Matiex Keylogger

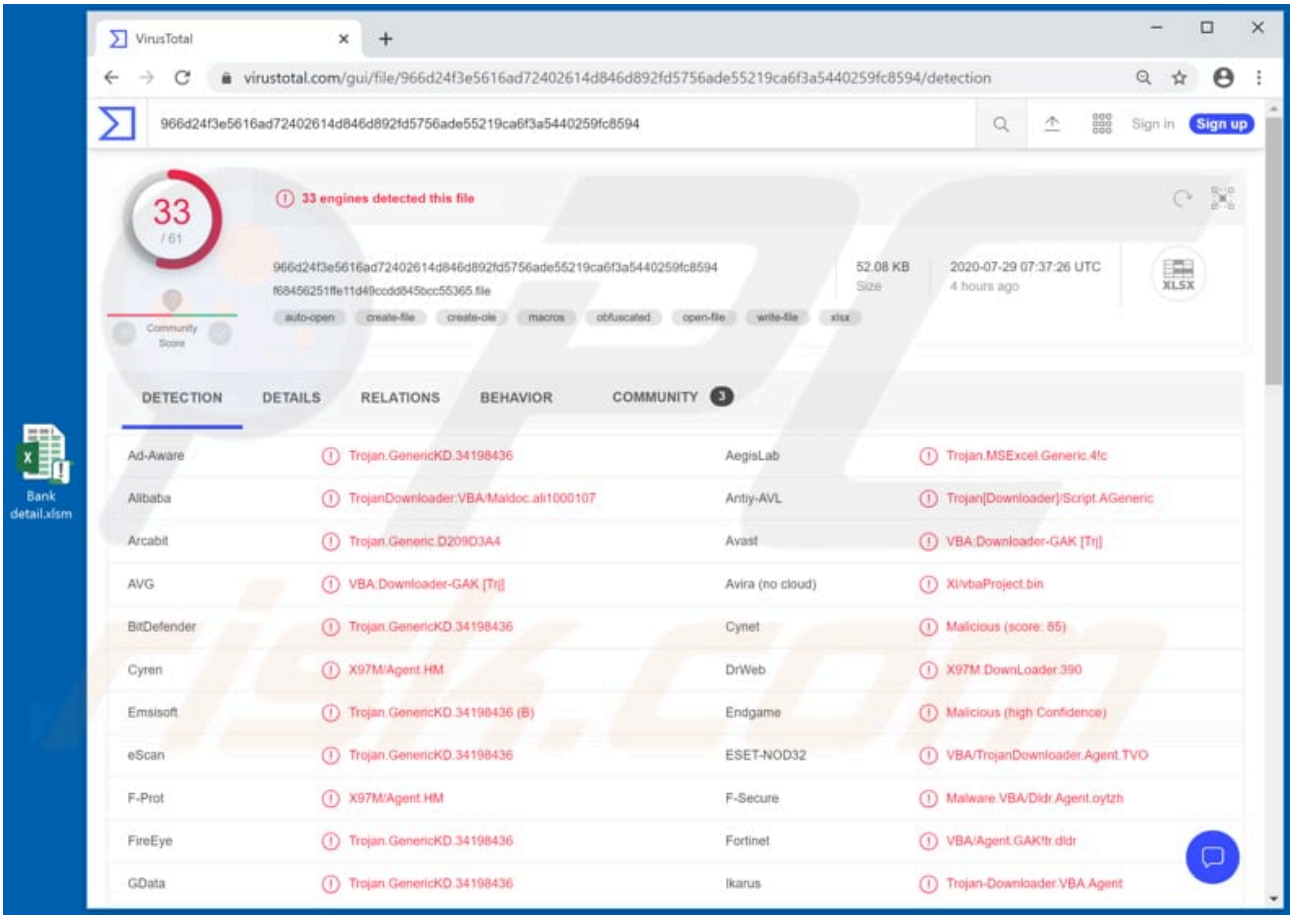
By Tomas Meskauskas

Published: 2025-06-09 · Archived: 2026-04-05 19:55:29 UTC

What is Matiex?

Matiex is a keystroke logger which is capable of taking screenshots, recording sound with the computer microphone and data saved in the system clipboard. Its users can receive logged data via Telegram, SMTP, FTP and Discord. Research shows that this keystroke logger can be purchased for US$25, $60, or $99 depending on the subscription plan.

Generally, cyber criminals attempt to deceive users into installing this software on their computers in order to steal sensitive information, which can then be misused to generate revenue.



Matiex malware overview

A keylogger is a type of software that is often used by cyber criminals to monitor and record each keystroke typed on an infected computer's keyboard. In most cases, cyber criminals seek to steal information such as logins, passwords (and other credentials), credit card details, and other personal, sensitive details.

This particular keylogger can be used to take screenshots, access and use the computer microphone and steal data saved on the operating system clipboard. Therefore, cyber criminals behind Matiex can misuse stolen information and/or access other data to steal identities, personal accounts, make fraudulent purchases and transactions, and for other malicious purposes.

Additionally, Matiex is capable of generating fake message boxes (pop-ups) containing any text. It also includes a "self destruct" feature, which allows this keylogger to uninstall itself at a certain designated time. If there is any reason to suspect that Matiex or other malware of this type is installed on your computer, remove it immediately.

Having a computer infected with a keylogger can be the reason behind serious issues such as identity theft, monetary loss, loss of access to personal and important online accounts, etc.

Threat Summary:

Name	Matiex keystroke logger
Threat Type	Keylogger, password-stealing virus, banking malware, spyware.
Detection Names	Avast (VBA:Downloader-GAK [Trj]), BitDefender (Trojan.GenericKD.34198436), ESET-NOD32 (VBA/TrojanDownloader.Agent.TVO), Kaspersky (HEUR:Trojan-Downloader.MSOffice.SLoad.gen), Full List (VirusTotal)
Symptoms	Keyloggers 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.

Similar malware examples

Hakops, Amadey and Cheetah are some of examples of other malicious programs that function as keyloggers. In most cases, cyber criminals attempt to trick users into installing this software so that they can steal information and misuse it to generate as much revenue as possible.

There are many legitimate keyloggers on the web, however, in some cases, cyber criminals use them to monitor victims. I.e., legitimate keyloggers can be used for malicious purposes.

How did Matiex infiltrate my computer?

Research shows that cyber criminals use malspam email campaigns to deceive users into installing Matiex on their computers. I.e., they send emails that contain a malicious attachment, a Microsoft Office Excel document capable of installing Matiex, but only if users open it and enable editing/content (macros commands).

Malicious documents opened with Microsoft Office versions that were released before 2010 infect computers automatically without asking any permissions. Microsoft Office 2010 and newer versions include "Protected View" mode, which prevents malicious documents from installing malware automatically.

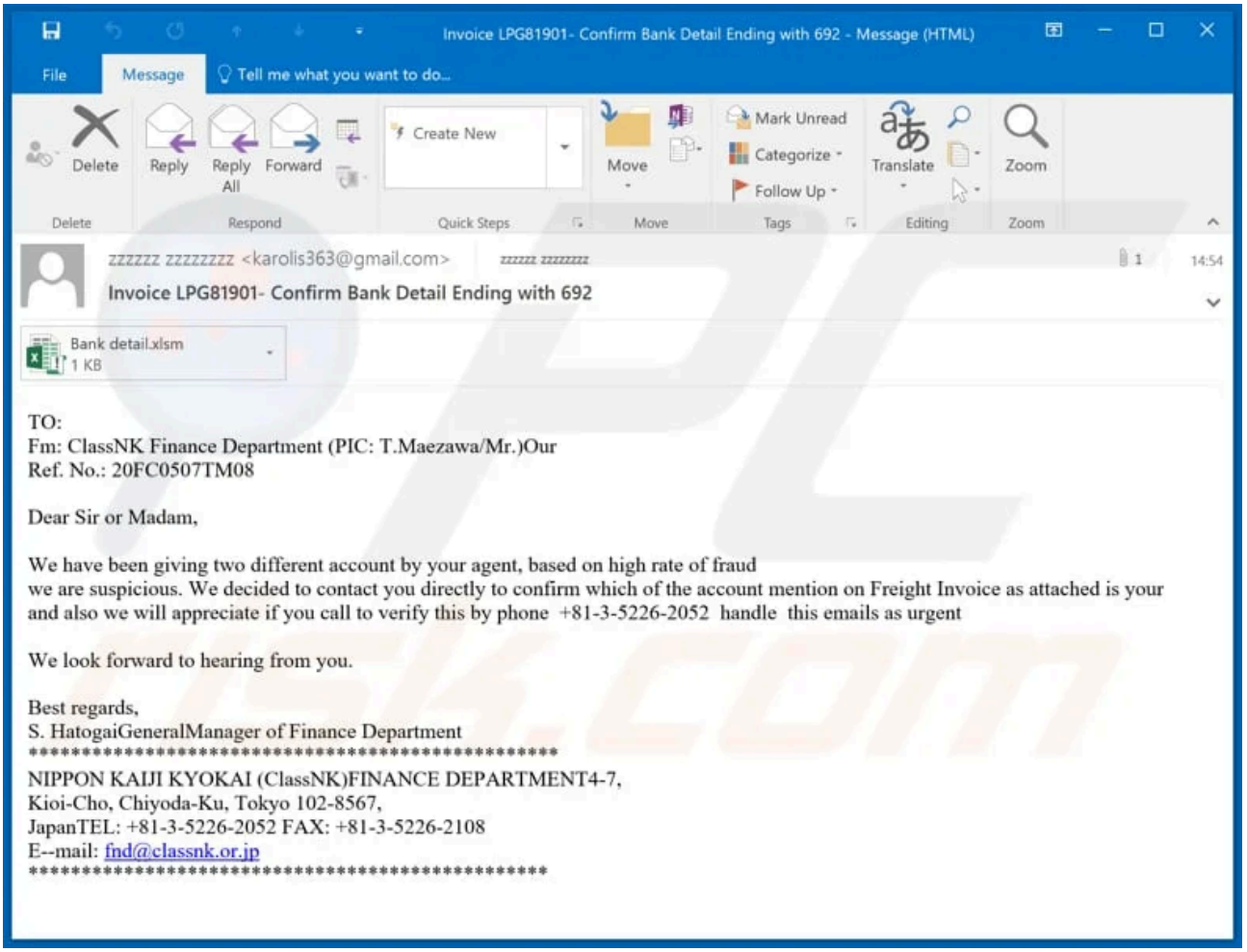
How to avoid installation of malware

You are strongly advised to ignore irrelevant emails that contain attachments or web links. Note that users often receive malspam campaign emails from unknown, suspicious addresses. The emails are often disguised as important and official as if sent from legitimate companies/organizations.

Furthermore, software and files should not be downloaded or installed via third party downloaders/installers, Peer-to-Peer networks, unofficial sites, unofficial pages, free file hosting sites, etc. Use official websites and direct links. It is also important to update and activate installed software only with tools or implemented functions that are designed by official software developers.

It is illegal to activate any licensed programs with 'cracking' tools. Finally, computers are safer when regularly scanned with reputable anti-spyware or antivirus 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.

Malicious email used to distribute Matiex:

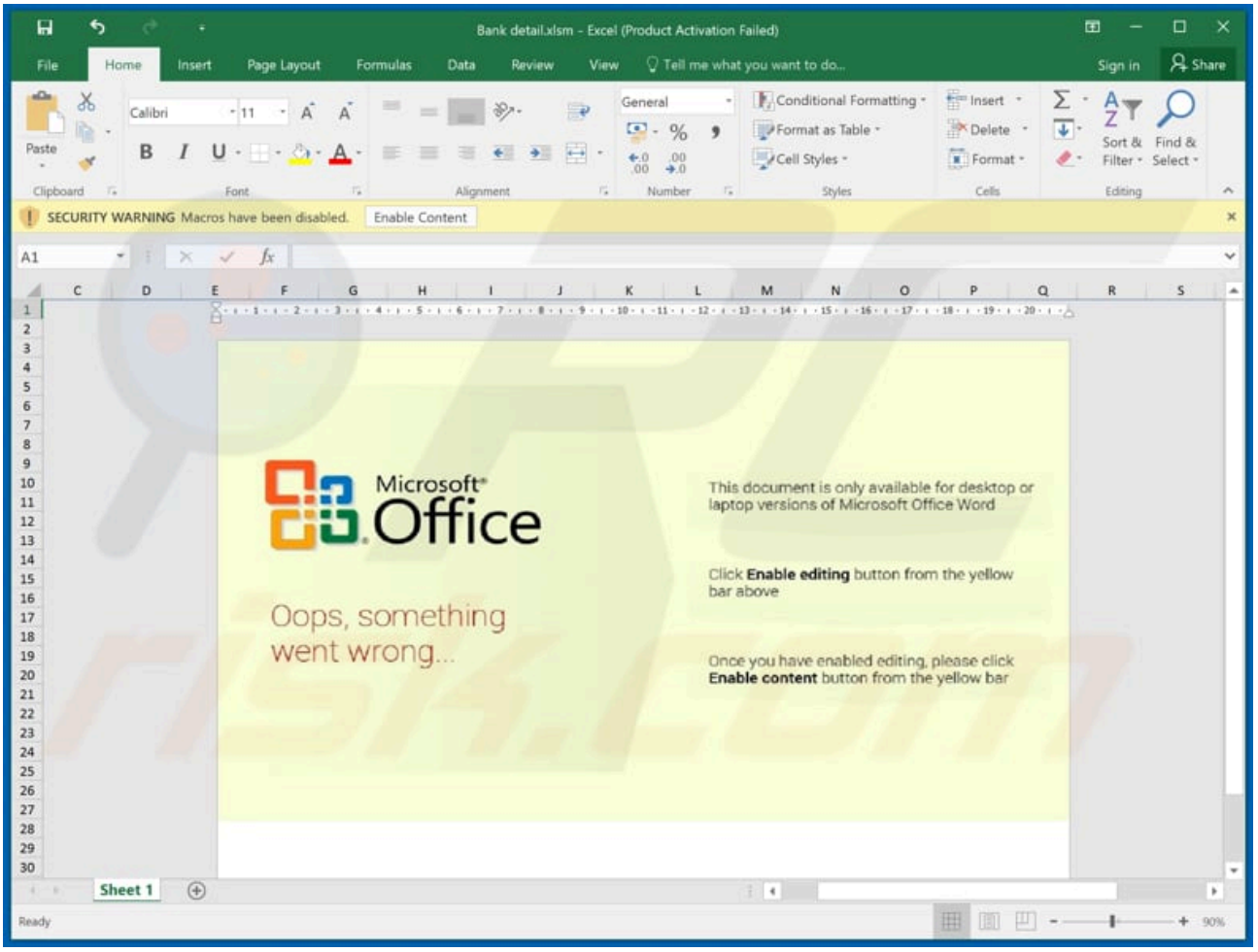


Text in this email:

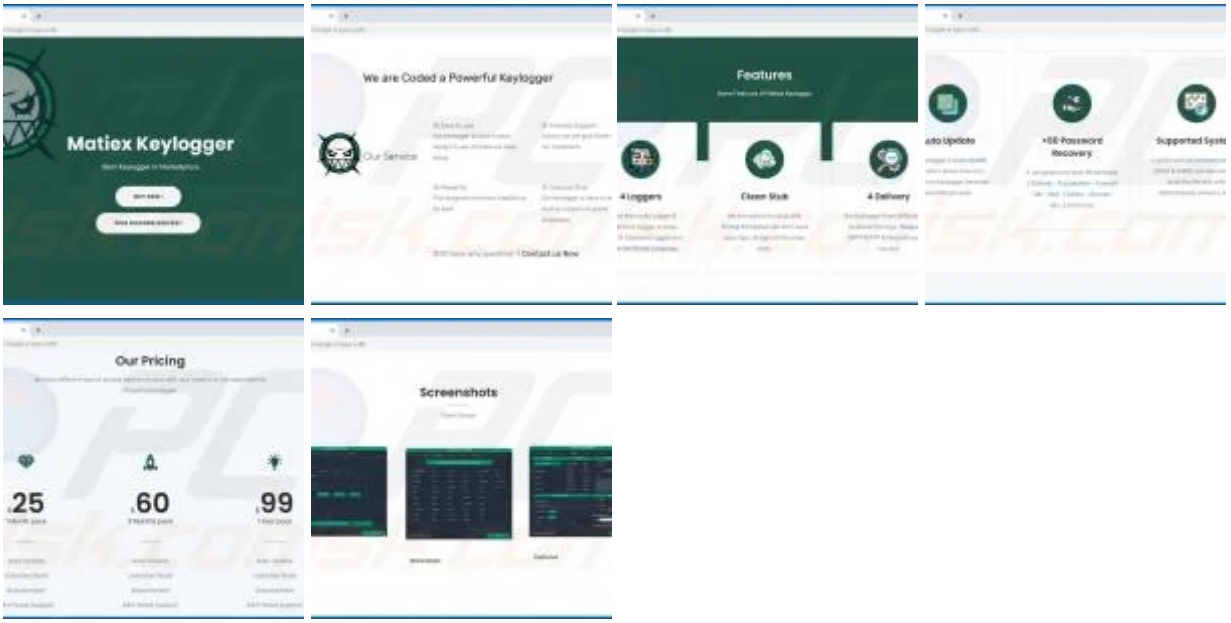
> Subject: Invoice LPG81901- Confirm Bank Detail Ending with 692
>
> TO:
> Fm: ClassNK Finance Department (PIC: T.Maezawa/Mr.)Our
> Ref. No.: 20FC0507TM08
>
> Dear Sir or Madam,
>
> We have been giving two different account by your agent, based on high rate of fraud
> we are suspicious. We decided to contact you directly to confirm which of the account mention on Freight Invoice as attached is your and also we will appreciate if you call to verify this by phone +81-3-5226-2052 handle this emails as urgent
>
> We look forward to hearing from you.
>
> Best regards,
> S. HatogaiGeneralManager of Finance Department
> **********
> NIPPON KAIJI KYOKAI (ClassNK)FINANCE DEPARTMENT4-7,
> Kioi-Cho, Chiyoda-Ku, Tokyo 102-8567,

> JapanTEL: +81-3-5226-2052 FAX: +81-3-5226-2108
> E--mail: fnd@classnk.or.jp
> **********

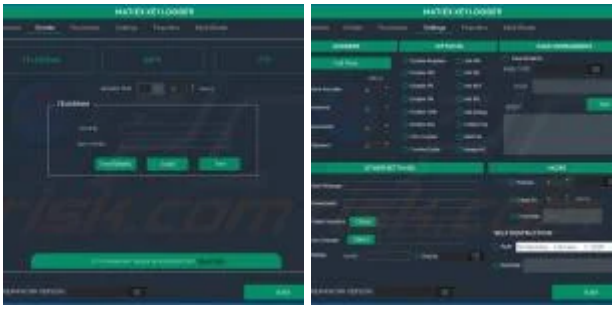
Malicious MS Excel document designed to install Matiex:



Screenshots of Matiex promotion page:



Screenshots of Matiex administration panel:



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

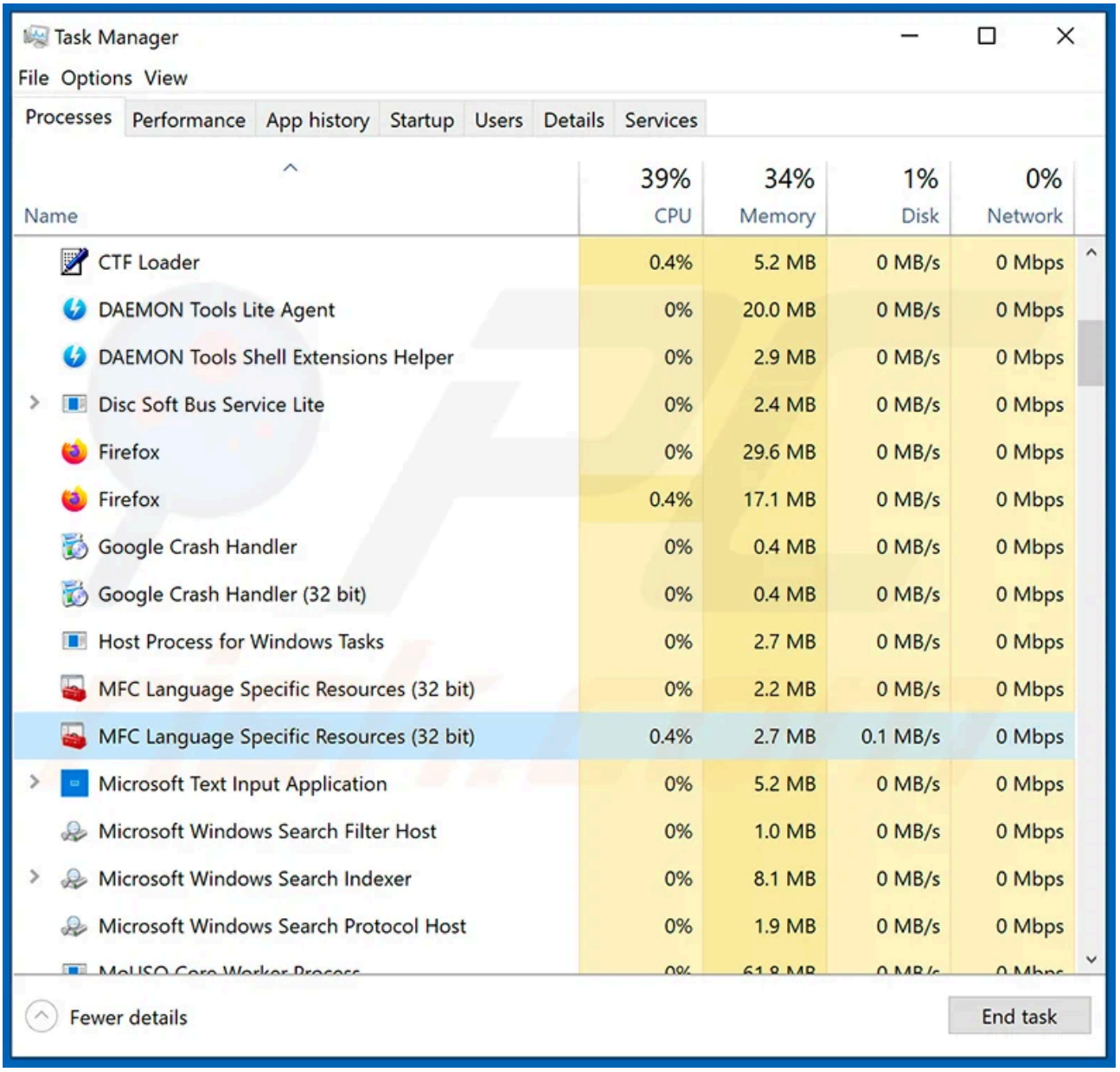
By downloading any software listed on this website you agree to our Privacy Policy and Terms of Use. To use full-featured product, you have to purchase a license for Combo Cleaner. 7 days free trial available. Combo Cleaner is owned and operated by RCS LT, the parent company of PCRisk.com.

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.

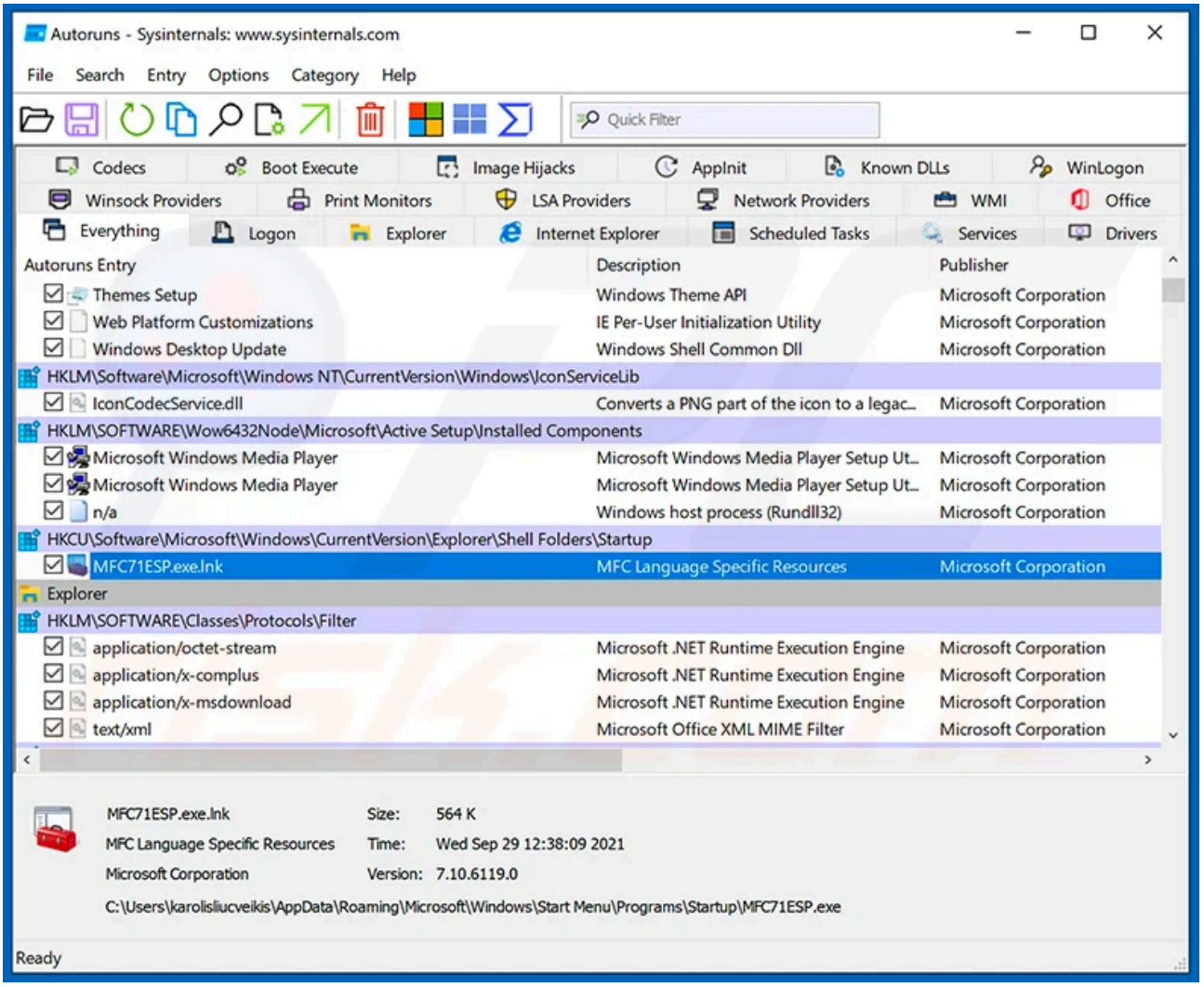
If you wish to remove malware manually, the first step is to identify the name of the malware that you are trying to remove. Here is an example of a suspicious program running on a user's computer:



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:

Step 1

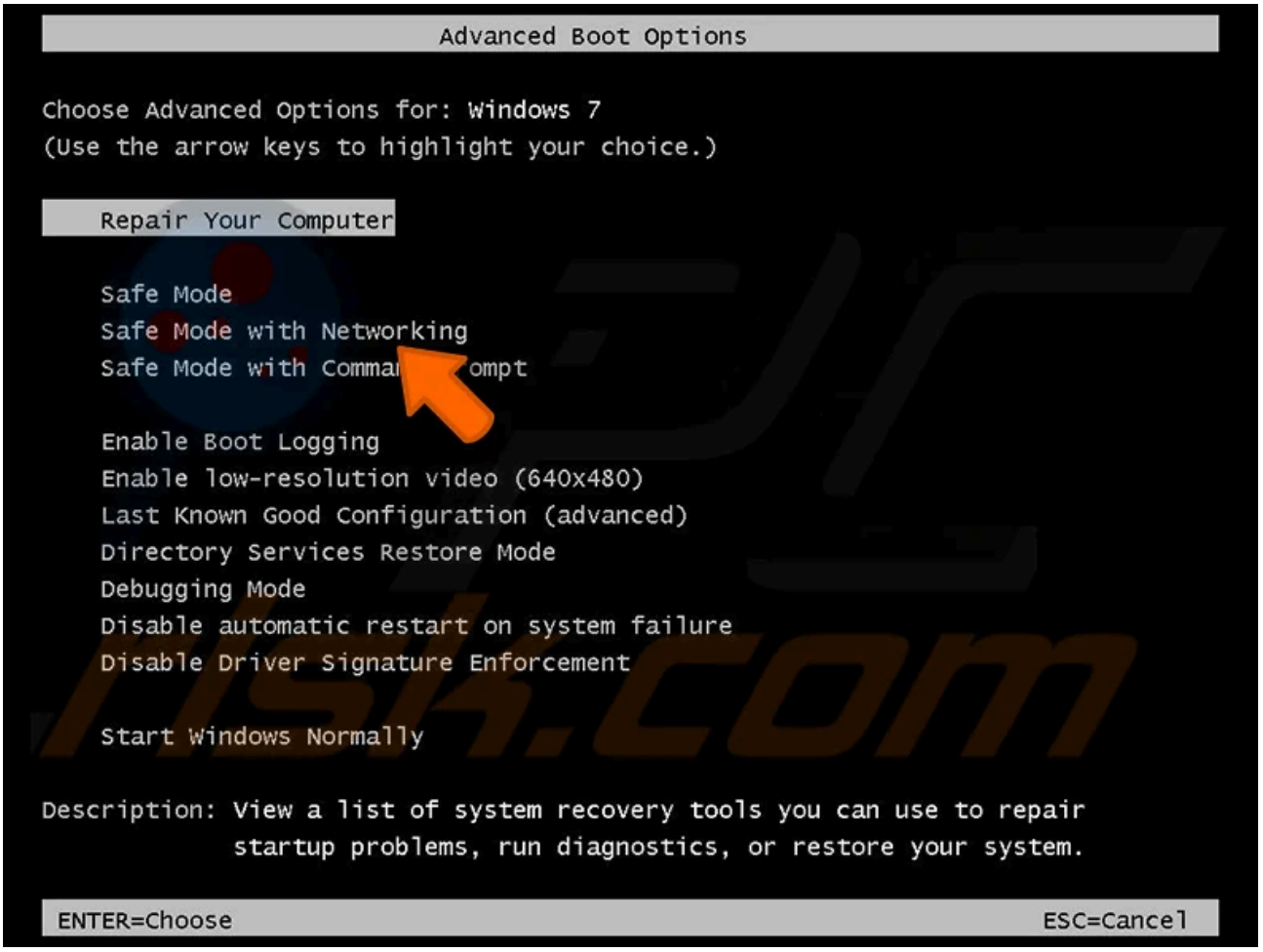
Download a program called Autoruns. This program shows auto-start applications, Registry, and file system locations:



Step 2

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.

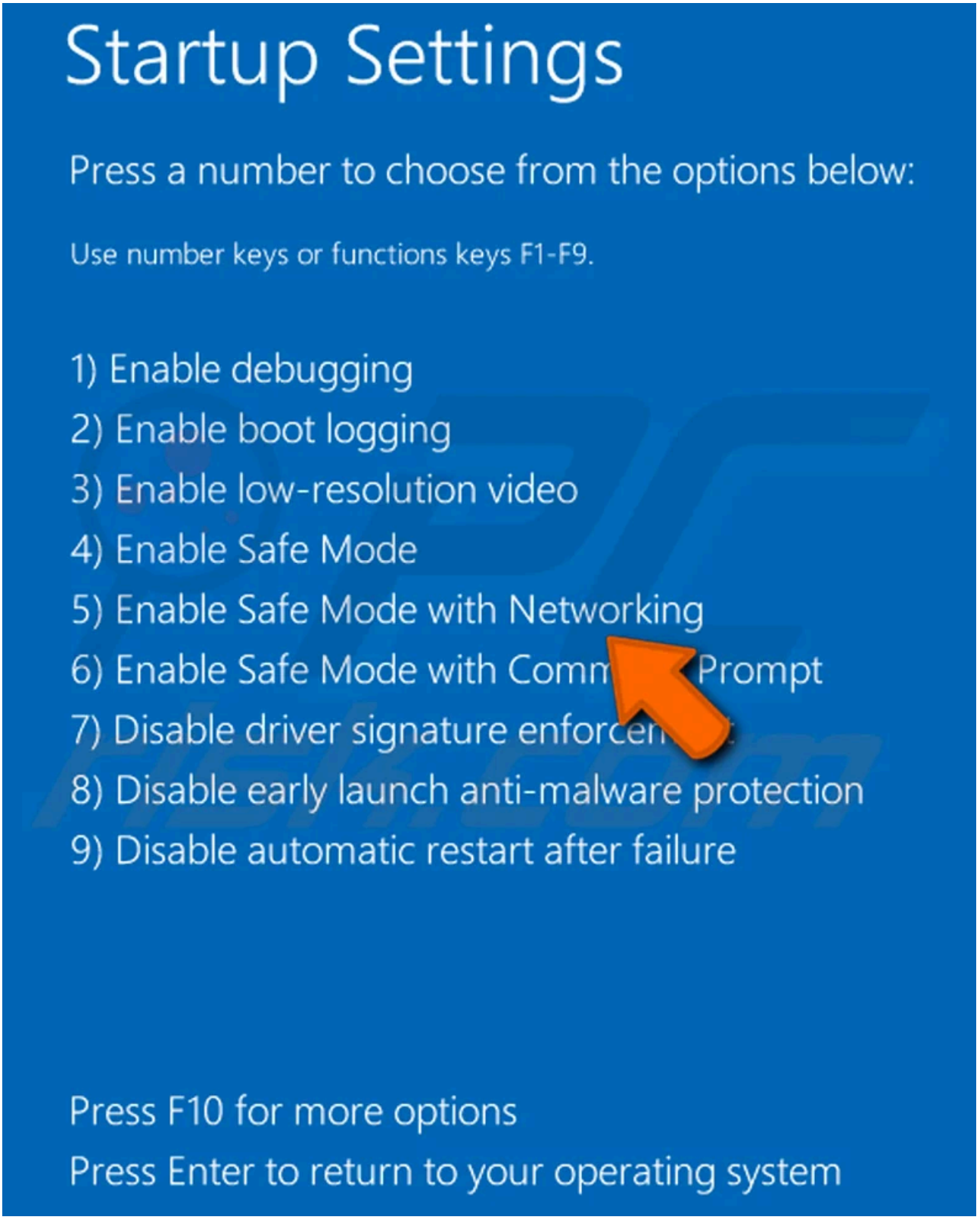


Video showing how to start Windows 7 in "Safe Mode with Networking":

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".

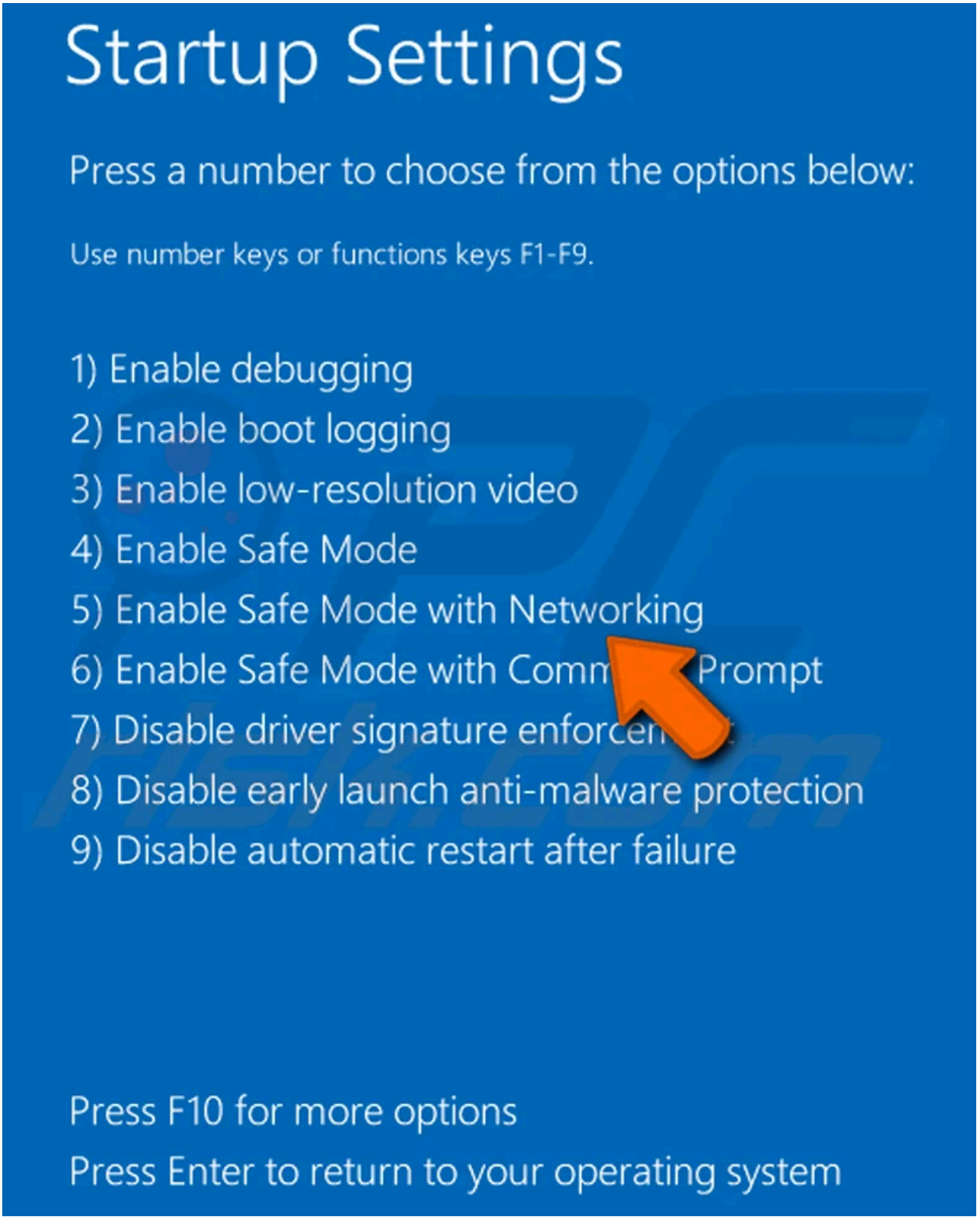
Click the "Restart" button. Your PC will restart into the Startup Settings screen. Press F5 to boot in Safe Mode with Networking.



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.



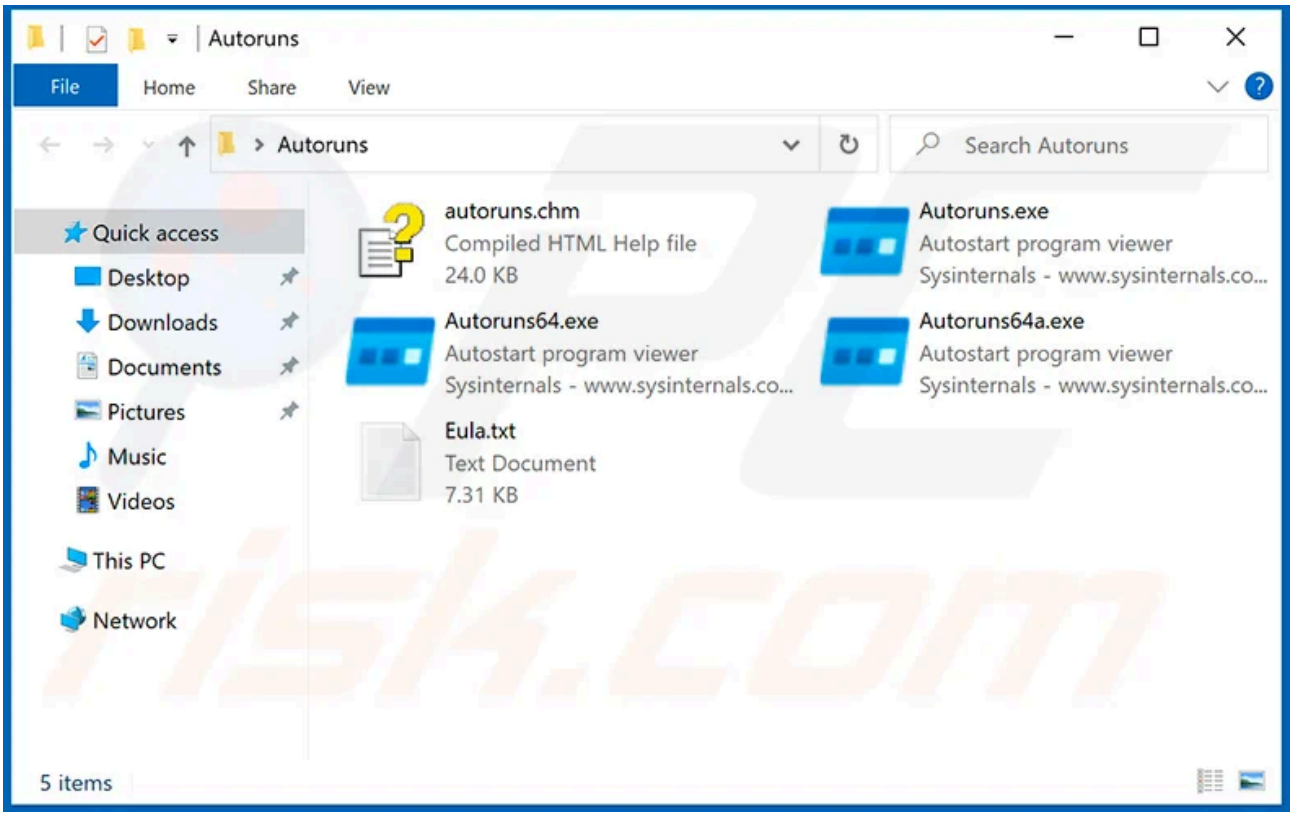
Video showing how to start Windows 10 in "Safe Mode with Networking":

Ett fel inträffade.

Det går inte att köra JavaScript.

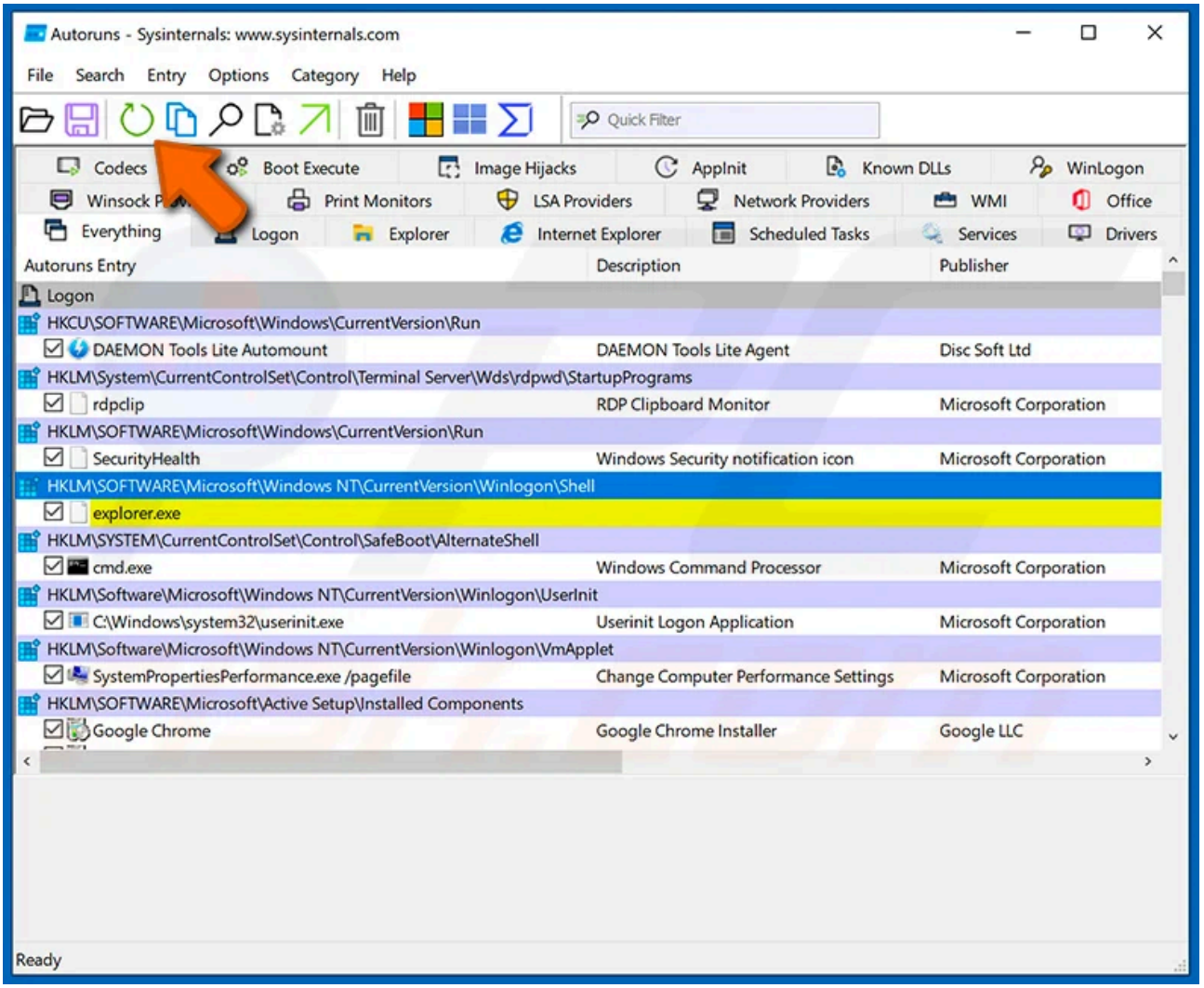
Step 3

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



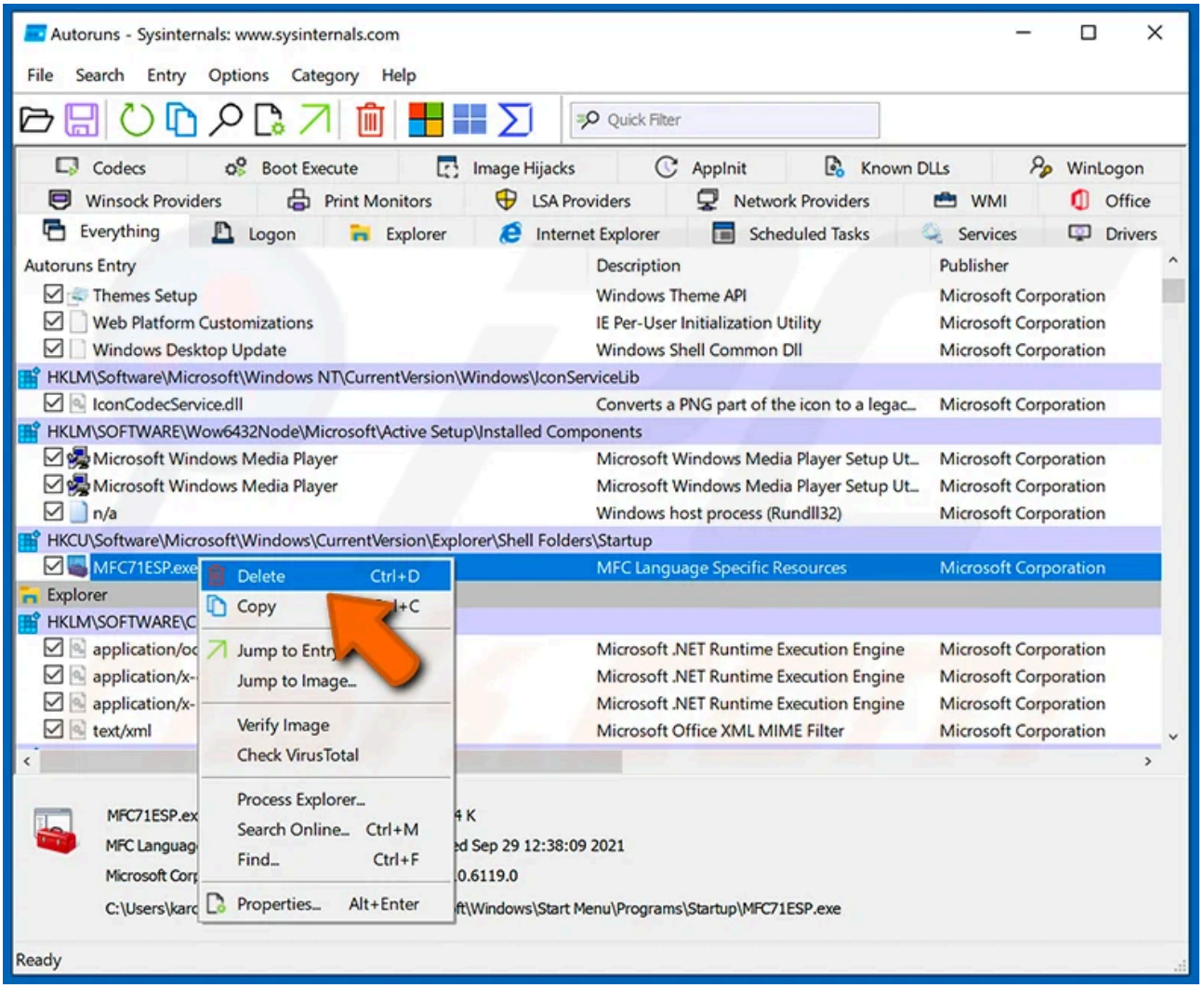
Step 4

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.

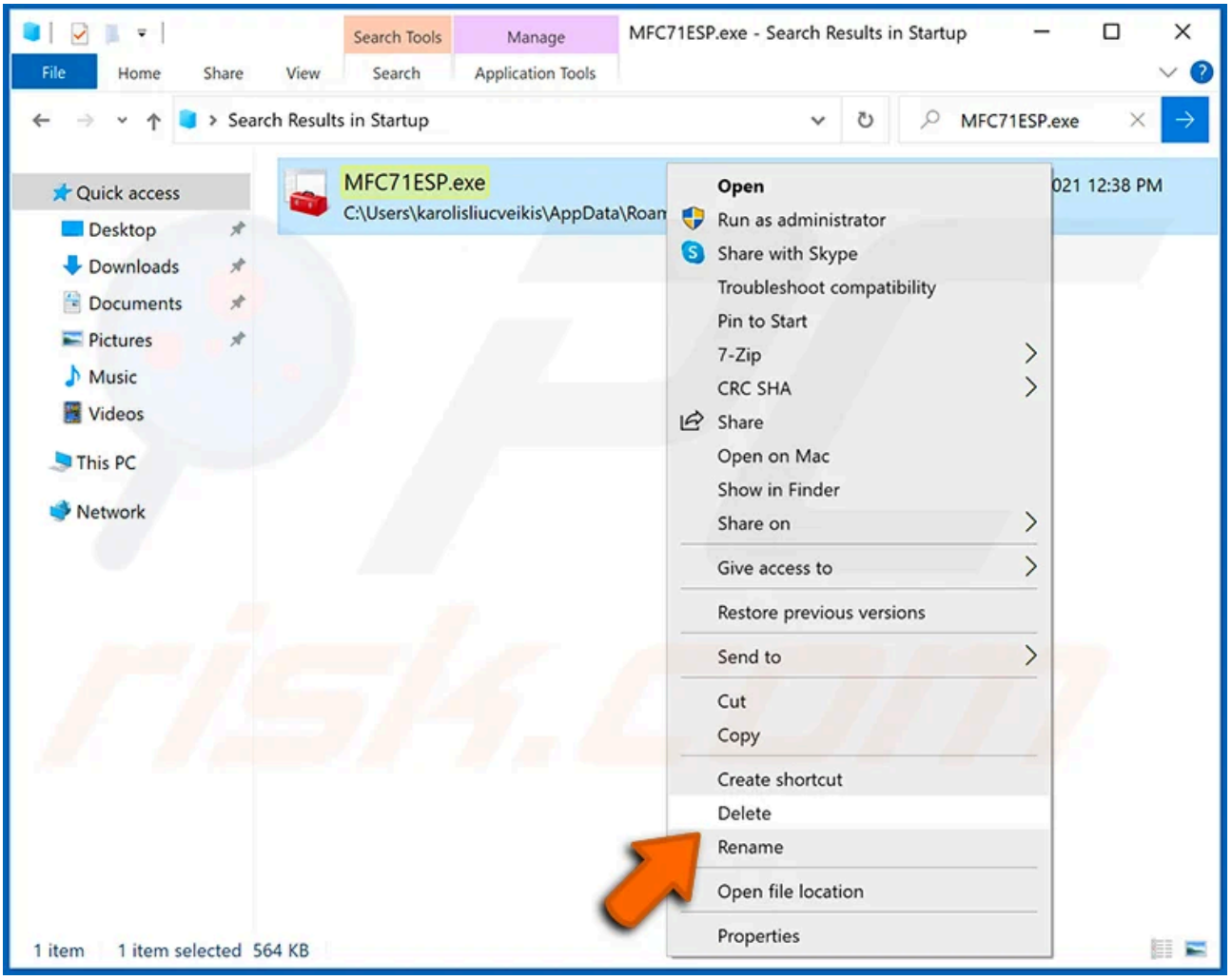


Check the list provided by the Autoruns application and locate the malware file that you want to eliminate.

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 Matiex malware, should I format my storage device to get rid of it?

No, Matiex's removal does not need formatting.

What are the biggest issues that Matiex malware can cause?

Matiex is a keylogger - a type of malware capable of recording keystrokes. However, this malware has other information-stealing abilities, such as password extraction, audio recording via device microphones, etc. Therefore, Matiex infections can lead to severe privacy issues, financial losses, and even identity theft.

What is the purpose of Matiex malware?

Most malicious programs are used for profit. However, cyber criminals can also use malware to amuse themselves, carry out personal grudges, disrupt processes (e.g., websites, services, companies, etc.), and even launch politically/geopolitically motivated attacks.

How did Matiex malware infiltrate my computer?

Malware is mainly distributed through drive-by downloads, spam emails and messages, untrustworthy download channels (e.g., unofficial and freeware sites, Peer-to-Peer sharing networks, etc.), illegal software activation tools ("cracks"), and fake updates. Furthermore, some malicious programs can self-proliferate via local networks and removable storage devices (e.g., external hard drives, USB flash drives, etc.).

Will Combo Cleaner protect me from malware?

Yes, Combo Cleaner can detect and eliminate almost all known malware infections. It must be mentioned that running a complete system scan is crucial - since high-end malicious software typically hides deep within systems.
