIf it asks you to restart your computer to complete the removal, do so

Click on Export Summary after the deletion (in the bottom-left corner) and select Copy to Clipboard. Paste the content in your next reply

roto25 - *March 8, 2018, 12:19 pm*
Scan resultats: https://hastebin.com/pequsodusi.sql

Sigma - *March 8, 2018, 12:28 pm*
Is Avira still showing up?

roto25 - *March 8, 2018, 12:30 pm*
Yes it is still showing up. http://prntscr.com/ion2jl

Sigma - *March 8, 2018, 12:38 pm*
Have you tried this: https://www.avira.com/en/support-download-avira-antivir-removal-tool/

roto25 - *March 8, 2018, 12:42 pm*
I can only download the handbook wich is in PDF, where they talk about how to use the program but i couldn't find the program itself.

Sigma - *March 8, 2018, 12:43 pm*
https://www.techsupportall.com/avira-uninstall-tool/

Also this: https://www.avira.com/en/download/product/avira-registry-cleaner

roto25 - *March 8, 2018, 12:47 pm*
All of the links on the site you provided links me back to Official Avira Website.
They are talking about REVO uninstaller, perhaps i should use that one?

Sigma - *March 8, 2018, 12:52 pm*
Yeah go ahead and try that. See if it shows up in the uninstall list.

roto25 - *March 8, 2018, 12:59 pm*
It did not show the avira on the original list of all the other programs but they did have something called "Forced Uninstall" Where i can locate the file i want to delete manually.
http://prntscr.com/ionghg

Do i have the green light to proceed?

Sigma - *March 8, 2018, 1:12 pm*
Yes go ahead and do that.

roto25 - *March 8, 2018, 1:29 pm*
Good news the file is fully deleted now,it deleted everything that avira left behind at least it did say so it did.

Sigma - *March 8, 2018, 2:53 pm*
Good News...

Firstly, lets remove the tools we put on your system earlier.
DelFix by XPlodeDownload Delfix and save it to your Desktop

Double click the icon

Place checkmarks in:Remove disinfection tools

Purge system restore

Click Run

The logs indicate you're in the all clear and the malware has been removed. Please consider acting upon my following recommendations
in order to help keep malware infections away from your system.
Keep your operating system up-to-date along with any updates Windows may suggest.

Keep your programs that help fight off malware up-to-date. Ensure you have a AntiVirus program up-to-date too.

Perform regular updates and scans with Malwarebytes Anti-Malware (MBAM).

You should only have 1 antivirus, firewall and antimalware protection software enabled at all times. It's crucial you have all three

types of software enabled at all times. Having multiple programs of the same type of software running at the same time will make the
software fight each other and conflict with one another. This may lead to a greater risk of malware residing on your system.

For more in-depth information regarding how and which Antivirus to pick, you may want to have a read over the following:
Antivirus Recommendations

If you are yet to choose a firewall, I recommend reading through this comprehensive guide on how firewalls work and popular firewalls:
Understanding and Using Firewalls

For any other recommendations and best practices, reading the following is an absolute must:
Answers to common security questions - Best Practices

If that's all, safe surfing.

roto25 - *March 9, 2018, 5:43 am*

Thank you so much for your help!
I do only have one question it is about the firewall. Right now i have the windows basic firewall But i heard that i should get zonealarm firewall. Do you think it will do the job?

Sigma - *March 9, 2018, 8:03 pm*

(Mar 9, 2018 06:43 AM)roto25 Wrote: *[CITE]* Thank you so much for your help!
I do only have one question it is about the firewall. Right now i have the windows basic firewall But i heard that i should get zonealarm firewall. Do you think it will do the job?
Regular Firewall works just fine, I recommend Windows Defender full protection for other malware though.