DarkRAT Malware

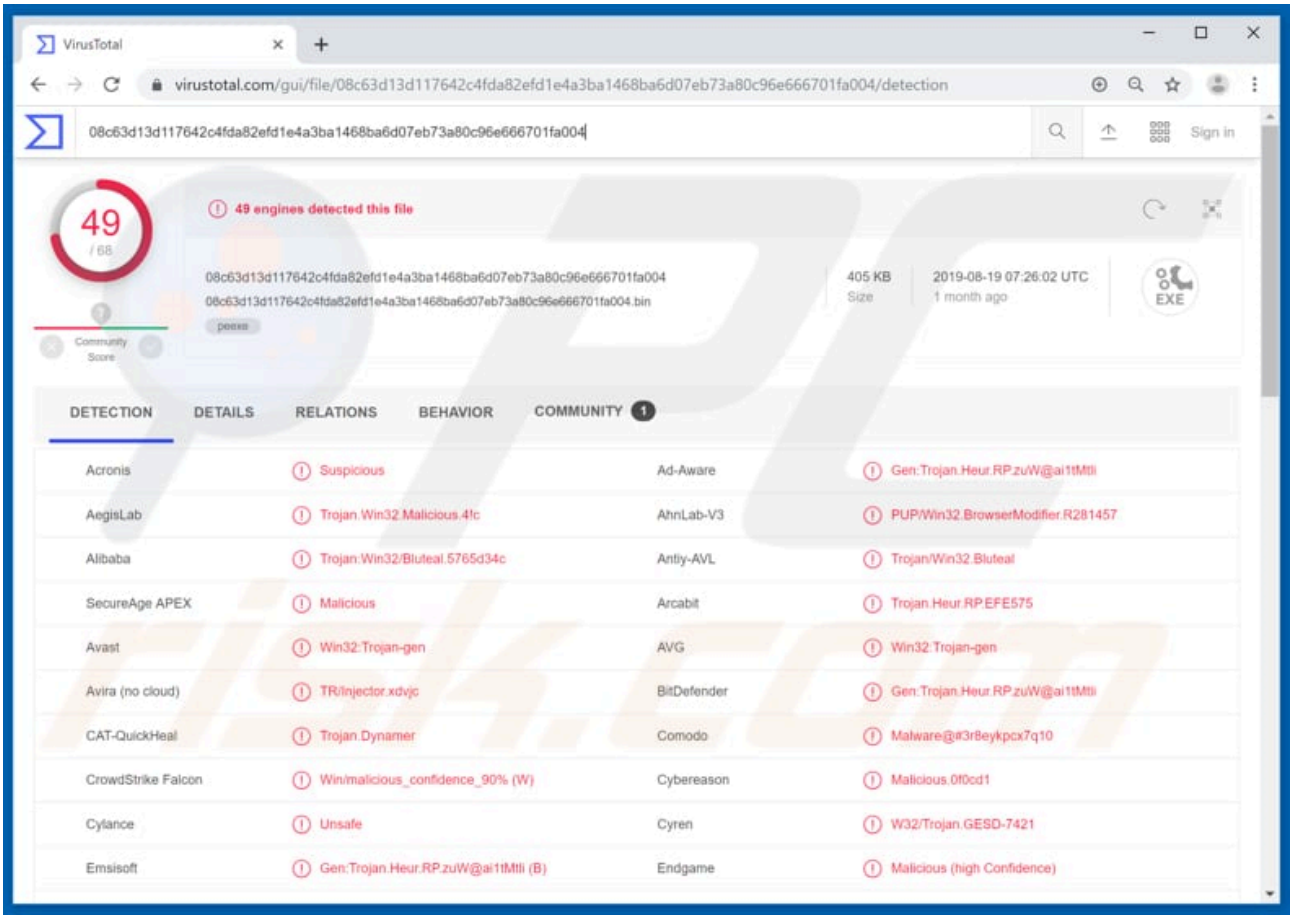
By Tomas Meskauskas

Published: 2025-06-06 · Archived: 2026-04-05 13:49:06 UTC

What is DarkRAT?

DarkRAT is one of many remote access tools (RATs) used to control connected computers remotely. Unfortunately, in many cases, cyber criminals trick people into installing RATs onto their systems and then use them to steal personal details, infect systems with malware, and cause other damage.

If your system is infected with this RAT, we strongly recommend that you uninstall it immediately.



One DarkRAT feature prevents users from killing its process. Therefore, it cannot be disabled and will run in the system background. Cyber criminals can then use its features when they wish. Additionally, it can prevent victims from removing it from the list of startup items. I.e., it can then launch itself at each startup automatically.

Furthermore, DarkRAT can be used to download and execute various files onto the victim's computer. Typically, cyber criminals download and execute malicious files that infect the system with malware. For example, ransomware, which encrypts files and prevents victims from accessing them.

Typically, the only way to decrypt data is to purchase decryption software and/or keys from the cyber criminals who designed the ransomware. Note that ransomware is not the only malware that can be installed through DarkRAT. This remote access tool is also capable of updating itself.

As soon as a newer version is released, it starts to update itself. Furthermore, cyber criminals can remotely load custom DLL files onto the victim's computer and affect behaviour of the operating system or installed programs. They can also use it to check which anti-virus software is installed on the operating system and then avoid detection.

Threat Summary:

Name	DarkRAT remote access trojan
Threat Type	Remote Access Trojan.
Detection Names	Avast (Win32:Trojan-gen), BitDefender (Gen:Trojan.Heur.RP.zuW@ai1tMtli), ESET-NOD32 (A Variant Of Win32/DarkRAT.A), McAfee (RDN/Generic.grp), Full List (VirusTotal)
Malicious Process Name(s)	fZYeMMBDUj.exe (it can also run a malicious process under a different name).
Payload	DarkRAT can be used to download and install various malware, including ransomware.
Symptoms	Trojans are designed to stealthily infiltrate the victim's computer and remain silent, and thus no particular symptoms are clearly visible on an infected machine.
Distribution methods	Infected email attachments, malicious online advertisements, social engineering, software 'cracks'.
Damage	Stolen banking information, passwords, identity theft, victim's computer added to a botnet.

Malware Removal (Windows)	To eliminate possible malware infections, scan your computer with legitimate antivirus software. Our security researchers recommend using Combo Cleaner. Download Combo Cleaner To use full-featured product, you have to purchase a license for Combo Cleaner. 7 days free trial available. Combo Cleaner is owned and operated by RCS LT, the parent company of PCRisk.com.

WSH, InnfiRAT, and Gh0st are just a number examples of other RATs that cyber criminals use to control users' computers remotely. Their aim is to steal personal details (logins, passwords of various accounts), install additional malware, and perform other actions. Being tricked into installing software of this type can lead to serious problems.

How did DarkRAT infiltrate my computer?

Criminals use various ways to trick people into installing RATs, malware, and other unwanted software. They send emails that contain malicious attachments including Microsoft Office documents, PDFs, executables such as .exe, archives (ZIP, RAR, and other files), JavaScript, and other files that, if opened, cause installation of malicious software.

Another way to achieve this is by first infecting computers with Trojans. Once installed, they cause chain infections and install additional malware. Furthermore, fake software updaters can lead to unwanted downloads and installations. If used, they can install malicious software rather than updating installed programs, or they exploit bugs/flaws of outdated programs.

Untrustworthy software download sources such as freeware download websites, free file hosting websites, Peer-to-Peer networks (torrents, eMule etc.), and various third party downloaders, are used to disguise malicious files as legitimate. When people open files downloaded from these sources, they often install malware inadvertently.

Malware is also spread through unofficial software activation tools. These programs supposedly activate licensed (paid) software free of charge, however, the tools are often designed to proliferate malicious programs (people who use them risk installation of malware).

How to avoid installation of malware

Do not open web links or files that are attached to irrelevant emails, especially if the emails are received from unknown, suspicious addresses. If there is reason to believe that an email is suspicious, the best option is to leave

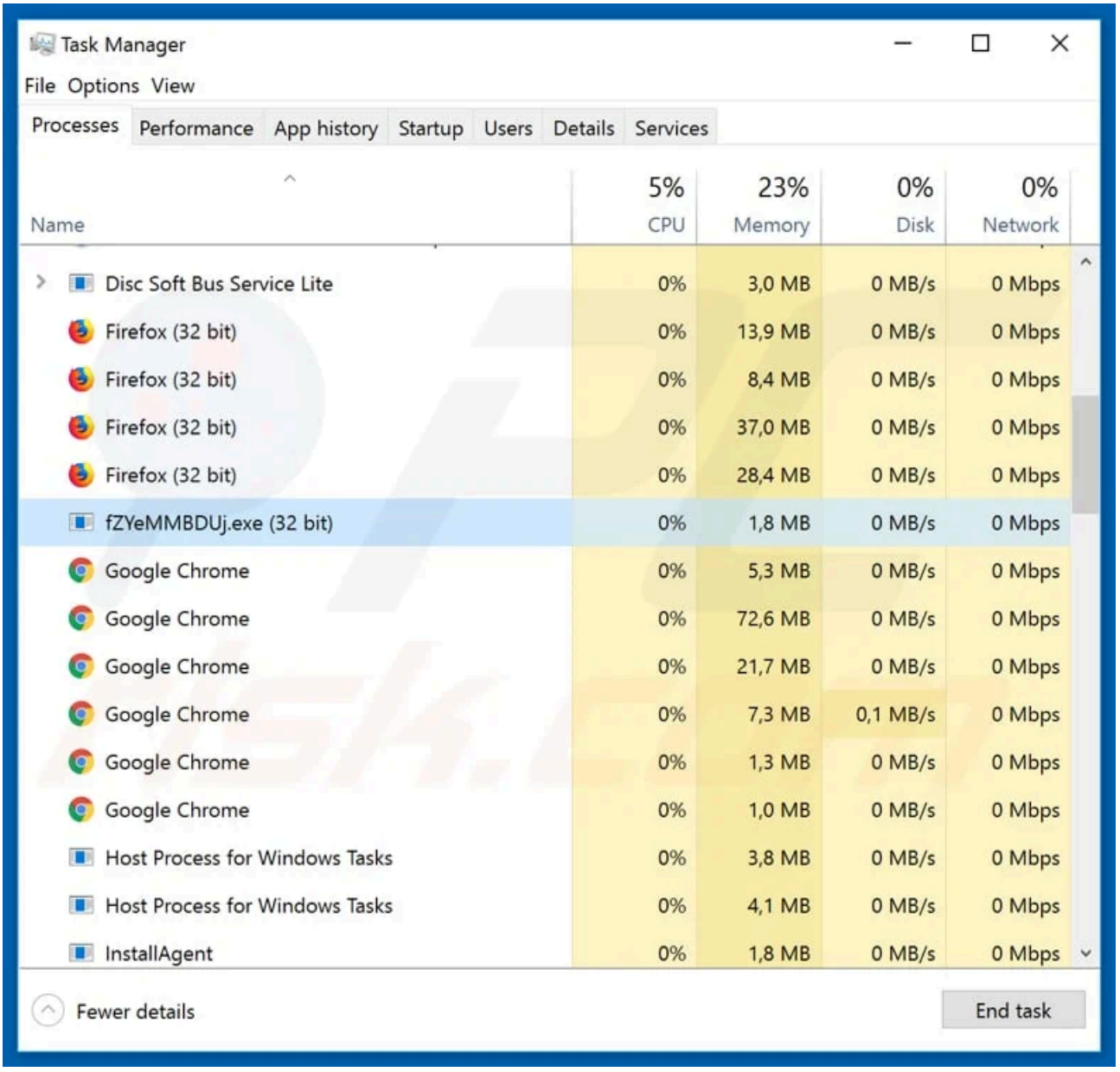
included links or files unopened.

Furthermore, download software from official, trustworthy sources websites. All channels mentioned above should not be trusted. All installed software must be updated through tools or implemented functions that are provided by official developers. Licensed/paid programs should not be activated using unofficial ('cracking') tools.

This is illegal and often leads to installation of malware. Keep computers safe by having reputable anti-spyware or anti-virus software installed. Scan systems regularly. If you believe that your computer is already infected, we recommend running a scan with Combo Cleaner Antivirus for Windows to automatically eliminate infiltrated malware.

DarkRAT administration panel:

Malicious DarkRAT process in Task Manager ("**fZYeMMBDUj.exe**"):



Instant automatic malware removal:

Manual threat removal might be a lengthy and complicated process that requires advanced IT skills. Combo Cleaner is a professional automatic malware removal tool that is recommended to get rid of malware. Download it by clicking the button below:

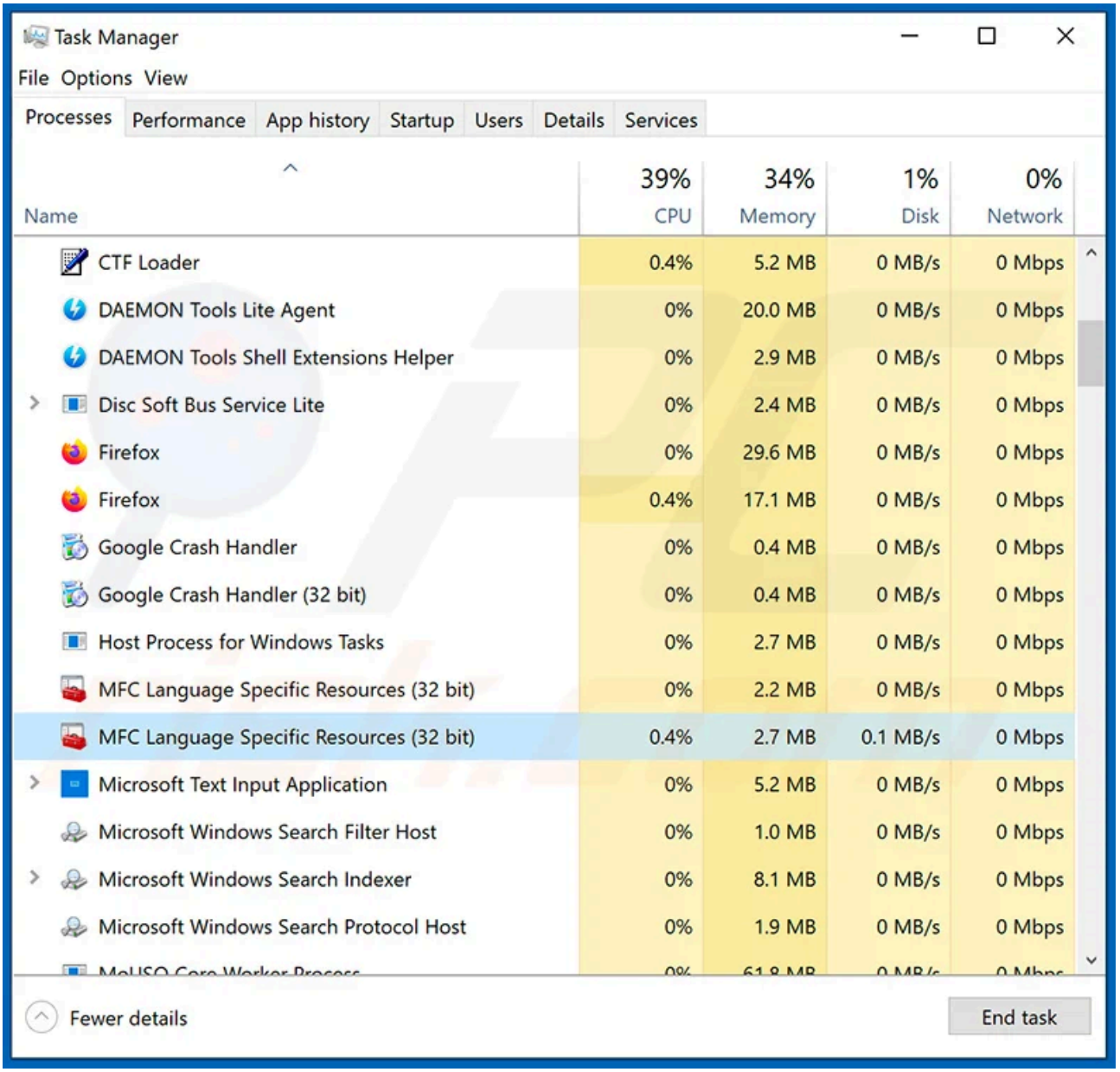
DOWNLOAD Combo Cleaner

Quick menu:

How to remove malware manually?

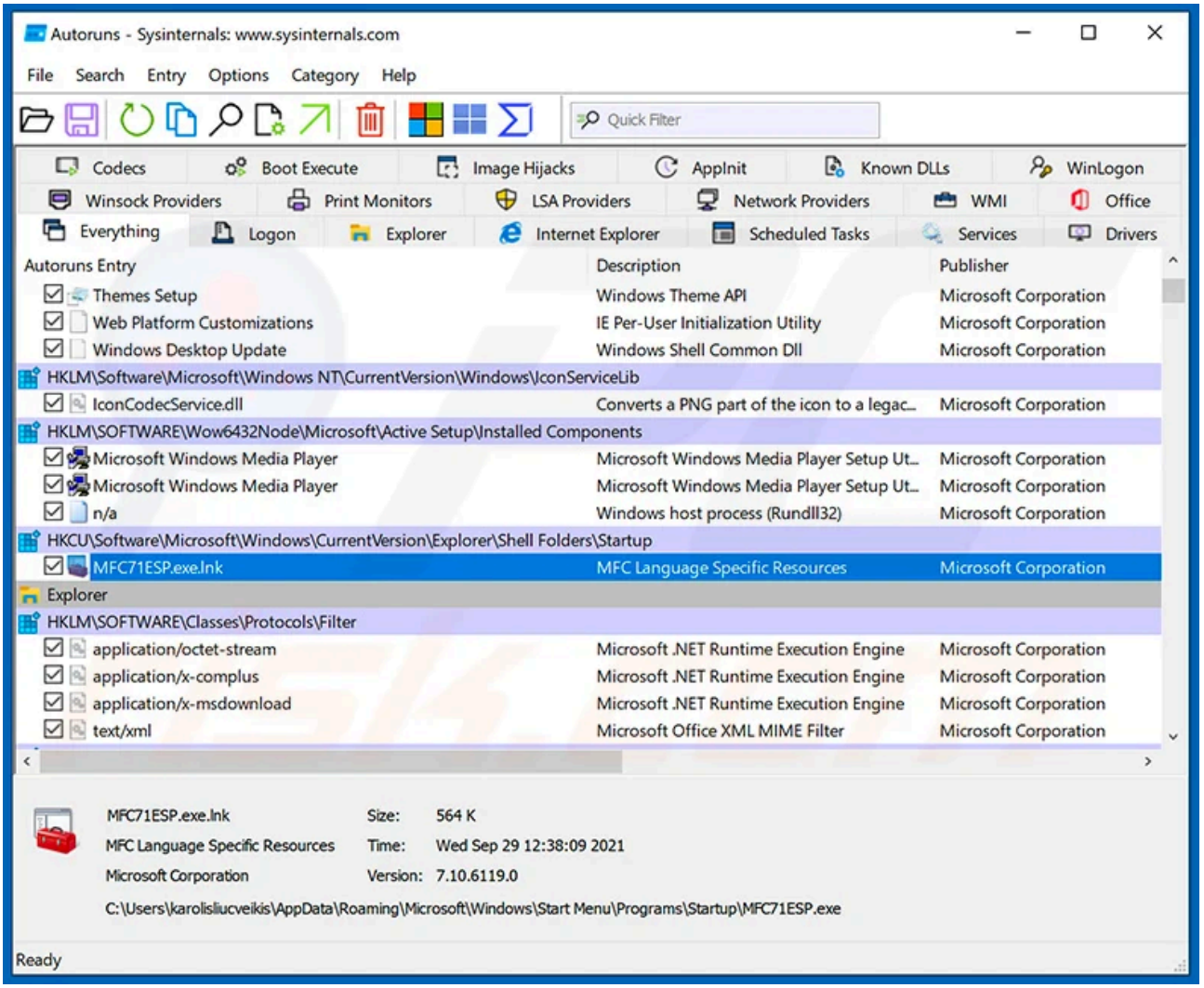
Manual malware removal is a complicated task - usually it is best to allow antivirus or anti-malware programs to do this automatically. To remove this malware we recommend using Combo Cleaner Antivirus for Windows.

If you wish to remove malware manually, the first step is to identify the name of the malware that you are trying to remove. Here is an example of a suspicious program running on a user's computer:



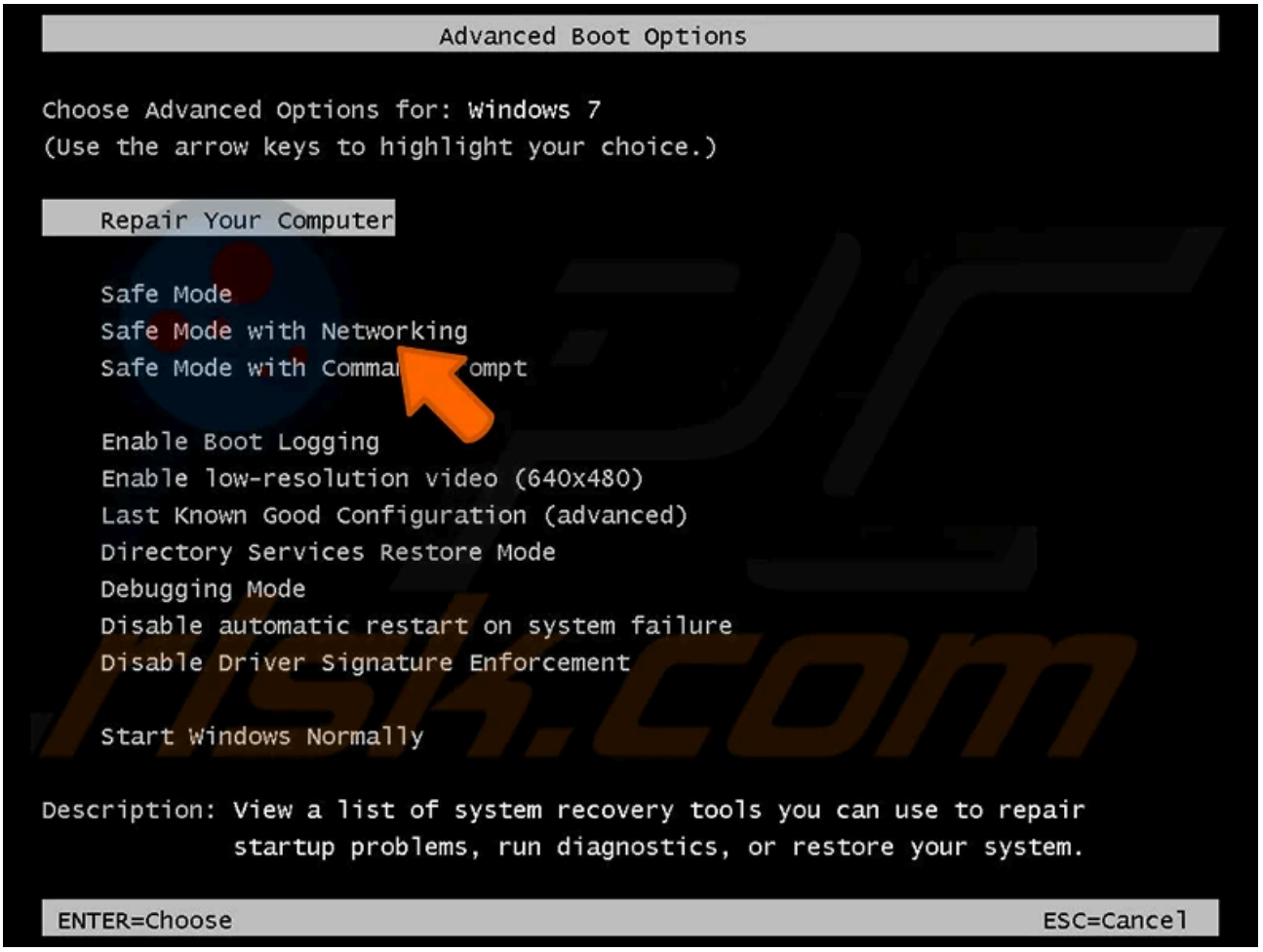
If you checked the list of programs running on your computer, for example, using task manager, and identified a program that looks suspicious, you should continue with these steps:

Download a program called Autoruns. This program shows auto-start applications, Registry, and file system locations:



Restart your computer into Safe Mode:

Windows XP and Windows 7 users: Start your computer in Safe Mode. Click Start, click Shut Down, click Restart, click OK. During your computer start process, press the F8 key on your keyboard multiple times until you see the Windows Advanced Option menu, and then select Safe Mode with Networking from the list.

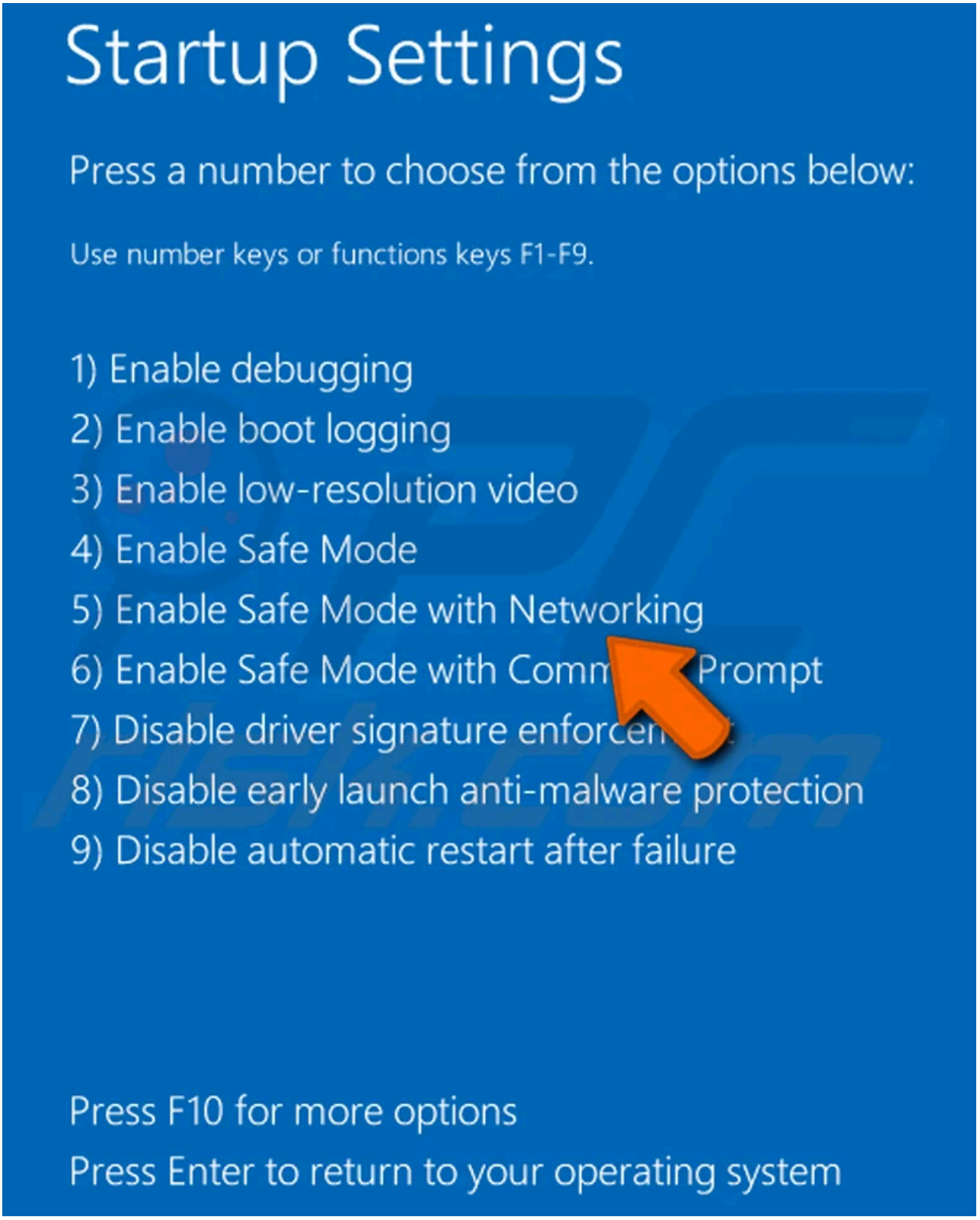


Video showing how to start Windows 7 in "Safe Mode with Networking":

Windows 8 users: Start Windows 8 is Safe Mode with Networking - Go to Windows 8 Start Screen, type Advanced, in the search results select Settings. Click Advanced startup options, in the opened "General PC Settings" window, select Advanced startup.

Click the "Restart now" button. Your computer will now restart into the "Advanced Startup options menu". Click the "Troubleshoot" button, and then click the "Advanced options" button. In the advanced option screen, click "Startup settings".

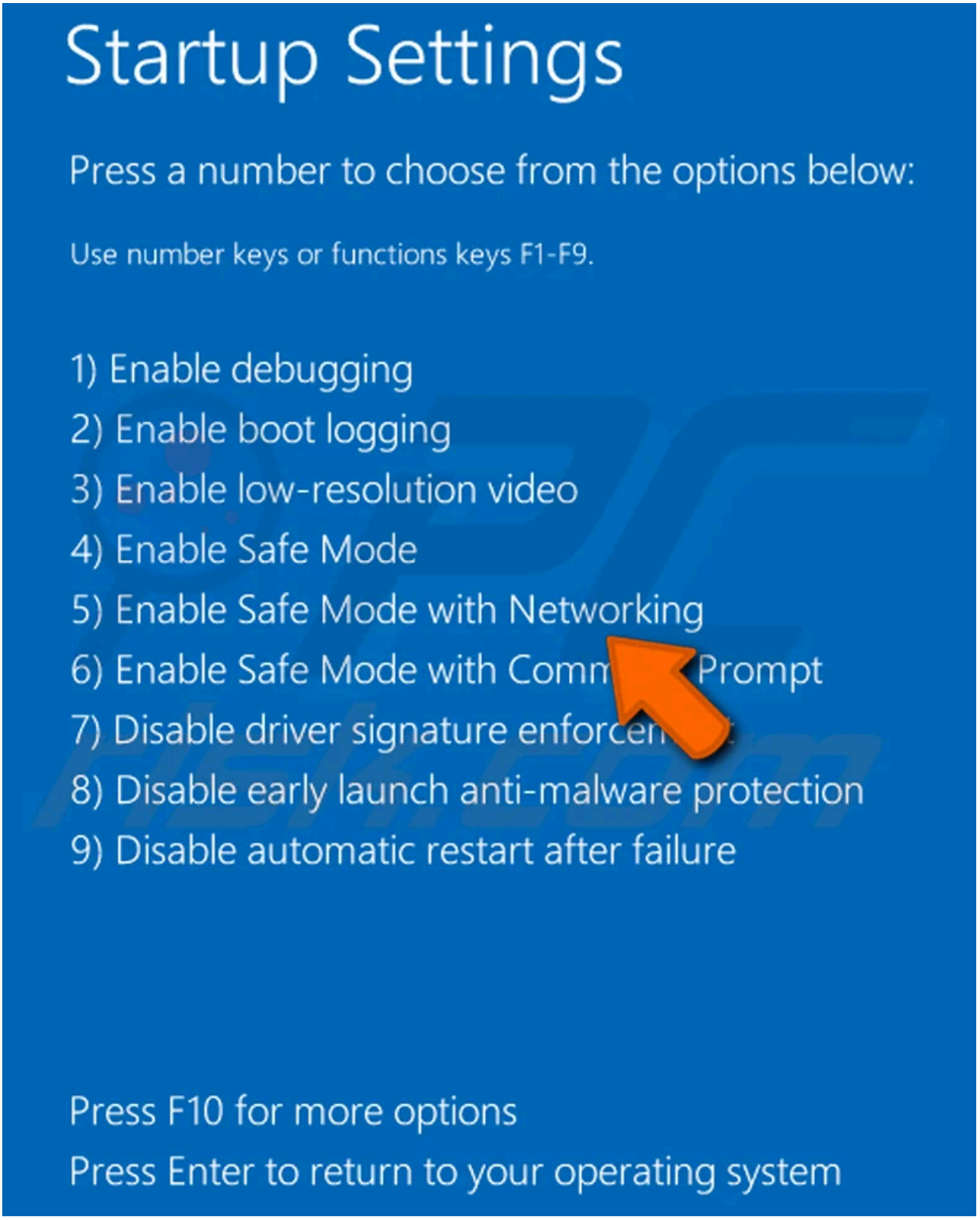
Click the "Restart" button. Your PC will restart into the Startup Settings screen. Press F5 to boot in Safe Mode with Networking.



Video showing how to start Windows 8 in "Safe Mode with Networking":

Windows 10 users: Click the Windows logo and select the Power icon. In the opened menu click "Restart" while holding "Shift" button on your keyboard. In the "choose an option" window click on the "Troubleshoot", next select "Advanced options".

In the advanced options menu select "Startup Settings" and click on the "Restart" button. In the following window you should click the "F5" button on your keyboard. This will restart your operating system in safe mode with networking.



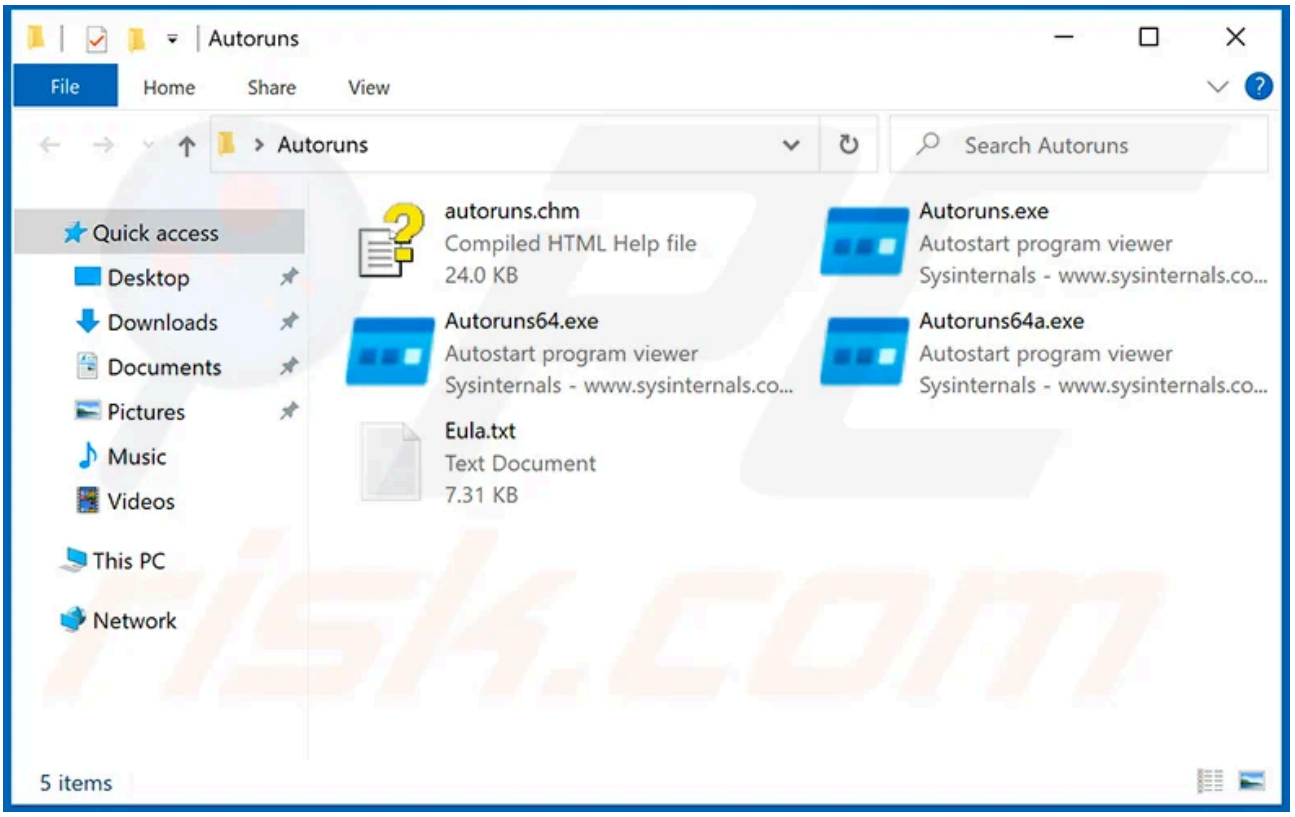
Video showing how to start Windows 10 in "Safe Mode with Networking":

Ett fel inträffade.

Det går inte att köra JavaScript.

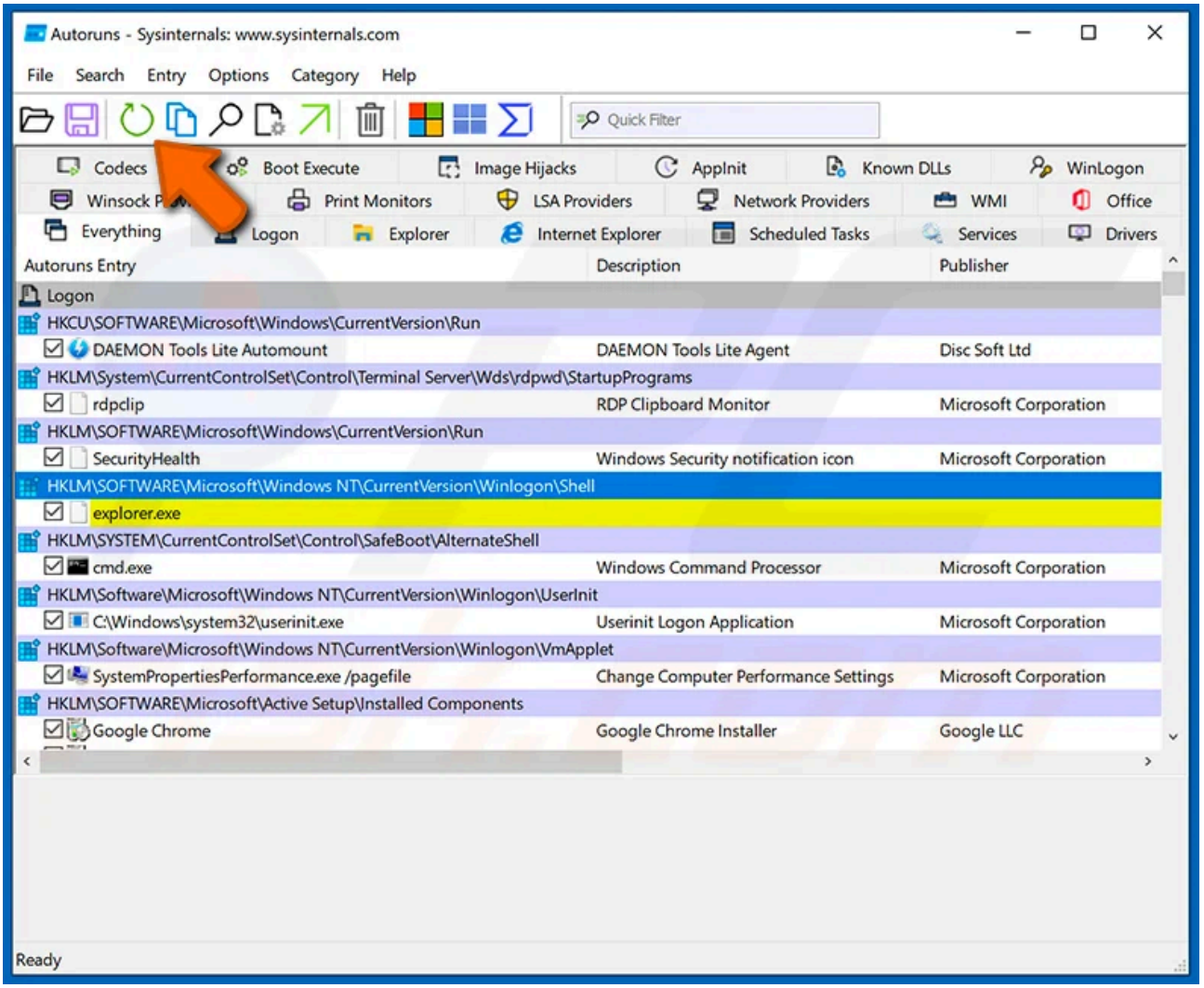
Step 3

Extract the downloaded archive and run the Autoruns.exe file.



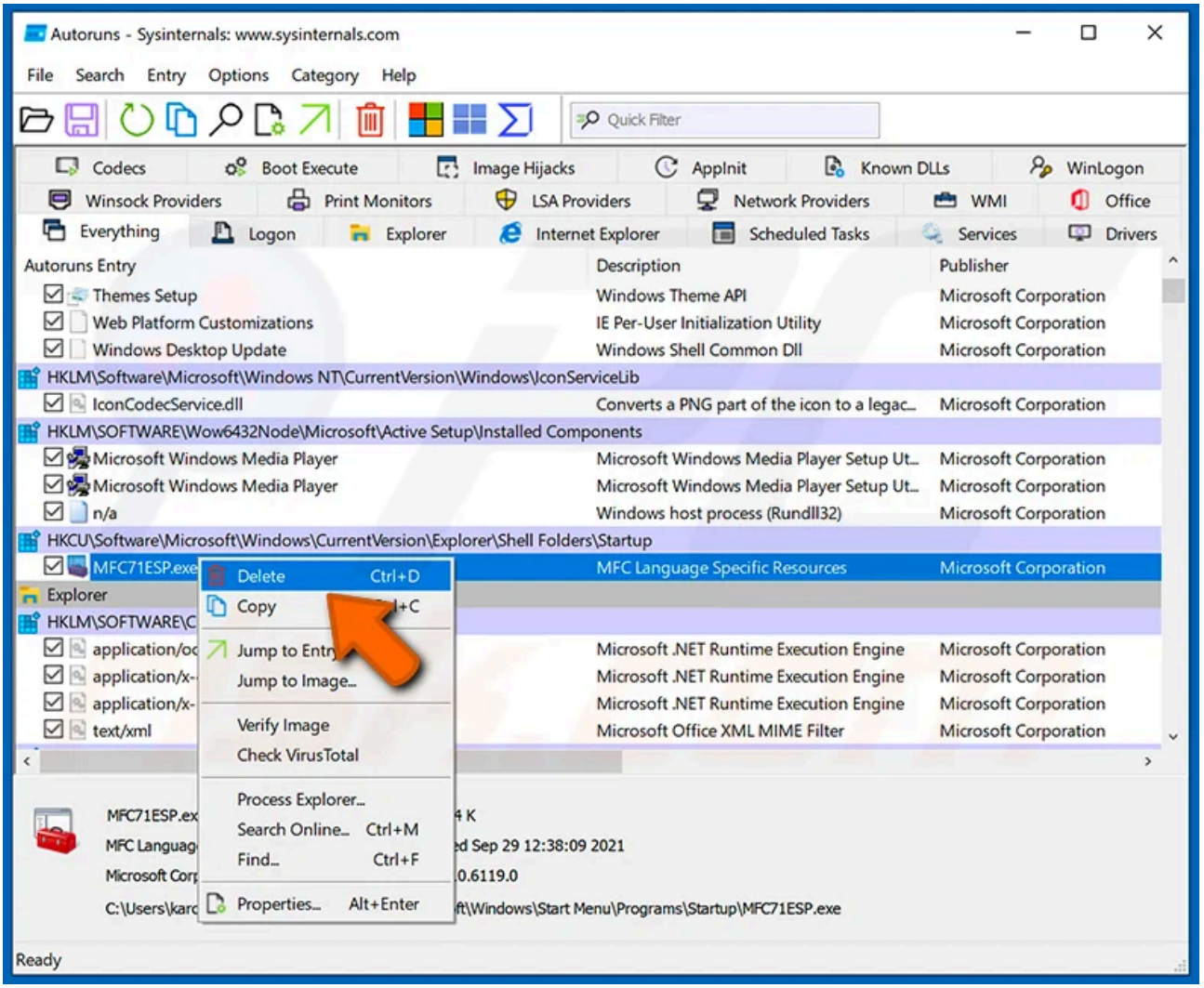
Step 4

In the Autoruns application, click "Options" at the top and uncheck "Hide Empty Locations" and "Hide Windows Entries" options. After this procedure, click the "Refresh" icon.

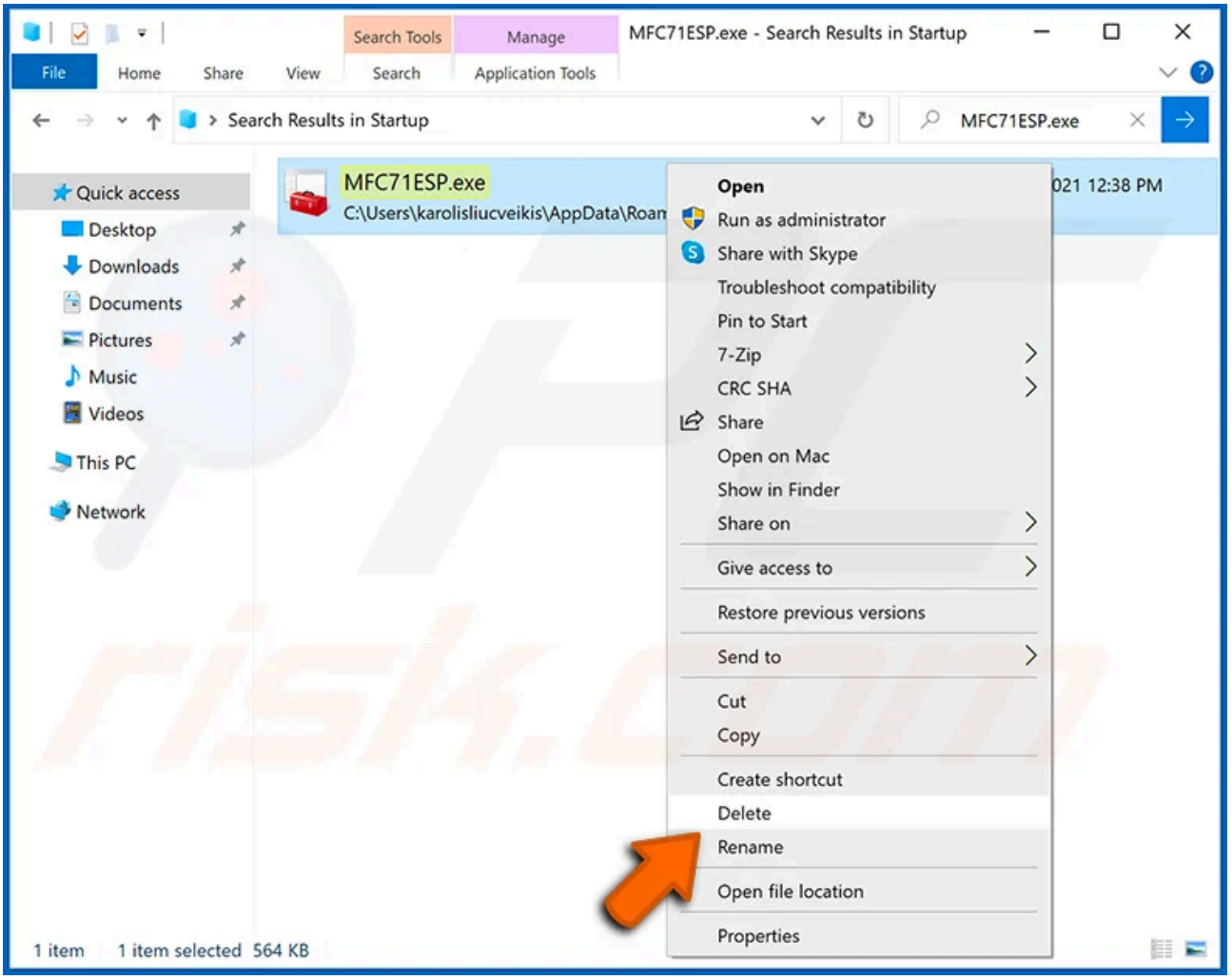


Check the list provided by the Autoruns application and locate the malware file that you want to eliminate.

You should write down its full path and name. Note that some malware hides process names under legitimate Windows process names. At this stage, it is very important to avoid removing system files. After you locate the suspicious program you wish to remove, right click your mouse over its name and choose "Delete".



After removing the malware through the Autoruns application (this ensures that the malware will not run automatically on the next system startup), you should search for the malware name on your computer. Be sure to enable hidden files and folders before proceeding. If you find the filename of the malware, be sure to remove it.



Reboot your computer in normal mode. Following these steps should remove any malware from your computer. Note that manual threat removal requires advanced computer skills. If you do not have these skills, leave malware removal to antivirus and anti-malware programs.

These steps might not work with advanced malware infections. As always it is best to prevent infection than try to remove malware later. To keep your computer safe, install the latest operating system updates and use antivirus software. To be sure your computer is free of malware infections, we recommend scanning it with [Combo Cleaner Antivirus for Windows](#).

Source: https://www.pcrisk.com/removal-guides/15893-darkrat-malware