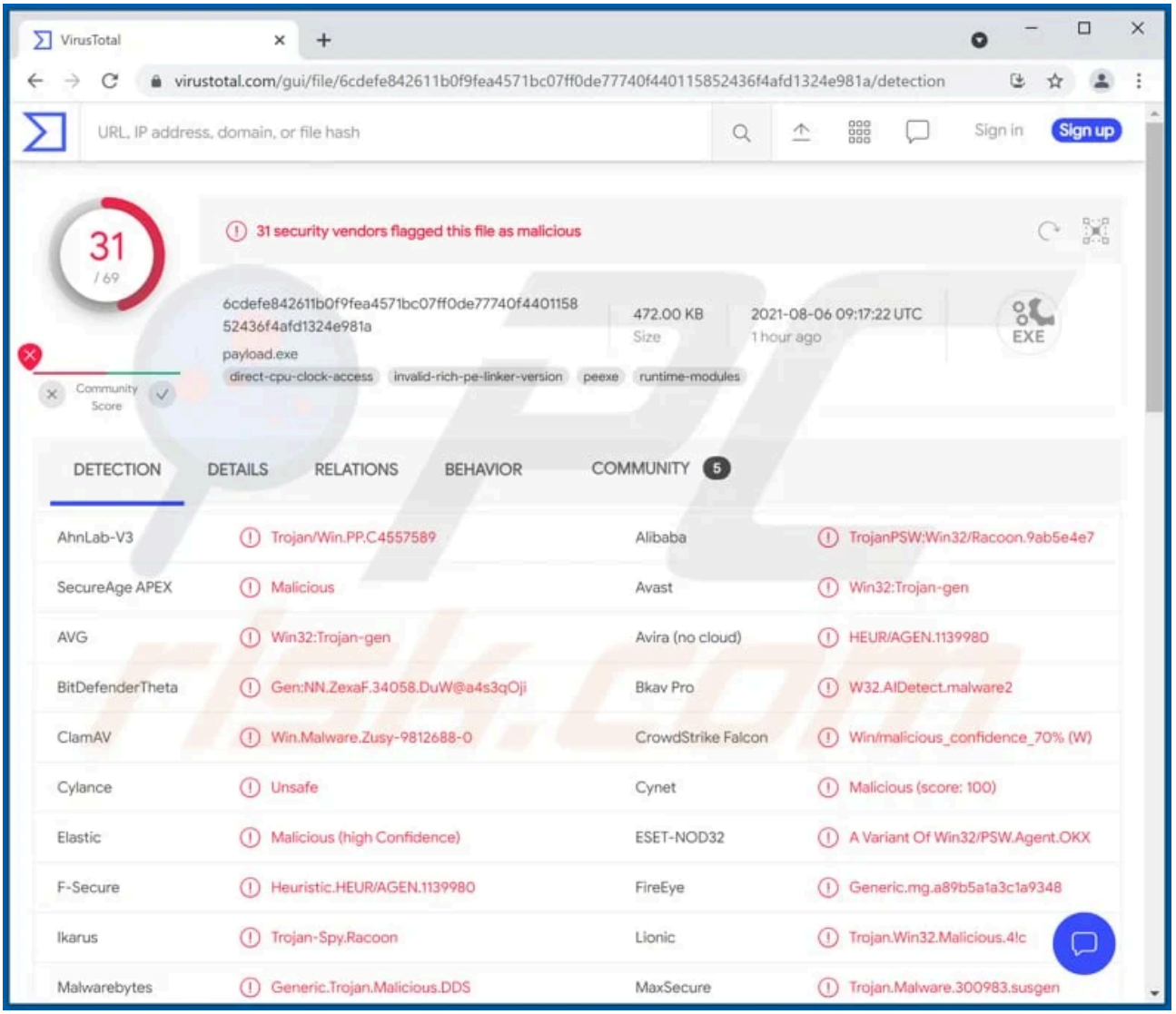
SHurk Steal Malware

By Tomas Meskauskas

Published: 2025-06-09 · Archived: 2026-04-05 22:54:31 UTC

What is SHurk Steal malware?

SHurk Steal is a piece of malicious software designed to steal sensitive information. It is written in C++ programming language and can be purchased on a hacker forum. It costs 400 rubles per week, 900 rubles per month or it can be purchased for a one-time fee of 3000 rubles. SHurk Steal targets Windows operating systems.



SHurk Steal in detail

SHurk Steal is advertised as an easy-to-use information stealer capable of stealing cookies, passwords, credit card details, and autofill data from browsers using the Chromium codebase. Also, it can steal cryptocurrency wallets

that are not connected to the internet (cold wallets), wallet files, IP addresses, and hijack Telegram sessions.

Typically, cybercriminals use malware like SHurk Steal to steal login credentials, credit card details, and other information that could be used to steal personal accounts (for example, email, social media, banking accounts), crypto wallets that could be used to distribute other malware, steal identities, money, make fraudulent purchases, transactions, etc.

Therefore, users who install malware like SHurk Steal become victims of identity theft, suffer monetary loss, cannot access their personal accounts, get their computers infected with ransomware, cryptocurrency miners, Trojans, or other malicious software, encounter problems related to browsing safety, online privacy, or other issues.

It is important to mention that cybercriminals behind SHurk Steal may use stolen information for personal gains or sell it to third parties (or do both). In one way or another, users who have a computer infected with SHurk Steal are likely to encounter financial and other problems. Therefore, this malware should be uninstalled from infected systems immediately.

Threat Summary:

Name	SHurk Steal information stealer
Threat Type	Information stealer, password-stealing virus
Detection Names	Avast (Win32:Trojan-gen), Combo Cleaner (Trojan.GenericKD.46749892), ESET-NOD32 (A Variant Of Win32/PSW.Agent.OKX), Kaspersky (Trojan-PSW.Win32.Agent.tnky), Microsoft (Trojan:Win32/Casdet!rfn), Full List (VirusTotal)
Symptoms	Most information stealers 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 passwords and banking information, identity theft, the 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.

Information stealers in general

In conclusion, information stealers like SHurk Steal are used to collect information that could be used to steal money, online accounts, and access even more personal information. More examples of information stealers are Mars Stealer, FickerStealer, and Bloody Stealer. Distribution methods for malicious programs are provided below.

How did SHurk Steal infiltrate my computer?

It is common for information stealers and other malicious programs to be distributed via emails. Recipients install malware by opening malicious files or website links in emails sent by cybercriminals. Typically, cybercriminals send malicious Microsoft Office documents, executable files (like EXE), RAR, ZIP and other archive files, JavaScript files, PDF documents.

Another way to distribute malware is to trick users into using fake software updaters. Those updaters are disguised as tools that fix., update installed software. However, they never update or fix any software - they install malware in a regular way or infect systems by exploiting bugs, flaws of outdated programs that are installed on them.

Trojans are malicious programs that can be used to distribute malware too. Usually, Trojans are distributed using the ways described in this section. As a rule, they are disguised as legitimate programs. Once installed, they can infect computers with additional malware.

Files downloaded via third-party downloaders, free file hosting or freeware download websites, Peer-to-Peer networks like torrent clients, eMule, and so on, can be malicious as well. Users cause installation of malware by downloading and executing those files. Typically, they are disguised as legitimate, regular, harmless files.

Software cracking tools are illegal programs that are supposed to activate licensed software without for free. Although, it is common that their users infect computers with malware. In other words, it is common for cracking tools to be bundled with malware.

How to avoid installation of malware?

Files and programs should be downloaded from legitimate, trustworthy pages and via direct download links. Files or programs downloaded via Peer-to-Peer networks, third-party downloaders, unofficial pages, free file hosting sites etc., or programs installed via third-party installers can be malicious.

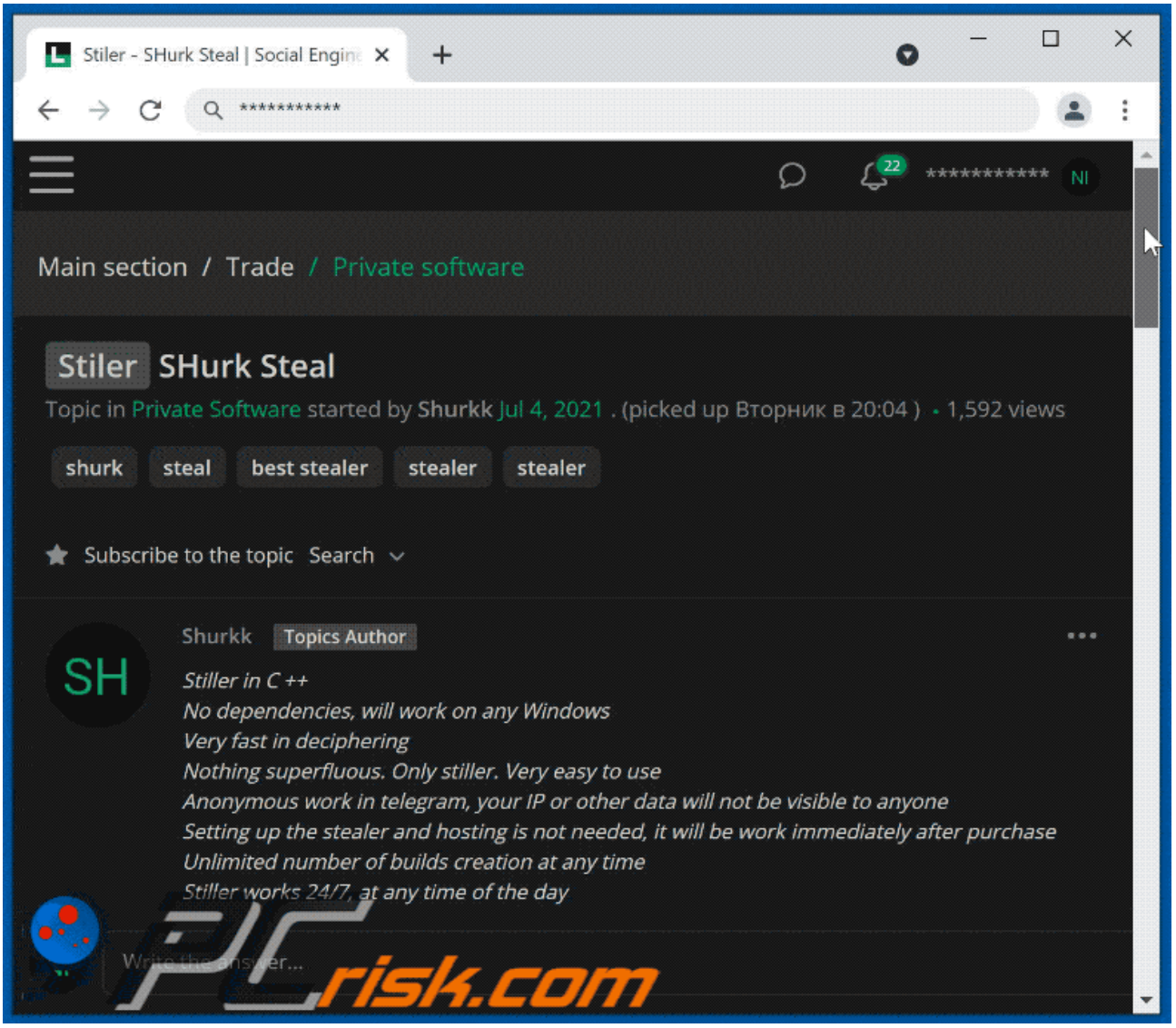
The operating system and programs installed on it have to be updated and activated with implemented functions or tools designed/provided by their official developers. Software cracking tools and third-party updaters can be designed to install malware. Moreover, it is not legal to use cracked software or cracking tools to activate it.

Attachments and website links in irrelevant emails sent from suspicious, unknown addresses should not be opened. Pretty often, links or files in emails of this kind are used to deliver malware - they are designed to

distribute malicious software. It is important to know that emails used to deliver malware often look like emails from legitimate companies.

The operating system should be scanned for threats regularly. It is recommended to scan it with a reputable antivirus or anti-spyware software. 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.

Appearance of the hacker forum used to promote SHurk Steal malware (GIF):



Instant automatic malware removal:

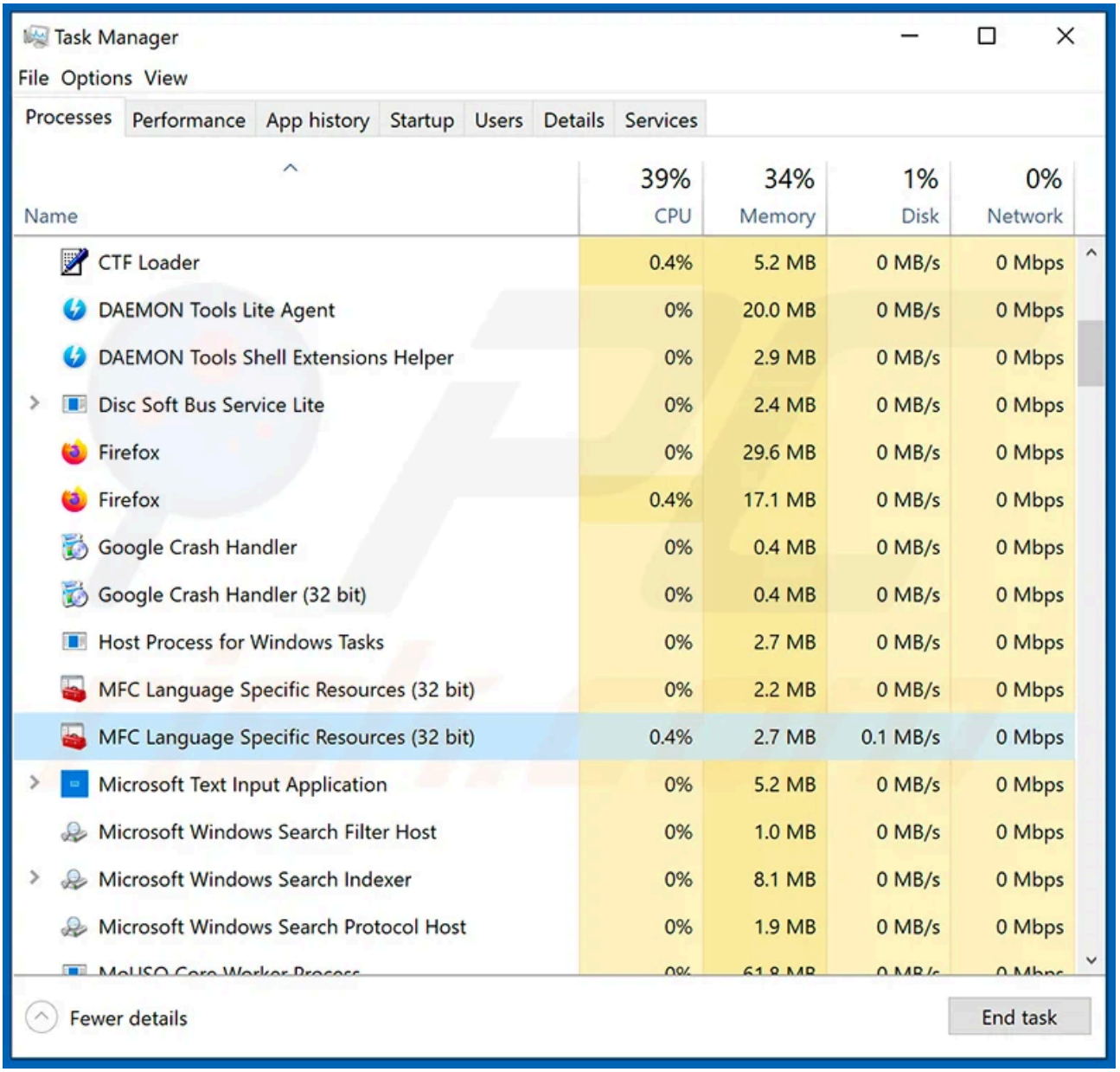
Manual threat removal might be a lengthy and complicated process that requires advanced IT skills. Combo Cleaner is a professional automatic malware removal tool that is recommended to get rid of malware. Download it by clicking the button below:

Quick menu:

How to remove malware manually?

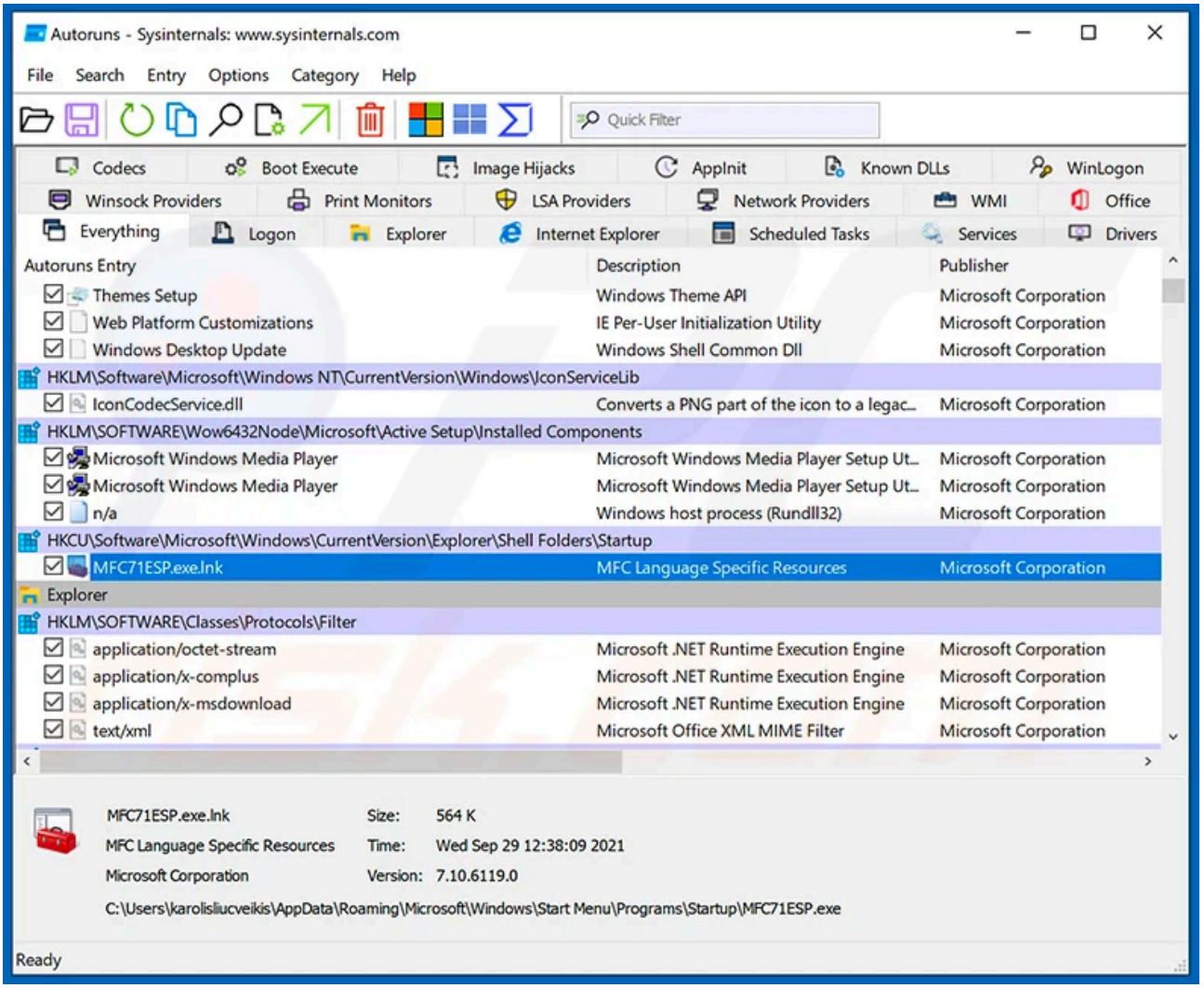
Manual malware removal is a complicated task - usually it is best to allow antivirus or anti-malware programs to do this automatically. To remove this malware we recommend using Combo Cleaner Antivirus for Windows.

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:



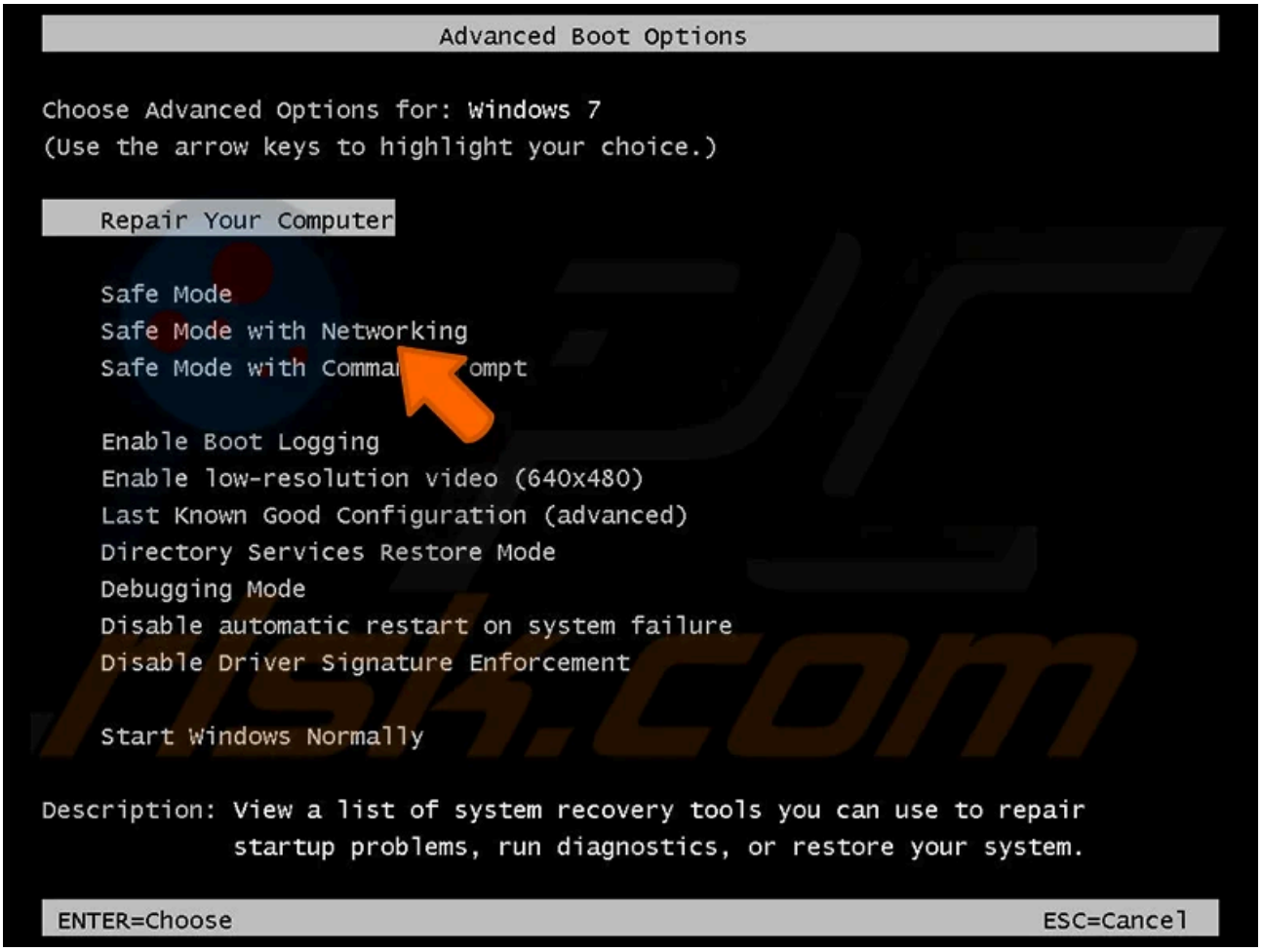
If you checked the list of programs running on your computer, for example, using task manager, and identified a program that looks suspicious, you should continue with these steps:

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.

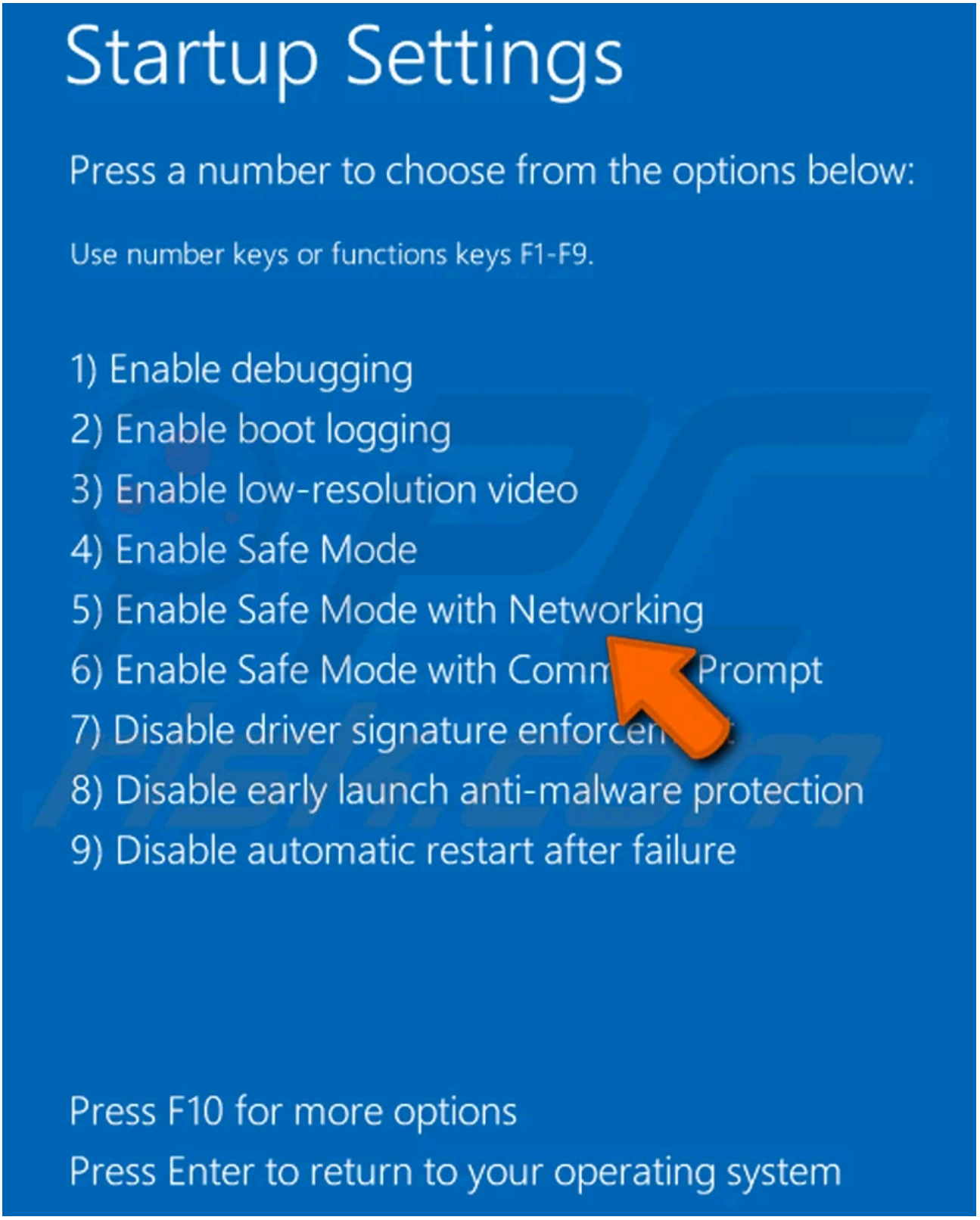


Video showing how to start Windows 7 in "Safe Mode with Networking":

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".

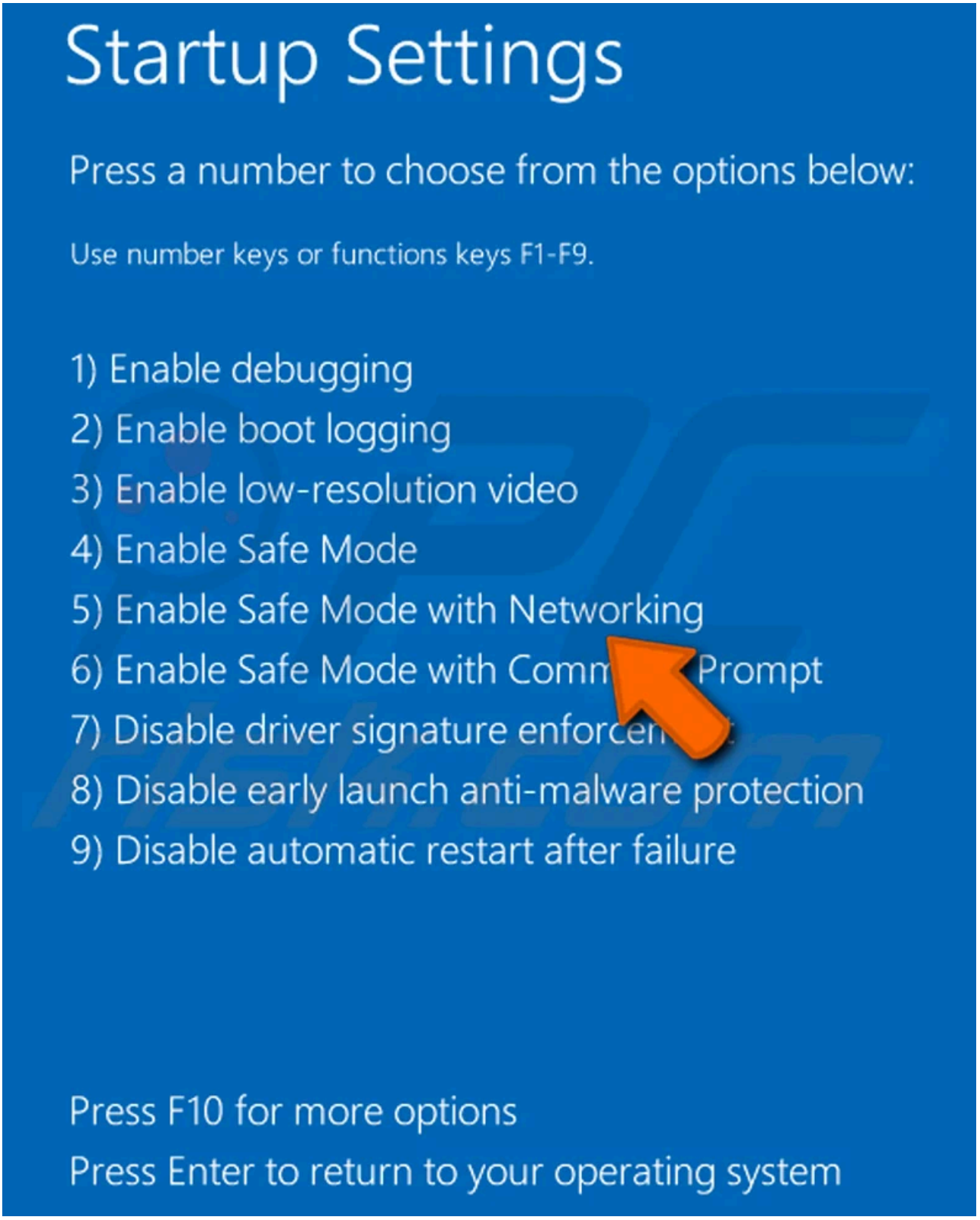
Click the "Restart" button. Your PC will restart into the Startup Settings screen. Press F5 to boot in Safe Mode with Networking.



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.



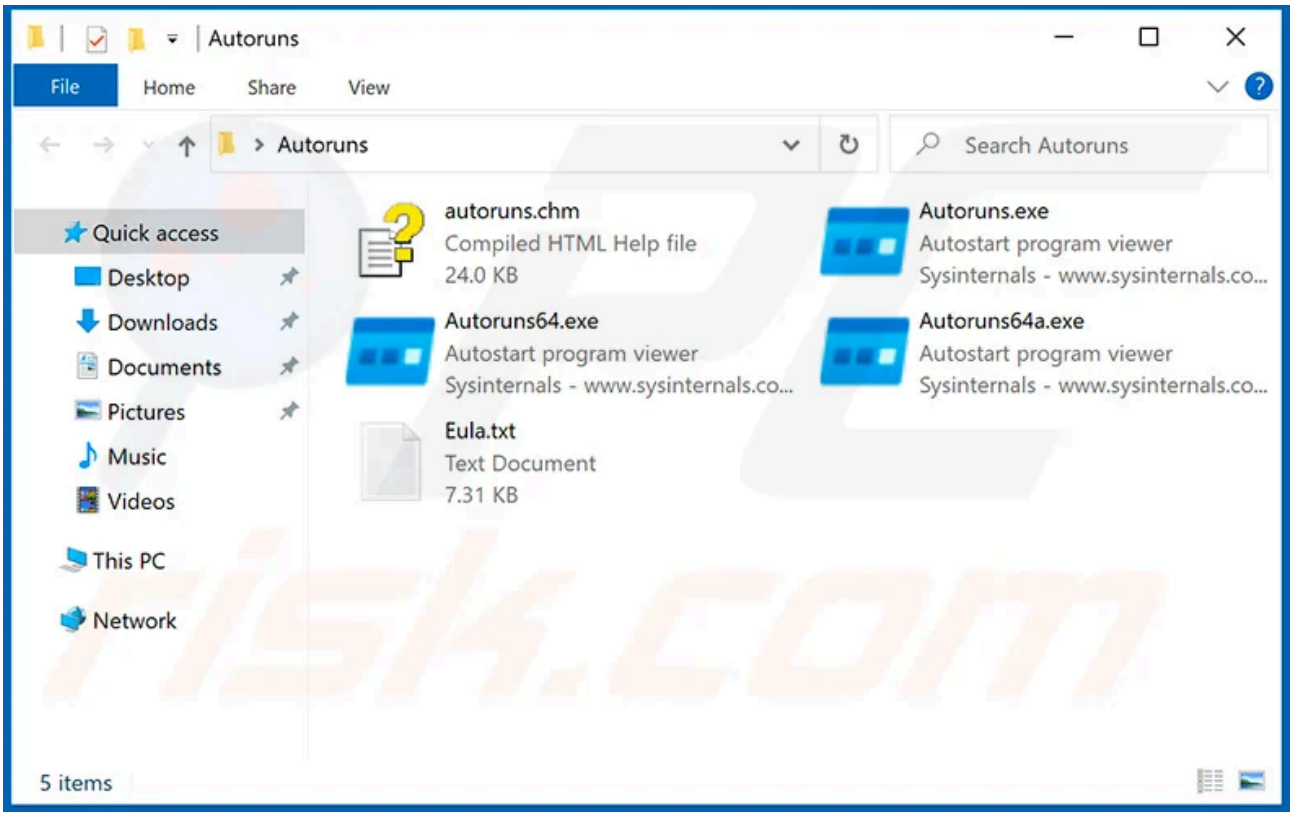
Video showing how to start Windows 10 in "Safe Mode with Networking":

Ett fel inträffade.

Det går inte att köra JavaScript.

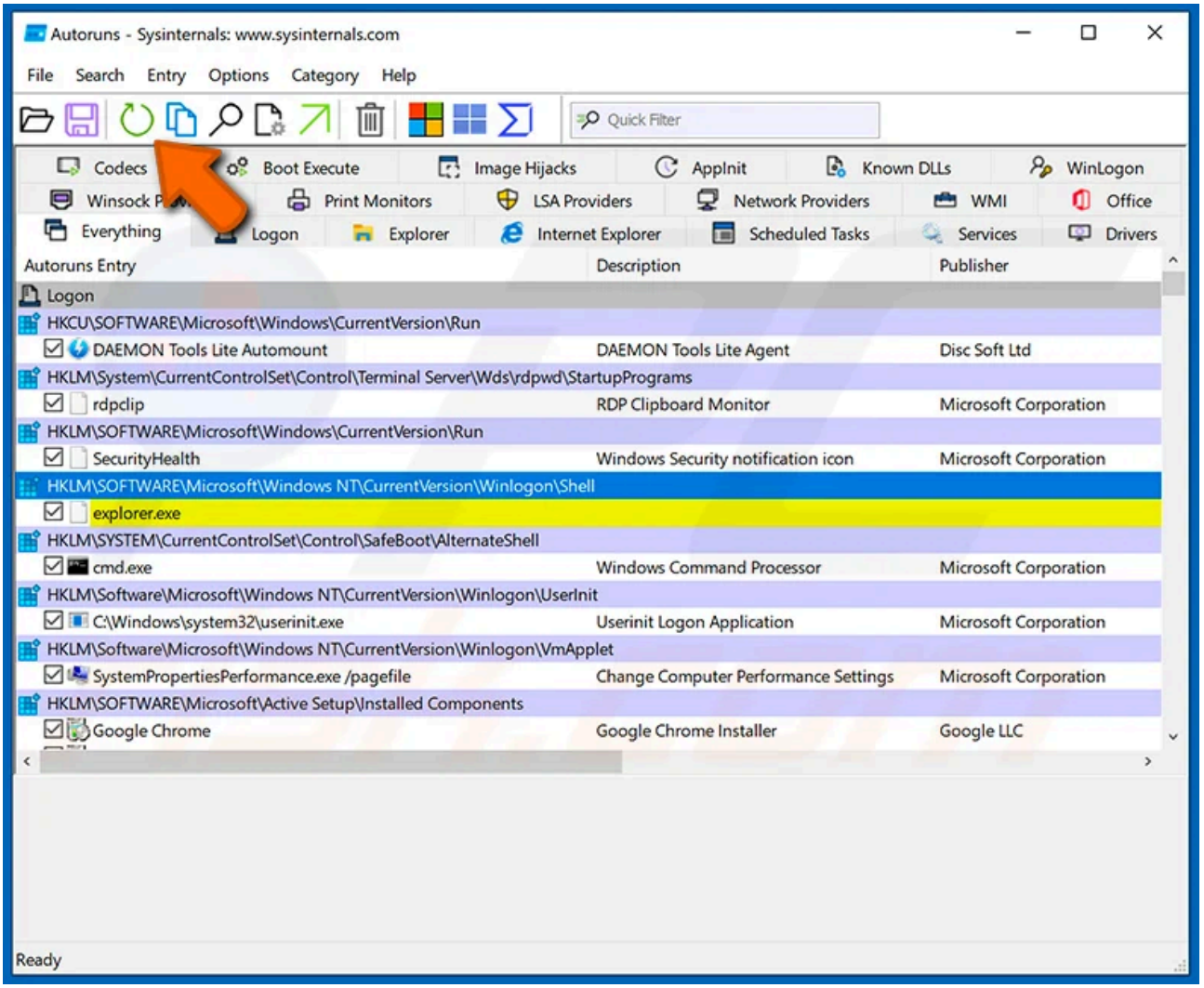
Step 3

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



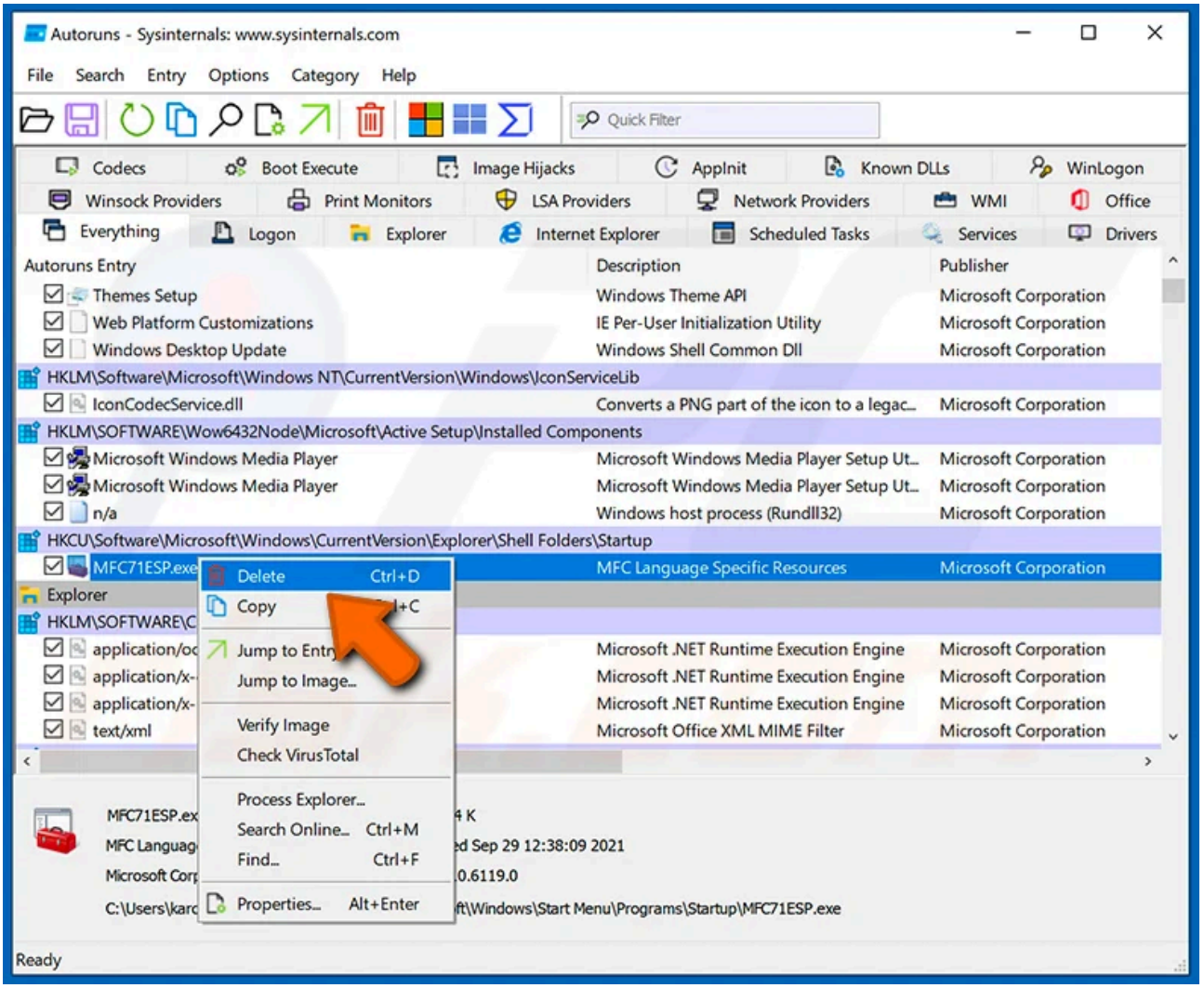
Step 4

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.

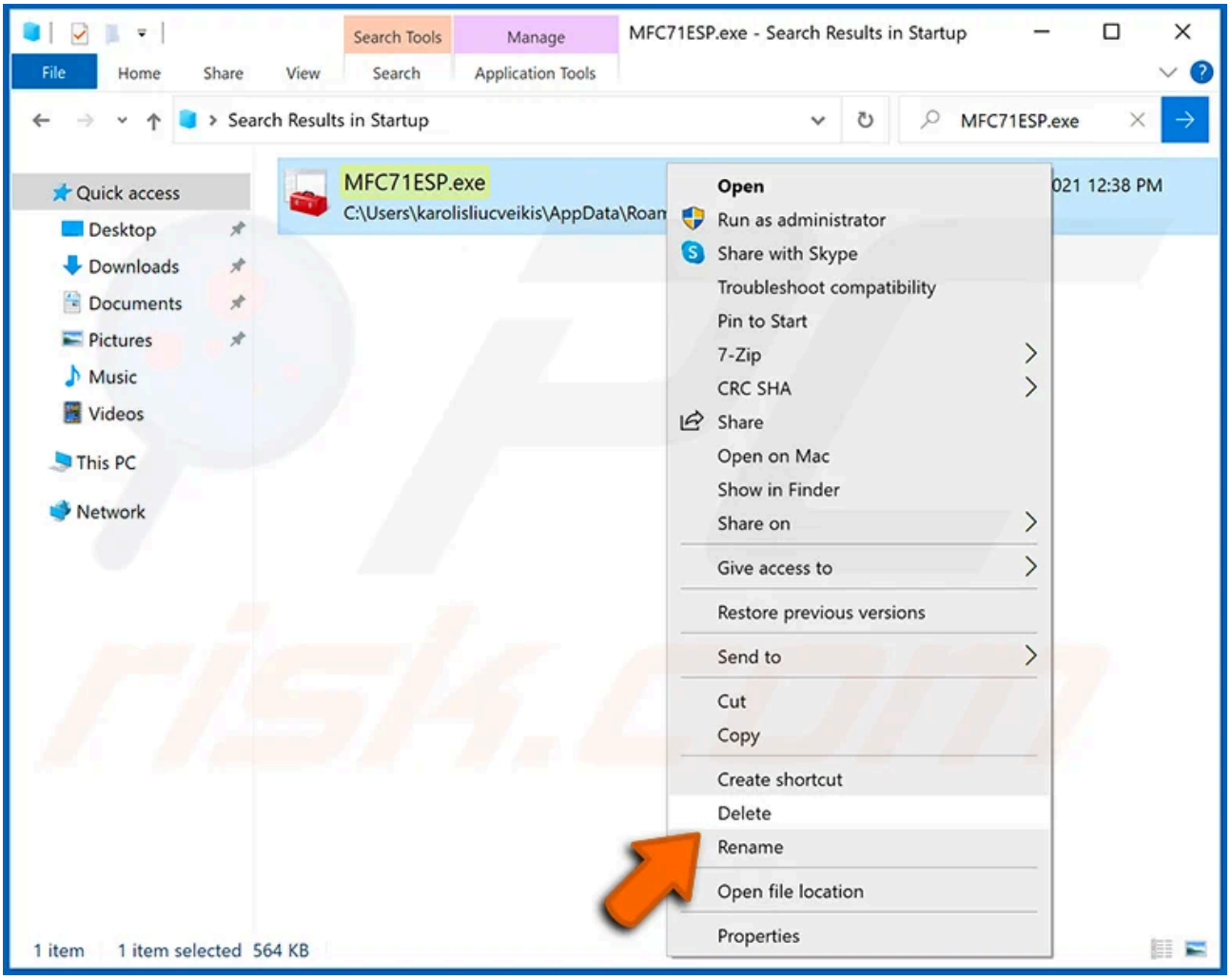


Check the list provided by the Autoruns application and locate the malware file that you want to eliminate.

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/21513-shurk-steal-malware