

Forum:[Hack Forums](#)

Thread: [\[Remove Rats/Check\] Tracking Startup/Location](#)

Velocity™ - August 31, 2015, 6:57 pm

So... As some of you may be able to tell I'm doing a compilation of tips to use to protect yourself from virus's such as rats/keyloggers, so if you haven't already check out my other threads! :D

[\[Remove Rats/Check\] TCPViewer](#)

So in this thread, I'll be telling you newbies how to terminate and 100% clear a rat/keylogger off of your computer using a few simple techniques.

If you are not aware of what most crypters do to rats that are not crypted, is that it can supply and option to set a start up... So every time your PC starts up, the executable virus will run instantly. This will fuck you up entirely and needs to be dealt with.

There are a few ways to search if your computer is infected with a startup option attached.

FIRST - USING MSCONFIG.

-Click the start menu and click "run" then type "msconfig" and hit enter

-Check your startup entries for any programs which you don't know what they are. Check every entry online to check if it's necessary. Some ARE necessary for everything from the system itself to random programs on your computer.

If you find anything suspicious uncheck it from the start up options.

SECOND - FILE SEARCHING.

So, I will go through the most common places where a rat/keylogger would be stored if it were start-up active.

1. APPDATA

- Click the start menu and click "run" then type "%appdata%"

- If there is some weird file in there, look it up. Find out what it is, and if you don't know what it is, investigate more. Don't delete if unless you're sure you don't need it.

- Additionally you may want to check in individual program APPDATA folders. Specifically your internet browsers, Java, and other ones which store temporary information.

- There have been reports of keylogger fragments infecting the LocalLow and Local directories in Vista and Windows 7 users, so search there if applicable.

2. PROGRAM DATA

-Click the start menu and click "run" then type "%programdata%"

Follow the same steps as APPDATA.

3. TEMP

-Click the start menu and click "run" then type "%temp"

Follow the same steps as above.

(Also search for documents, and any others you may find)

After you delete the start up file you have located, be sure to restart your PC and you are now rat free from start-ups :)

Thank you for reading this far!

desynk - September 1, 2015, 2:08 pm

While I can appreciate what you're trying to do there are a lot of holes in this guide. You don't really want to use msconfig, but rather something like Autoruns. There are many malicious infections that will not be easily removed by something as simple as msconfig or even autoruns itself. There are also a lot more locations that bad files hide in. Although your post doesn't explicitly that it won't remove ALL infections, it specifically alludes to it by saying "terminate and 100% clear a rat/keylogger" which is just not true. Be wary those who follow this, your system still very well could be, and likely is, infected.