

Forum:[Hack Forums](#)

Thread: [Infected Maybe? mrt.exe and mrtstub.exe](#)

The OG FurFag ? - December 11, 2015, 6:32 pm

I was going to the Steam folder when I noticed a random named folder. These files are inside.
Any form of malware or?

<http://prntscr.com/9d5pkr>

.Cherry - December 11, 2015, 6:34 pm

Scan them looks like a virus!

ty the cyber bully - December 11, 2015, 6:34 pm

upload it to malwr.com see if it connects to any hosts.

The OG FurFag ? - December 11, 2015, 6:36 pm

(Dec 11, 2015 07:34 PM)*Sinon Wrote: [CITE](#) upload it to malwr.com see if it connects to any hosts.
An attempt to scan both files results in a permission denied error.

<http://prntscr.com/9d5qiq>

Wired? - December 11, 2015, 9:37 pm

From what you have posted, the location and the random popup of these files indicates a red flag. Since you don't have permission to access these files in that location, this also indicates a red flag. This is probably a piece of malicious software attempting to disguise itself as mrt.exe, which is part of Microsoft's malicious software removal tool, and I assume you haven't installed that software. Even if you have, it definitely would not appear in that location with a permission denied error.

I will help remove any malicious files from your computer.

Please download [Farbar Recovery Scan Tool](#) and save it to your desktop or another directory that you can remember.

Note: You need to run the version (32/64 bit) compatible with your system. If you are not sure which version applies to your system download both of them and try to run them. Only one of them will run on your system, that will be the right version.

Right click to run as administrator. When the tool opens click Yes to the disclaimer.

Press the Scan button.

It will produce a log called FRST.txt in the desktop directory unless the tool is run from another directory, in which case it will be in that location.

Please copy and paste the EXACT contents of the log to [Pastebin](#) and post that in your reply.

The first time the tool is run it generates another log (Addition.txt - also located in the same directory as FRST.exe/FRST64.exe). Please also paste that along with the FRST.txt into your reply.

So that I can help you to the best of my abilities, please consider the following.

If you would like for me to continue helping you, please follow all of my instructions.

Do not download any new programs until I am done helping you and have deemed your computer clear of any malicious activity.

Please don't try and remove anything yourself unless you would not like my assistance.

The OG FurFag ? - December 11, 2015, 10:02 pm

(Dec 11, 2015 10:37 PM)Wired? Wrote: [\[CITE\]](#) From what you have posted, the location and the random popup of these files indicates a red flag. Since you don't have permission to access these files in that location, this also indicates a red flag. This is probably a piece of malicious software attempting to disguise itself as mrt.exe, which is part of Microsoft's malicious software removal tool, and I assume you haven't installed that software. Even if you have, it definitely would not appear in that location with a permission denied error.

I will help remove any malicious files from your computer.

Please download [Farbar Recovery Scan Tool](#) and save it to your desktop or another directory that you can remember.

Note: You need to run the version (32/64 bit) compatible with your system. If you are not sure which version applies to your system download both of them and try to run them. Only one of them will run on your system, that will be the right version.

Right click to run as administrator. When the tool opens click Yes to the disclaimer.

Press the Scan button.

It will produce a log called FRST.txt in the desktop directory unless the tool is run from another directory, in which case it will be in that location.

Please copy and paste the EXACT contents of the log to [Pastebin](#) and post that in your reply.

The first time the tool is run it generates another log (Addition.txt - also located in the same directory as FRST.exe/FRST64.exe). Please also paste that along with the FRST.txt into your reply.

So that I can help you to the best of my abilities, please consider the following.

If you would like for me to continue helping you, please follow all of my instructions.

Do not download any new programs until I am done helping you and have deemed your computer clear of any malicious activity.

Please don't try and remove anything yourself unless you would not like my assistance.

<http://pastebin.com/paRCi98a>

Both scans are divided and located here.

5chn4pp - December 12, 2015, 7:28 am

These files are related to a update for the default security program built in windows, you are fine.