

Forum:[Hack Forums](#)

Thread: [How to find and remove a rat on your pc without having to fac reset?](#)

stimpyyoutube - January 15, 2017, 4:00 pm

How to find and remove a rat on your pc without having to fac reset?

SoulZeh - January 15, 2017, 4:20 pm

Run a scan of Malwarebytes and it should detect if you have a virus.

P.E.Investigations - January 15, 2017, 7:06 pm

I know Malwarebytes is very good but I also know that it does not detect newly and effectively cryped RATs.

How can I search for RATs if I think I have been RATED?

If possible, I would like to do this search without downloading and installing software I do not know. Is there an (easy to follow) manual or run down list I can refer too?

Thanks.

LS RX7 - January 15, 2017, 7:08 pm

have you tried security task manager? I think it works for a lot of stuff.

P.E.Investigations - January 15, 2017, 7:47 pm

Thank you. Screen shots look similar to Processes from Task manager and Resource Monitor plus a rating they provide.

What would be involved if I want to see the DNS or IP address the RAT is broadcasting to? That information must be in the RAT and also show up somewhere in the lists of connections, no?

?Ñâzg?l - January 15, 2017, 8:14 pm

use process explorer and TCPview to find and remove malware manually

Farbar Recovery Scan is another great tool to use (however it does not list network activity)

or use process hacker (the name might sound odd but it's great open source software)

removing malware manually allows you to find new malware which an Anti-virus won't detect

you can use wireshark for finding the DNS adress and also for finding the server that a keylogger will send it's logs

however you should have an anti-rootkit scanner avaible on your system at all times
some malware can hide themselves from the entire system

WRX - January 15, 2017, 8:18 pm

Do you know anything about what your computer usually runs and the names of the programs you use?

If so you can remove these pretty easily manually.

I would talk to Aura he really knows his shit

?Ñâzg?l - January 15, 2017, 8:26 pm

(Jan 15, 2017 08:06 PM)P.E.Investigations Wrote: [\[CITE\]](#) How can I search for RATs if I think I have been RATed?

If possible, I would like to do this search without downloading and installing software I do not know. Is there an (easy to follow) manual or run down list I can refer too?

Thanks.

if you want I can help you with that
just PM me

combovirus - January 16, 2017, 12:58 am

My method may look complicated but hope it is best one. Download and install process hacker and check all the established connection under network. If you find the rat then, with this you directly go process and delete the root file of rat even if it is protected.

Hackoo - January 16, 2017, 2:03 am

Farbar Recovery Scan Tool (FRST) ScanPlease download [Farbar Recovery Scan Tool \(x32\)](#) or [Farbar Recovery Scan Tool \(x64\)](#) and save the file to your Desktop.

Note: Download and run the version compatible with your system (32 or 64-bit). Download both if you're unsure; only one will run.

Double-Click FRST.exe or 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.

In your next reply I get from youFRST.txt

Addition.txt

P.E.Investigations - January 16, 2017, 10:06 pm

Thank you all. I downloaded three of the programs already and will do Farbar Recovery Scan Tool next too. I think I am not allowed to posts links yet so maybe I need to post the results as a thread.

Please continue to support me. Recently I had an error message in a foreign language appear so I think the RATER's OS language might not be English.

Aura - January 17, 2017, 4:16 pm

You can always PM me the logs and I can check them (though I won't be providing a fixlist sadly).

Sab4fa - January 20, 2017, 8:45 am

(Jan 16, 2017 03:03 AM)Hackoo Wrote: [\[CITE\]](#) Farbar Recovery Scan Tool (FRST) ScanPlease download or and save the file to your Desktop.

Note: Download and run the version compatible with your system (32 or 64-bit). Download both if you're unsure; only one will run.

Double-Click FRST.exe or 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.

In your next reply I get from youFRST.txt

Addition.txt

DONT DOWNLOAD IT!!! ITS A VIRUS SOMEONE HACKED ME THROUGH IT!
This sameguy did it to me! please dont!

Hackoo - January 20, 2017, 9:08 am

(Jan 20, 2017 09:45 AM)Sab4fa Wrote: [\[CITE\]](#) DONT DOWNLOAD IT!!! ITS A VIRUS SOMEONE HACKED ME THROUGH IT!

This sameguy did it to me! please dont!

What did you mean by that ?

Can you explain us more ? did you mean that FRST.exe is a virus ???? ? ?

Aura - January 20, 2017, 4:21 pm

(Jan 20, 2017 09:45 AM)Sab4fa Wrote: [\[CITE\]](#) DONT DOWNLOAD IT!!! ITS A VIRUS SOMEONE HACKED ME THROUGH IT!

This sameguy did it to me! please dont!

FRST is a legitimate malware removal tool created by farbar. As long as you download it from BleepingComputer.com, it'll be safe. It is known for tools like this to trigger Antivirus and Antimalware programs, though they are false positives that can be safely ignored.

axoltr - January 22, 2017, 7:11 am

When I feel like my computer's being infected the safest way I've heard is reinstall everything, even if the tools you use shows nothing it's still pretty scary.