

Forum:[Hack Forums](#)

Thread: [I ran one doggy program](#)

- Z - - November 14, 2018, 3:32 pm

Hello HF,

Today I was checking out a program that a fellow HF member made, And It did not follow through what it was made for. Ran with Malwarebytes, Clean but I still feel paranoid, let me know what else I should try with next thank you in advance.

?

ZIKO000 - November 14, 2018, 3:39 pm

Use several different programs to scan it not only Malwarebytes get an AV and use rouge killer and check it out with virus-total.

One question would you allow me to use your profile pic on hack forums.

- Z - - November 14, 2018, 3:44 pm

Using McAfee right now, but here is the results from [VT](#) let me know what you think.

Said it was clean, any other suggestions.

- Z - - November 24, 2018, 10:18 am

Just today, I was smoking my juul and was close to my pc and I had Hf opened but minimize as normal then I had in cog open with my google account and shit. But then when I was smoking my screen changed to HF so I was like ok...then a window popped up and said 86% completed, relized it was transfeing my fucking files, I need some help ASAP.

VoIPv2 - November 24, 2018, 10:53 am

(Nov 24, 2018 11:18 AM)- Z - Wrote: [\[CITE\]](#) Just today, I was smoking my juul and was close to my pc and I had Hf opened but minimize as normal then I had in cog open with my google account and shit. But then when I was smoking my screen changed to HF so I was like ok...then a window popped up and said 86% completed, relized it was transfeing my fucking files, I need some help ASAP.

Upload the sample to virustotal.com if you see any list of malware names then provide that in the thread. Virustotal will scan with around 50+ Antivirus and also check the signature for new or old malware codecs. Then at worst, wait for Aura or someone from the original MRT team to provide the next steps.

- Z - - November 24, 2018, 12:54 pm

(Nov 24, 2018 11:53 AM)VoIPv2 Wrote: [\[CITE\]](#) Upload the sample to virustotal.com if you see any list of malware names then provide that in the thread. Virustotal will scan with around 50+ Antivirus and also check the signature for new or old malware codecs. Then at worst, wait for Aura or someone from the original MRT team to provide the next steps.

Been done that, said it was clean and everything, now I just think it's something else.

Super - November 24, 2018, 1:11 pm

Hey OP,

I'd be happy to help. First let's run some preliminary scans before I give you a manual checkup.

Step 1: Malware scan (Malwarebytes)

Download 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 button. If 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

Step 2: Rootkit scan (RogueKiller)

Download the right version of [RogueKiller](#) for your Windows version (32 or 64-bit)

Once done, move the executable file to your Desktop, right-click on it and select Run as Administrator (for Windows Vista, 7, 8, 8.1 and 10 users)

Click on the Start Scan button in the right panel, which will bring you to another tab, and click on it again (this time it'll be in the bottom right corner)

Wait for the scan to complete

On completion, the results will be displayed. Click on the Open Report button in the bottom left corner, followed by the Open TXT button (also in the bottom left corner)

This will open the report in Notepad. Copy/paste its content in your next reply

Be sure to quarantine the threats that RogueKiller and Malwarebytes detect. Upload your logs to <https://hastebin.com> and give me the links in your reply.

Let me know if you have any questions ?
Dynamo

- Z - - November 24, 2018, 3:38 pm

(Nov 24, 2018 02:11 PM)Dynamo Wrote: [\[CITE\]](#) Hey OP,
I'd be happy to help. First let's run some preliminary scans before I give you a manual checkup.

Step 1: Malware scan (Malwarebytes)

Download 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 button. If 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

Step 2: Rootkit scan (RogueKiller)

Download the right version of [RogueKiller](#)
for your Windows version (32 or 64-bit)

Once done, move the executable file to your Desktop, right-click on it and select Run as Administrator (for Windows Vista, 7, 8, 8.1 and 10 users)

Click on the Start Scan button in the right panel, which will bring you to another tab, and click on it again (this time it'll be in the bottom right corner)

Wait for the scan to complete

On completion, the results will be displayed. Click on the Open Report button in the bottom left corner, followed by the Open TXT button (also in the bottom left corner)

This will open the report in Notepad. Copy/paste its content in your next reply

Be sure to quarantine the threats that RogueKiller and Malwarebytes detect.
Upload your logs to <https://hastebin.com> and give me the links in your reply.

Let me know if you have any questions ?

Dynamo

<https://ghostbin.com/paste/adprj29s> (RogueKiller)

<https://justpaste.it/55rm1> (Malwarebytes)

Sorry, Hastebin is not working, and after I did one ghostbin it gave me some error so I had to use another uploader.

Super - November 24, 2018, 6:31 pm

(Nov 24, 2018 04:38 PM)- Z - Wrote: [\[CITE\]](#) <https://ghostbin.com/paste/adprj29s> (RogueKiller)

<https://justpaste.it/55rm1> (Malwarebytes)

Sorry, Hastebin is not working, and after I did one ghostbin it gave me some error so I had to use another uploader.

Everything looks okay according to the scans - I don't think you're infected. If you still think you're infected, I can preform a manual checkup for you.

?

Dynamo

- Z - - November 24, 2018, 6:46 pm

(Nov 24, 2018 07:31 PM)Dynamo Wrote: [\[CITE\]](#) Everything looks okay according to the scans - I don't think you're infected. If you still think you're infected, I can preform a manual checkup for you.

?

Dynamo

Kk, thank you and I will contact you later of if that's fine.

Aura - November 25, 2018, 7:54 am

Farbar Recovery Scan Tool (FRST) - Scan mode

Follow the instructions below to download and execute a scan on your system with FRST, and provide the logs in your next reply. 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

Super - November 25, 2018, 1:13 pm

Let Aura help you from here. He knows what he's doing.

- Z - - November 25, 2018, 1:42 pm

(Nov 25, 2018 08:54 AM)Aur? Wrote: [\[CITE\]](#) Farbar Recovery Scan Tool (FRST) - Scan mode
Follow the instructions below to download and execute a scan on your system with FRST, and provide the logs in your next reply. 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

<https://ghostbin.com/paste/4e9cdut4> (FRST.txt)

<https://ghostbin.com/paste/pmf9b758> (Addition.txt)

PerfectStorm - November 25, 2018, 1:46 pm

Its time to get a VM wouldn't you agree?

- Z - - November 25, 2018, 1:47 pm

(Nov 25, 2018 02:46 PM)PerfectStorm Wrote: [\[CITE\]](#) Its time to get a VM wouldn't you agree?
I agree 100% but I don't have the best computer. ?

PerfectStorm - November 25, 2018, 1:49 pm

(Nov 25, 2018 02:47 PM)- Z - Wrote: [\[CITE\]](#) I agree 100% but I don't have the best computer. ?
Well If you're talking about not caring because of that, Its not really the PC its the personal information you should worry about.

- Z - - November 25, 2018, 2:05 pm

(Nov 25, 2018 02:49 PM)PerfectStorm Wrote: [\[CITE\]](#) Well If you're talking about not caring because of that, Its not really the PC its the personal information you should worry about.

I really care about my PC and my personal information, but my laptop can't run a VM stable enough, and as well the program was made by a member on HF.

PerfectStorm - November 25, 2018, 2:08 pm

(Nov 25, 2018 03:05 PM)- Z - Wrote: [\[CITE\]](#) I really care about my PC and my personal information, but my laptop can't run a VM stable enough, and as well the program was made by a member on HF.

Oh you dont have the horse power ?

- Z - - November 25, 2018, 2:15 pm

(Nov 25, 2018 03:08 PM)PerfectStorm Wrote: [\[CITE\]](#) Oh you dont have the horse power ?
XD, yeah basically.

A Few Problems - August 5, 2019, 9:50 pm

try using vmware and windows xp

ComputerScience - August 5, 2019, 10:16 pm

Use sandboxie to check the files, best solution if you can" t run VM

AnonFawkes - August 14, 2019, 10:07 am

Scan your network traffic to determine if a RAT is accessing a remote C&C server.