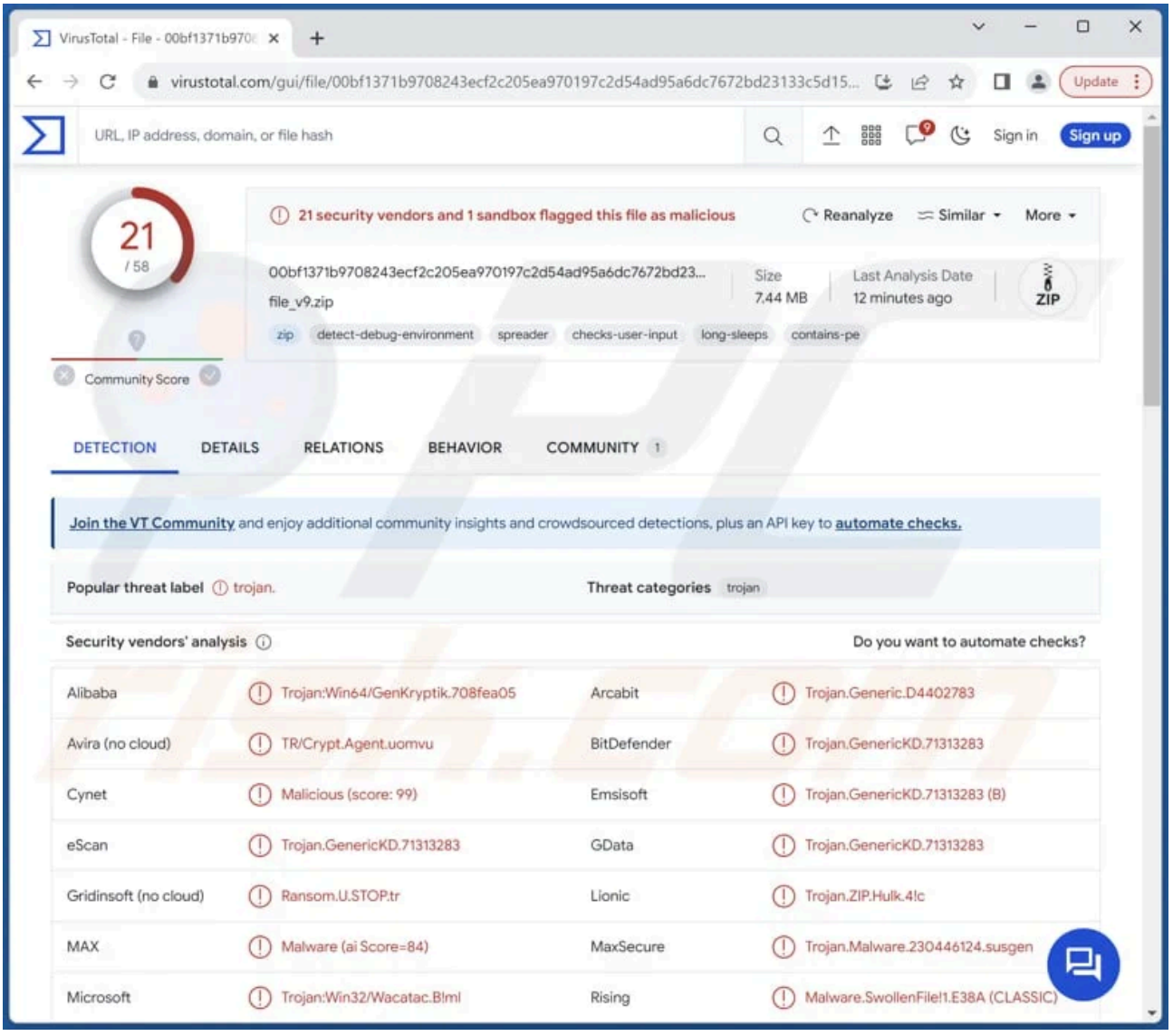
CrackedCantil Malware

By Tomas Meskauskas

Published: 2024-02-28 · Archived: 2026-04-05 16:03:37 UTC

What kind of malware is CrackedCantil?

CrackedCantil is a dropper malware designed to distribute a variety of malicious software, encompassing loaders, information stealers, cryptocurrency miners, proxy bots, and ransomware. The primary method of disseminating this malware involves leveraging cracked software on dubious websites or forums.



More about CrackedCantil

Upon downloading and executing an installer that appears legitimate, the user's computer becomes a target for malware infiltration. Upon activation, the malware initiates a system-wide infection, undertaking various actions

such as injecting additional malware, pilfering data, encrypting files for ransom, and assimilating the infected device into a botnet.

The intricacy of the incident involves a complex network of processes, with several notorious malware families identified as contributors. These include PrivateLoader, SmokeLoader, Lumma, RedLine, RisePro, Amadey, Stealc, Socks5Systemz, and STOP.

PrivateLoader is a malicious loader family notorious for disseminating a variety of malware, such as stealers, rootkits, and spyware. This loader commonly exploits cracked software as a prevalent avenue for infection. Furthermore, it deploys diverse payloads contingent on the victim's system configuration.

SmokeLoader, recognized as modular malware, is acknowledged for downloading additional malicious software and engaging in information theft. This versatile malware is capable of loading multiple files, executing them, emulating legitimate processes, and more. It employs the injection of malicious code into system processes such as "explorer.exe", enabling it to carry out nefarious activities while skillfully avoiding detection.

Lumma, an infostealer, possesses the capability to extract personal and financial data from diverse sources on compromised computers, encompassing web browsers, email clients, and cryptocurrency wallet files. Primarily disseminated through social engineering and phishing attacks, Lumma Stealer adeptly sidesteps antivirus detection and transmits the gathered data to a remote command and control (C&C) server.

RedLine functions as an infostealer, gathering a range of information including passwords, credit card details, cookies, and location data. Moreover, RedLine has the capability to serve as a conduit for additional malware, such as ransomware, RATs, trojans, miners, and various other threats.

RisePro is a data-stealing malware that specializes in harvesting sensitive information like credit card data, passwords, and cryptocurrency wallet details. It employs a sophisticated system of embedded DLL dependencies to execute its malicious activities.

Amadey proves to be a highly adaptable malware with dual roles as both a loader and an infostealer. Its capabilities extend across a diverse range of malicious activities, spanning from reconnaissance and data exfiltration to the deployment of additional payloads.

Stealc is an information-stealing malware that specializes in extracting sensitive data from browsers, transmitting the pilfered information to its Command and Control (C2) through HTTP POST requests. The evolution of Stealc hinges on collaborative efforts with other stealers like Vidar, Racoon, RedLine, and Mars.

Socks5Systemz employs PrivateLoader and Amadey as vectors for infecting devices. Once compromised, these devices are transformed into proxies, forwarding malicious traffic. The malware maintains communication with its Command and Control (C2) server through a Domain Generation Algorithm (DGA).

STOP, a ransomware strain encrypting user data, has a variant known as Djvu, which incorporates multiple obfuscation layers for enhanced analysis complexity. STOP/Djvu employs encryption algorithms like AES-256 and Salsa20. Notably, DJVU collaborates with other malware, such as infostealer malware, to exfiltrate sensitive information before initiating the encryption process.

Threat Summary:

Name	CrackedCantil dropper
Threat Type	Dropper
Detection Names	Alibaba (Trojan:Win64/GenKryptik.708fea05), Combo Cleaner (Trojan.GenericKD.71313283), ESET-NOD32 (A Variant Of Win64/GenKryptik.GPXJ), MaxSecure (Trojan.Malware.230446124.susgen), Microsoft (Trojan:Win32/Wacatac.B!ml), Full List (VirusTotal)
Malicious Process Name(s)	Numerous proceesses with random names or names of non-existent programs (or programs that are not currently installed)
Payload	PrivateLoader, SmokeLoader, Lumma, RedLine, RisePro, Amadey, Stealc, Socks5Systemz, and STOP.
Symptoms	Droppers tend to be 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	Dubious websites and formus, software 'cracks', pirated software.
Damage	Stolen passwords and banking information, identity theft, the victim's computer added to a botnet, data encryption, monetary loss, privacy breaches, and more.
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.

Conclusion

In conclusion, the commencement of this malware narrative, triggered by CrackedCantil, sets in motion a series of escalating threats. Malicious programs like Lumma, Amadey, and Stealc, acting as loaders and infostealers, along

with the collaborative initiatives of Socks5Systemz, add to the increasing complexity.

The potential dangers cover a wide spectrum, including data loss, privacy breaches, system disruptions, and financial consequences. These risks emphasize the comprehensive impact introduced by CrackedCantil.

How did CrackedCantil infiltrate my computer?

CrackedCantil typically infiltrates computers through a deceptive process initiated by the user's pursuit of cracked software. Individuals seeking free versions of paid software often download "cracked" versions, applications modified to circumvent licensing mechanisms. Exploiting this demand, attackers employ cracked software as a vehicle to propagate malware.

The infection chain commences on dubious websites or forums that host these cracked versions. Users, lured by the promise of free software, unwittingly download what appears to be an installer. However, this seemingly innocent installer is a gateway for CrackedCantil to establish itself on the user's computer. The malware may cloak itself as useful files or integrate into the installation executables, remaining undetected during installation.

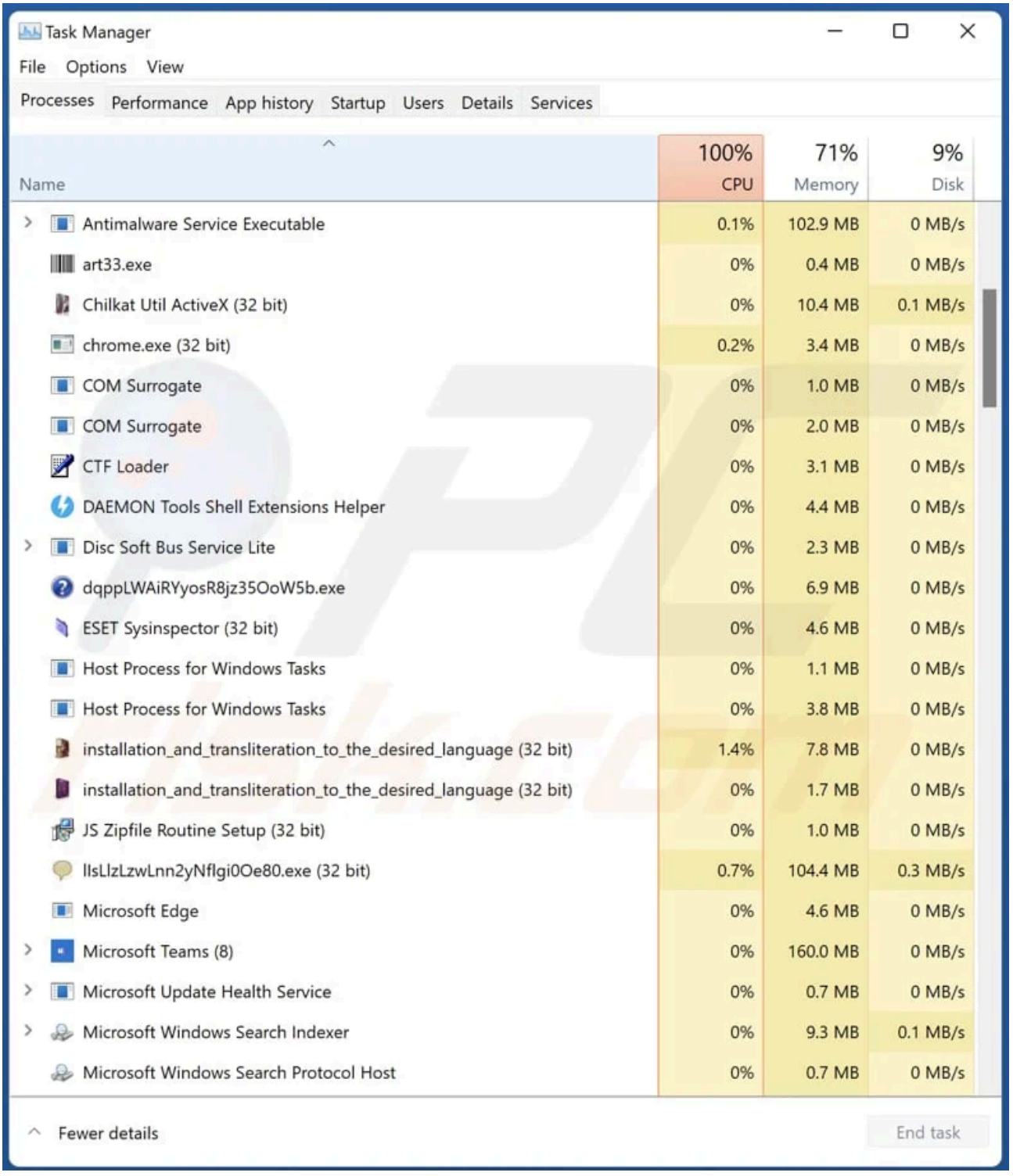
Once activated, CrackedCantil initiates a series of actions to infect the system comprehensively. This includes installing additional malware, pilfering data, encrypting files for ransom, and potentially converting the infected device into a component of a botnet.

How to avoid installation of malware?

Stick to reputable sources, such as official websites or authorized app stores, to ensure the legitimacy of the software. Avoid downloading cracked or pirated versions of paid software, as these often serve as vectors for malware. Keep your operating system, antivirus software, and other applications up to date.

Be wary of clicking suspicious links, ads, and pop-ups, especially on shady websites, or downloading attachments in irrelevant or unexpected emails from unknown addresses. Use a reliable antivirus solution and scan your computer 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.

Processes in the Task Manager with random names or names of non-existent programs (or programs that are not currently installed) initiated by CrackedCantil:



Dubious pages hosting cracked software distributing CrackedCantil:



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

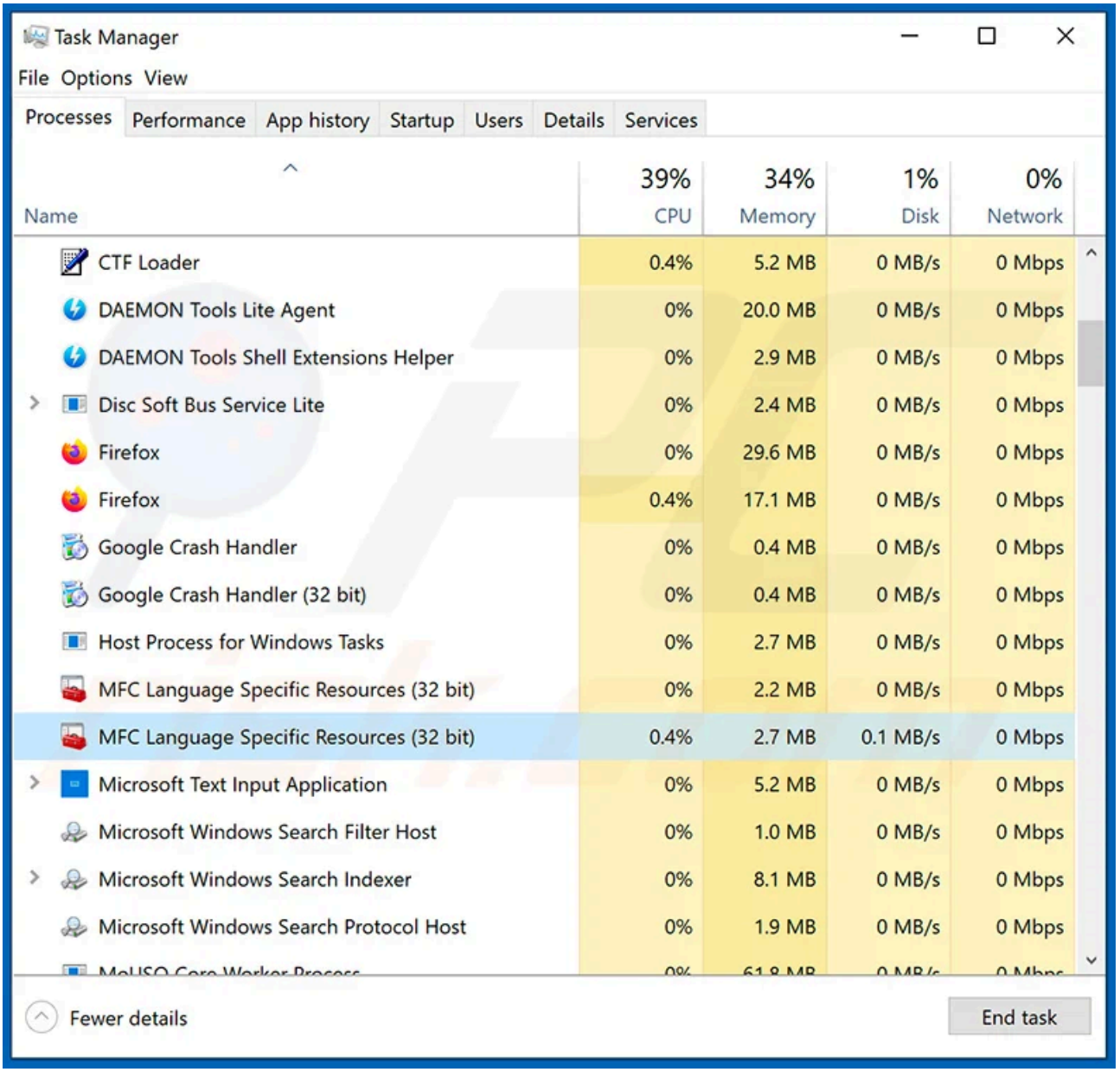
By downloading any software listed on this website you agree to our Privacy Policy and Terms of Use. To use full-featured product, you have to purchase a license for Combo Cleaner. 7 days free trial available. Combo Cleaner is owned and operated by RCS LT, the parent company of PCRisk.com.

Quick menu:

How to remove malware manually?

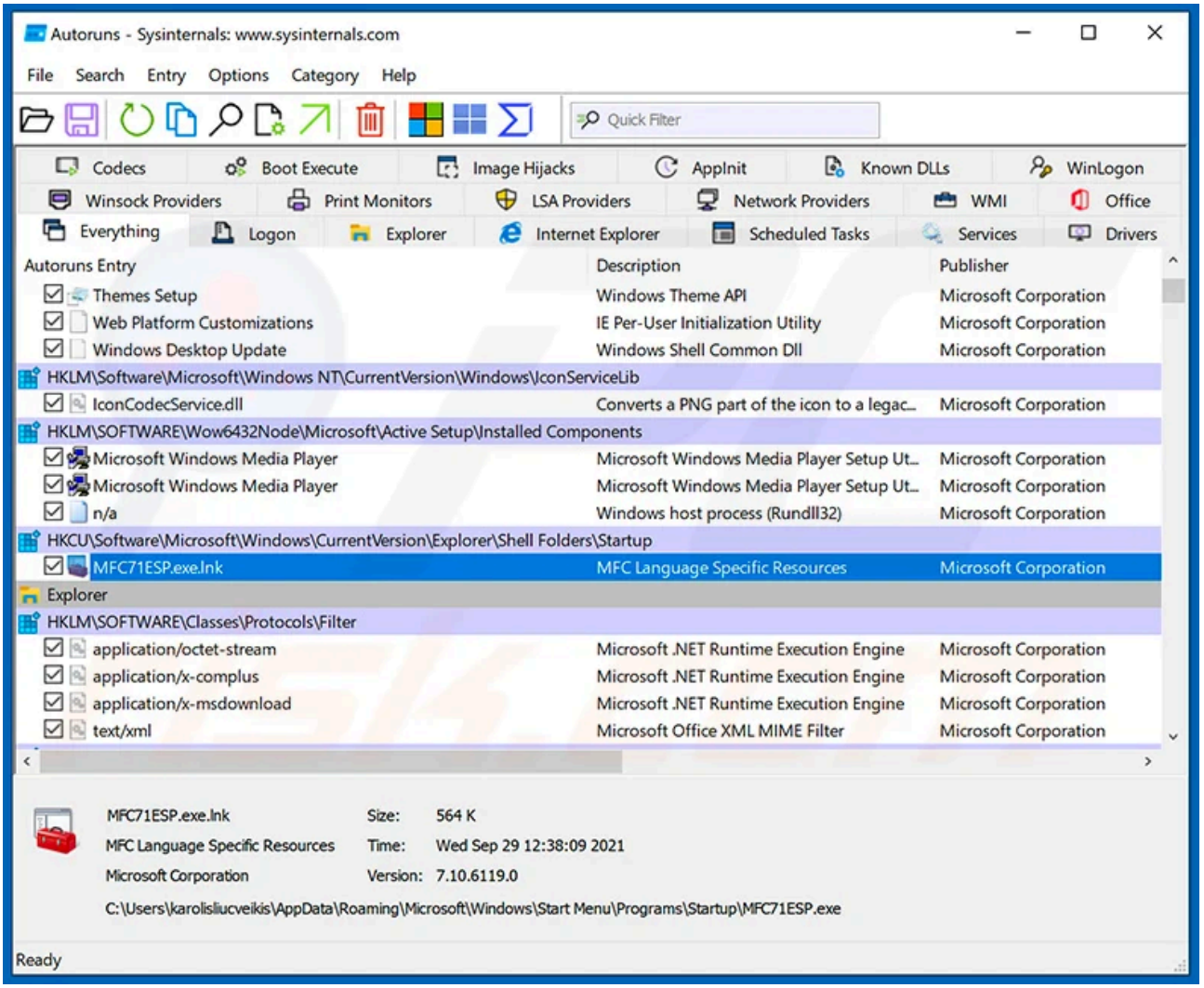
Manual malware removal is a complicated task - usually it is best to allow antivirus or anti-malware programs to do this automatically. To remove this malware we recommend using Combo Cleaner Antivirus for Windows.

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:



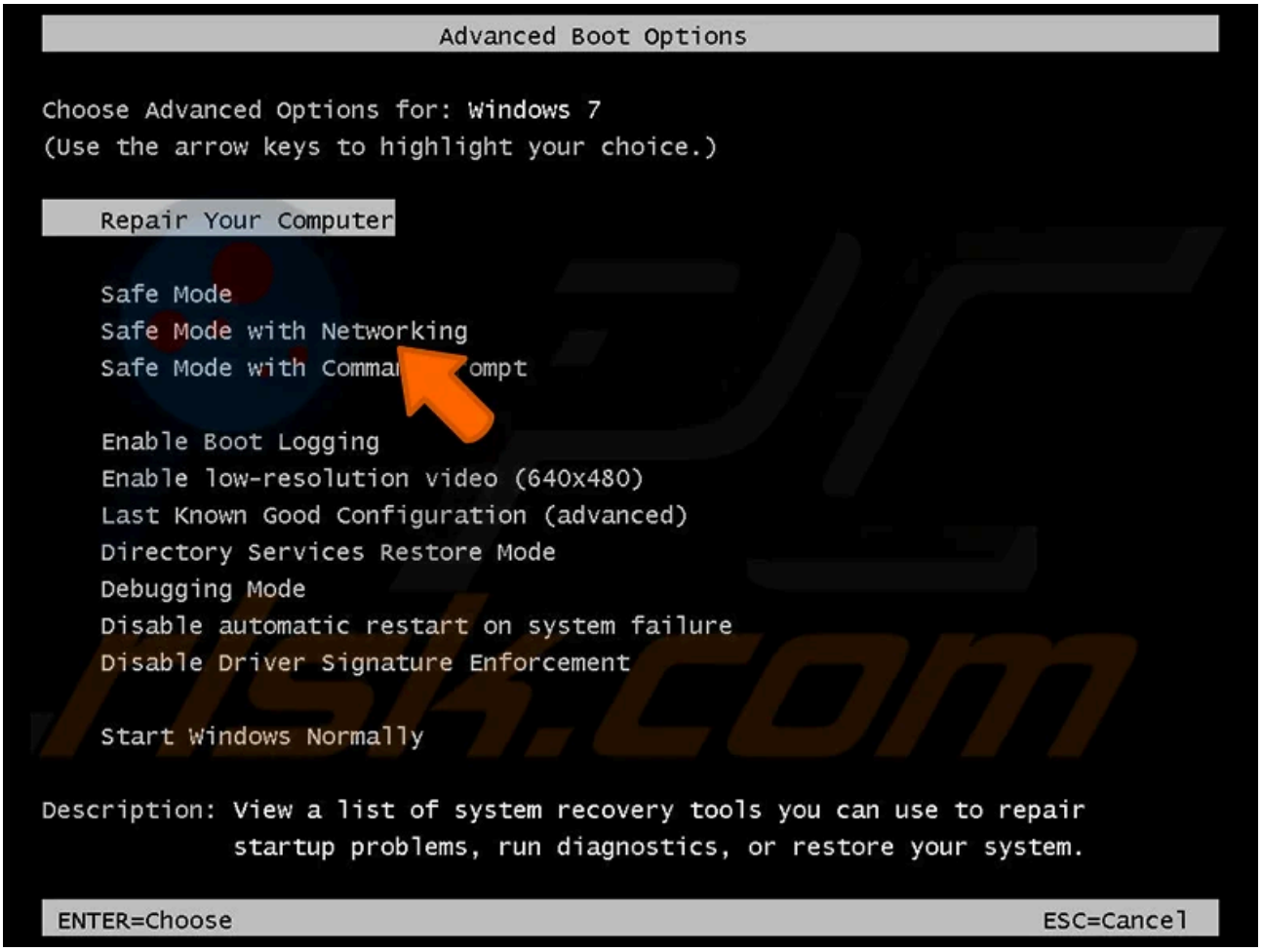
If you checked the list of programs running on your computer, for example, using task manager, and identified a program that looks suspicious, you should continue with these steps:

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.

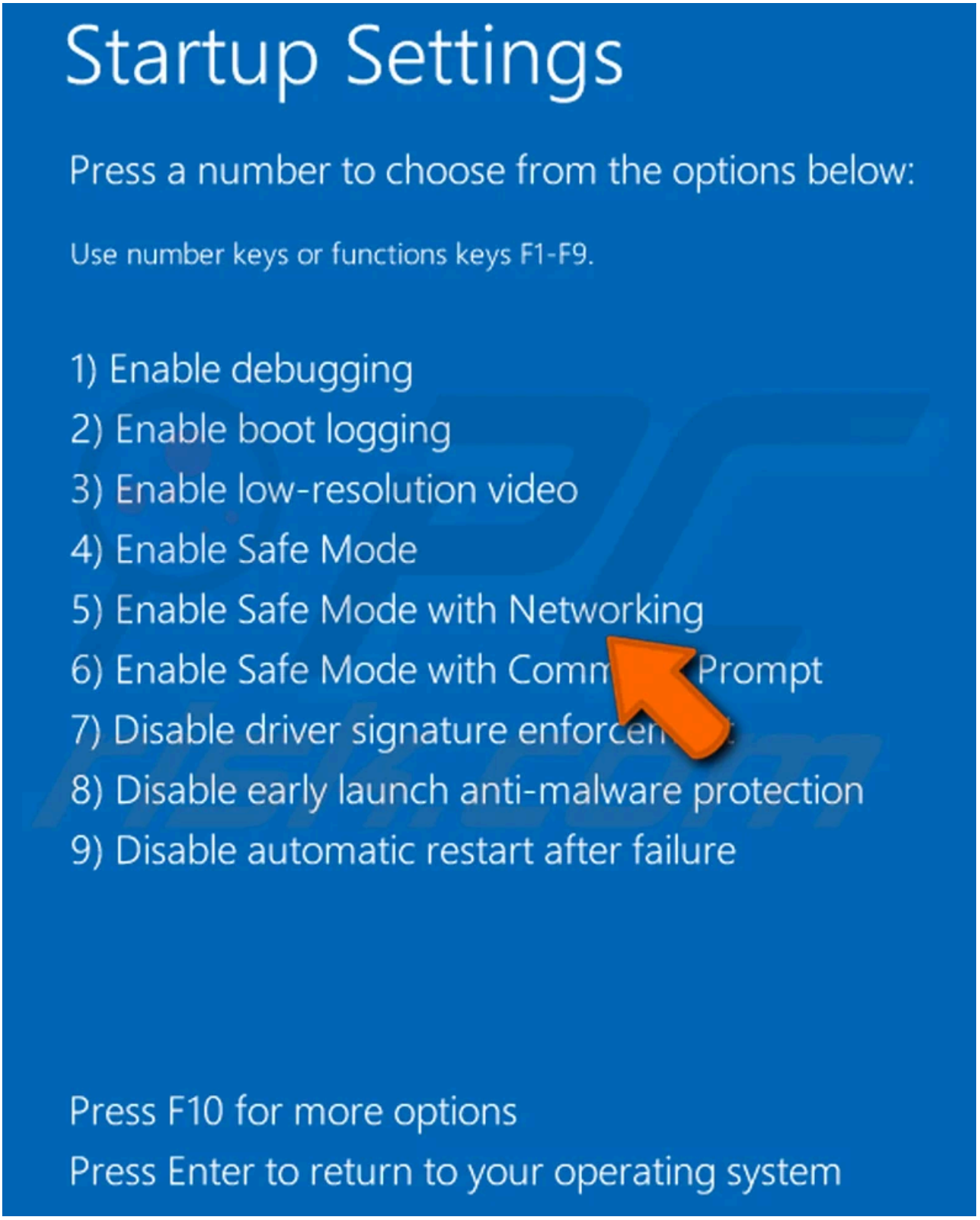


Video showing how to start Windows 7 in "Safe Mode with Networking":

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".

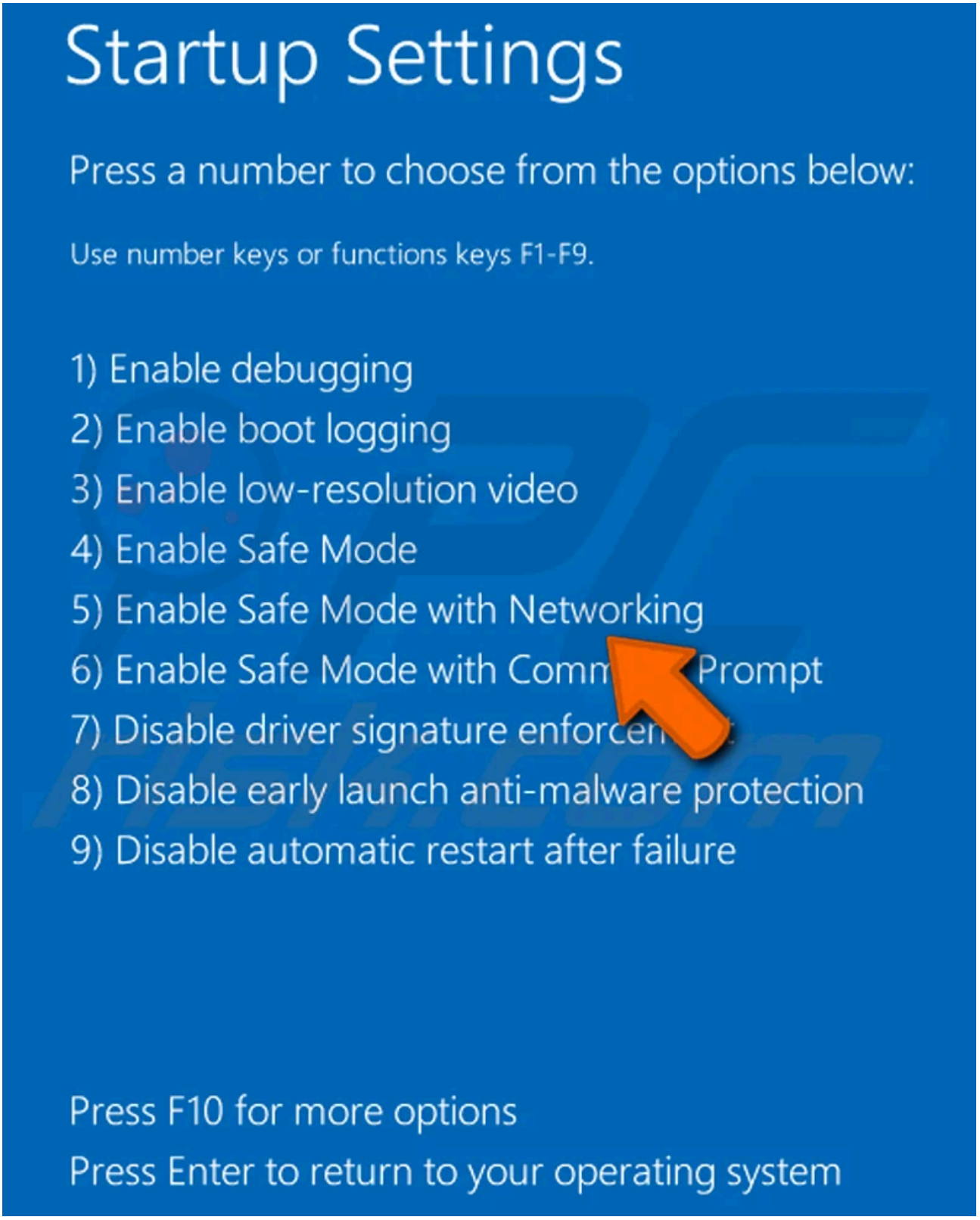
Click the "Restart" button. Your PC will restart into the Startup Settings screen. Press F5 to boot in Safe Mode with Networking.



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.



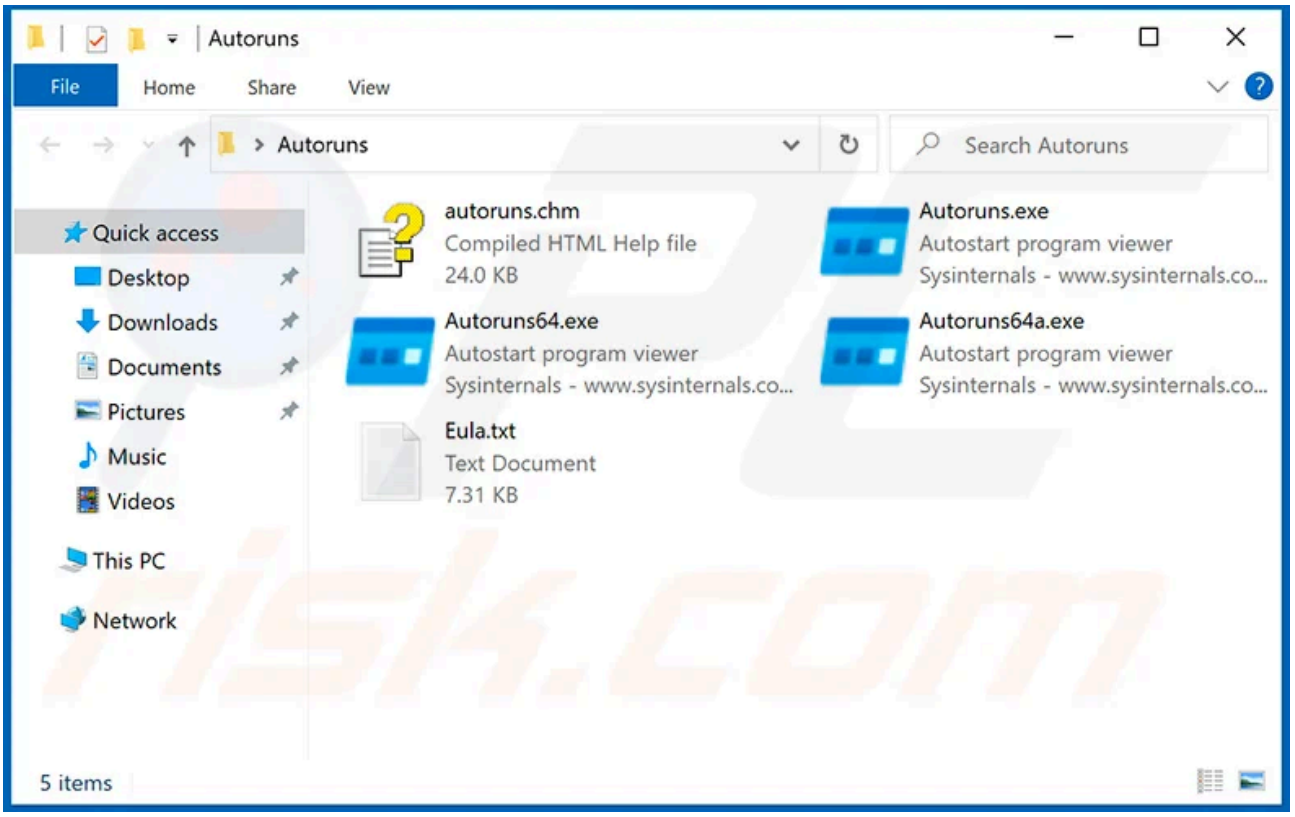
Video showing how to start Windows 10 in "Safe Mode with Networking":

Ett fel inträffade.

Det går inte att köra JavaScript.

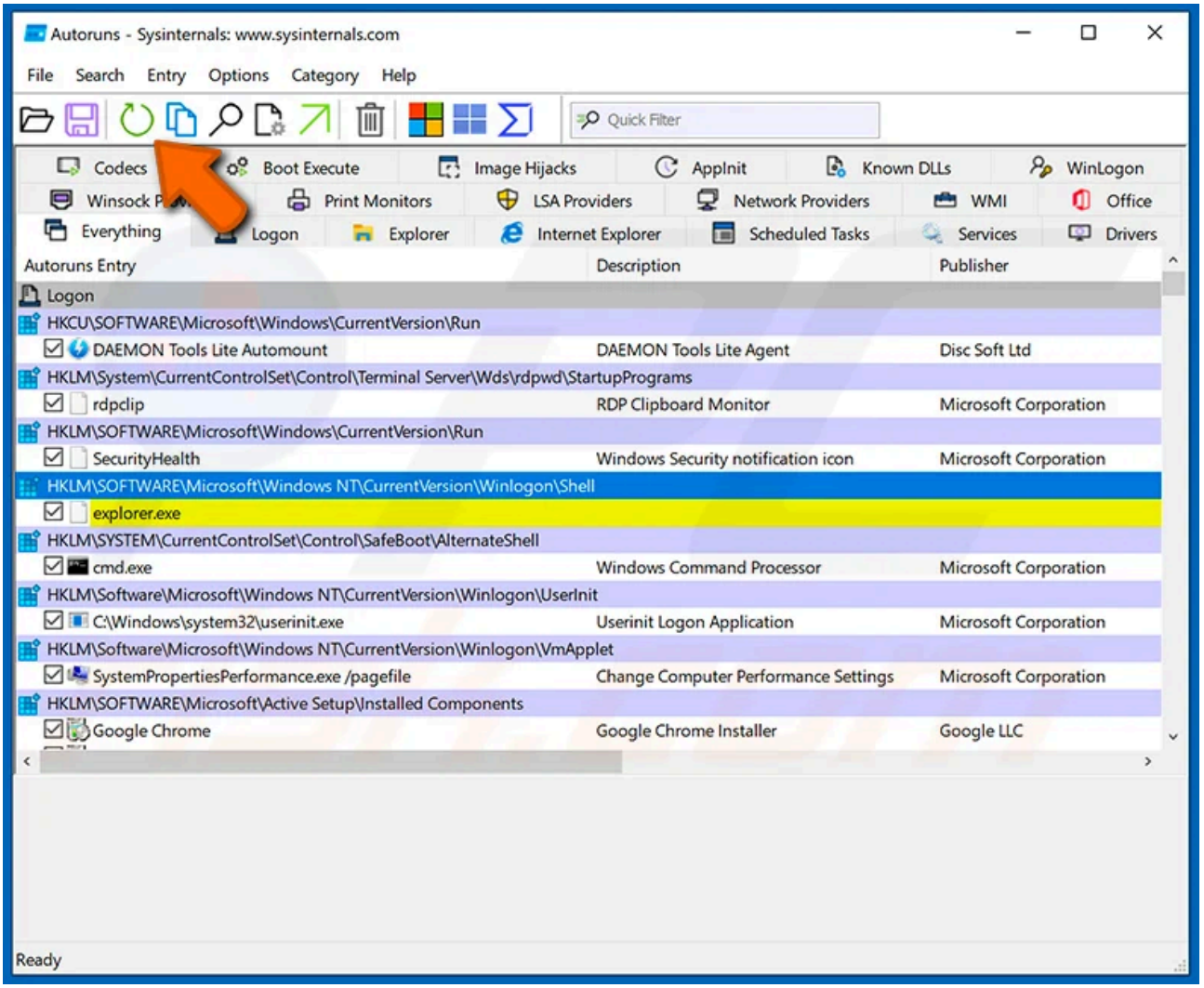
Step 3

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



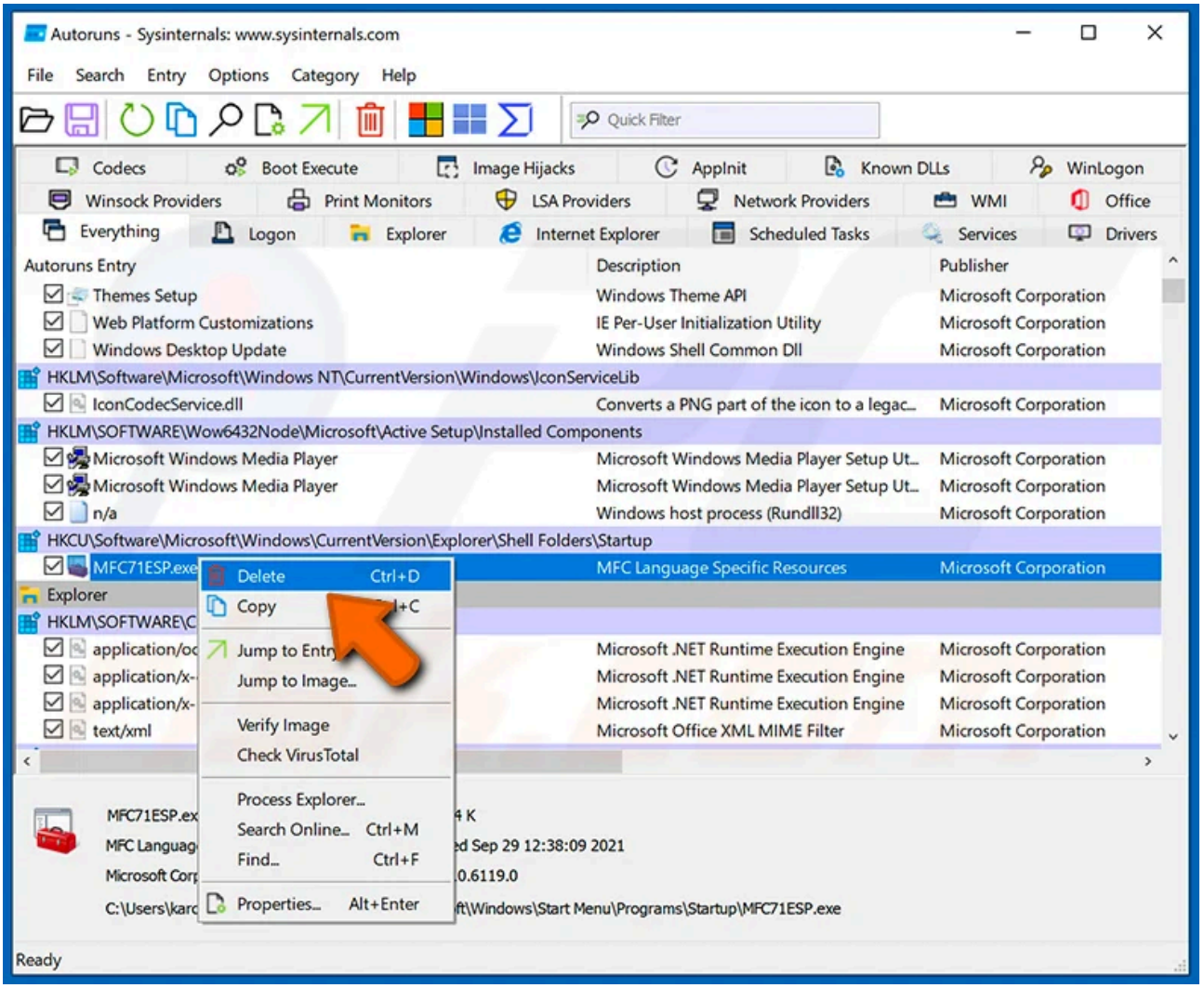
Step 4

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.

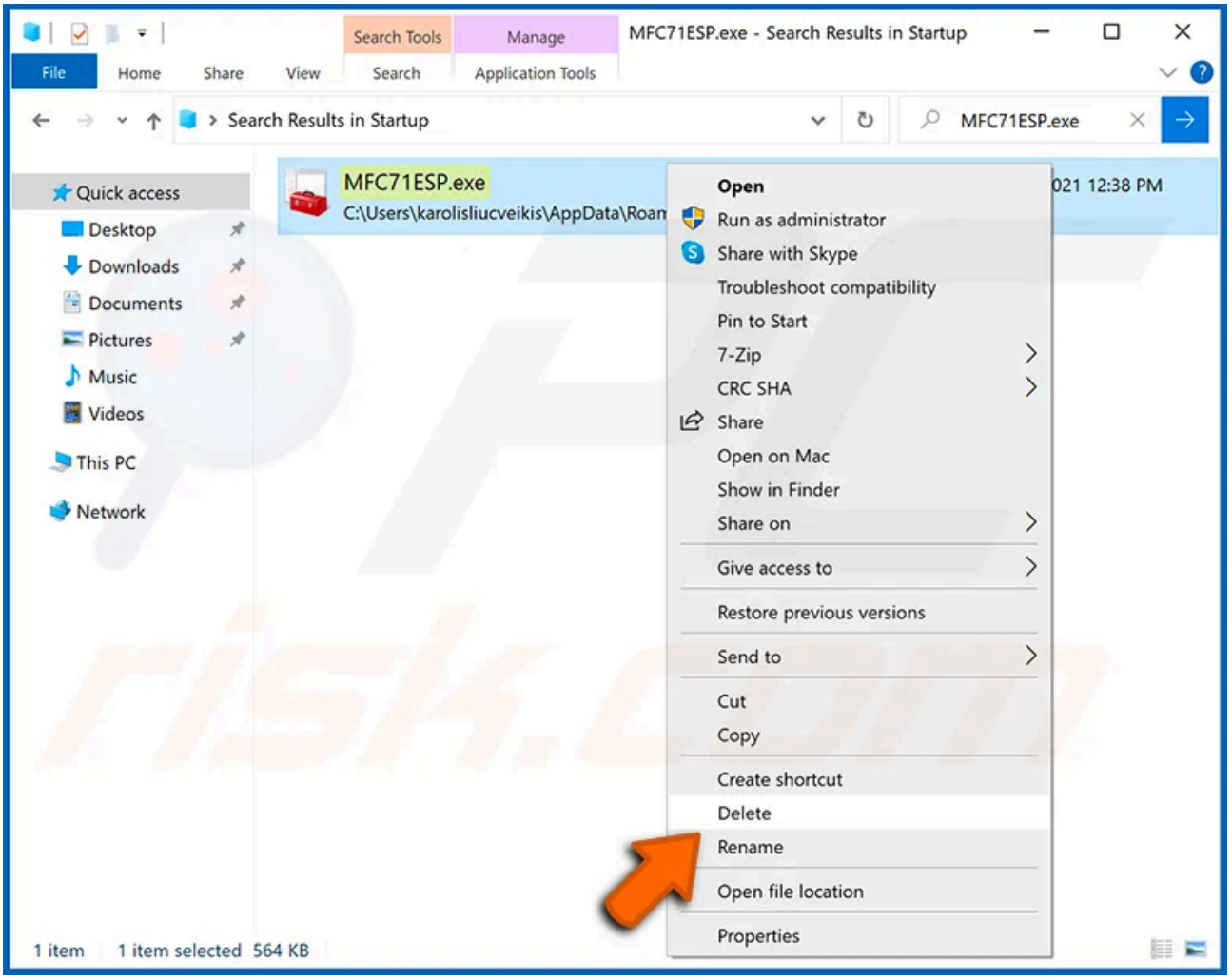


Check the list provided by the Autoruns application and locate the malware file that you want to eliminate.

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.

Frequently Asked Questions (FAQ)

My computer is infected with CrackedCantil malware, should I format my storage device to get rid of it?

Before resorting to formatting your storage device, it is advisable to initiate a scan using a reliable antivirus or anti-malware program. These tools are designed to detect and remove various types of malware, offering a less intrusive solution compared to formatting.

What are the biggest issues that malware can cause?

Malware can lead to significant issues such as unauthorized access to sensitive data, financial losses through activities like ransomware, and the disruption of critical system functions, potentially causing downtime and

operational setbacks. Additionally, malware can compromise user privacy, leading to identity theft and other forms of cyber threats.

What is the purpose of CrackedCantil?

The primary purpose of CrackedCantil is to act as a dropper malware, facilitating the distribution of various types of malicious software (including PrivateLoader, SmokeLoader, Lumma, RedLine, RisePro, Amadey, Stealc, Socks5Systemz, and STOP).

How did CrackedCantil infiltrate my computer?

CrackedCantil typically targets users who seek cracked or pirated versions of paid software. It exploits the demand for such software by providing seemingly legitimate but modified versions that bypass licensing mechanisms. Once a user downloads and runs what appears to be an installer for cracked software, CrackedCantil takes advantage of this opportunity to infiltrate the user's computer.

Will Combo Cleaner protect me from malware?

Certainly, Combo Cleaner can identify and remove nearly all recognized malware infections. It is important to note that sophisticated malware often conceals itself deeply within the system, emphasizing the necessity of conducting a full system scan.
