flare

Inside the Information Stealer Ecosystem:

From Compromise to Countermeasure

Olivier Bilodeau
Principal Cybersecurity Researcher

flare.io

🥰 Copenhagen & FIRSTCON

Who Are We?

Olivier Bilodeau & Mathieu Lavoie

- 15 years cybersecurity industry experience
- Principal Cybersecurity Researcher at Flare
- Former GoSecure, ESET
- Founder MontréHack
- NorthSec's President
- Serial presenter: DEFCON, BlackHat,
  SecTor, Botconf, CERT-EU, AtlSecCon

Who Deserves Additional Credit?

Eric Clay

- Contributed to this presentation
- "likely the most threat-intelligence-obsessed CMO in cybersecurity" according to Olivier

Estelle Ruellan

- Data Science Extraordinaire!
- Screenshot LLM Analysis

Spending hours coding your own RCE 0-days
Logging in with free creds found on 🔥🎉🔥 PIMPIN LOGS CLOUD 🔥🎉🔥 Telegram

flare

Agenda

- What is Information Stealer Malware?
- Infection Vectors Analysis Through Victim Desktop Screenshots
- Beyond Credentials: What else is stolen?
- Redline/META Takedown
- Defense and Mitigation Strategies
- Community Contributions

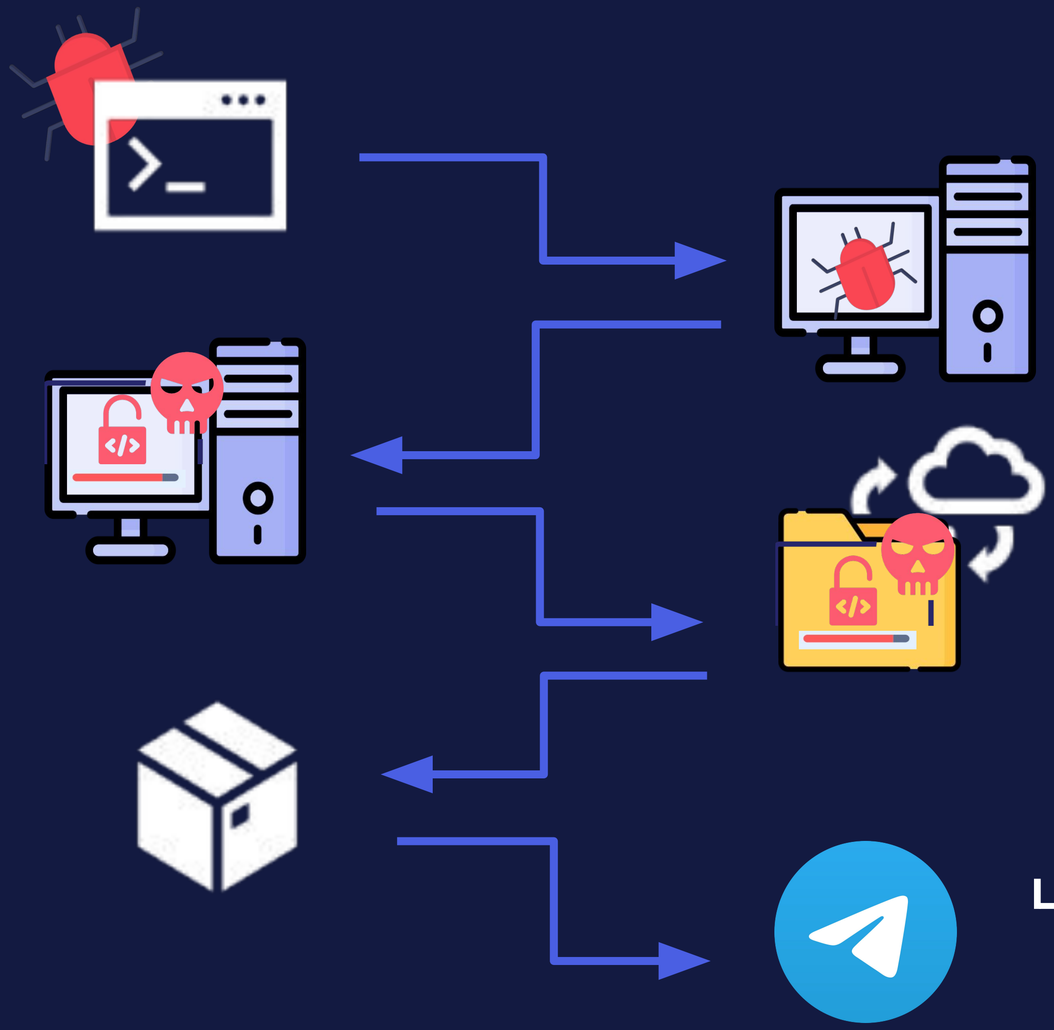
flare

Information Stealer Malware

Quick Reminder (or Intro)

What is an Infostealer?

The Malware you (may) have never heard of:



User downloads cracked software

Malware is executed on victim computer

Infostealer grabs:
- credentials
- crypto wallets
- browser Data ...

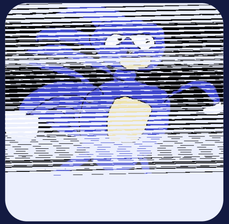
Data exfiltrated to C2 infrastructure

Individual logs are packaged together

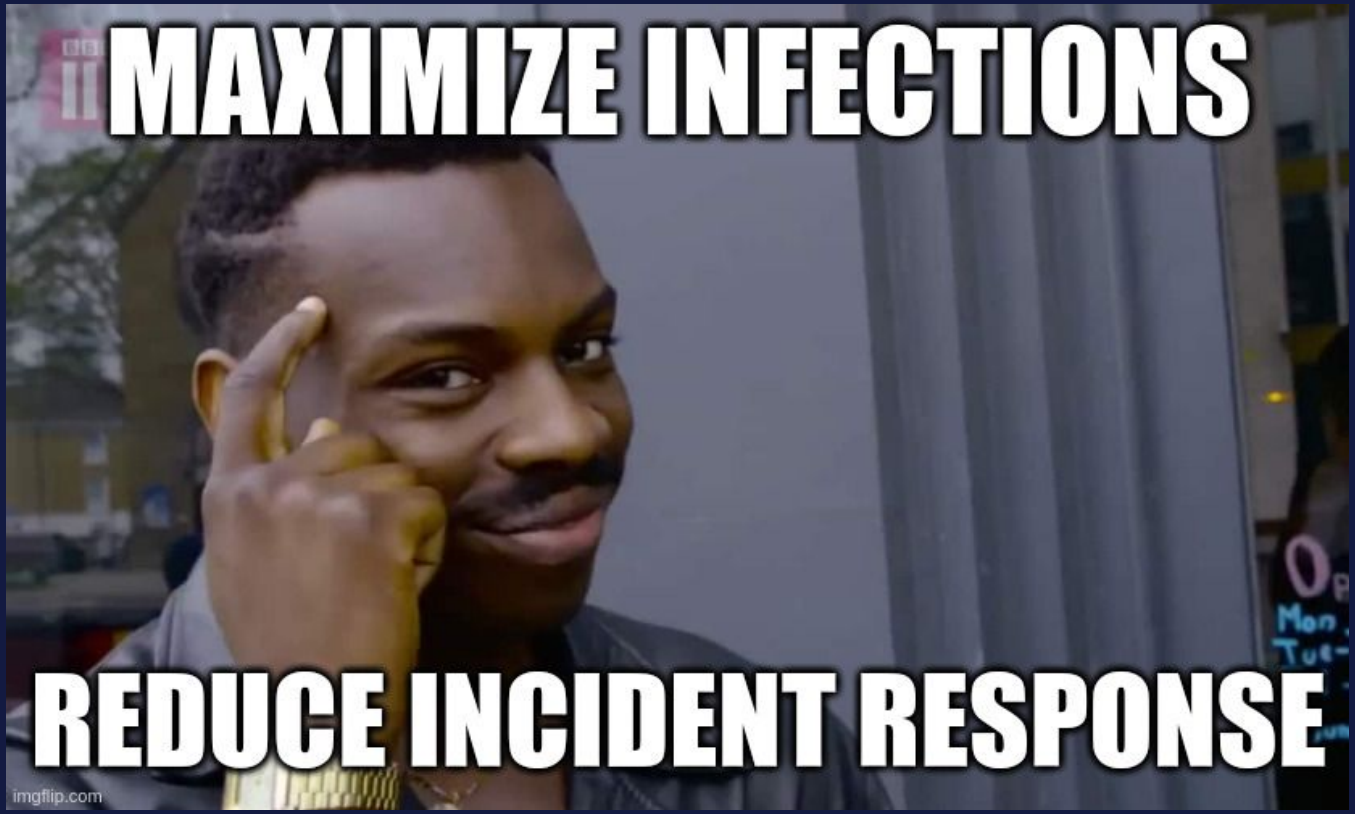
Log Files are distributed in Telegram Channels

Little Known Facts About Information Stealer Malware

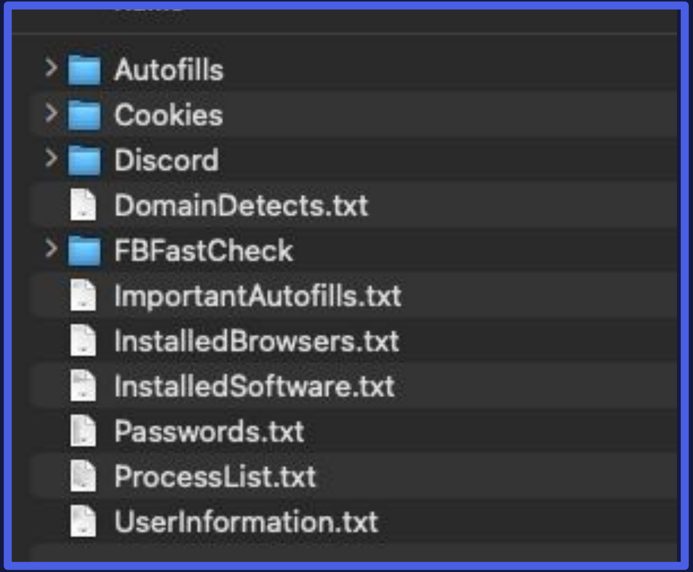
No Admin Rights Required



No Persistence

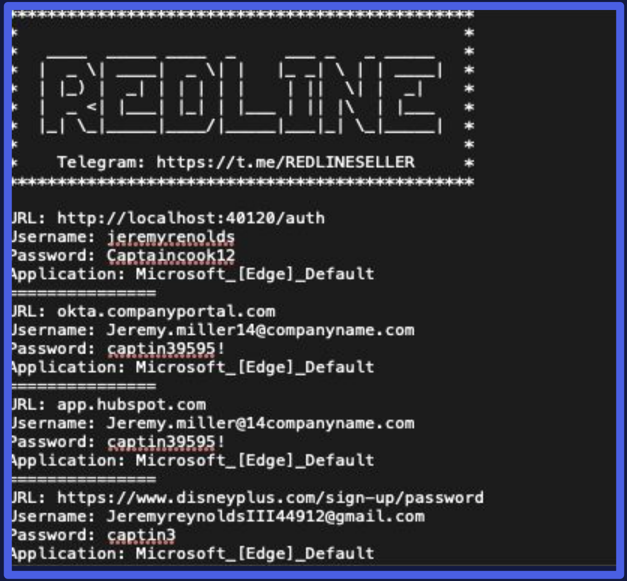


The Anatomy of a Stealer Log



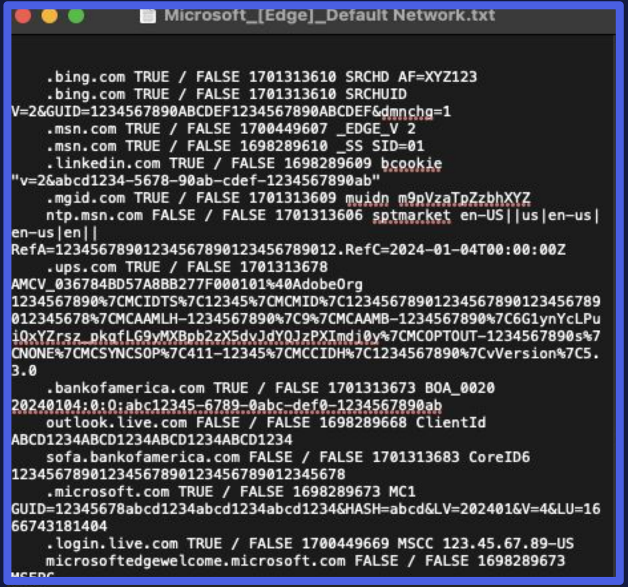
- Autofills
- Cookies
- Discord
- DomainDetects.txt
- FBFastCheck
- ImportantAutofills.txt
- InstalledBrowsers.txt
- InstalledSoftware.txt
- Passwords.txt
- ProcessList.txt
- UserInformation.txt

High Level view of a single stealer log showcasing data stolen from the host.



```
**************************************************
*                                                *
*                                                *
*   ____  _____ ____  _     ___ _   _ _____      *
*  |  _ \| ____|  _ \| |   |_ _| \ | | ____|     *
*  | |_) |  _| | | | | |    | ||  \| |  _|       *
*  |  _ <| |___| |_| | |___ | || |\  | |___      *
*  |_| \_\_____|____/|_____|___|_| \_|_____|     *
*                                                *
*    Telegram: https://t.me/REDLINESELLER        *
**************************************************

URL: http://localhost:40120/auth
Username: jeremyrenolds
Password: Captaincook12
Application: Microsoft_[Edge]_Default
===============
URL: okta.companyportal.com
Username: Jeremy.miller14@companyname.com
Password: captin39595!
Application: Microsoft_[Edge]_Default
===============
URL: app.hubspot.com
Username: Jeremy.miller@14companyname.com
Password: captin39595!
Application: Microsoft_[Edge]_Default
===============
URL: https://www.disneyplus.com/sign-up/password
Username: JeremyreynoldsIII44912@gmail.com
Password: captin3
Application: Microsoft_[Edge]_Default
```

View of the passwords in the "passwords.txt" section of the stealer log, containing all of the passwords from a single user.



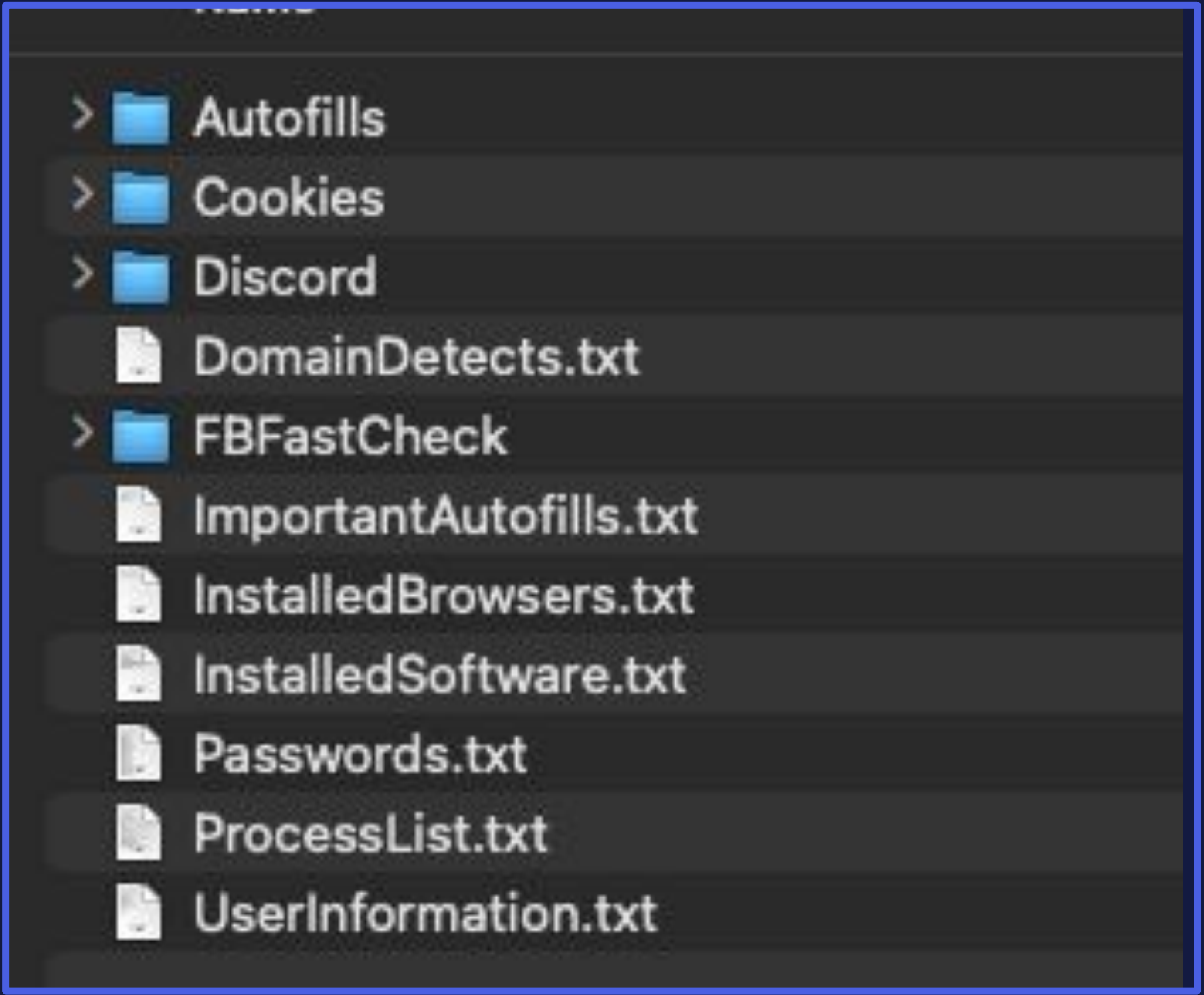
Microsoft_[Edge]_Default Network.txt

```
    .bing.com TRUE / FALSE 1701313610 SRCHD AF=XYZ123
    .bing.com TRUE / FALSE 1701313610 SRCHUID
V=2&GUID=1234567890ABCDEF1234567890ABCDEF&dmnchg=1
    .msn.com TRUE / FALSE 1700449607 _EDGE_V 2
    .msn.com TRUE / FALSE 1698289610 _SS SID=01
    .linkedin.com TRUE / FALSE 1698289609 bcookie
"v=2&abcd1234-5678-90ab-cdef-1234567890ab"
    .mgid.com TRUE / FALSE 1701313609 muidn m9pVzaTpZzbhXYZ
    ntp.msn.com FALSE / FALSE 1701313606 sptmarket en-US||us|en-us|
en-us|en||
RefA=12345678901234567890123456789012.RefC=2024-01-04T00:00:00Z
    .ups.com TRUE / FALSE 1701313678
AMCV_036784BD57A8BB277F000101%40AdobeOrg
1234567890%7CMCIDTS%7C12345%7CMCMID%7C12345678901234567890123456789
012345678%7CMCAAMLH-1234567890%7C9%7CMCAAMB-1234567890%7C6G1ynYcLPu
iQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y%7CMCOPTOUT-1234567890s%7
CNONE%7CMCSYNCSOP%7C411-12345%7CMCCIDH%7C1234567890%7CvVersion%7C5.
3.0
    .bankofamerica.com TRUE / FALSE 1701313673 BOA_0020
20240104:0:O:abc12345-6789-0abc-def0-1234567890ab
    outlook.live.com FALSE / FALSE 1698289668 ClientId
ABCD1234ABCD1234ABCD1234ABCD1234
    sofa.bankofamerica.com FALSE / FALSE 1701313683 CoreID6
12345678901234567890123456789012345678
    .microsoft.com TRUE / FALSE 1698289673 MC1
GUID=12345678abcd1234abcd1234abcd1234&HASH=abcd&LV=202401&V=4&LU=16
66743181404
    .login.live.com TRUE / FALSE 1700449669 MSCC 123.45.67.89-US
    microsoftedgewelcome.microsoft.com FALSE / FALSE 1698289673
```

Data in the "Cookies" section of the stealer log

The Anatomy of a Stealer Log

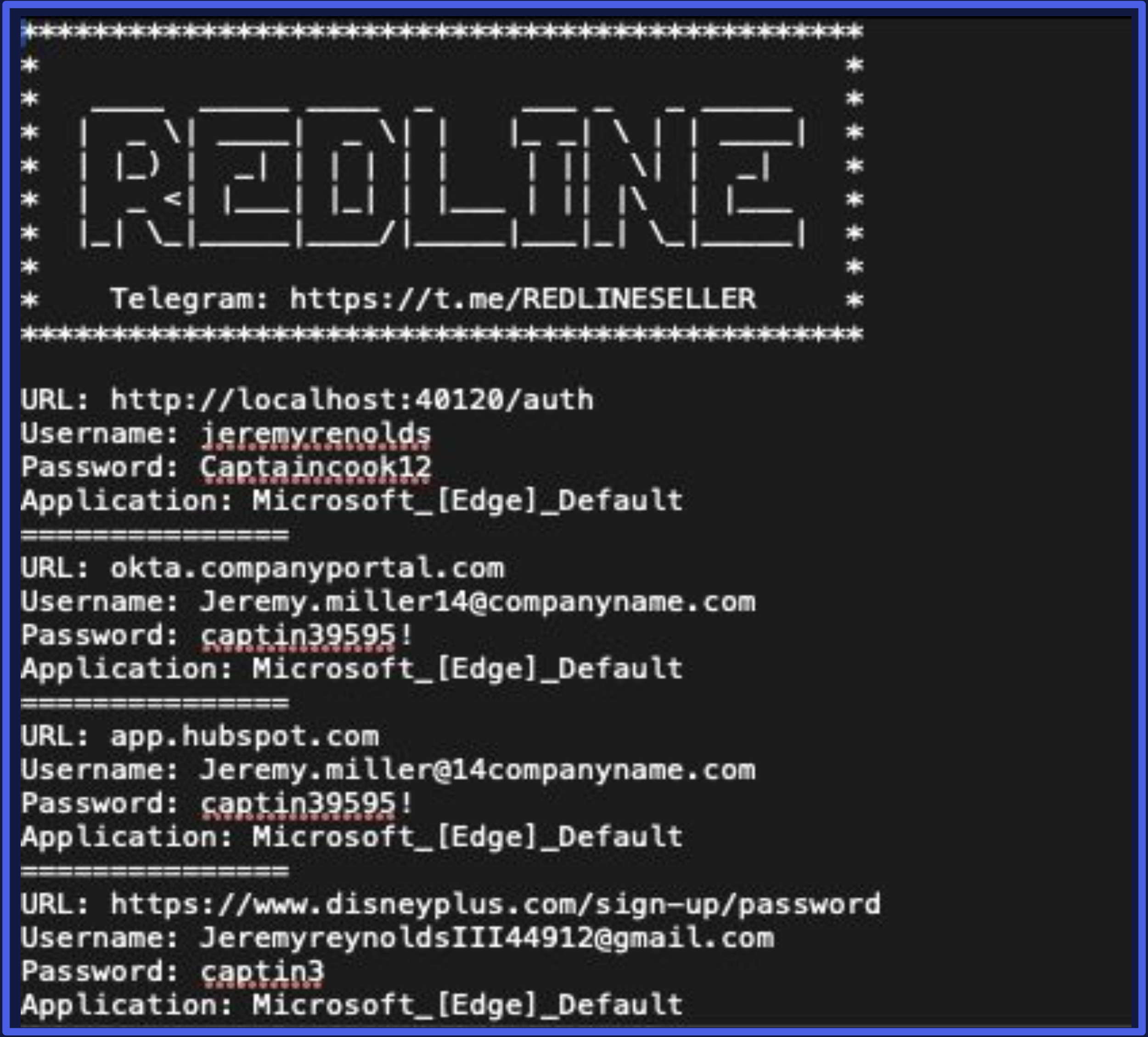
High Level view of a single stealer log showcasing data stolen from the host.



- Autofills
- Cookies
- Discord
- DomainDetects.txt
- FBFastCheck
- ImportantAutofills.txt
- InstalledBrowsers.txt
- InstalledSoftware.txt
- Passwords.txt
- ProcessList.txt
- UserInformation.txt

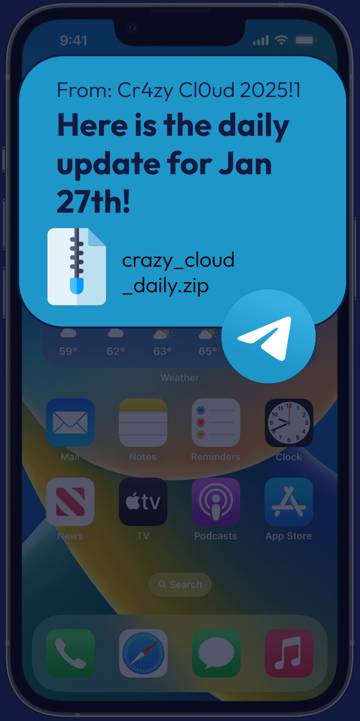
The Anatomy of a Stealer Log

View of the passwords in the “passwords.txt” section of the stealer log, containing all of the passwords from a single user.



```
***********************************************
*                                             *
*   ____  _____ ____  _     ___ _   _ _____   *
*  |  _ \| ____|  _ \| |   |_ _| \ | | ____|  *
*  | |_) |  _| | | | | |    | ||  \| |  _|    *
*  |  _ <| |___| |_| | |___ | || |\  | |___   *
*  |_| \_\_____|____/|_____|___|_| \_|_____|  *
*                                             *
*    Telegram: https://t.me/REDLINESELLER     *
***********************************************

URL: http://localhost:40120/auth
Username: jeremyrenolds
Password: Captaincook12
Application: Microsoft_[Edge]_Default
===============
URL: okta.companyportal.com
Username: Jeremy.miller14@companyname.com
Password: captin39595!
Application: Microsoft_[Edge]_Default
===============
URL: app.hubspot.com
Username: Jeremy.miller@14companyname.com
Password: captin39595!
Application: Microsoft_[Edge]_Default
===============
URL: https://www.disneyplus.com/sign-up/password
Username: JeremyreynoldsIII44912@gmail.com
Password: captin3
Application: Microsoft_[Edge]_Default
```

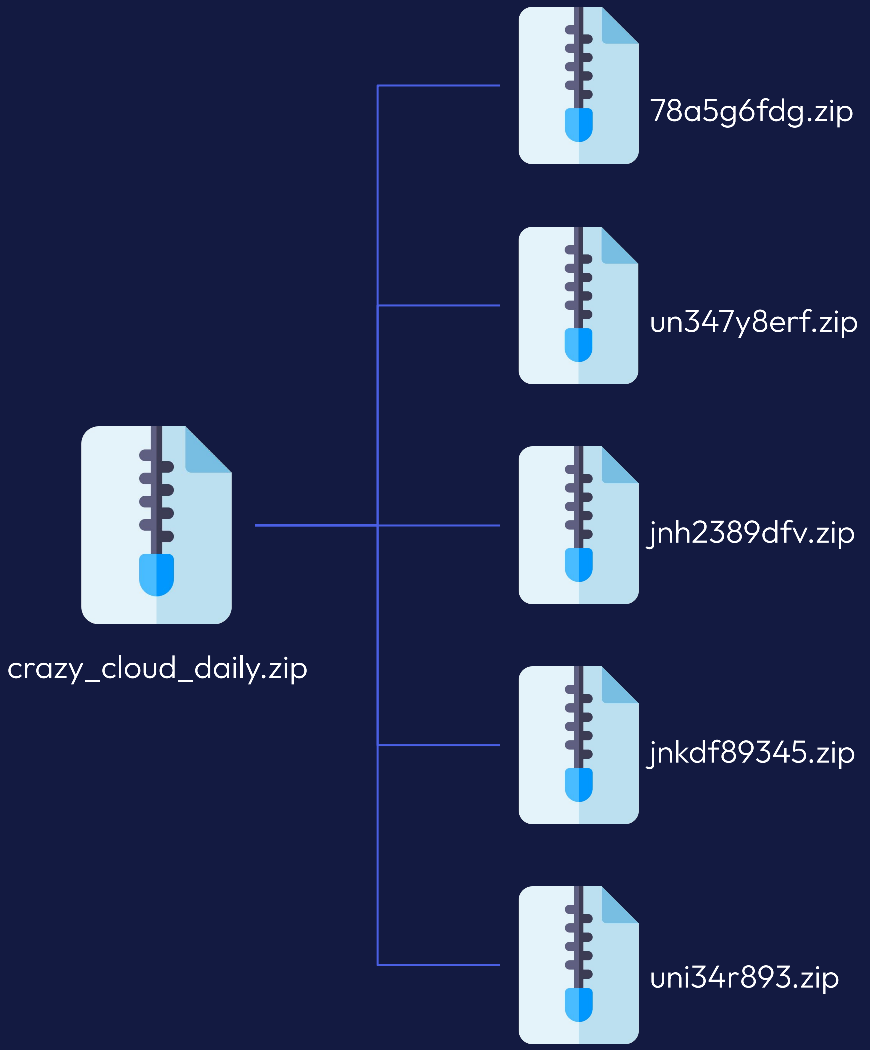
Stealer Log: Distribution



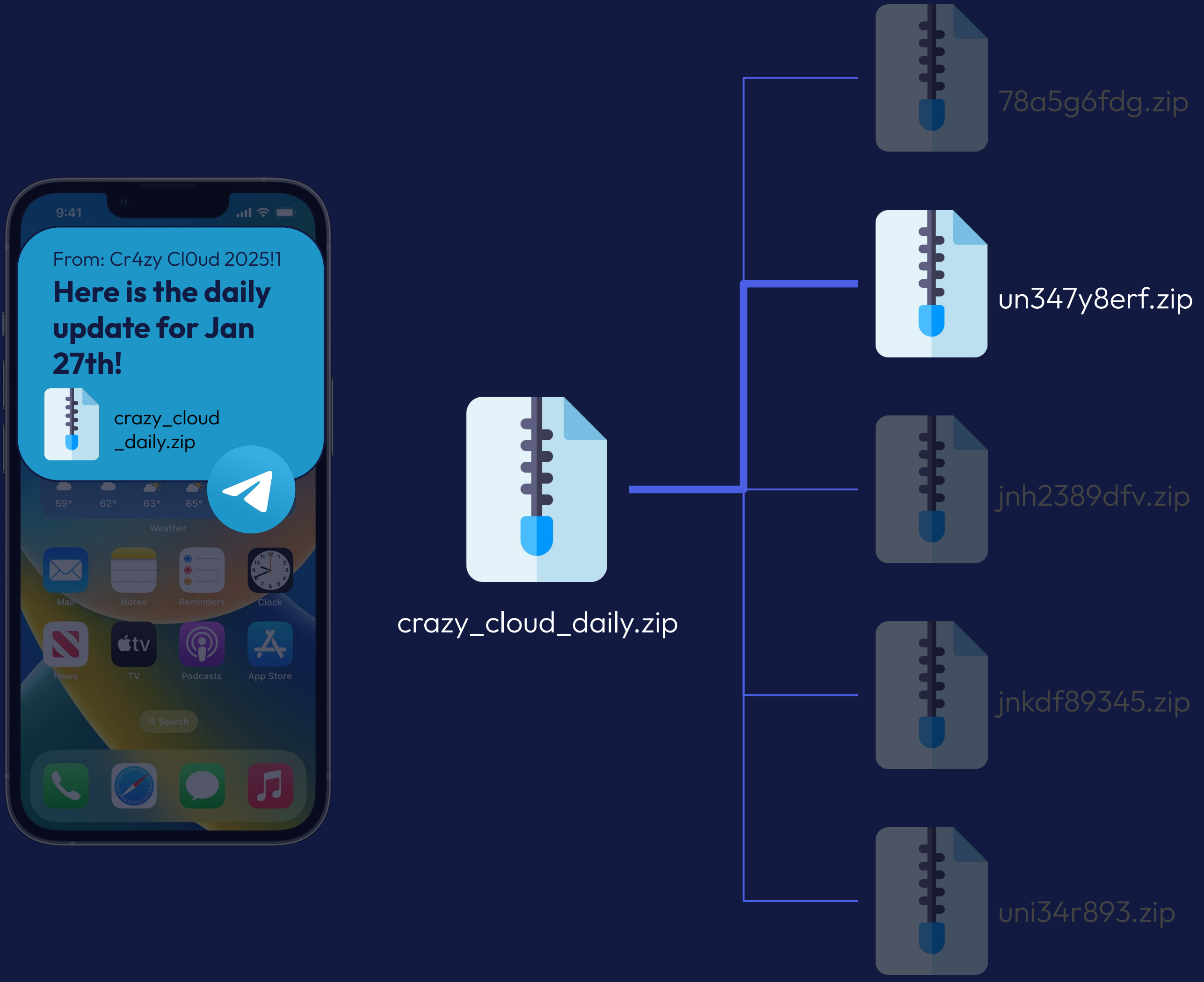
From: Cr4zy Cl0ud 2025!1

Here is the daily update for Jan 27th!

crazy_cloud _daily.zip



Stealer Log: Distribution - Individual Logs

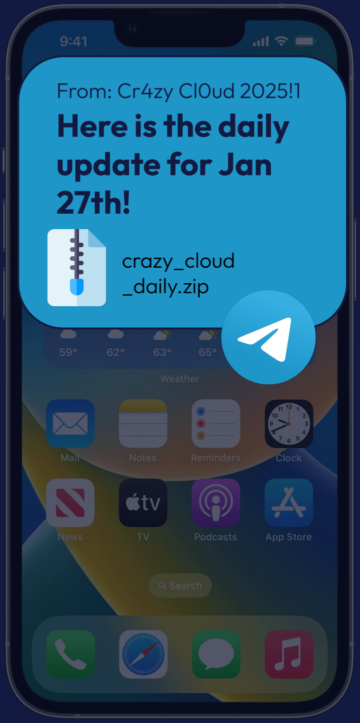


From: Cr4zy Cl0ud 2025!1

Here is the daily update for Jan 27th!

crazy_cloud _daily.zip

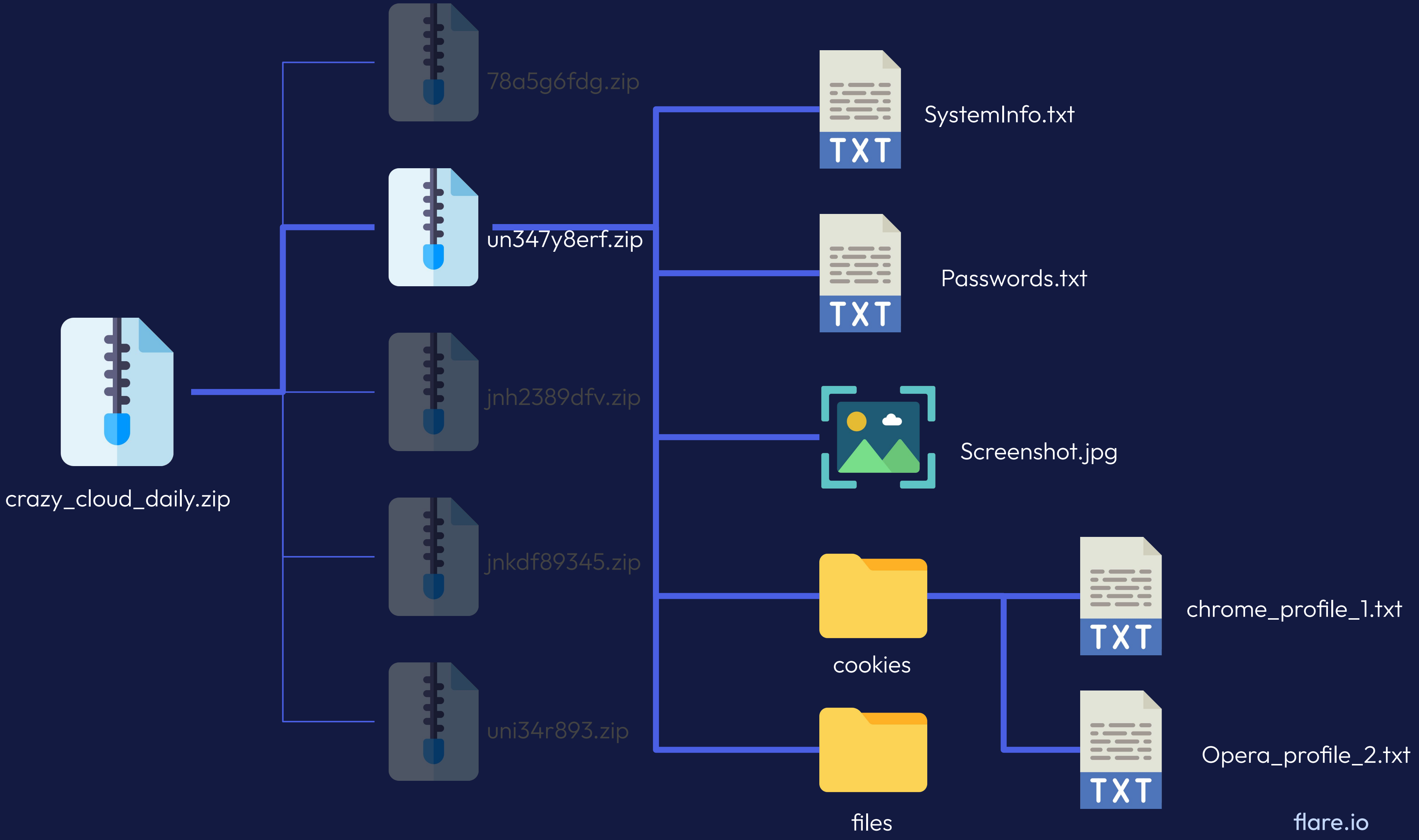
Stealer Log: Distribution - Content



From: Cr4zy Cl0ud 2025!1

Here is the daily update for Jan 27th!

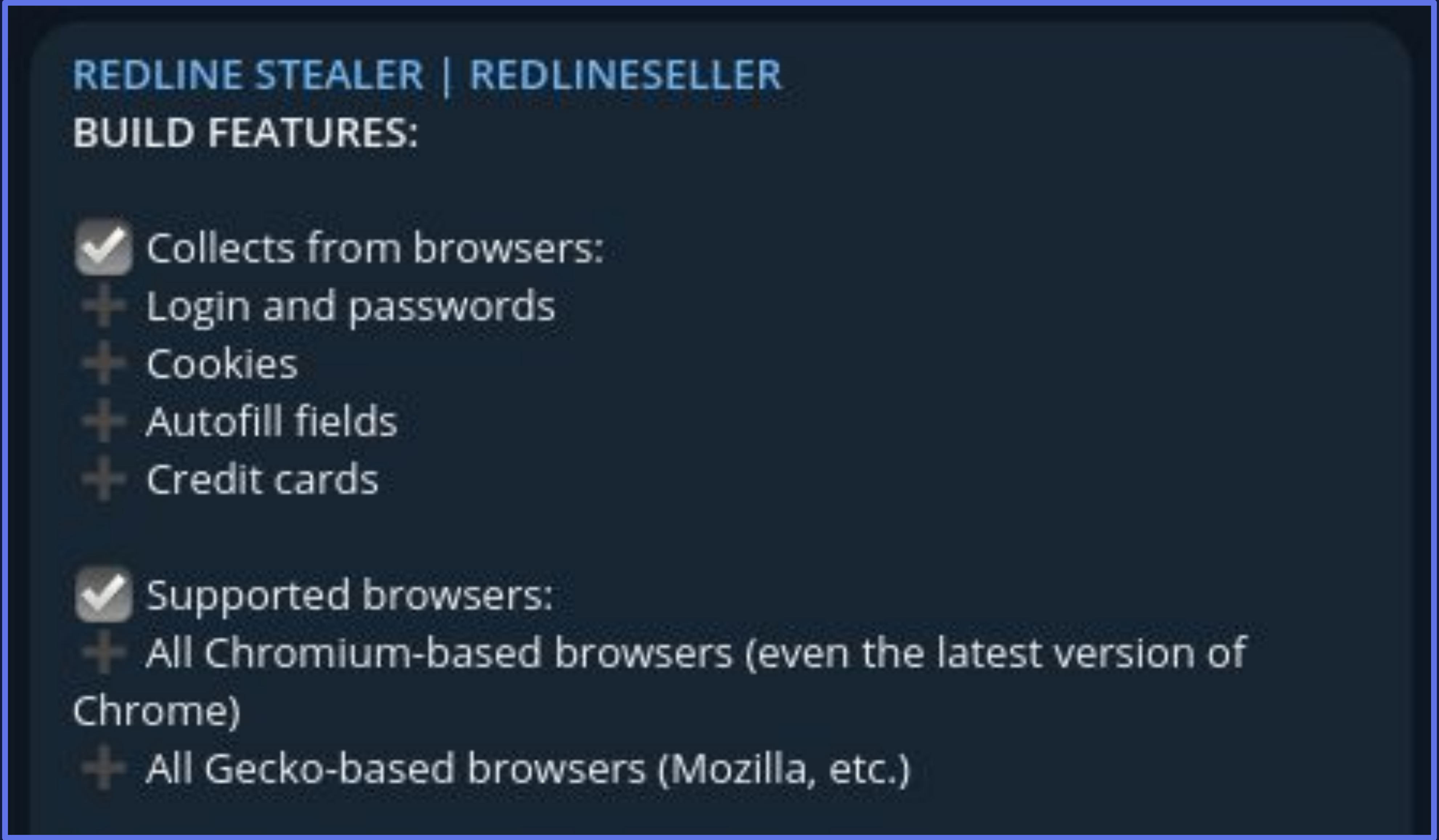
crazy_cloud _daily.zip



flare

The Fascinating Infostealer Economy

Malware as a Service



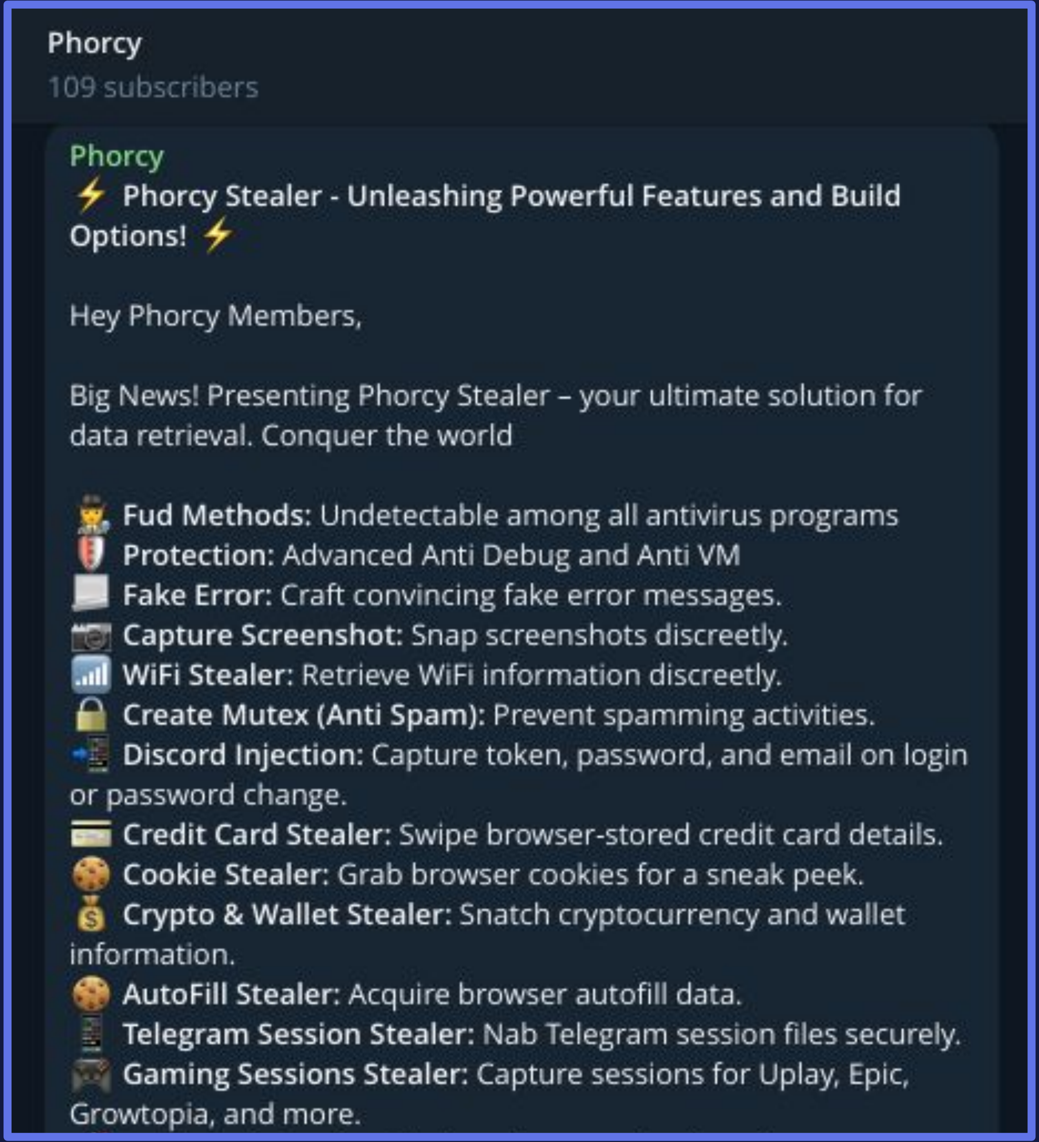
REDLINE STEALER | REDLINESELLER

BUILD FEATURES:

☑ Collects from browsers:
➕ Login and passwords
➕ Cookies
➕ Autofill fields
➕ Credit cards

☑ Supported browsers:
➕ All Chromium-based browsers (even the latest version of Chrome)
➕ All Gecko-based browsers (Mozilla, etc.)

Malware as a Service



Phorcy
109 subscribers

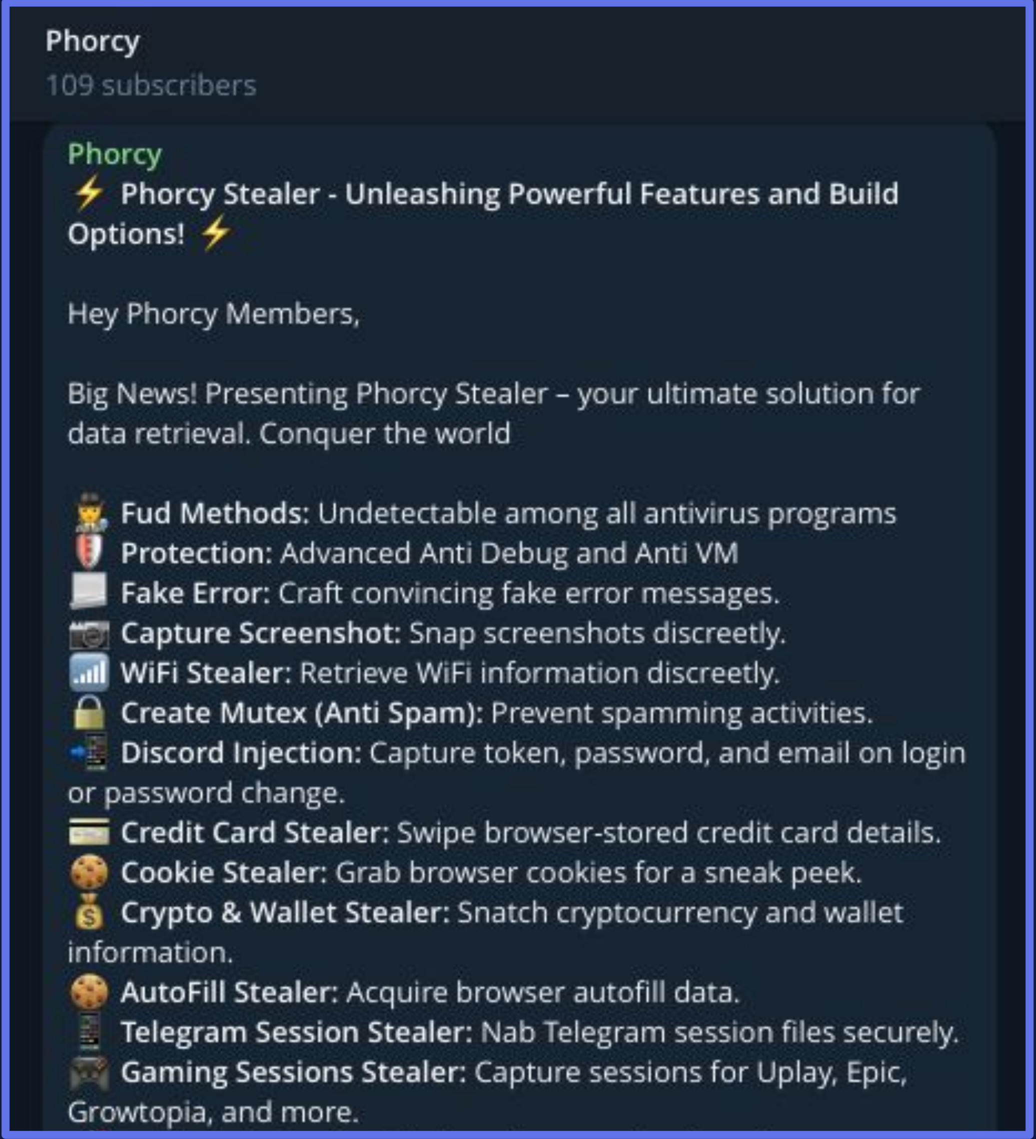
Phorcy
⚡ **Phorcy Stealer - Unleashing Powerful Features and Build Options!** ⚡

Hey Phorcy Members,

Big News! Presenting Phorcy Stealer – your ultimate solution for data retrieval. Conquer the world

🕵️ **Fud Methods:** Undetectable among all antivirus programs
🛡️ **Protection:** Advanced Anti Debug and Anti VM
💻 **Fake Error:** Craft convincing fake error messages.
📷 **Capture Screenshot:** Snap screenshots discreetly.
📶 **WiFi Stealer:** Retrieve WiFi information discreetly.
🔒 **Create Mutex (Anti Spam):** Prevent spamming activities.
📲 **Discord Injection:** Capture token, password, and email on login or password change.
💳 **Credit Card Stealer:** Swipe browser-stored credit card details.
🍪 **Cookie Stealer:** Grab browser cookies for a sneak peek.
💰 **Crypto & Wallet Stealer:** Snatch cryptocurrency and wallet information.
🍪 **AutoFill Stealer:** Acquire browser autofill data.
📱 **Telegram Session Stealer:** Nab Telegram session files securely.
🎮 **Gaming Sessions Stealer:** Capture sessions for Uplay, Epic, Growtopia, and more.

Malware as a Service



Phorcy
109 subscribers

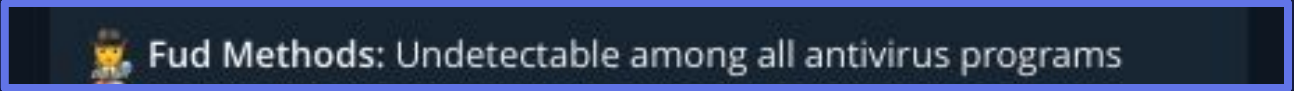
Phorcy

⚡ **Phorcy Stealer - Unleashing Powerful Features and Build Options!** ⚡

Hey Phorcy Members,

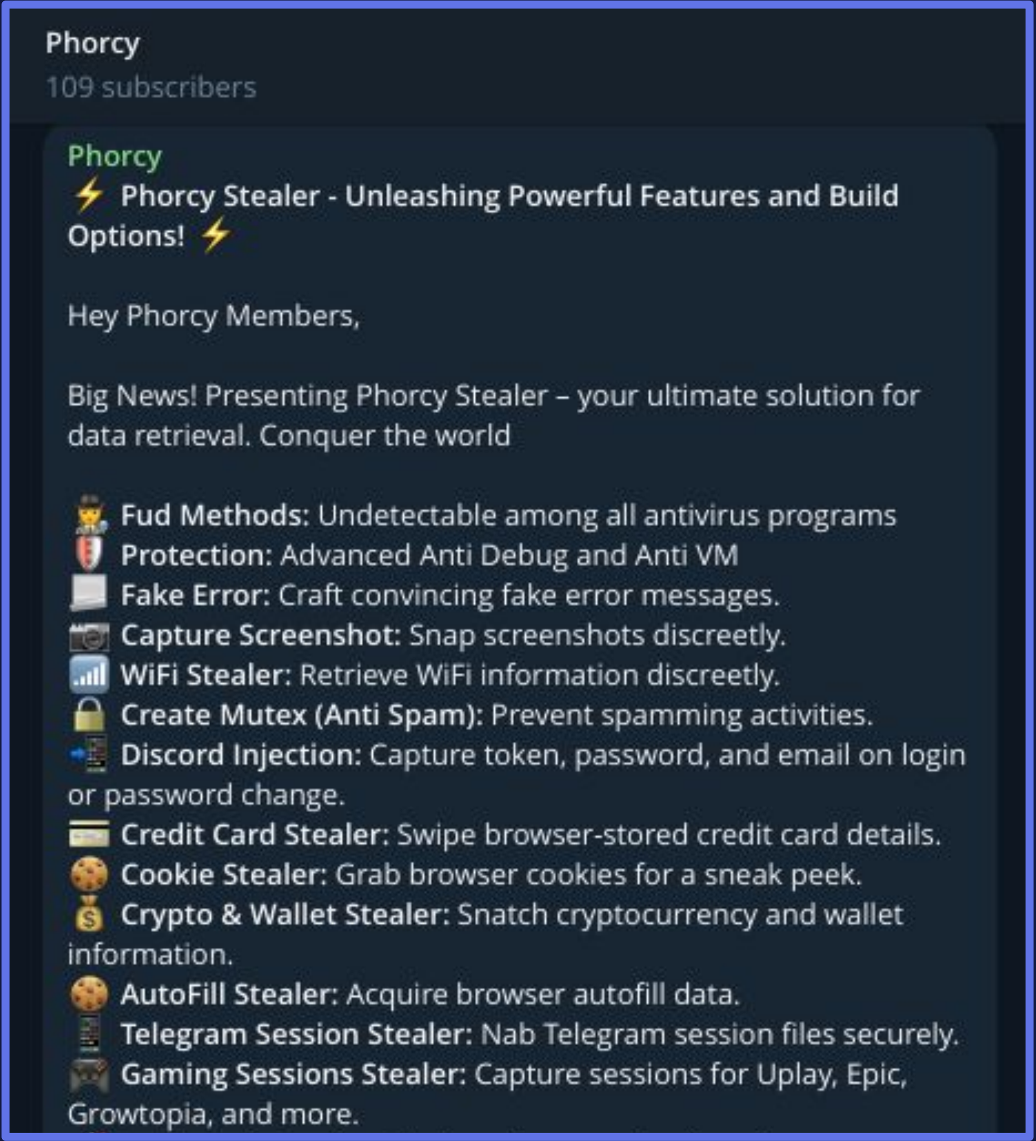
Big News! Presenting Phorcy Stealer – your ultimate solution for data retrieval. Conquer the world

🕵 **Fud Methods:** Undetectable among all antivirus programs
🛡 **Protection:** Advanced Anti Debug and Anti VM
💻 **Fake Error:** Craft convincing fake error messages.
📷 **Capture Screenshot:** Snap screenshots discreetly.
📶 **WiFi Stealer:** Retrieve WiFi information discreetly.
🔒 **Create Mutex (Anti Spam):** Prevent spamming activities.
📲 **Discord Injection:** Capture token, password, and email on login or password change.
💳 **Credit Card Stealer:** Swipe browser-stored credit card details.
🍪 **Cookie Stealer:** Grab browser cookies for a sneak peek.
💰 **Crypto & Wallet Stealer:** Snatch cryptocurrency and wallet information.
🍪 **AutoFill Stealer:** Acquire browser autofill data.
📱 **Telegram Session Stealer:** Nab Telegram session files securely.
🎮 **Gaming Sessions Stealer:** Capture sessions for Uplay, Epic, Growtopia, and more.



🕵 **Fud Methods:** Undetectable among all antivirus programs

Malware as a Service



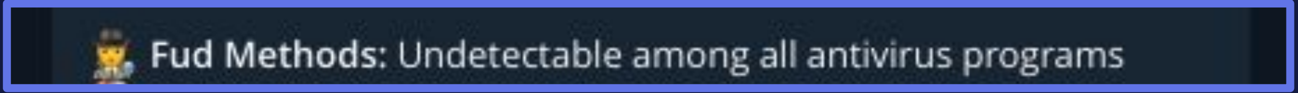
Phorcy
109 subscribers

Phorcy
⚡ Phorcy Stealer - Unleashing Powerful Features and Build Options! ⚡

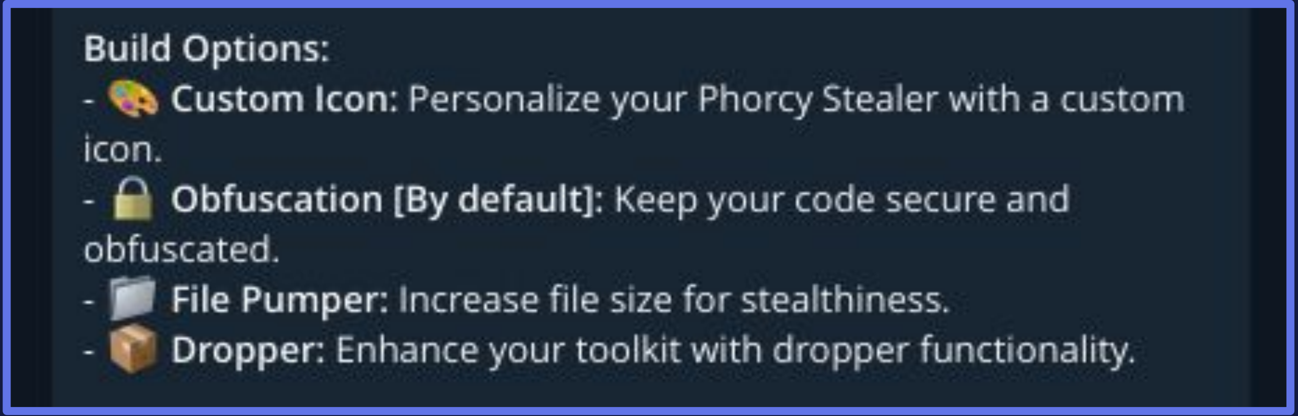
Hey Phorcy Members,

Big News! Presenting Phorcy Stealer – your ultimate solution for data retrieval. Conquer the world

👮 **Fud Methods:** Undetectable among all antivirus programs
🛡️ **Protection:** Advanced Anti Debug and Anti VM
💻 **Fake Error:** Craft convincing fake error messages.
📷 **Capture Screenshot:** Snap screenshots discreetly.
📶 **WiFi Stealer:** Retrieve WiFi information discreetly.
🔒 **Create Mutex (Anti Spam):** Prevent spamming activities.
📲 **Discord Injection:** Capture token, password, and email on login or password change.
💳 **Credit Card Stealer:** Swipe browser-stored credit card details.
🍪 **Cookie Stealer:** Grab browser cookies for a sneak peek.
💰 **Crypto & Wallet Stealer:** Snatch cryptocurrency and wallet information.
🍪 **AutoFill Stealer:** Acquire browser autofill data.
📱 **Telegram Session Stealer:** Nab Telegram session files securely.
🎮 **Gaming Sessions Stealer:** Capture sessions for Uplay, Epic, Growtopia, and more.

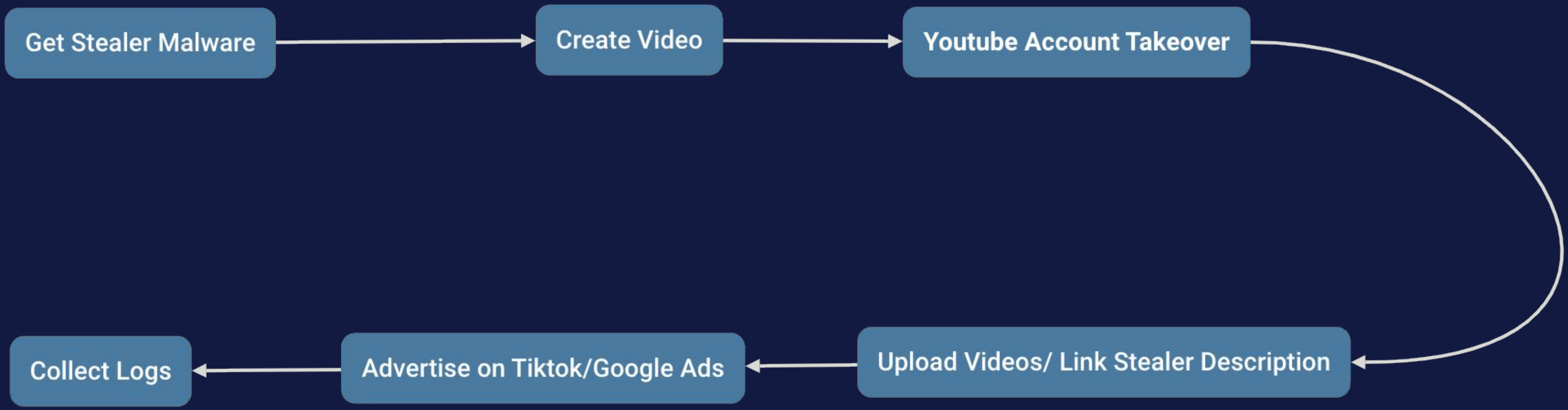


👮 **Fud Methods:** Undetectable among all antivirus programs

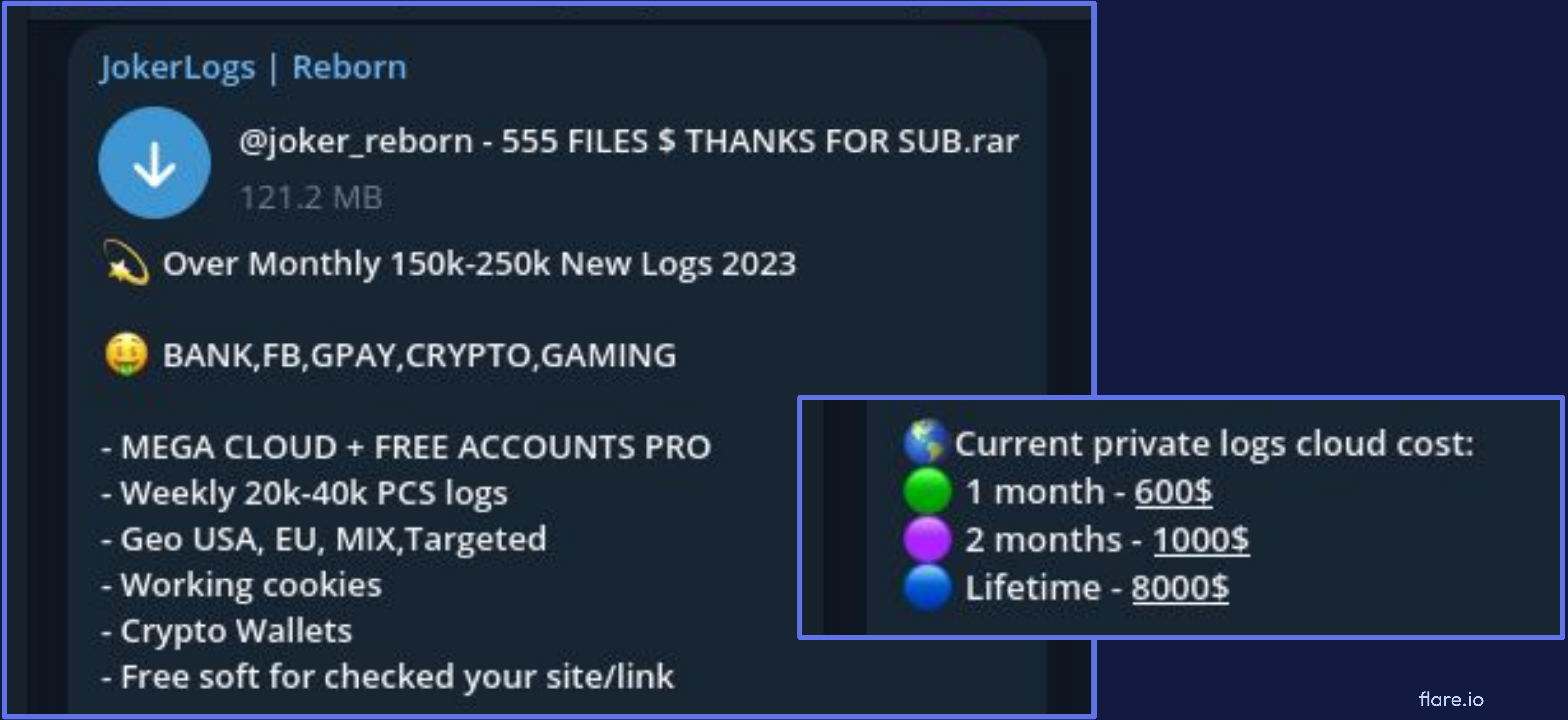


Build Options:
- 🎨 **Custom Icon:** Personalize your Phorcy Stealer with a custom icon.
- 🔒 **Obfuscation [By default]:** Keep your code secure and obfuscated.
- 📁 **File Pumper:** Increase file size for stealthiness.
- 📦 **Dropper:** Enhance your toolkit with dropper functionality.

Infostealer Campaign: One Example


Get Stealer Malware
Create Video
Youtube Account Takeover
Upload Videos/ Link Stealer Description
Advertise on Tiktok/Google Ads
Collect Logs

How does distribution work?



JokerLogs | Reborn

@joker_reborn - 555 FILES $ THANKS FOR SUB.rar

121.2 MB

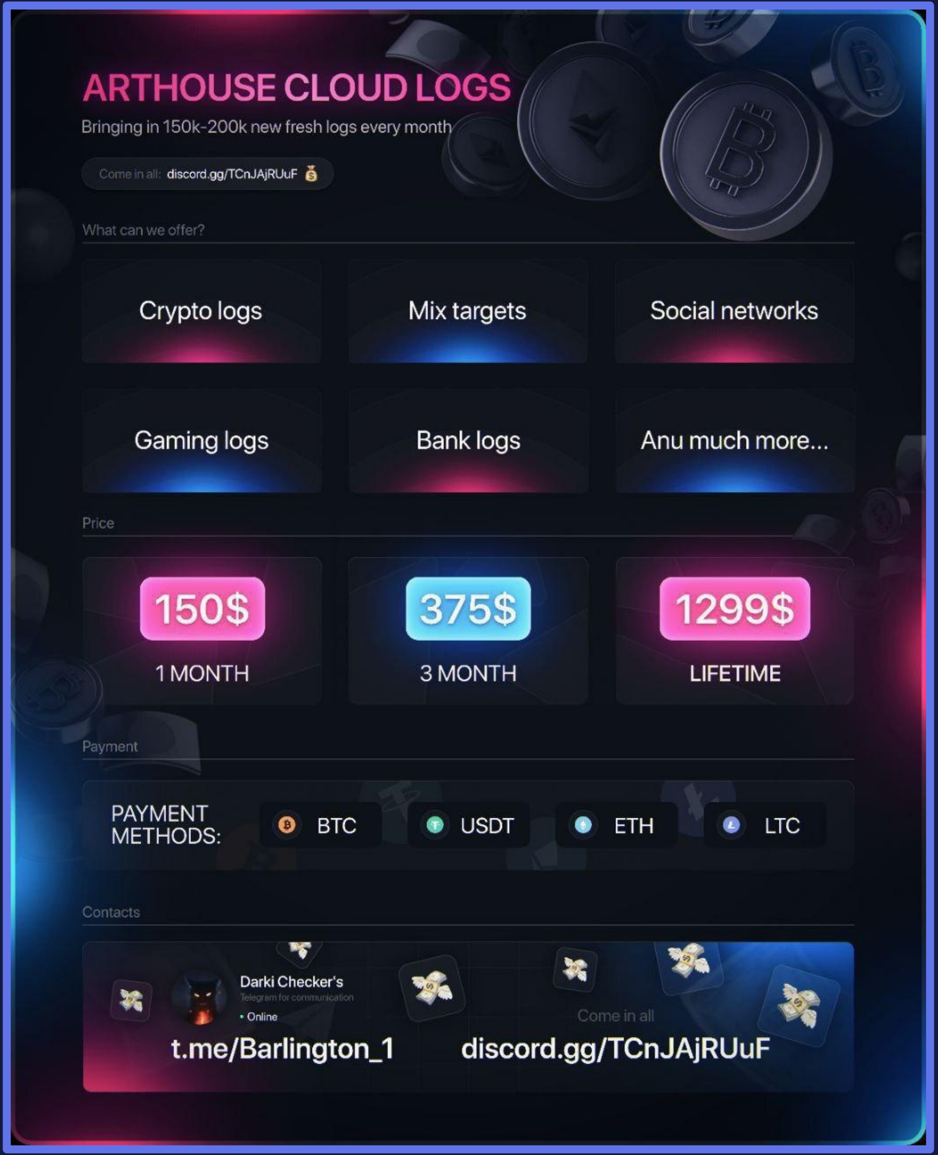
💫 Over Monthly 150k-250k New Logs 2023

🤑 BANK,FB,GPAY,CRYPTO,GAMING

- MEGA CLOUD + FREE ACCOUNTS PRO
- Weekly 20k-40k PCS logs
- Geo USA, EU, MIX,Targeted
- Working cookies
- Crypto Wallets
- Free soft for checked your site/link

🌎 Current private logs cloud cost:
🟢 1 month - 600$
🟣 2 months - 1000$
🔵 Lifetime - 8000$

How does distribution work?



ARTHOUSE CLOUD LOGS

Bringing in 150k-200k new fresh logs every month

Come in all: discord.gg/TCnJAjRUuF 💰

What can we offer?

Crypto logs

Mix targets

Social networks

Gaming logs

Bank logs

Anu much more...

Price

150$ 1 MONTH

375$ 3 MONTH

1299$ LIFETIME

Payment

PAYMENT METHODS: BTC USDT ETH LTC

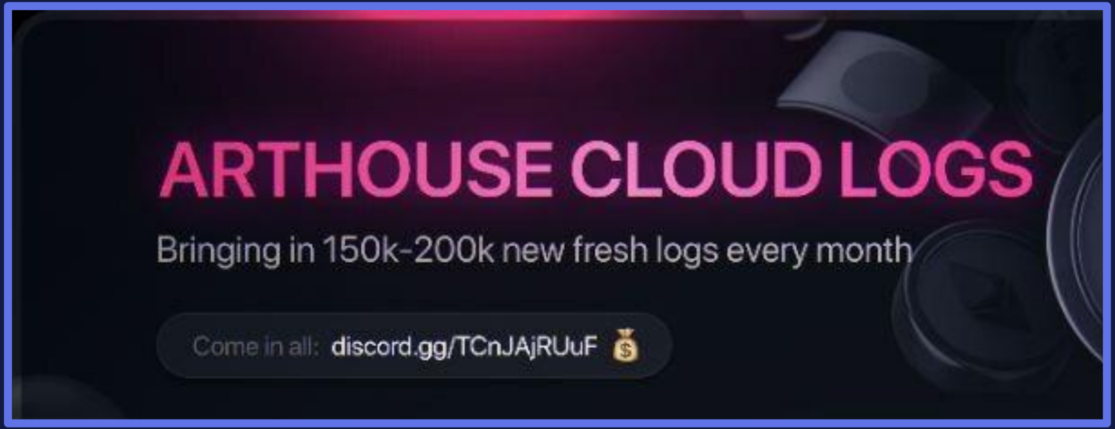
Contacts

Darki Checker's
Telegram for communication
• Online

t.me/Barlington_1

Come in all

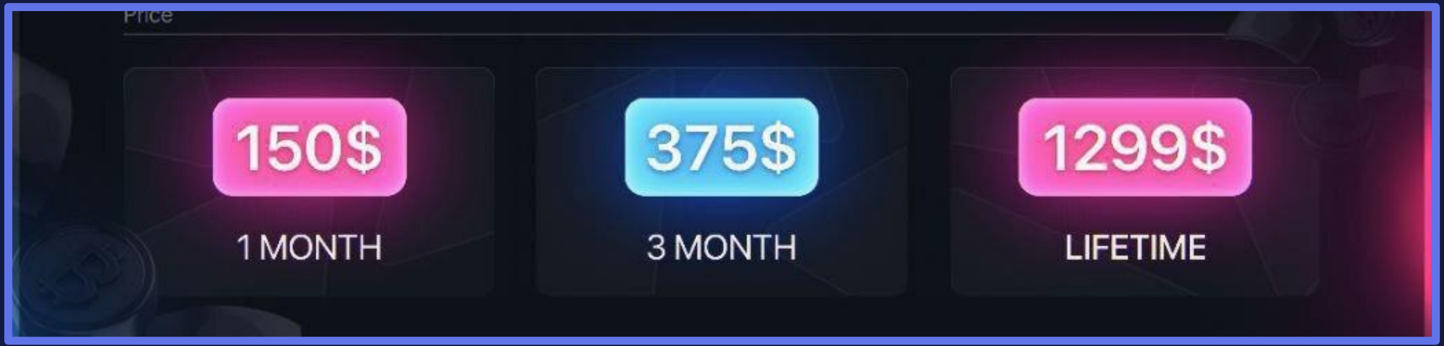
discord.gg/TCnJAjRUuF



ARTHOUSE CLOUD LOGS

Bringing in 150k-200k new fresh logs every month

Come in all: discord.gg/TCnJAjRUuF 💰



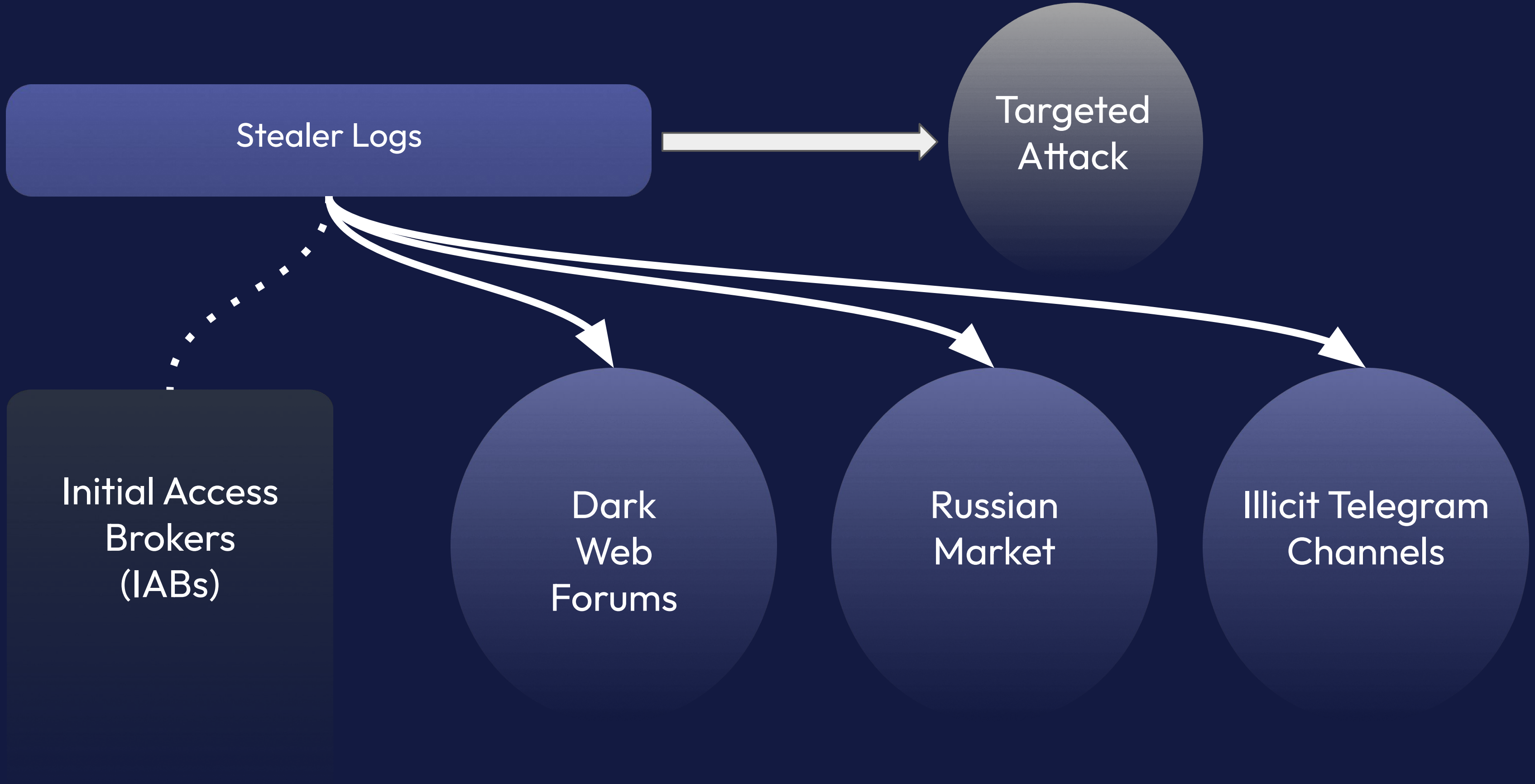
Price

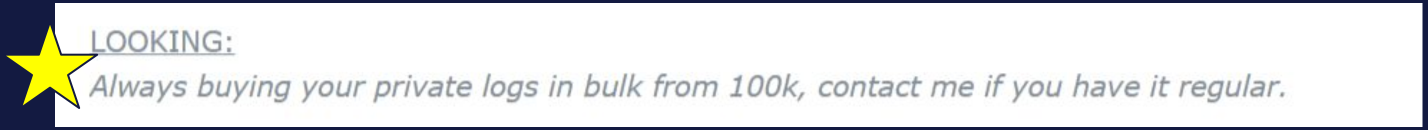
150$ 1 MONTH

375$ 3 MONTH

1299$ LIFETIME

Where do "High Value Logs" Go?




LOOKING:

Always buying your private logs in bulk from 100k, contact me if you have it regular.

Wanna free Stealer Log, dear?
KIRKLAND
Chicken Breast
Kids love The Cheeses!
8.99
6.99
FIRE EXTINGUISHER
TOOTH PICKS
30268 LIBBY'S VIENNA SAUSAGES
4.49

Wanna free
Stealer Log, dear?
KIRKLAND
Chicken Breast
Kids love The Cheeses!
TOOTH PICKS
30268
LIBBY'S
VIENNA SAUSAGES
4.49

How widespread exactly is this?

Stealer Logs by the Numbers:

- ~1 Million Logs Per Week
- 120 Million Total Logs identified (Unique)
- Roughly 15 Million Logs Contain Corporate Credentials
- Responsible for many major breaches including Ticketmaster, AT&T, Santander Bank.
- Threat actors can target customer accounts of major providers using these logs

> “In this era, the focus has shifted to *logging in* rather than *hacking in*”
>
> ***IBM X-FORCE Threat intelligence Report, 2024***

snowflake

ticketmaster

Santander
Consumer Bank

23andMe

CHANGE
HEALTHCARE

okta

flare

The shiny “new” feature

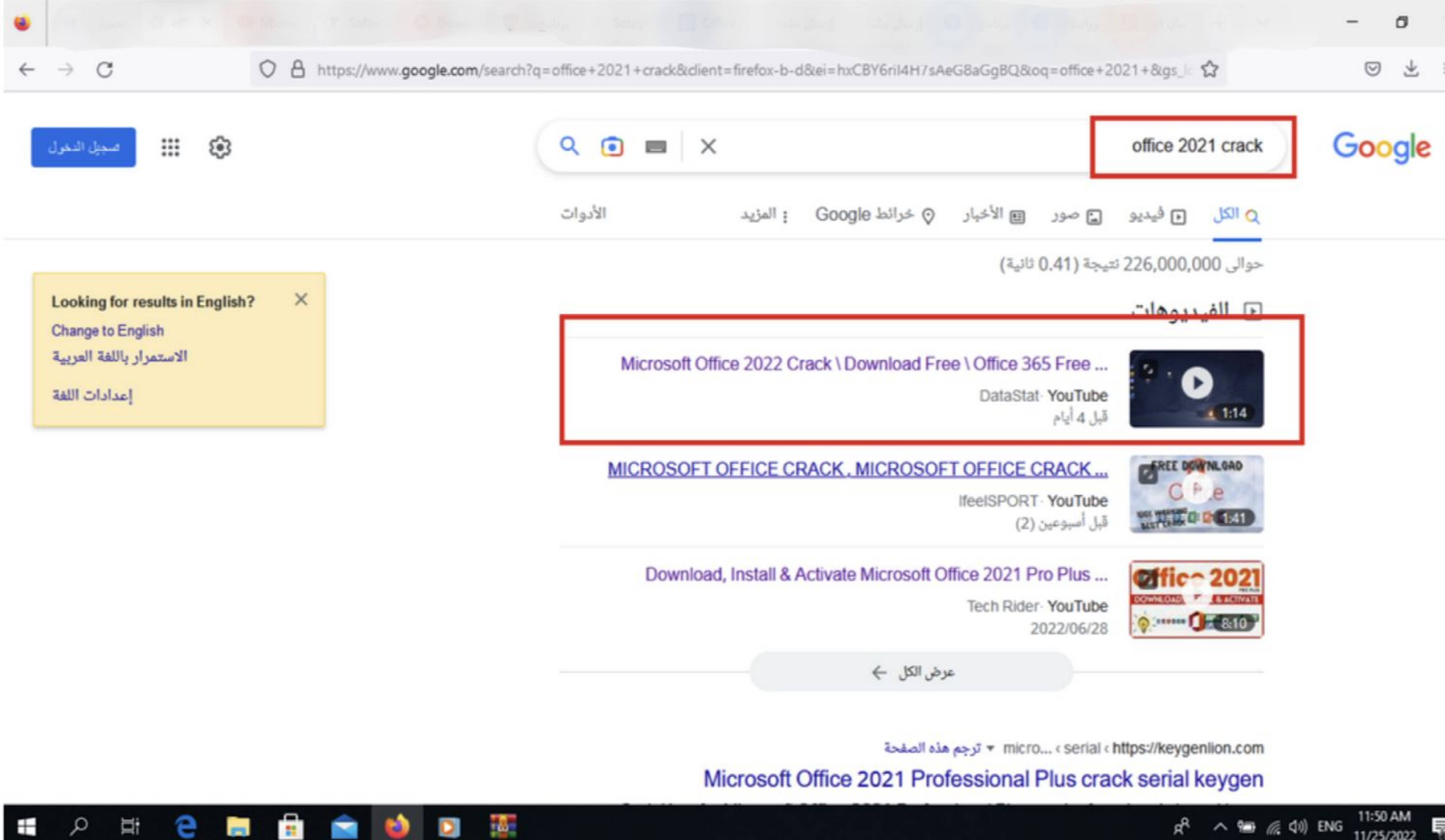
Mid-Heist selfies

Two Campaigns

Microsoft

MidJ0urney

Microsoft



https://www.google.com/search?q=office+2021+crack&client=firefox-b-d&ei=hxCBY6riI4H7sAeG8aGgBQ&oq=office+2021+&gs_l

office 2021 crack

حوالى 226,000,000 نتيجة (0.41 ثانية)

الفيديوهات

Microsoft Office 2022 Crack \ Download Free \ Office 365 Free ...
YouTube ·DataStat
قبل 4 أيام

MICROSOFT OFFICE CRACK , MICROSOFT OFFICE CRACK ...
YouTube ·IfeelSPORT
قبل أسبوعين (2)

Download, Install & Activate Microsoft Office 2021 Pro Plus ...
YouTube ·Tech Rider
2022/06/28

عرض الكل ←

https://keygenlion.com › serial › micro... ▾ ترجم هذه الصفحة

Microsoft Office 2021 Professional Plus crack serial keygen

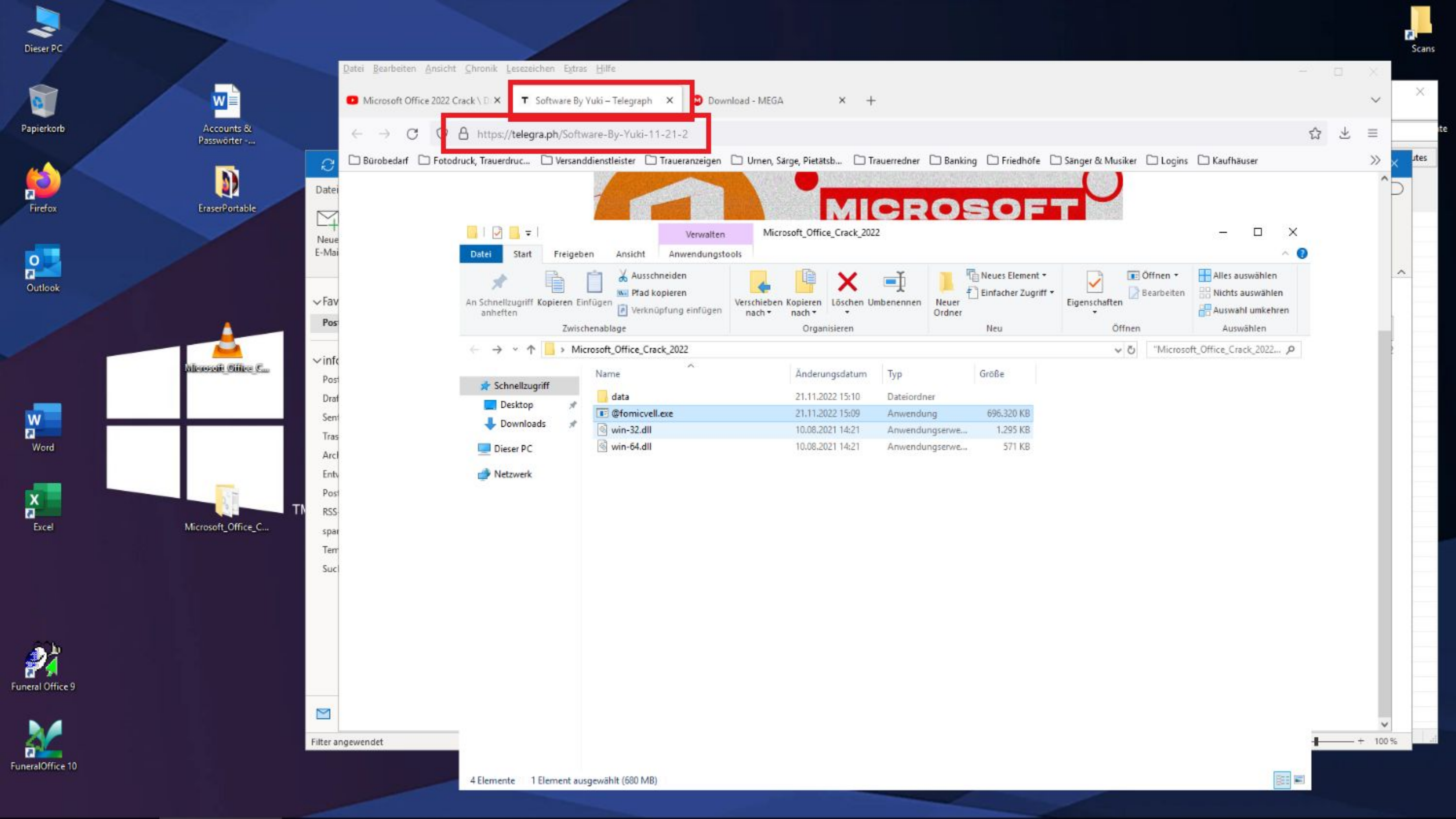
Looking for results in English?

Change to English

الاستمرار باللغة العربية

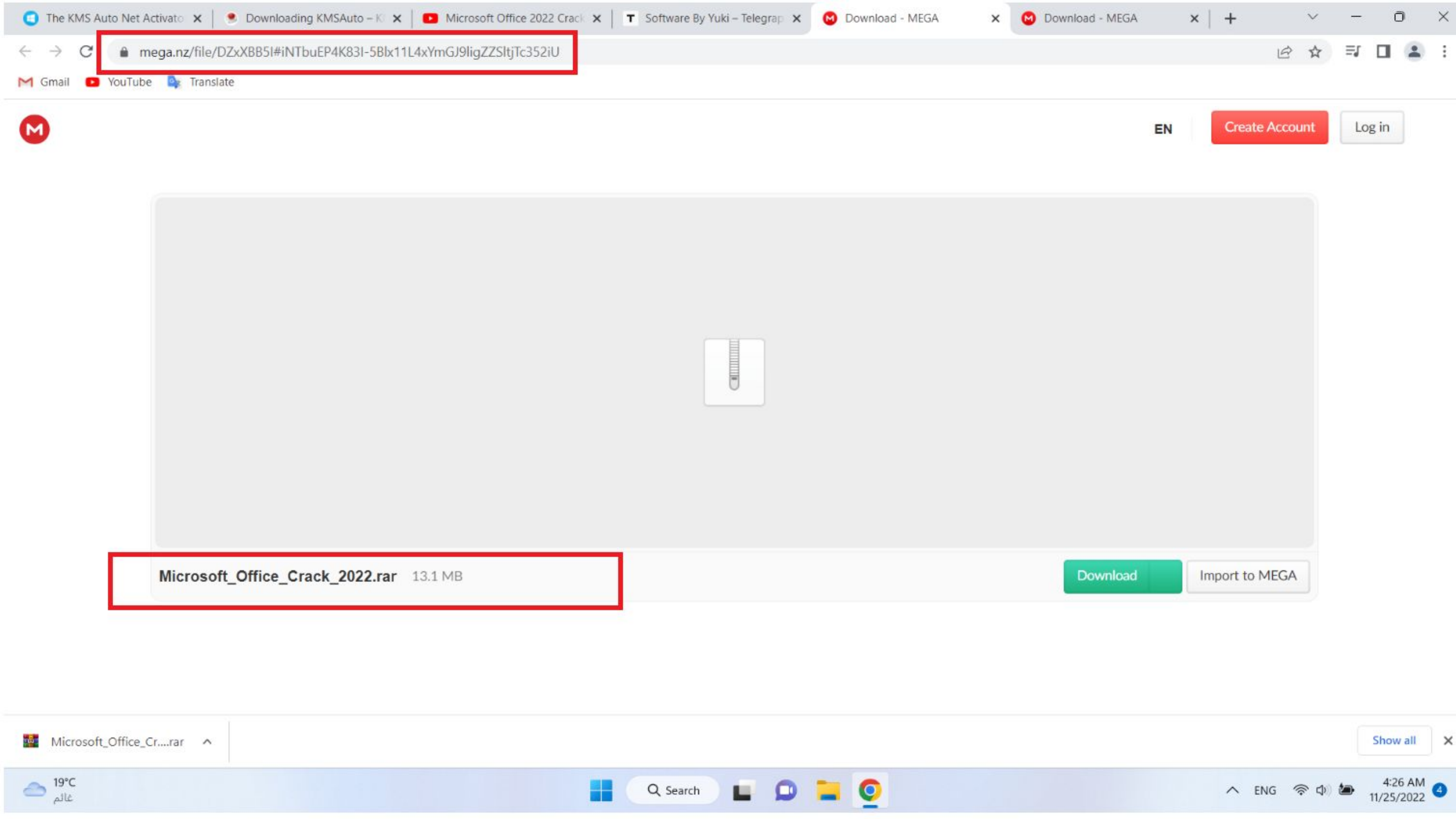
إعدادات اللغة

11:50 AM
11/25/2022



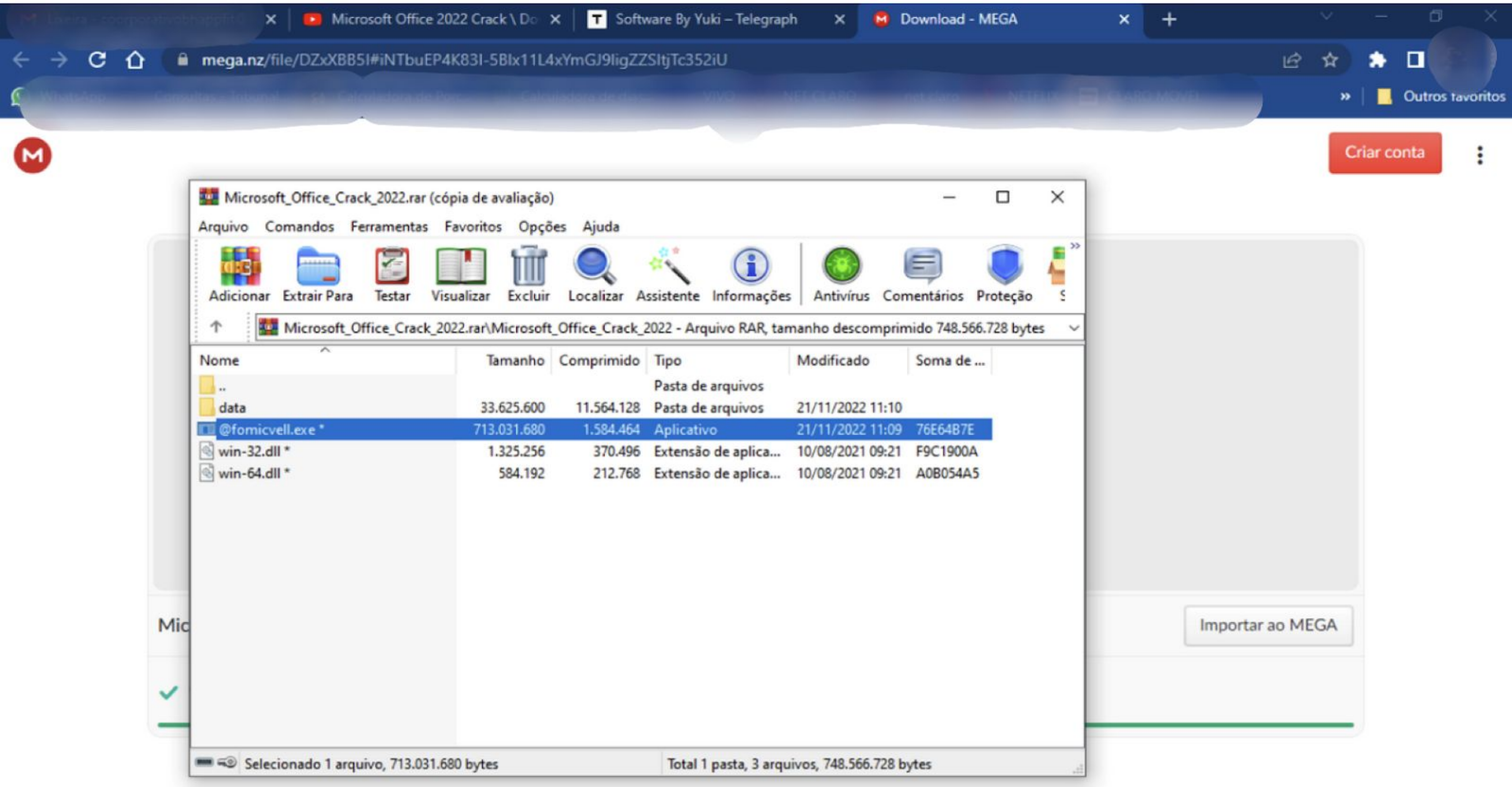
Name	Änderungsdatum	Typ	Größe
data	21.11.2022 15:10	Dateiordner	
@fomicvell.exe	21.11.2022 15:09	Anwendung	696.320 KB
win-32.dll	10.08.2021 14:21	Anwendungserwe...	1.295 KB
win-64.dll	10.08.2021 14:21	Anwendungserwe...	571 KB

4 Elemente 1 Element ausgewählt (680 MB)



mega.nz/file/DZxXBB5I#iNTbuEP4K83I-5Blx11L4xYmGJ9ligZZSltjTc352iU

Microsoft_Office_Crack_2022.rar 13.1 MB



mega.nz/file/DZxXBB5I#iNTbuEP4K83I-5BIx11L4xYmGJ9ligZZSItjTc352iU

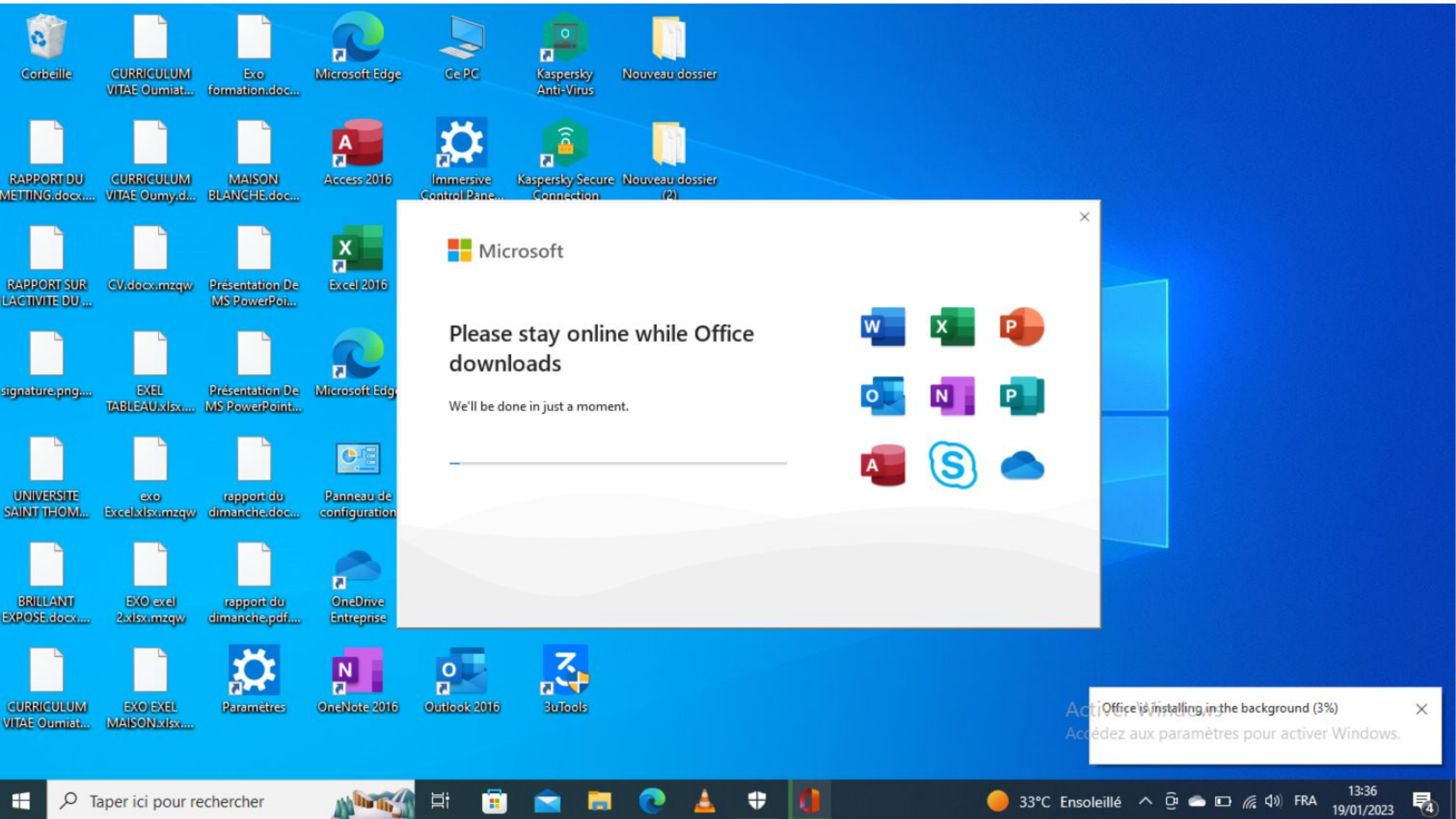
Microsoft_Office_Crack_2022.rar (cópia de avaliação)

Microsoft_Office_Crack_2022.rar\Microsoft_Office_Crack_2022 - Arquivo RAR, tamanho descomprimido 748.566.728 bytes

Nome	Tamanho	Comprimido	Tipo	Modificado	Soma de ...
..			Pasta de arquivos		
data	33.625.600	11.564.128	Pasta de arquivos	21/11/2022 11:10	
@fomicvell.exe *	713.031.680	1.584.464	Aplicativo	21/11/2022 11:09	76E64B7E
win-32.dll *	1.325.256	370.496	Extensão de aplica...	10/08/2021 09:21	F9C1900A
win-64.dll *	584.192	212.768	Extensão de aplica...	10/08/2021 09:21	A0B054A5

Selecionado 1 arquivo, 713.031.680 bytes

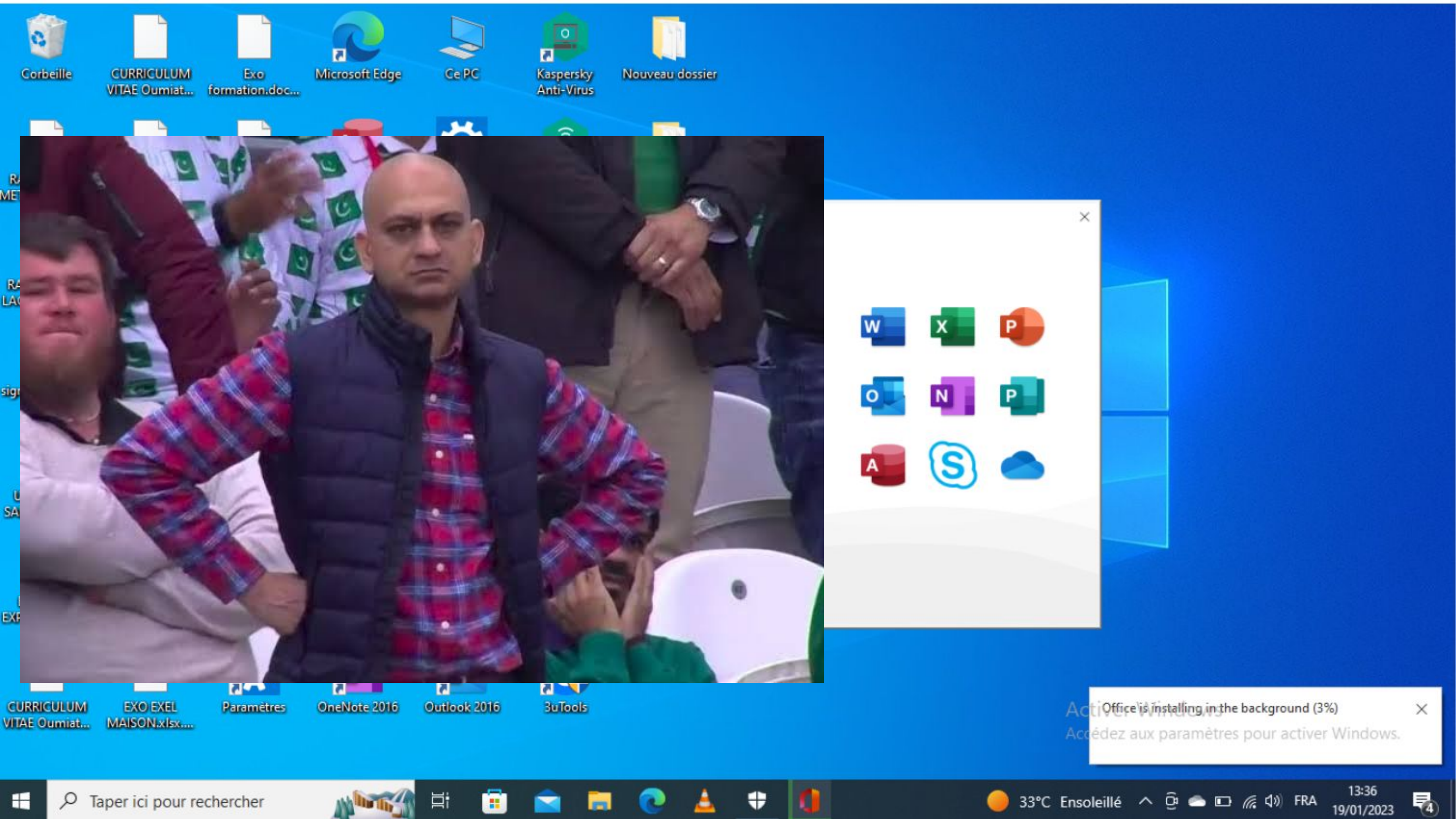
Total 1 pasta, 3 arquivos, 748.566.728 bytes



Please stay online while Office downloads

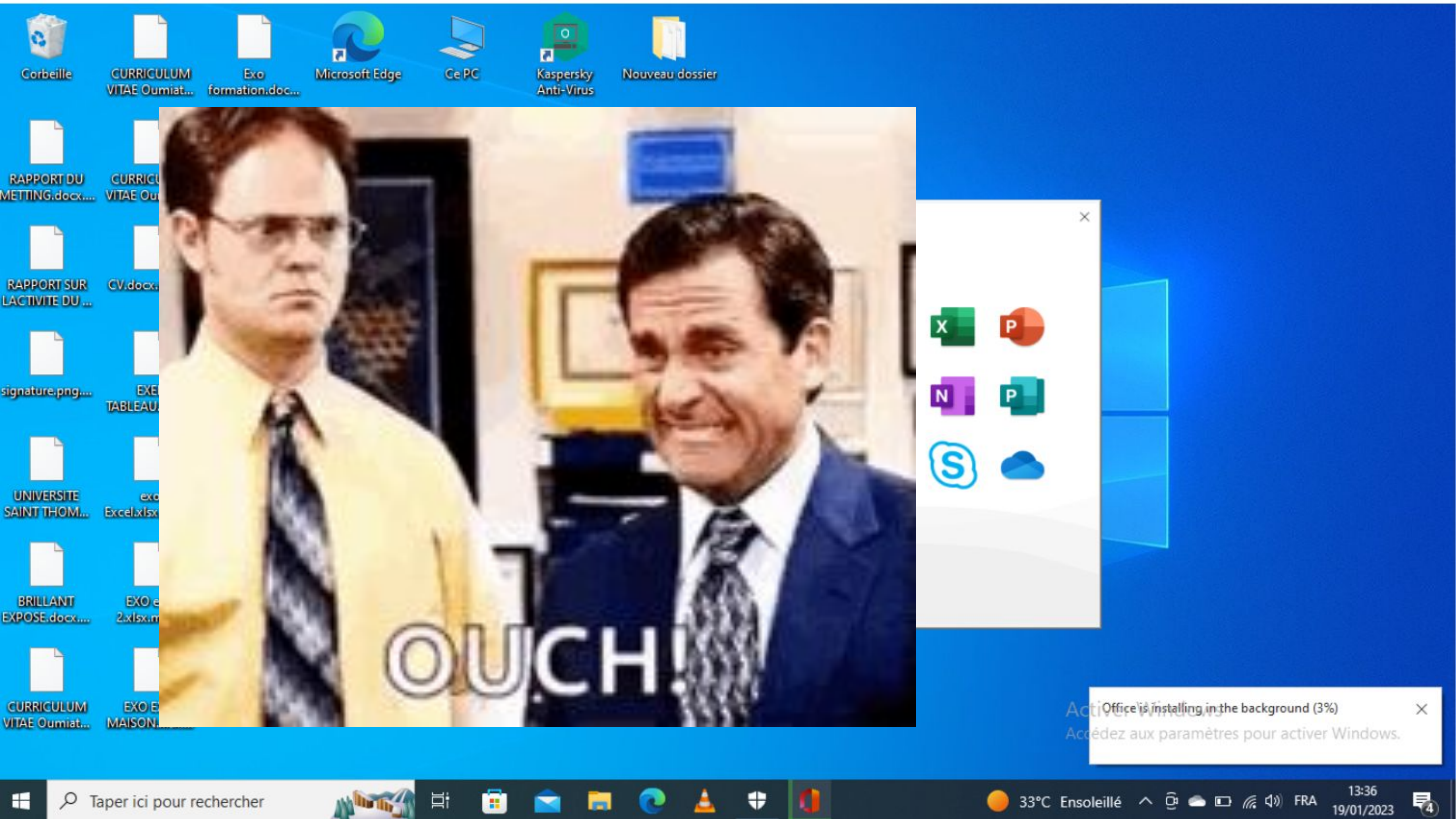
We'll be done in just a moment.

Office is installing in the background (3%)



Office is installing in the background (3%)

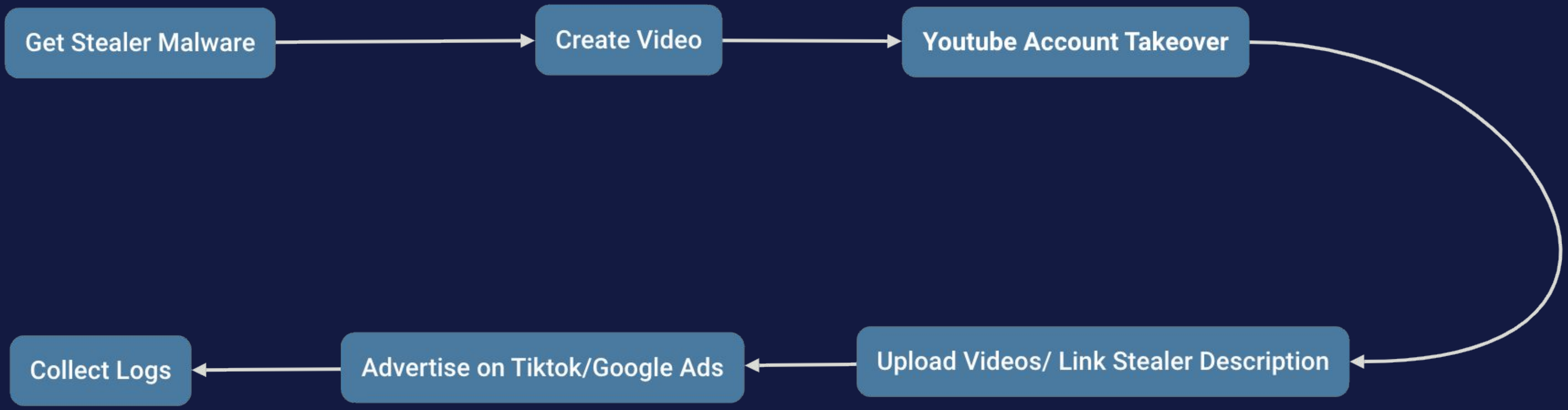
Activer Windows
Accédez aux paramètres pour activer Windows.



Office is installing in the background (3%)

Activer Windows
Accédez aux paramètres pour activer Windows.

Infostealer Campaign: One Example



Get Stealer Malware

Create Video

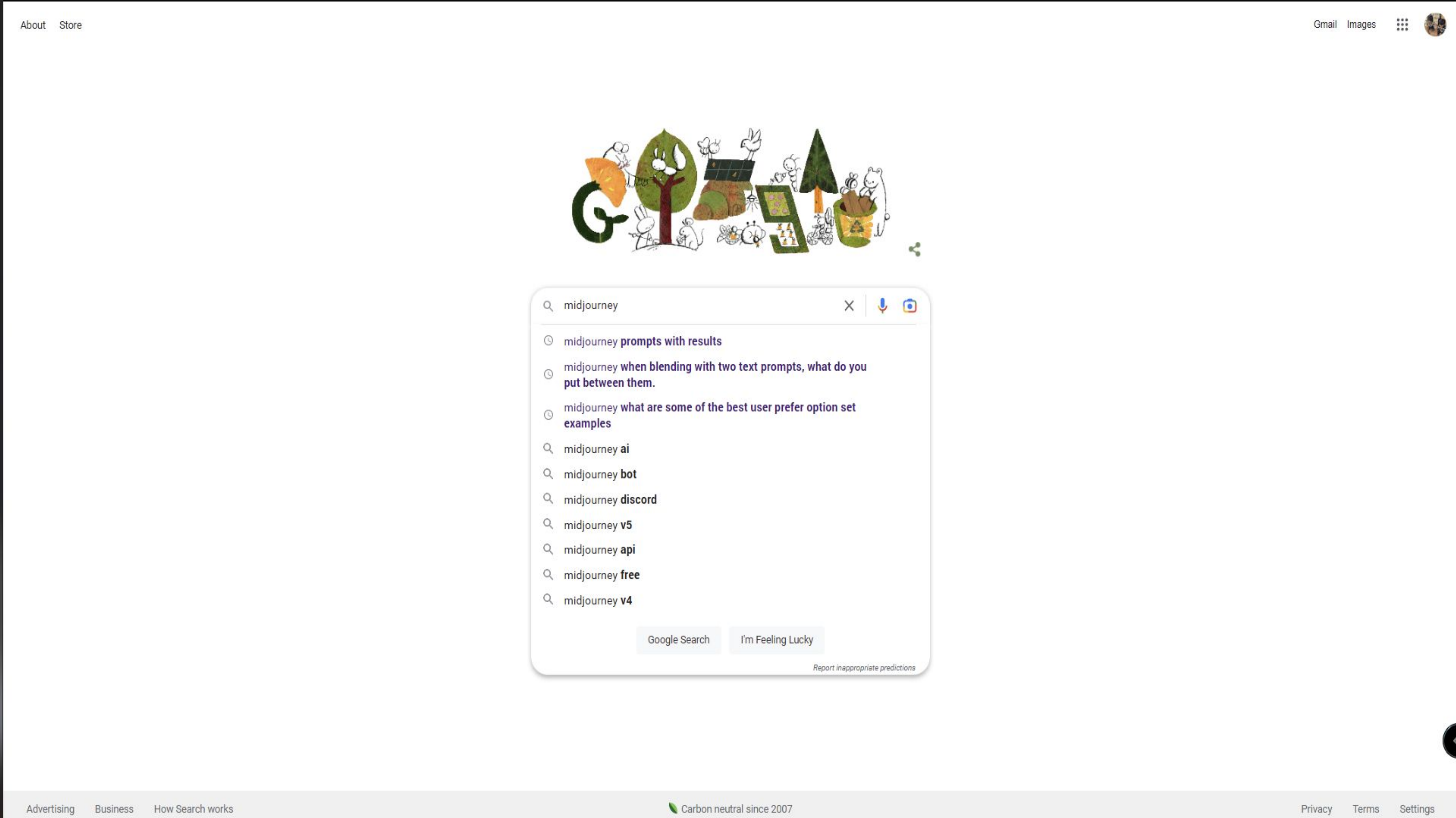
Youtube Account Takeover

Upload Videos/ Link Stealer Description

Advertise on Tiktok/Google Ads

Collect Logs

MidJ0urney



midjourney

midjourney **prompts with results**

midjourney **when blending with two text prompts, what do you put between them.**

midjourney **what are some of the best user prefer option set examples**

midjourney **ai**

midjourney **bot**

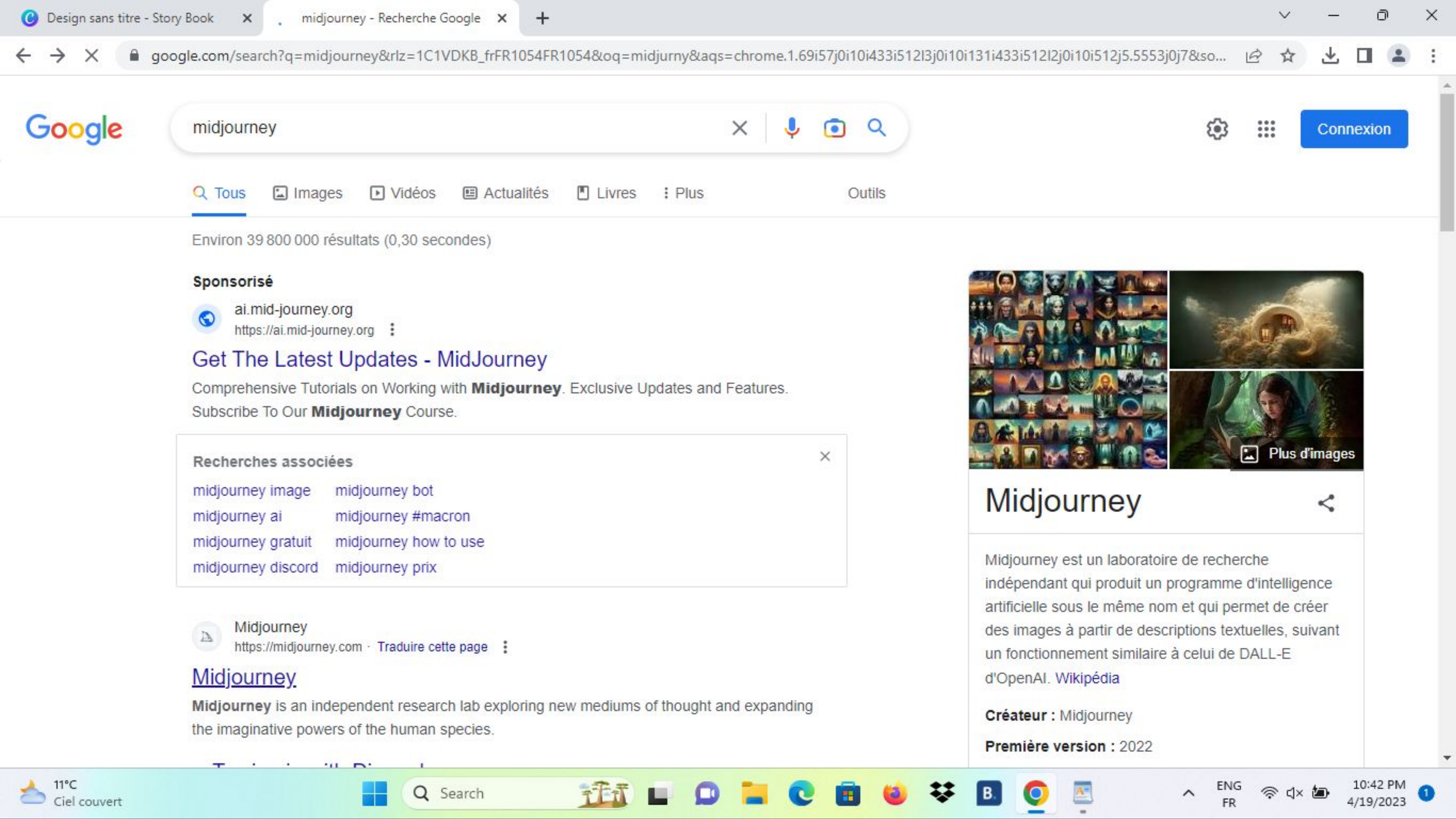
midjourney **discord**

midjourney **v5**

midjourney **api**

midjourney **free**

midjourney **v4**



Design sans titre - Story Book
midjourney - Recherche Google
google.com/search?q=midjourney&rlz=1C1VDKB_frFR1054FR1054&oq=midjurny&aqs=chrome.1.69i57j0i10i433i512l3j0i10i131i433i512l2j0i10i512j5.5553j0j7&so...
Google
midjourney
Connexion
Tous
Images
Vidéos
Actualités
Livres
Plus
Outils

Environ 39 800 000 résultats (0,30 secondes)

Sponsorisé

ai.mid-journey.org
https://ai.mid-journey.org

Get The Latest Updates - MidJourney

Comprehensive Tutorials on Working with **Midjourney**. Exclusive Updates and Features. Subscribe To Our **Midjourney** Course.

Recherches associées

midjourney image	midjourney bot
midjourney ai	midjourney #macron
midjourney gratuit	midjourney how to use
midjourney discord	midjourney prix

Midjourney
https://midjourney.com · Traduire cette page

Midjourney

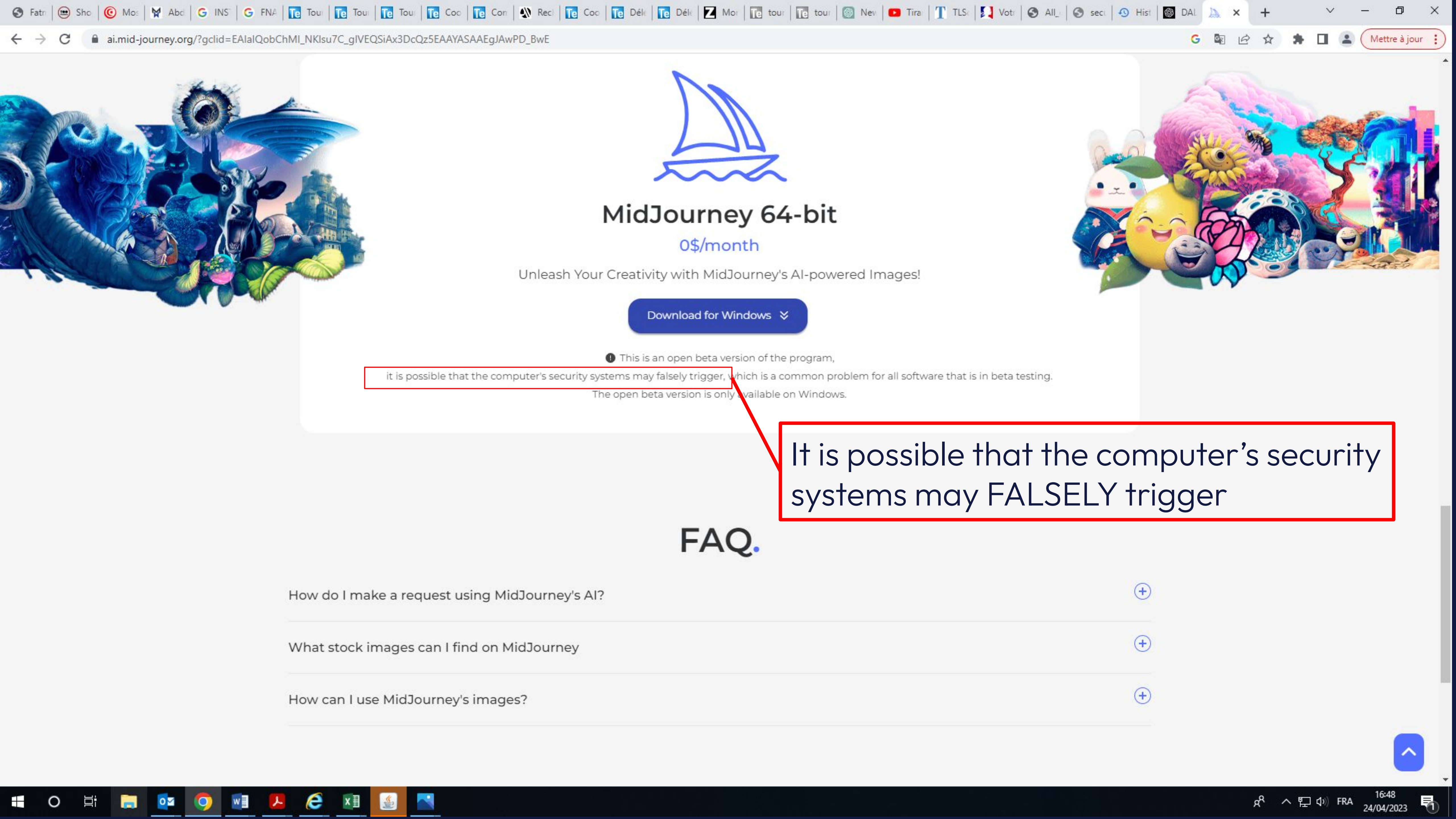
Midjourney is an independent research lab exploring new mediums of thought and expanding the imaginative powers of the human species.

Midjourney

Midjourney est un laboratoire de recherche indépendant qui produit un programme d'intelligence artificielle sous le même nom et qui permet de créer des images à partir de descriptions textuelles, suivant un fonctionnement similaire à celui de DALL-E d'OpenAI. Wikipédia

Créateur : Midjourney

Première version : 2022



ai.mid-journey.org/?gclid=EAIaIQobChMI_NKIsu7C_gIVEQSiAx3DcQz5EAAYASAAEgJAwPD_BwE
Mettre à jour
FRA
16:48
24/04/2023

MidJourney 64-bit

0$/month

Unleash Your Creativity with MidJourney's AI-powered Images!

Download for Windows

This is an open beta version of the program,
it is possible that the computer's security systems may falsely trigger, which is a common problem for all software that is in beta testing.
The open beta version is only available on Windows.

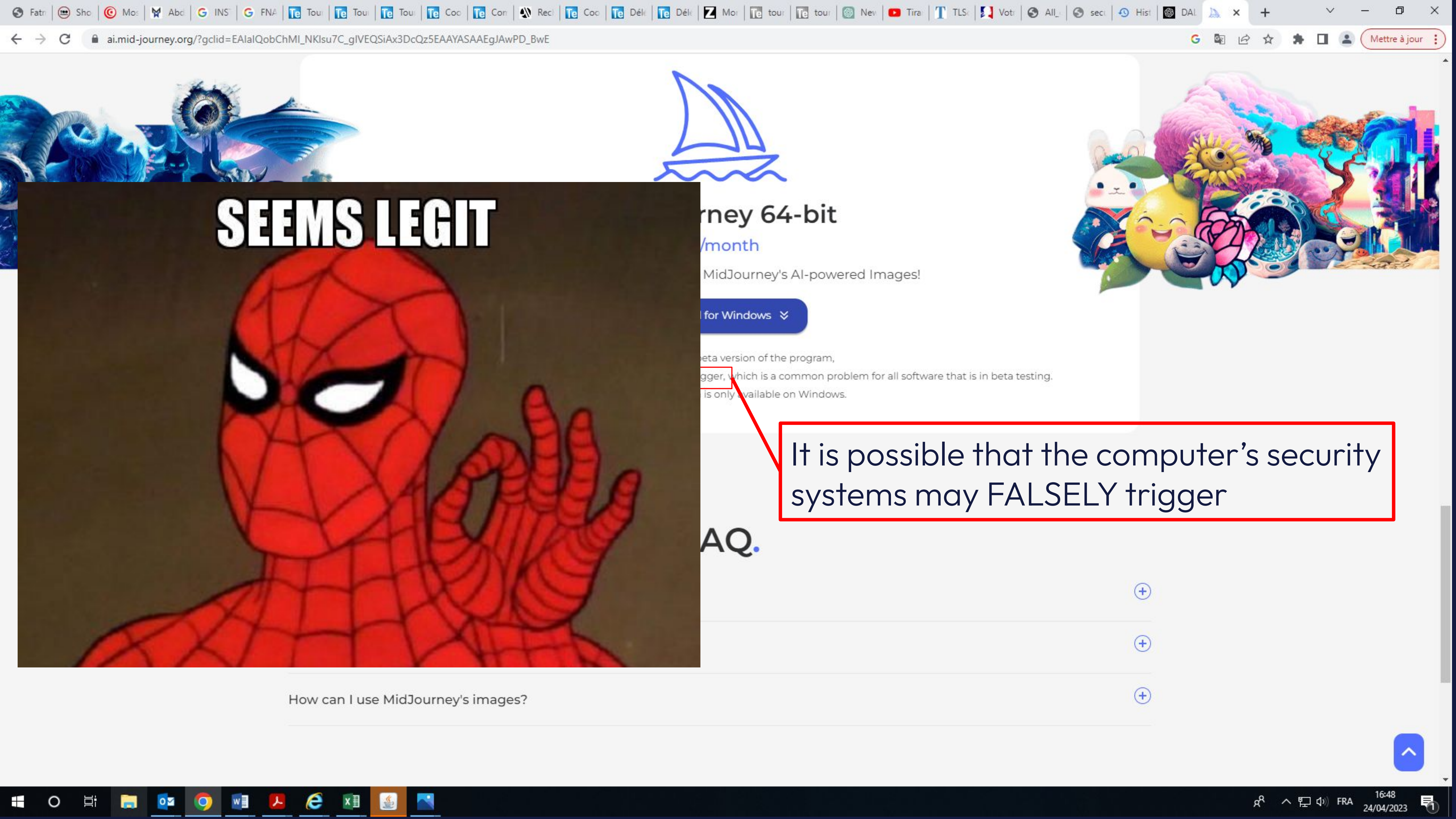
FAQ.

How do I make a request using MidJourney's AI? ⊕

What stock images can I find on MidJourney ⊕

How can I use MidJourney's images? ⊕

It is possible that the computer's security systems may FALSELY trigger



ai.mid-journey.org/?gclid=EAIaIQobChMI_NKlsu7C_gIVEQSiAx3DcQz5EAAYASAAEgJAwPD_BwE
Mettre à jour
SEEMS LEGIT
FRA
16:48
24/04/2023

rney 64-bit

/month

MidJourney's AI-powered Images!

for Windows

eta version of the program,

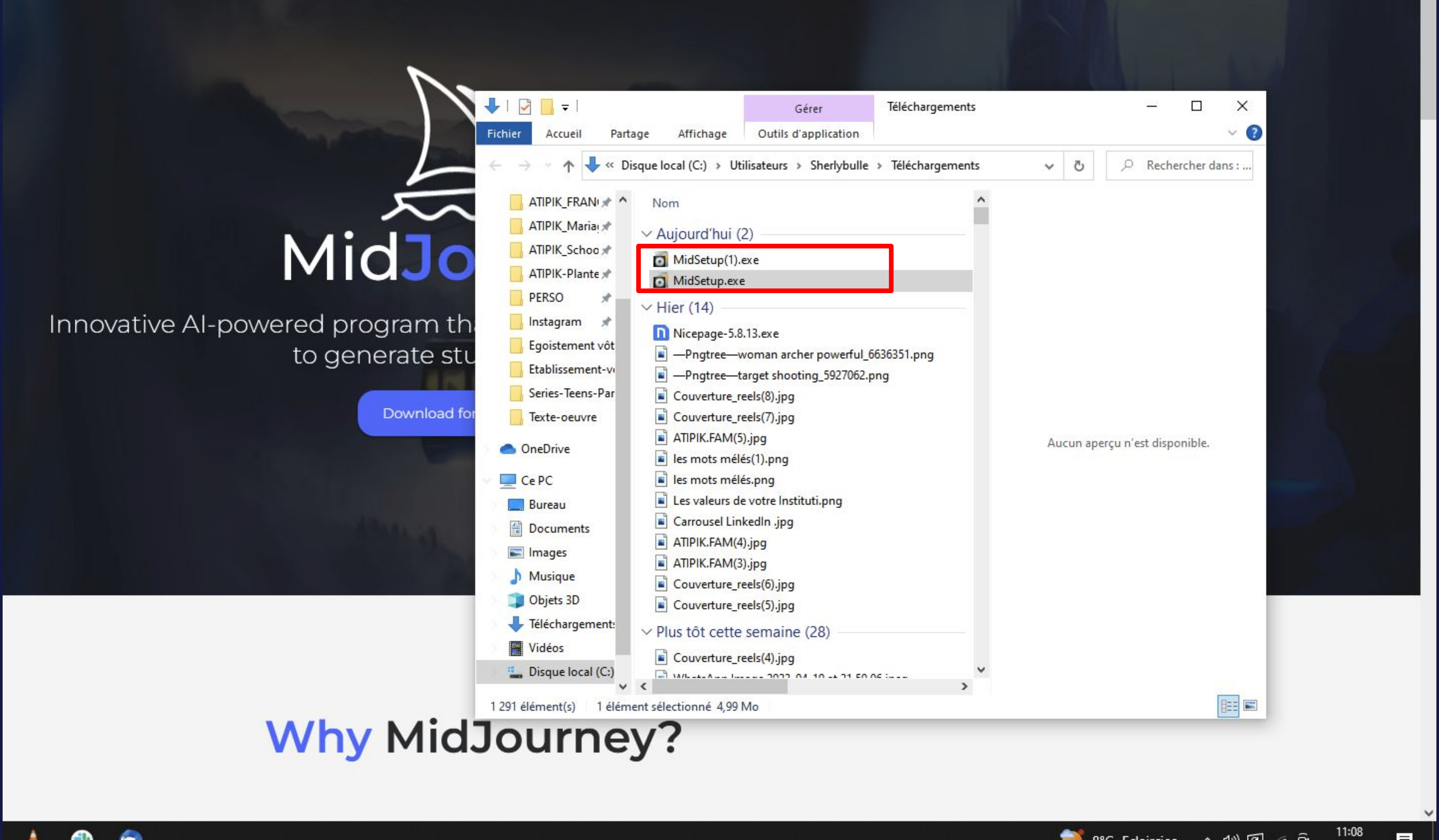
gger, which is a common problem for all software that is in beta testing.

is only available on Windows.

AQ.

How can I use MidJourney's images?

It is possible that the computer's security systems may FALSELY trigger



Aujourd'hui (2)

- MidSetup(1).exe
- MidSetup.exe

Hier (14)

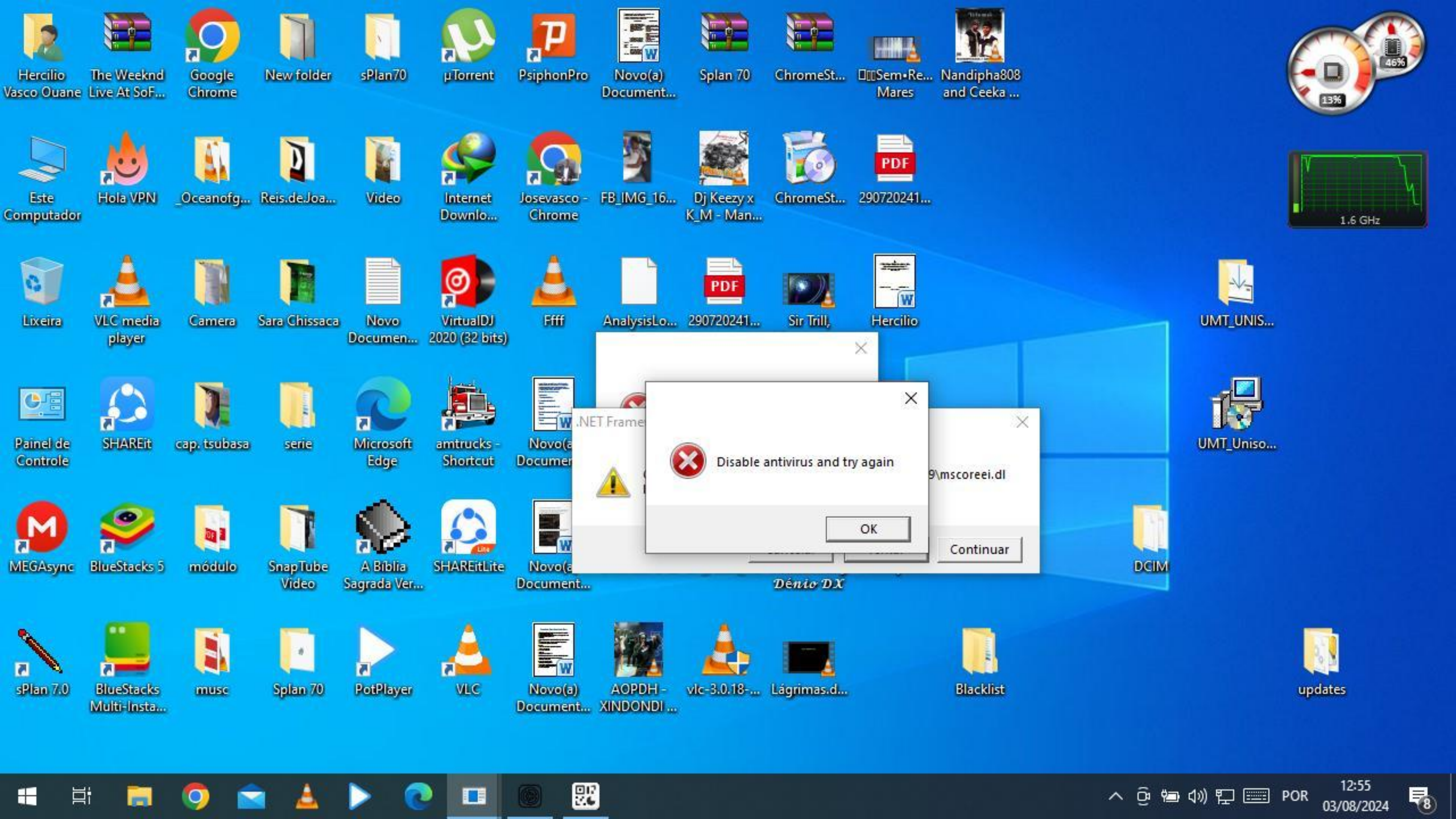
- Nicepage-5.8.13.exe
- —Pngtree—woman archer powerful_6636351.png
- —Pngtree—target shooting_5927062.png
- Couverture_reels(8).jpg
- Couverture_reels(7).jpg
- ATIPIK.FAM(5).jpg
- les mots mêlés(1).png
- les mots mêlés.png
- Les valeurs de votre Instituti.png
- Carrousel LinkedIn .jpg
- ATIPIK.FAM(4).jpg
- ATIPIK.FAM(3).jpg
- Couverture_reels(6).jpg
- Couverture_reels(5).jpg

Plus tôt cette semaine (28)

- Couverture_reels(4).jpg

1 291 élément(s) 1 élément sélectionné 4,99 Mo

Why MidJourney?



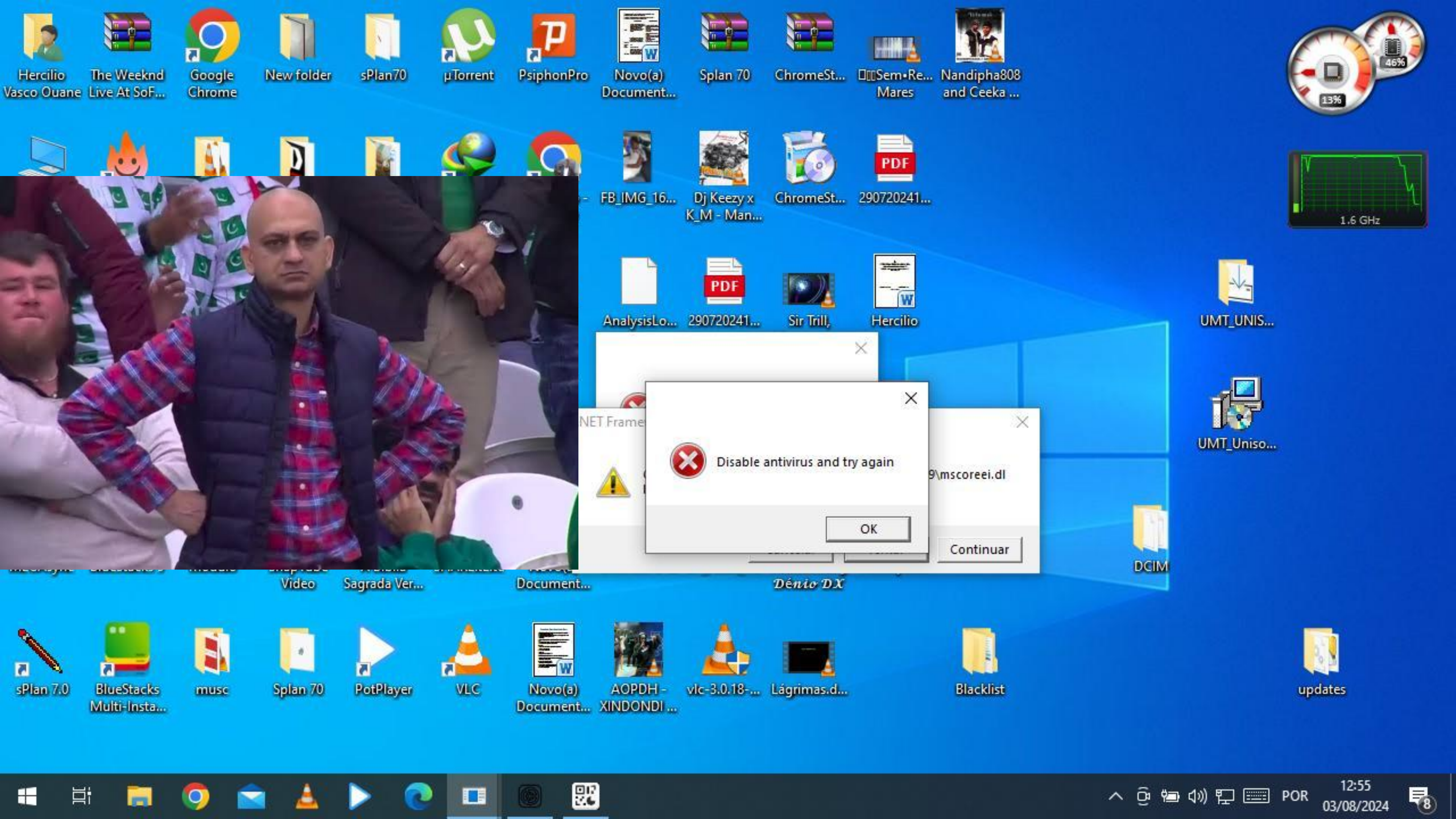
.NET Frame

9\mscoreei.dl

Disable antivirus and try again

OK

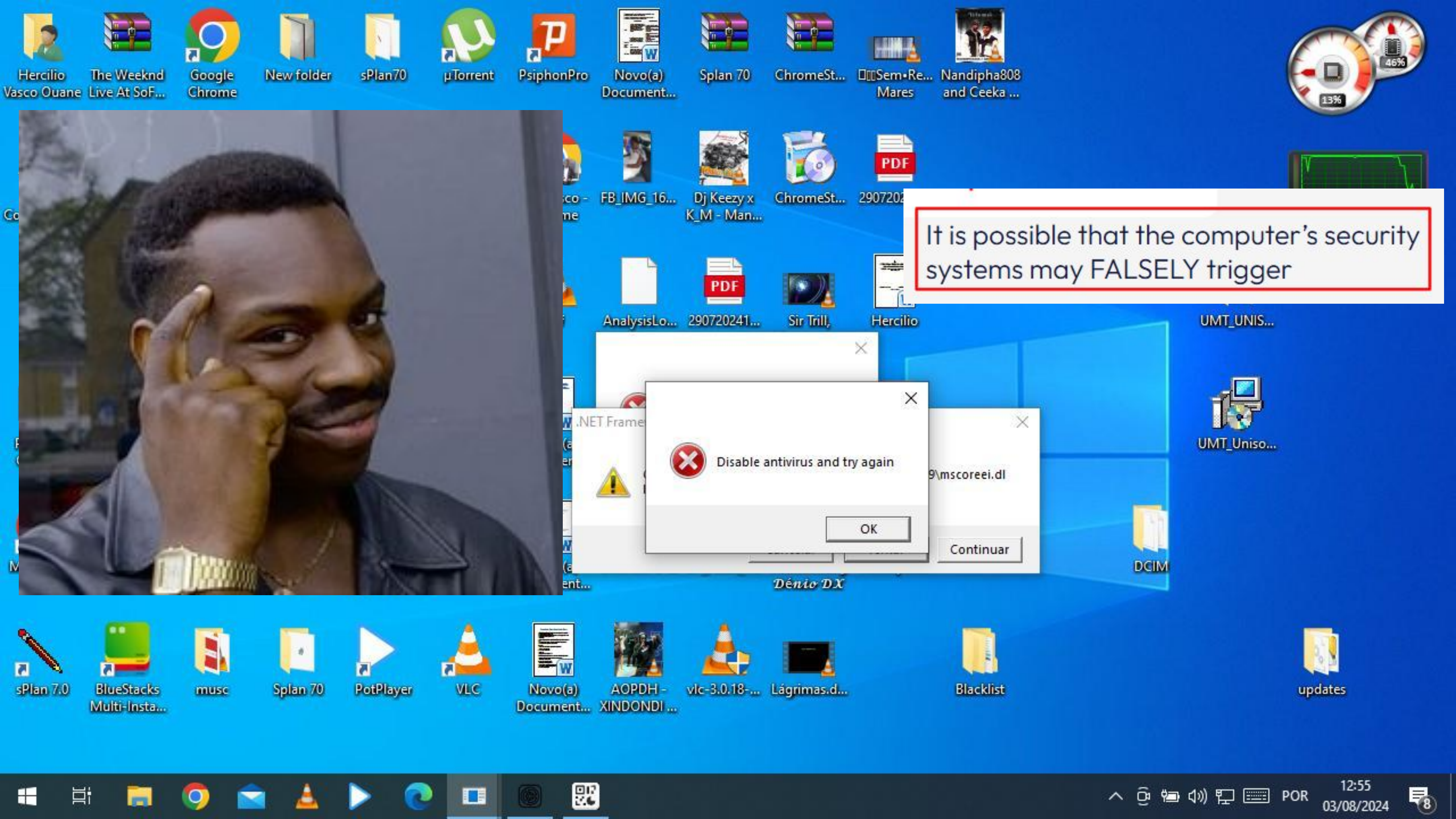
Continuar



Disable antivirus and try again

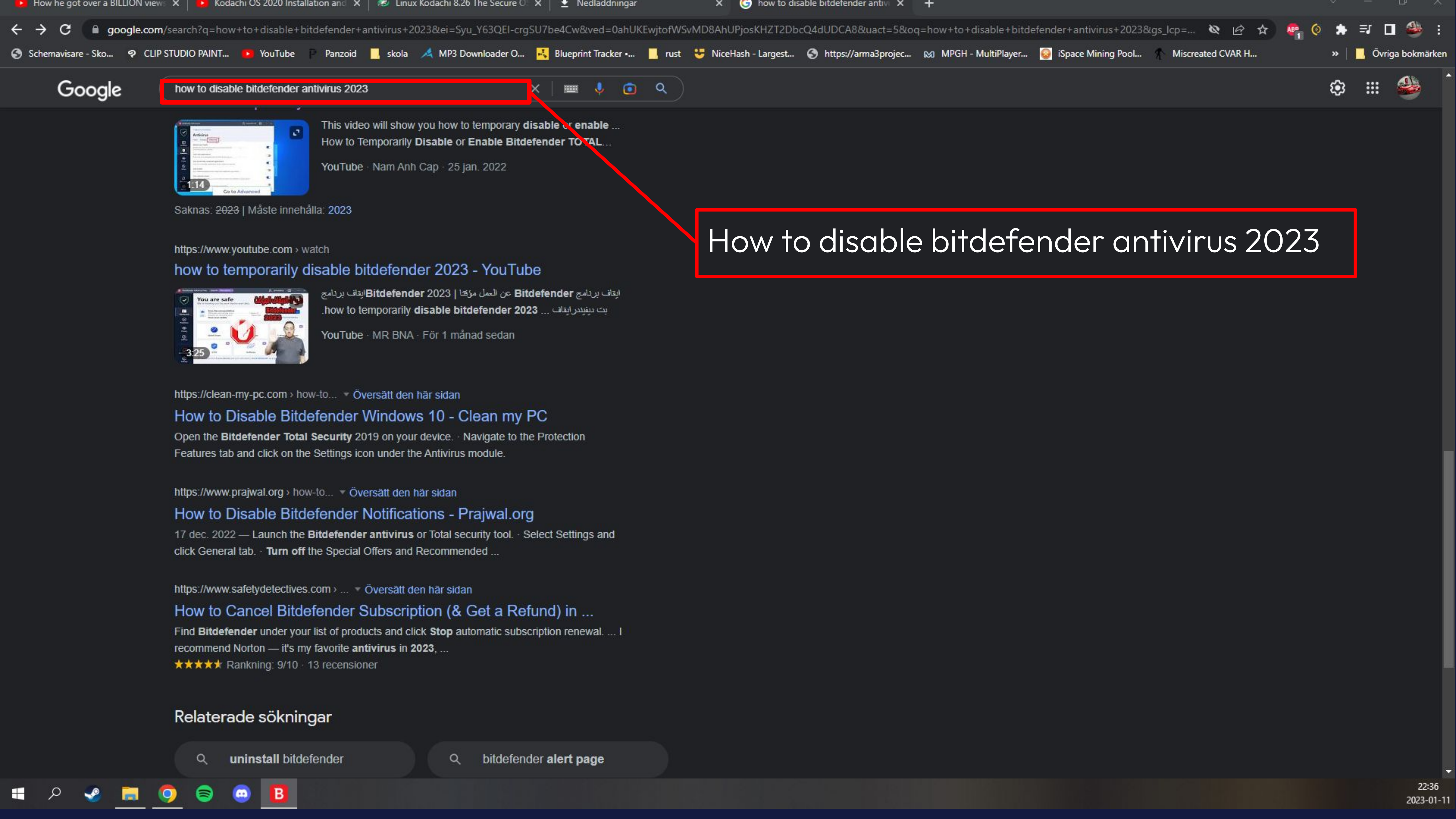
NET Frame

9\mscoreei.dl



It is possible that the computer's security systems may FALSELY trigger

Disable antivirus and try again



How to disable bitdefender antivirus 2023

google.com/search?q=how+to+disable+bitdefender+antivirus+2023&ei=Syu_Y63QEI-crgSU7be4Cw&ved=0ahUKEwjtofWSvMD8AhUPjosKHZT2DbcQ4dUDCA8&uact=5&oq=how+to+disable+bitdefender+antivirus+2023&gs_lcp=...
Google
how to disable bitdefender antivirus 2023

This video will show you how to temporary **disable** or **enable** ...
How to Temporarily **Disable** or **Enable Bitdefender TOTAL**...

YouTube · Nam Anh Cap · 25 jan. 2022

Saknas: ~~2023~~ | Måste innehålla: 2023

https://www.youtube.com › watch

how to temporarily disable bitdefender 2023 - YouTube

ايقاف برنامج **Bitdefender** عن العمل مؤقتا | 2023 **Bitdefender**ايقاف برنامج
بت ديفيندر ايقاف ... **disable bitdefender 2023** how to temporarily.

YouTube · MR BNA · För 1 månad sedan

https://clean-my-pc.com › how-to... ▾ Översätt den här sidan

How to Disable Bitdefender Windows 10 - Clean my PC

Open the **Bitdefender Total Security** 2019 on your device. · Navigate to the Protection Features tab and click on the Settings icon under the Antivirus module.

https://www.prajwal.org › how-to... ▾ Översätt den här sidan

How to Disable Bitdefender Notifications - Prajwal.org

17 dec. 2022 — Launch the **Bitdefender antivirus** or Total security tool. · Select Settings and click General tab. · **Turn off** the Special Offers and Recommended ...

https://www.safetydetectives.com › ... ▾ Översätt den här sidan

How to Cancel Bitdefender Subscription (& Get a Refund) in ...

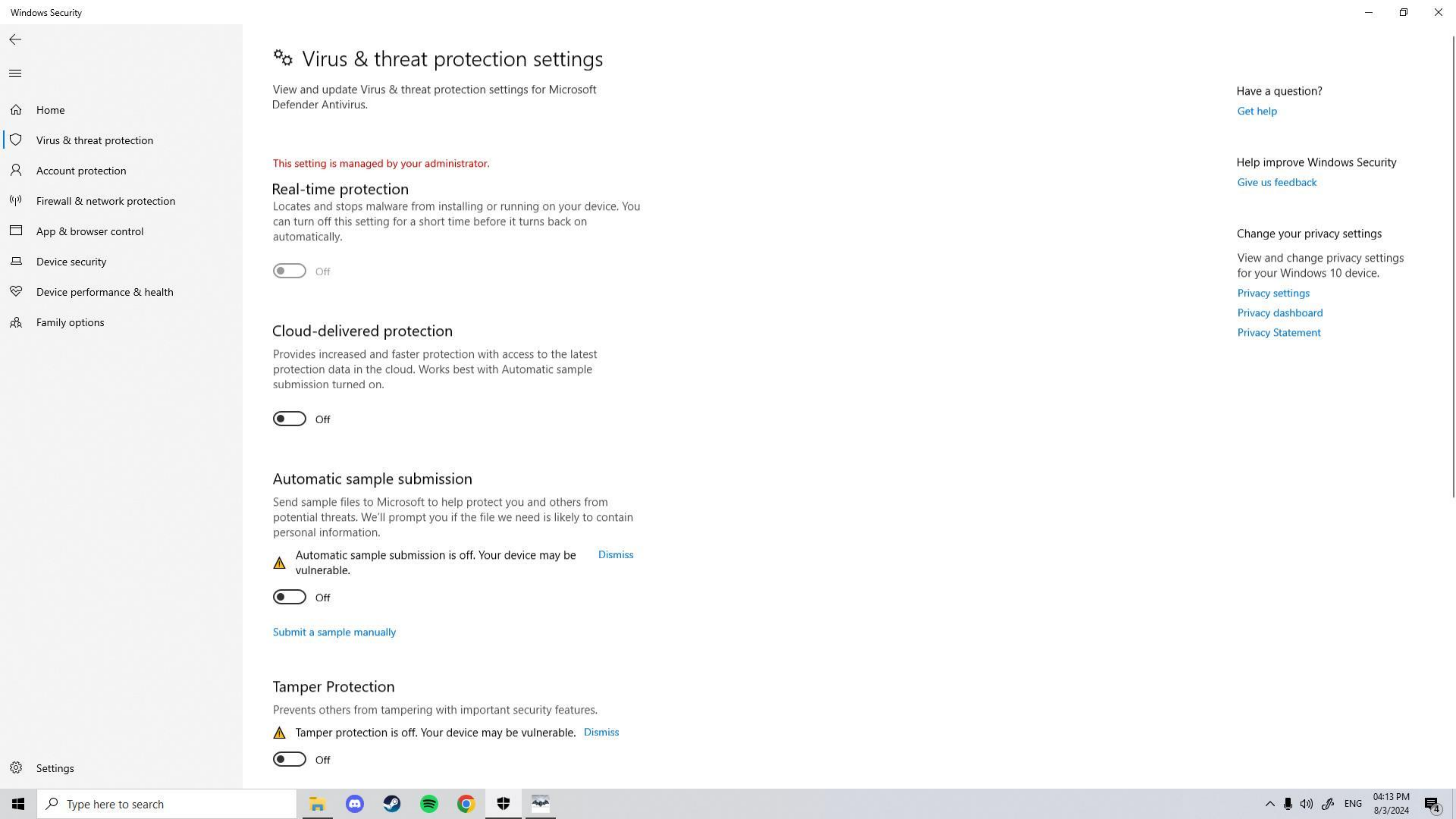
Find **Bitdefender** under your list of products and click **Stop** automatic subscription renewal. ... I recommend Norton — it's my favorite **antivirus** in **2023**, ...

★★★★★ Rankning: 9/10 · 13 recensioner

Relaterade sökningar

uninstall bitdefender

bitdefender **alert page**



Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

This setting is managed by your administrator.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

○ Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

○ Off

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

⚠ Automatic sample submission is off. Your device may be vulnerable. Dismiss

○ Off

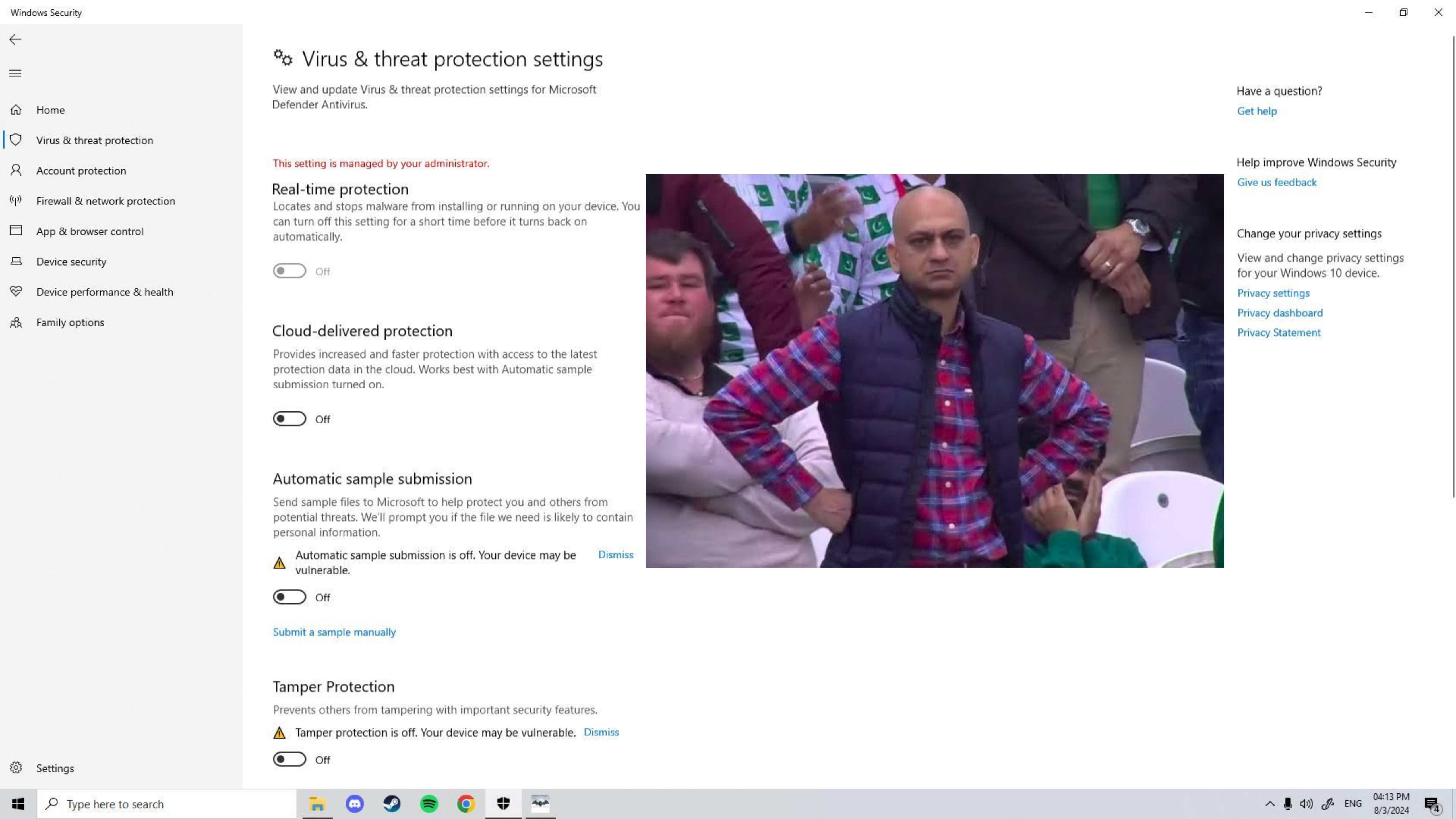
Submit a sample manually

Tamper Protection

Prevents others from tampering with important security features.

⚠ Tamper protection is off. Your device may be vulnerable. Dismiss

○ Off



Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

This setting is managed by your administrator.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

Off

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

⚠ Automatic sample submission is off. Your device may be vulnerable. Dismiss

Off

Submit a sample manually

Tamper Protection

Prevents others from tampering with important security features.

⚠ Tamper protection is off. Your device may be vulnerable. Dismiss

Off

Have a question?

Get help

Help improve Windows Security

Give us feedback

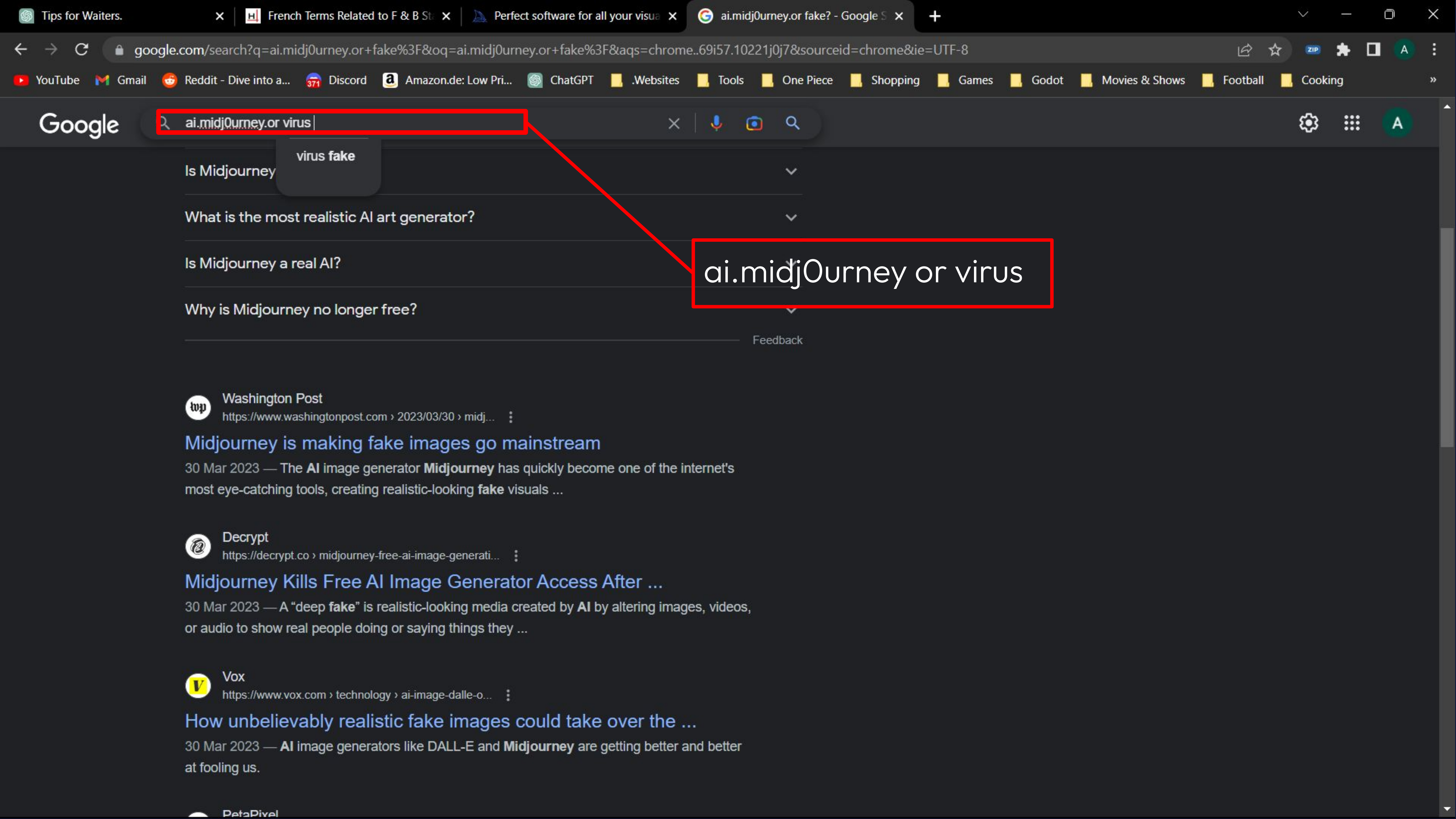
Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings

Privacy dashboard

Privacy Statement


Tips for Waiters.
French Terms Related to F & B St
Perfect software for all your visua
ai.midj0urney.or fake? - Google S
google.com/search?q=ai.midj0urney.or+fake%3F&oq=ai.midj0urney.or+fake%3F&aqs=chrome..69i57.10221j0j7&sourceid=chrome&ie=UTF-8
YouTube
Gmail
Reddit - Dive into a...
Discord
Amazon.de: Low Pri...
ChatGPT
.Websites
Tools
One Piece
Shopping
Games
Godot
Movies & Shows
Football
Cooking
Google
ai.midj0urney.or virus
virus fake

ai.midj0urney or virus

Is Midjourney

What is the most realistic AI art generator?

Is Midjourney a real AI?

Why is Midjourney no longer free?

Feedback

Washington Post
https://www.washingtonpost.com › 2023/03/30 › midj...

Midjourney is making fake images go mainstream

30 Mar 2023 — The **AI** image generator **Midjourney** has quickly become one of the internet's most eye-catching tools, creating realistic-looking **fake** visuals ...

Decrypt
https://decrypt.co › midjourney-free-ai-image-generati...

Midjourney Kills Free AI Image Generator Access After ...

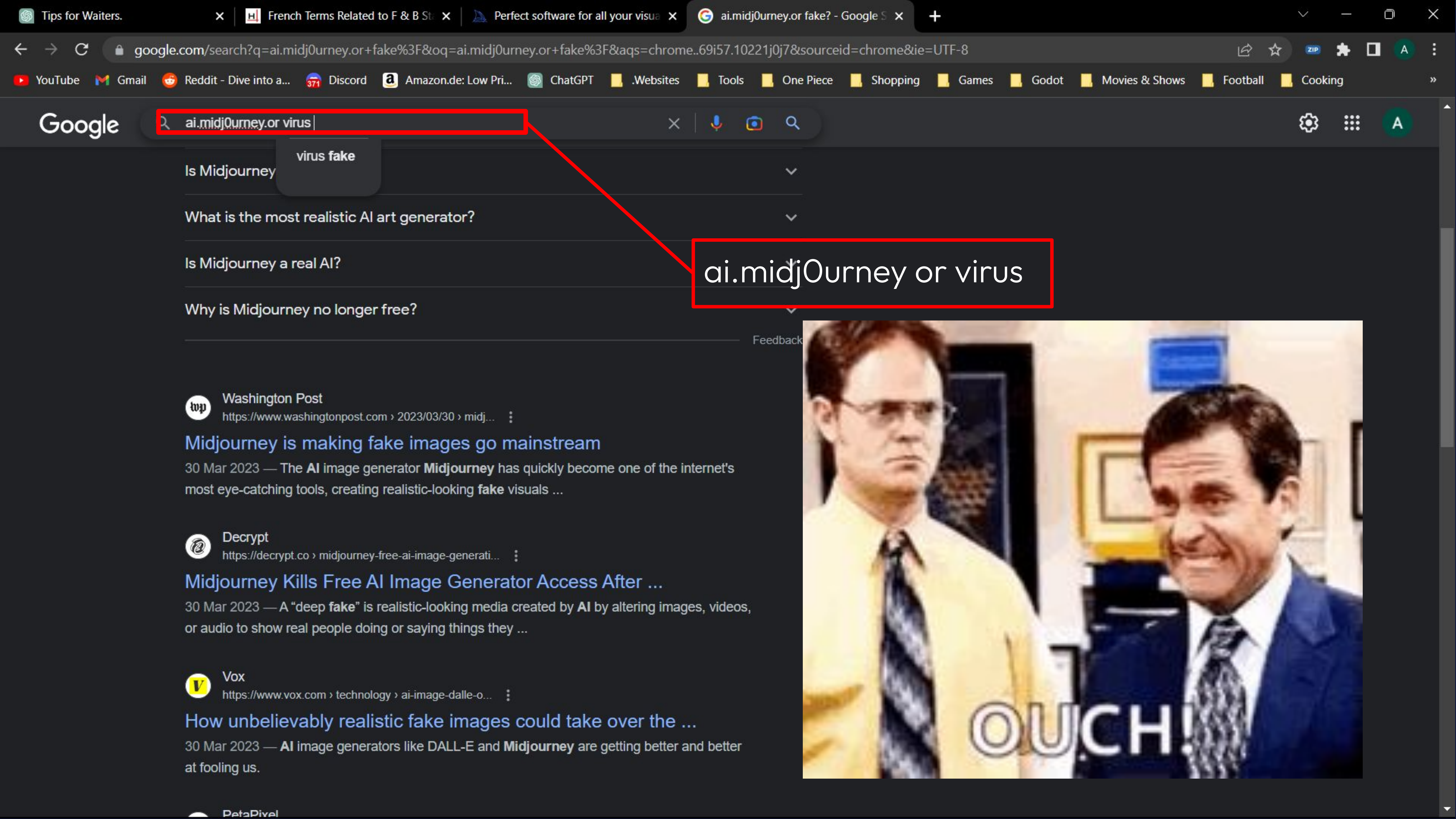
30 Mar 2023 — A "deep **fake**" is realistic-looking media created by **AI** by altering images, videos, or audio to show real people doing or saying things they ...

Vox
https://www.vox.com › technology › ai-image-dalle-o...

How unbelievably realistic fake images could take over the ...

30 Mar 2023 — **AI** image generators like DALL-E and **Midjourney** are getting better and better at fooling us.

PetaPixel


Tips for Waiters.
French Terms Related to F & B St
Perfect software for all your visua
ai.midj0urney.or fake? - Google S
google.com/search?q=ai.midj0urney.or+fake%3F&oq=ai.midj0urney.or+fake%3F&aqs=chrome..69i57.10221j0j7&sourceid=chrome&ie=UTF-8
YouTube
Gmail
Reddit - Dive into a...
Discord
Amazon.de: Low Pri...
ChatGPT
.Websites
Tools
One Piece
Shopping
Games
Godot
Movies & Shows
Football
Cooking
Google
OUCH!

ai.midj0urney.or virus

virus **fake**

Is Midjourney

What is the most realistic AI art generator?

Is Midjourney a real AI?

Why is Midjourney no longer free?

Feedback

ai.midj0urney or virus

Washington Post
https://www.washingtonpost.com › 2023/03/30 › midj...

Midjourney is making fake images go mainstream

30 Mar 2023 — The **AI** image generator **Midjourney** has quickly become one of the internet's most eye-catching tools, creating realistic-looking **fake** visuals ...

Decrypt
https://decrypt.co › midjourney-free-ai-image-generati...

Midjourney Kills Free AI Image Generator Access After ...

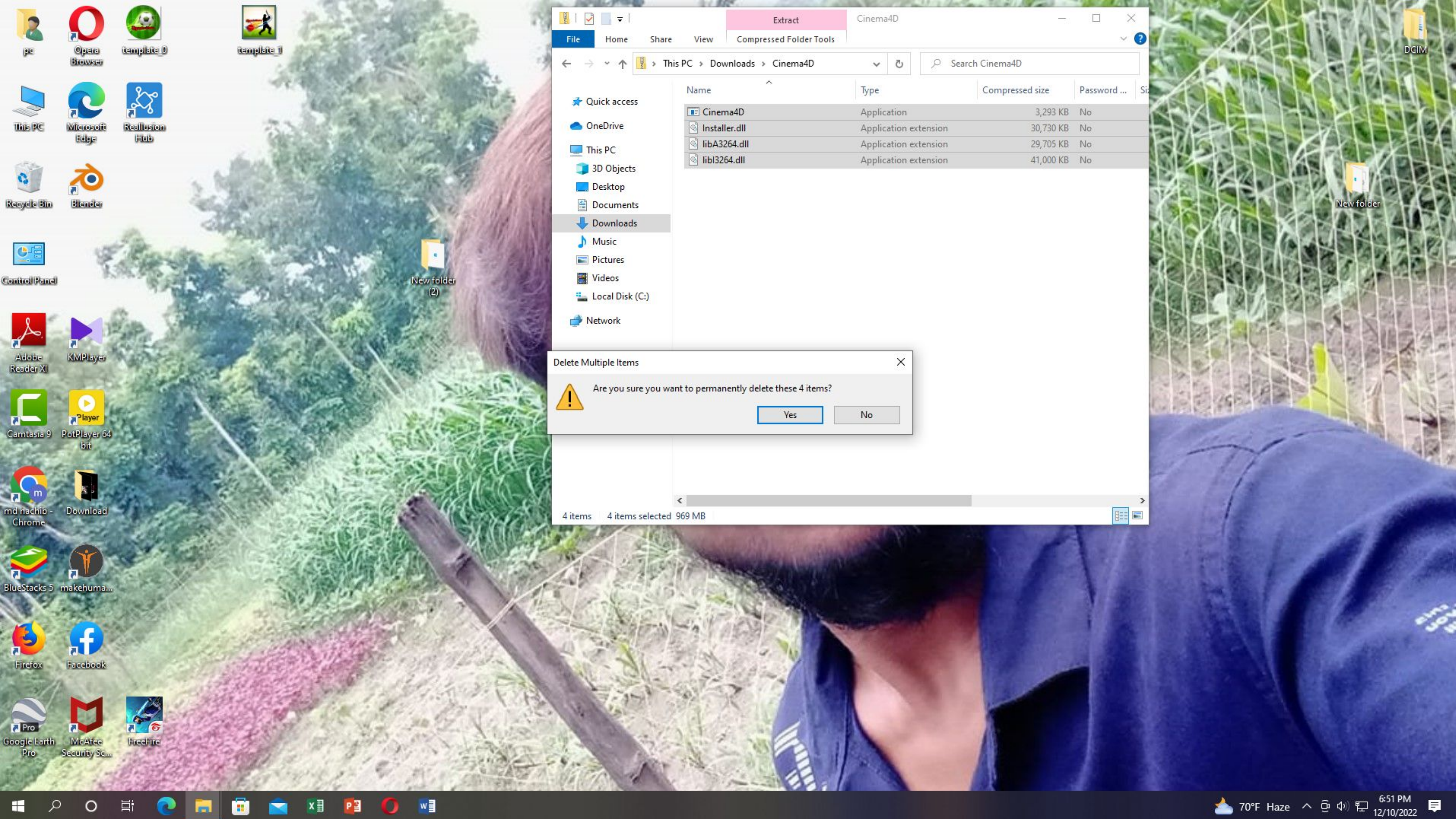
30 Mar 2023 — A "deep **fake**" is realistic-looking media created by **AI** by altering images, videos, or audio to show real people doing or saying things they ...

Vox
https://www.vox.com › technology › ai-image-dalle-o...

How unbelievably realistic fake images could take over the ...

30 Mar 2023 — **AI** image generators like DALL-E and **Midjourney** are getting better and better at fooling us.

PetaPixel



Name	Type	Compressed size	Password ...
Cinema4D	Application	3,293 KB	No
Installer.dll	Application extension	30,730 KB	No
libA3264.dll	Application extension	29,705 KB	No
libI3264.dll	Application extension	41,000 KB	No

Delete Multiple Items

Are you sure you want to permanently delete these 4 items?

Yes No

flare

Beyond Credentials

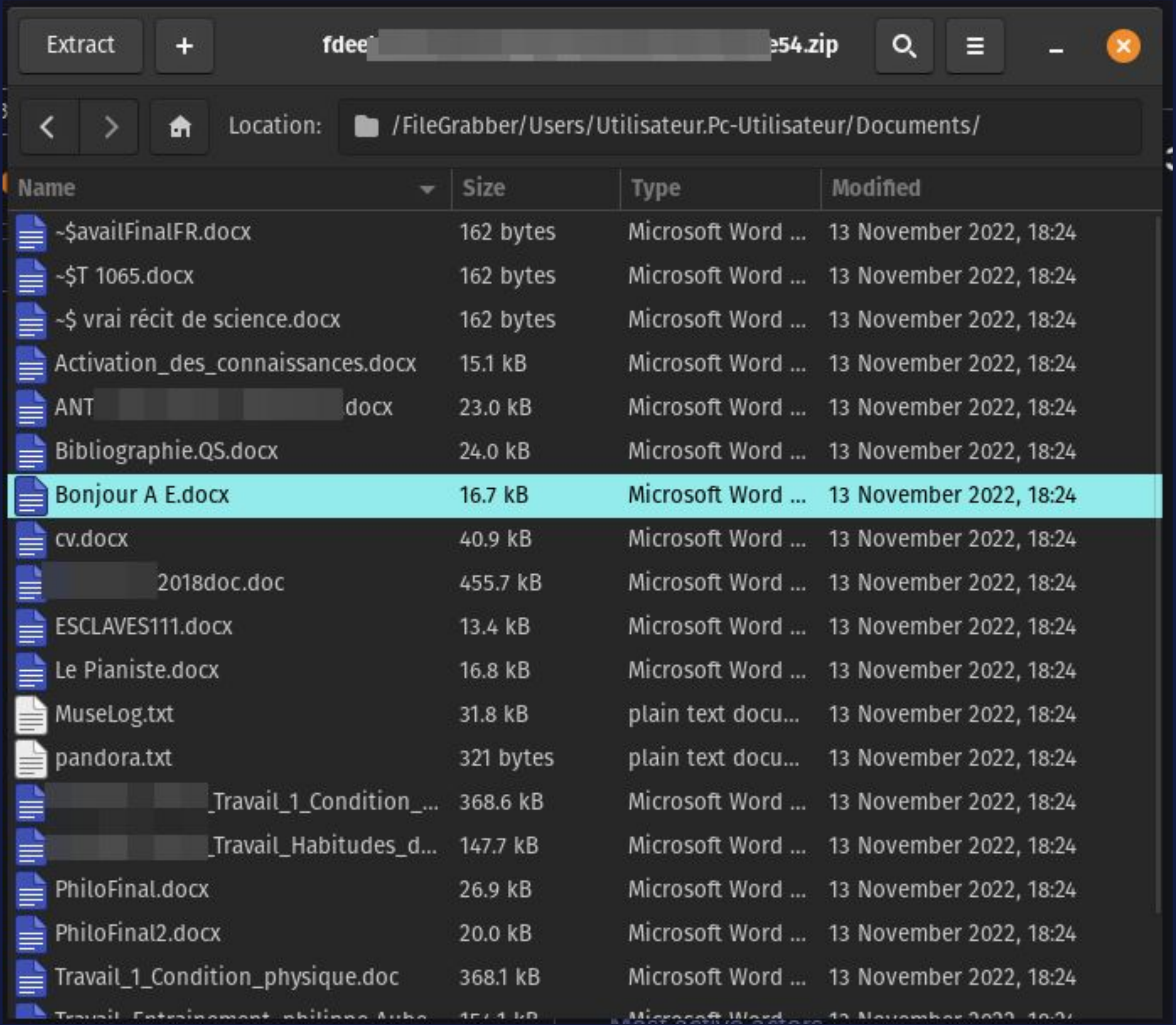
The Full Attack Surface

File Harvester Modules

Goes after many file types

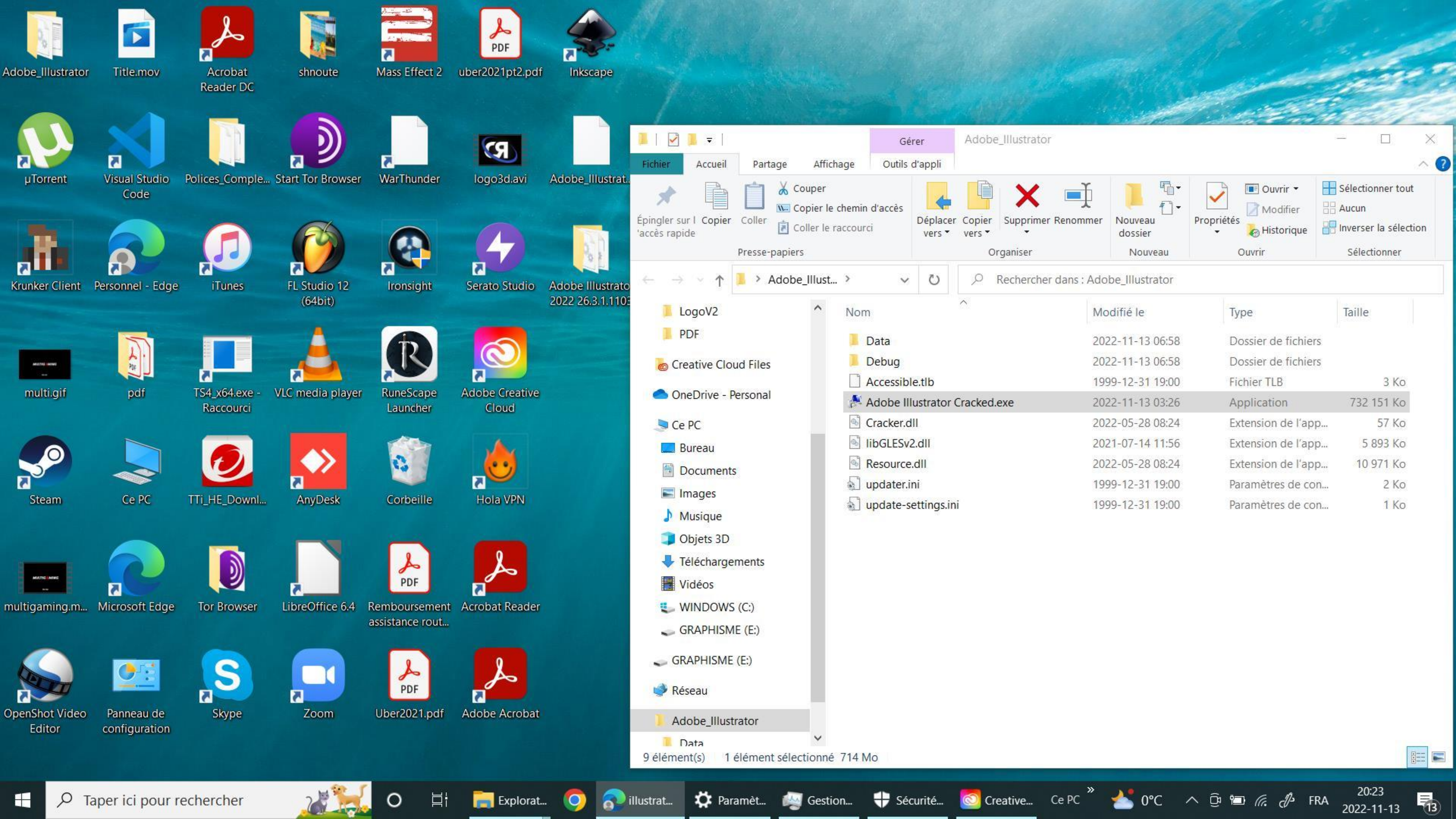
- Docs (pdf, doc, docx, etc.)
- xls
- txt
- kdb, kdbx (KeePass)

Focused on “Documents” and “Desktop” folders



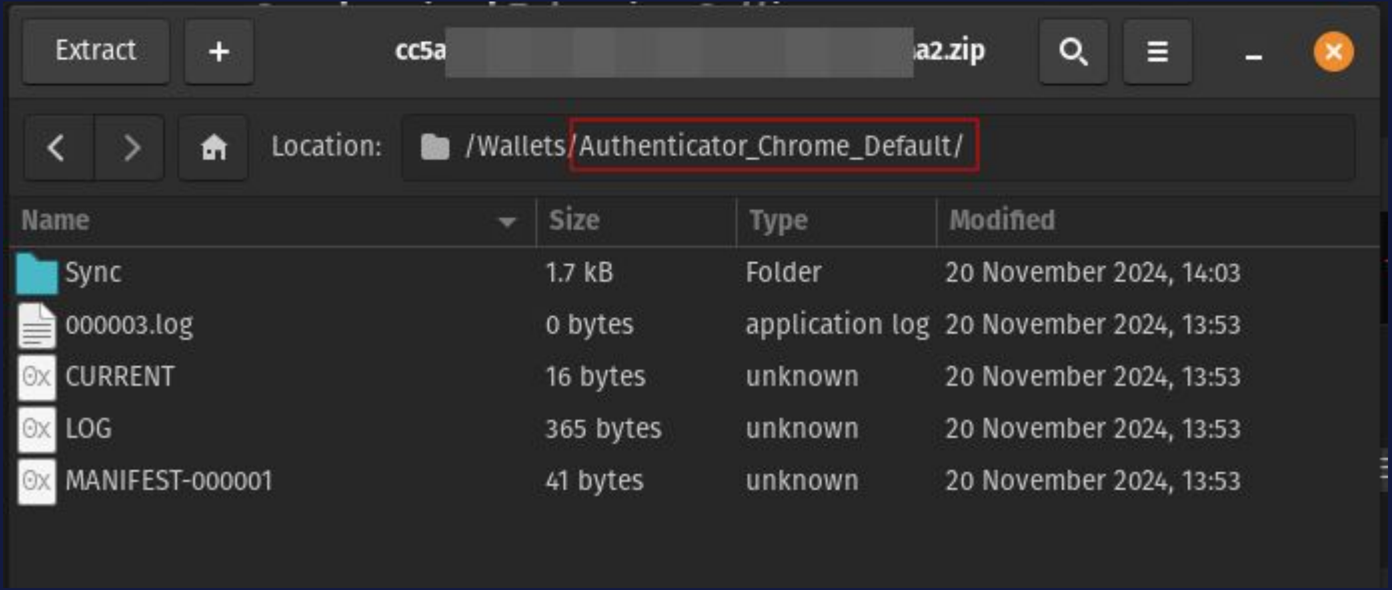
/FileGrabber/Users/Utilisateur.Pc-Utilisateur/Documents/

Name	Size	Type	Modified
~$availFinalFR.docx	162 bytes	Microsoft Word ...	13 November 2022, 18:24
~$T 1065.docx	162 bytes	Microsoft Word ...	13 November 2022, 18:24
~$ vrai récit de science.docx	162 bytes	Microsoft Word ...	13 November 2022, 18:24
Activation_des_connaissances.docx	15.1 kB	Microsoft Word ...	13 November 2022, 18:24
ANT[redacted]docx	23.0 kB	Microsoft Word ...	13 November 2022, 18:24
Bibliographie.QS.docx	24.0 kB	Microsoft Word ...	13 November 2022, 18:24
Bonjour A E.docx	16.7 kB	Microsoft Word ...	13 November 2022, 18:24
cv.docx	40.9 kB	Microsoft Word ...	13 November 2022, 18:24
[redacted]2018doc.doc	455.7 kB	Microsoft Word ...	13 November 2022, 18:24
ESCLAVES111.docx	13.4 kB	Microsoft Word ...	13 November 2022, 18:24
Le Pianiste.docx	16.8 kB	Microsoft Word ...	13 November 2022, 18:24
MuseLog.txt	31.8 kB	plain text docu...	13 November 2022, 18:24
pandora.txt	321 bytes	plain text docu...	13 November 2022, 18:24
[redacted]Travail_1_Condition_...	368.6 kB	Microsoft Word ...	13 November 2022, 18:24
[redacted]Travail_Habitudes_d...	147.7 kB	Microsoft Word ...	13 November 2022, 18:24
PhiloFinal.docx	26.9 kB	Microsoft Word ...	13 November 2022, 18:24
PhiloFinal2.docx	20.0 kB	Microsoft Word ...	13 November 2022, 18:24
Travail_1_Condition_physique.doc	368.1 kB	Microsoft Word ...	13 November 2022, 18:24
Travail_Entrainement_philippe_Aube	154.1 kB	Microsoft Word ...	13 November 2022, 18:24



Nom	Modifié le	Type	Taille
Data	2022-11-13 06:58	Dossier de fichiers	
Debug	2022-11-13 06:58	Dossier de fichiers	
Accessible.tlb	1999-12-31 19:00	Fichier TLB	3 Ko
Adobe Illustrator Cracked.exe	2022-11-13 03:26	Application	732 151 Ko
Cracker.dll	2022-05-28 08:24	Extension de l'app...	57 Ko
libGLESv2.dll	2021-07-14 11:56	Extension de l'app...	5 893 Ko
Resource.dll	2022-05-28 08:24	Extension de l'app...	10 971 Ko
updater.ini	1999-12-31 19:00	Paramètres de con...	2 Ko
update-settings.ini	1999-12-31 19:00	Paramètres de con...	1 Ko

When MFA is no longer MFA

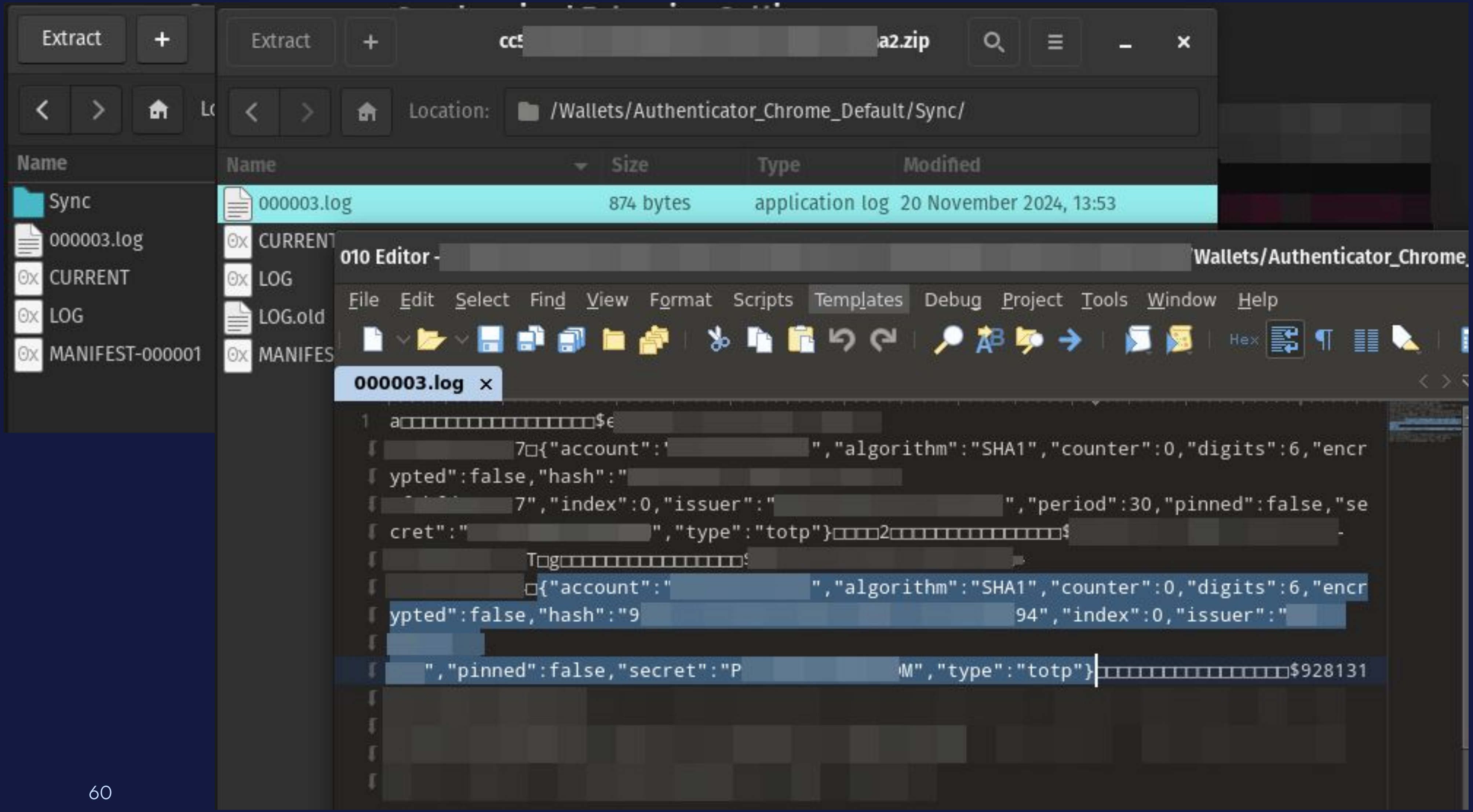


cc5a[redacted]a2.zip

Location: /Wallets/Authenticator_Chrome_Default/

Name	Size	Type	Modified
Sync	1.7 kB	Folder	20 November 2024, 14:03
000003.log	0 bytes	application log	20 November 2024, 13:53
CURRENT	16 bytes	unknown	20 November 2024, 13:53
LOG	365 bytes	unknown	20 November 2024, 13:53
MANIFEST-000001	41 bytes	unknown	20 November 2024, 13:53

When MFA is no longer MFA



Extract +

Name

- Sync
- 000003.log
- CURRENT
- LOG
- MANIFEST-000001

Extract + cc5[redacted]a2.zip

Location: /Wallets/Authenticator_Chrome_Default/Sync/

Name	Size	Type	Modified
000003.log	874 bytes	application log	20 November 2024, 13:53
CURRENT			
LOG			
LOG.old			
MANIFES			

010 Editor - [redacted]Wallets/Authenticator_Chrome_

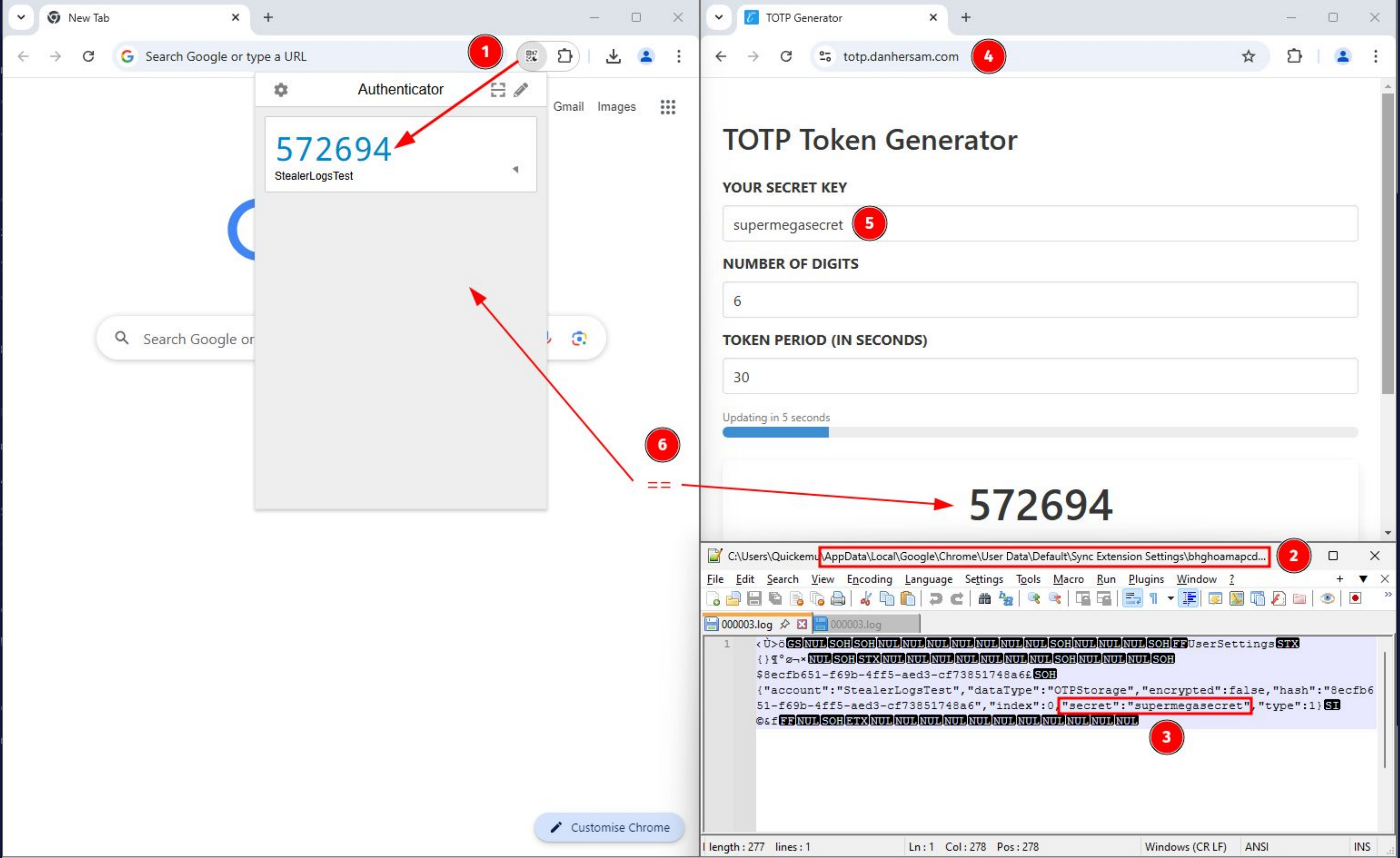
File Edit Select Find View Format Scripts Templates Debug Project Tools Window Help
Hex
000003.log ×

```
a□□□□□□□□□□□□□□□□□□□$€[redacted]
[redacted]7□{"account":"[redacted]","algorithm":"SHA1","counter":0,"digits":6,"encr
ypted":false,"hash":"[redacted]
[redacted]7","index":0,"issuer":"[redacted]","period":30,"pinned":false,"se
cret":"[redacted]","type":"totp"}□□□□2□□□□□□□□□□□□□□□□$[redacted]-
[redacted]T□g□□□□□□□□□□□□□□□□□$[redacted]
[redacted]□{"account":"[redacted]","algorithm":"SHA1","counter":0,"digits":6,"encr
ypted":false,"hash":"9[redacted]94","index":0,"issuer":"[redacted]
[redacted]
[redacted]","pinned":false,"secret":"P[redacted]M","type":"totp"}□□□□□□□□□□□□□□□□□$928131
[redacted]
```

JSON Encoded TOTP “Account”?

```
{
  "account": "9[redacted]3",
  "algorithm": "SHA1",
  "counter": 0,
  "digits": 6,
  "encrypted": false,
  "hash": "92[redacted]d94",
  "index": 0,
  "issuer": "[redacted]",
  "pinned": false,
  "secret": "P[redacted]M",
  "type": "totp"
}
```

Wait... But does it work?



572694
StealerLogsTest

TOTP Token Generator

YOUR SECRET KEY

supermegasecret

NUMBER OF DIGITS

6

TOKEN PERIOD (IN SECONDS)

30

Updating in 5 seconds

572694

C:\Users\Quickemu\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\bhghoamapcd...

000003.log

000003.log

```
<Ù>öGSNULSOHSOHNULNULNULNULNULNULNULSOHNULNULNULSOHFFUserSettingsSTX
{}¶°ø¬×NULSOHSTXNULNULNULNULNULNULNULSOHNULNULNULSOH
$8ecfb651-f69b-4ff5-aed3-cf73851748a6£SOH
{"account":"StealerLogsTest","dataType":"OTPStorage","encrypted":false,"hash":"8ecfb6
51-f69b-4ff5-aed3-cf73851748a6","index":0,"secret":"supermegasecret","type":1}SI
©&fFFNULSOHETXNULNULNULNULNULNULNULNULNULNULNUL
```

length : 277   lines : 1   Ln : 1   Col : 278   Pos : 278   Windows (CR LF)   ANSI   INS

Targeted Browser Extensions

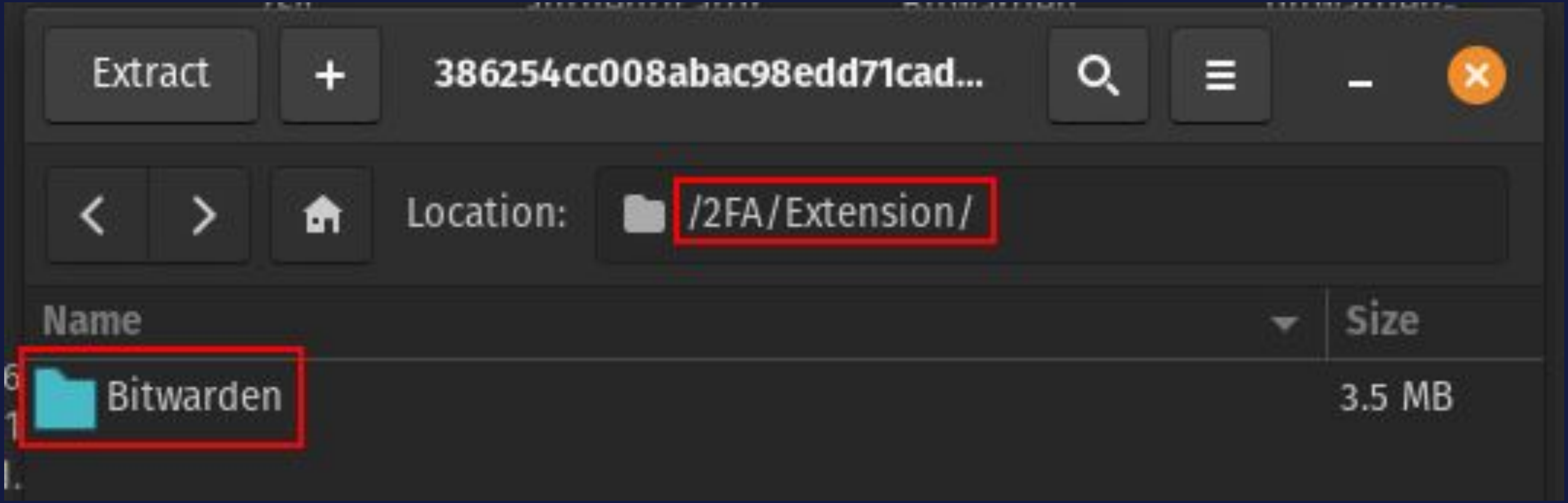
- Files for both Local and Synced Extensions are exfiltrated
  - `%APPDATA%\Local\Google\Chrome\User Data\<Profile>\Local Extension Settings\<Extension-Id>`
  - `%APPDATA%\Local\Google\Chrome\User Data\<Profile>\Sync Extension Settings\<Extension-Id>`

- Storage format is IndexDB/LevelDB (a lot is viewable in plaintext)

- Parsable with this IR tool: https://github.com/cclgroupltd/ccl_chromium_reader/blob/master/tools_and_utilities/dump_leveldb.py

Password Managers Browser Extensions

- Found some BitWarden

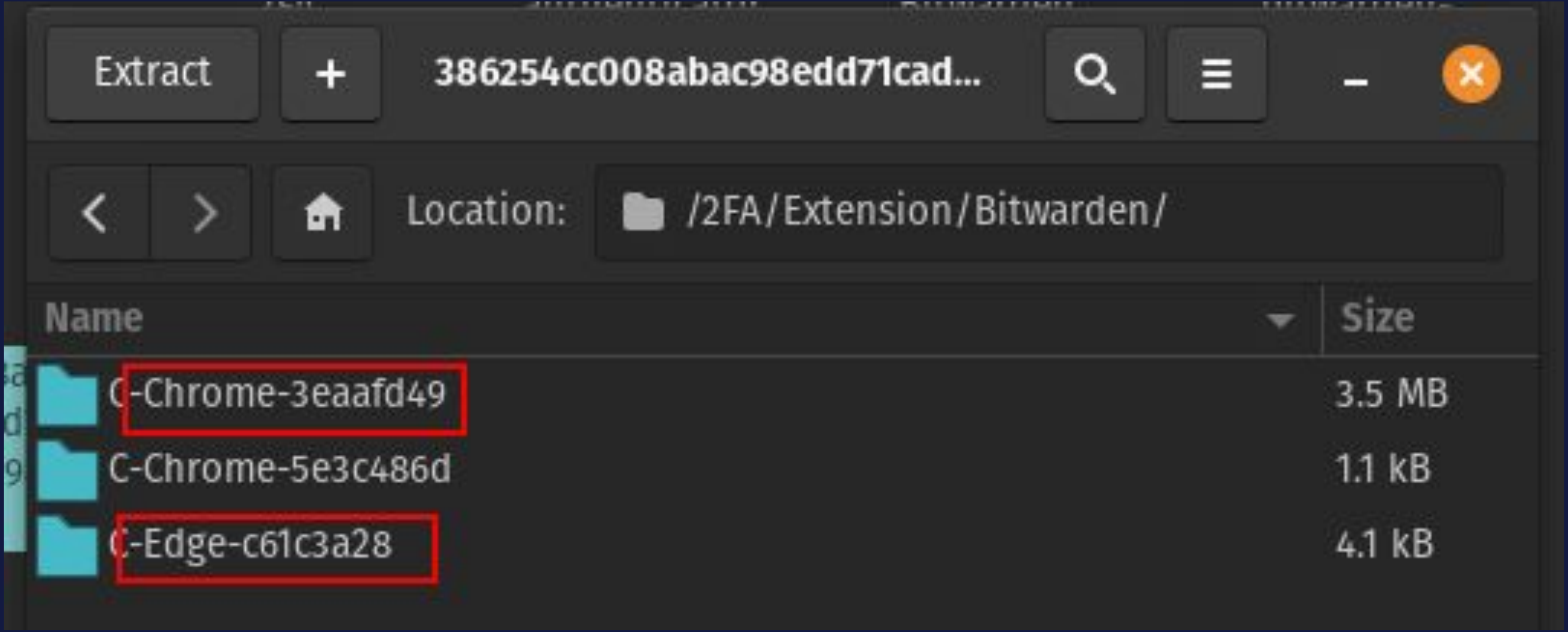


Location: /2FA/Extension/

Name	Size
Bitwarden	3.5 MB

Password Managers Browser Extensions

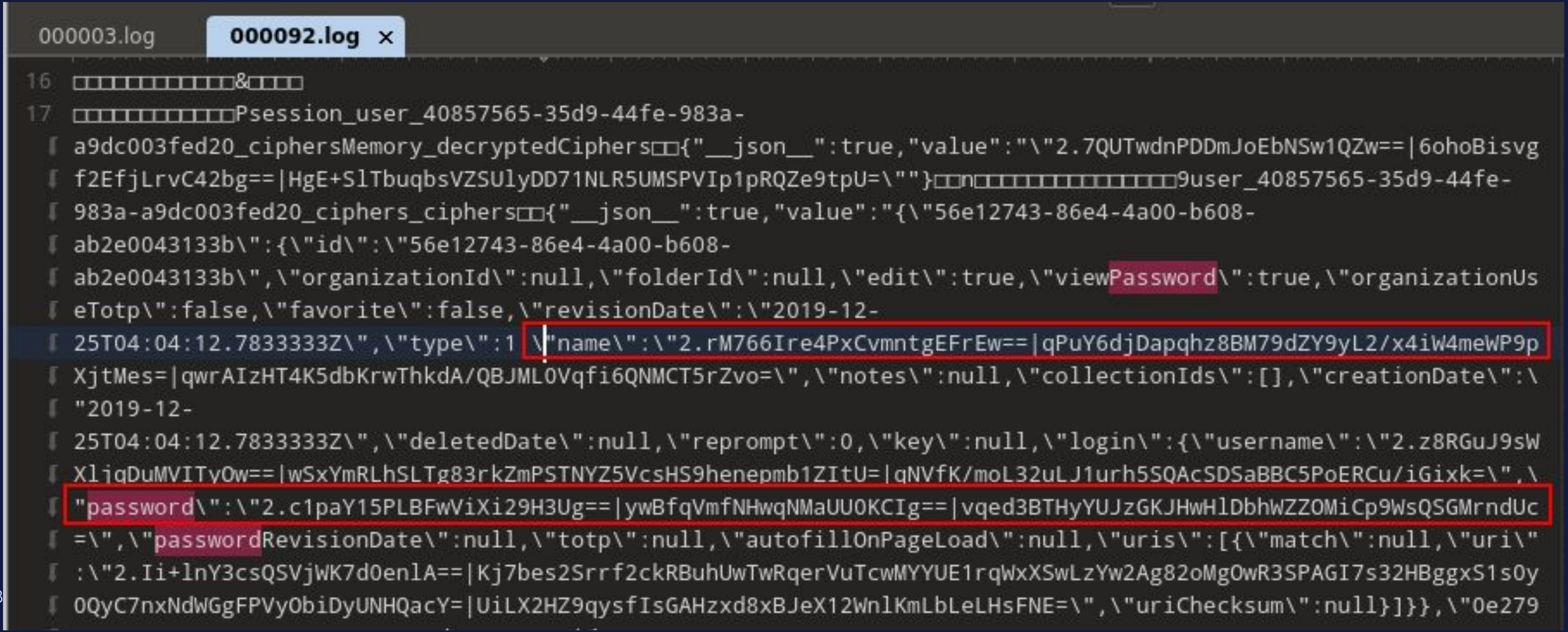
- Multiple Browsers and Multiple Profiles Support



Name	Size
C-Chrome-3eaafd49	3.5 MB
C-Chrome-5e3c486d	1.1 kB
C-Edge-c61c3a28	4.1 kB

Password Managers Browser Extensions

- Plaintext JSON with embedded encrypted strings

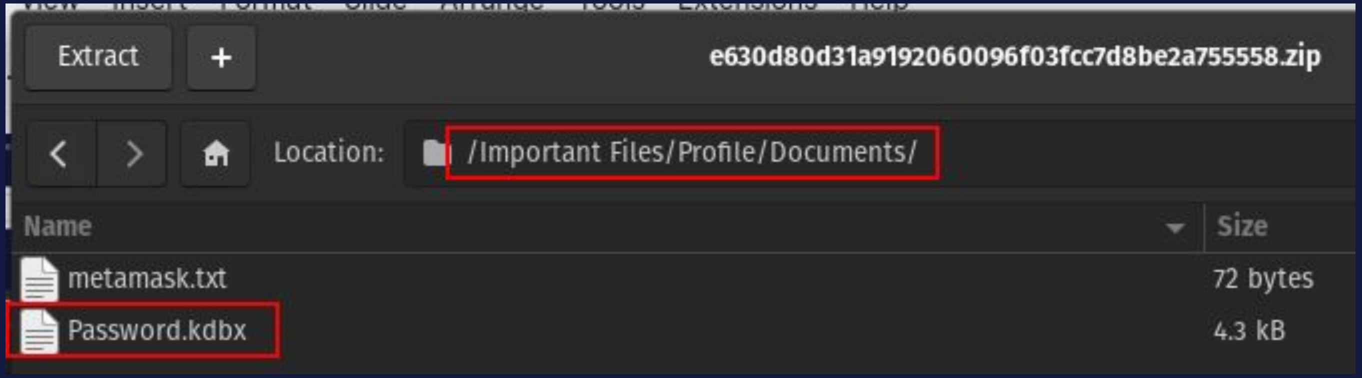


```
□□□□□□□□□□□□&□□□□
□□□□□□□□□□□□Psession_user_40857565-35d9-44fe-983a-
a9dc003fed20_ciphersMemory_decryptedCiphers□□{"__json__":true,"value":"\"2.7QUTwdnPDDmJoEbNSw1QZw==|6ohoBisvg
f2EfjLrvC42bg==|HgE+SlTbuqbsVZSUlyDD71NLR5UMSPVIp1pRQZe9tpU=\""}□□n□□□□□□□□□□□□□□□□9user_40857565-35d9-44fe-
983a-a9dc003fed20_ciphers_ciphers□□{"__json__":true,"value":"{\"56e12743-86e4-4a00-b608-
ab2e0043133b\":{\"id\":\"56e12743-86e4-4a00-b608-
ab2e0043133b\",\"organizationId\":null,\"folderId\":null,\"edit\":true,\"viewPassword\":true,\"organizationUs
eTotp\":false,\"favorite\":false,\"revisionDate\":\"2019-12-
25T04:04:12.7833333Z\",\"type\":1 \"name\":\"2.rM766Ire4PxCvmntgEFrEw==|qPuY6djDapqhz8BM79dZY9yL2/x4iW4meWP9p
XjtMes=|qwrAIzHT4K5dbKrwThkdA/QBJML0Vqfi6QNMCT5rZvo=\",\"notes\":null,\"collectionIds\":[],\"creationDate\":\
"2019-12-
25T04:04:12.7833333Z\",\"deletedDate\":null,\"reprompt\":0,\"key\":null,\"login\":{\"username\":\"2.z8RGuJ9sW
XljqDuMVITyOw==|wSxYmRLhSLTg83rkZmPSTNYZ5VcsHS9henepmb1ZItU=|qNVfK/moL32uLJ1urh5SQAcSDSaBBC5PoERCu/iGixk=\",\
"password\":\"2.c1paY15PLBFwViXi29H3Ug==|ywBfqVmfNHwqNMaUU0KCIg==|vqed3BTHyYUJzGKJHwHlDbhWZZOMiCp9WsQSGMrndUc
=\",\"passwordRevisionDate\":null,\"totp\":null,\"autofillOnPageLoad\":null,\"uris\":[{\"match\":null,\"uri\"
:\"2.Ii+lnY3csQSVjWK7d0enlA==|Kj7bes2Srrf2ckRBuhUwTwRqerVuTcwMYYUE1rqWxXSwLzYw2Ag82oMgOwR3SPAGI7s32HBggxS1sOy
0QyC7nxNdWGgFPVyObiDyUNHQacY=|UiLX2HZ9qysfIsGAHzxd8xBJeX12WnlKmLbLeLHsFNE=\",\"uriChecksum\":null}]}},\"0e279
```

Password Vaults

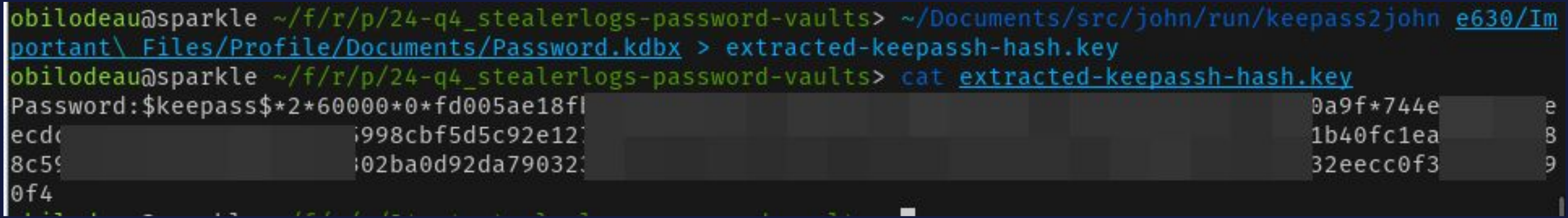
KeePass Password Vaults

- .kdb
- .kdbx


Extract
+
e630d80d31a9192060096f03fcc7d8be2a755558.zip
Location:
/Important Files/Profile/Documents/

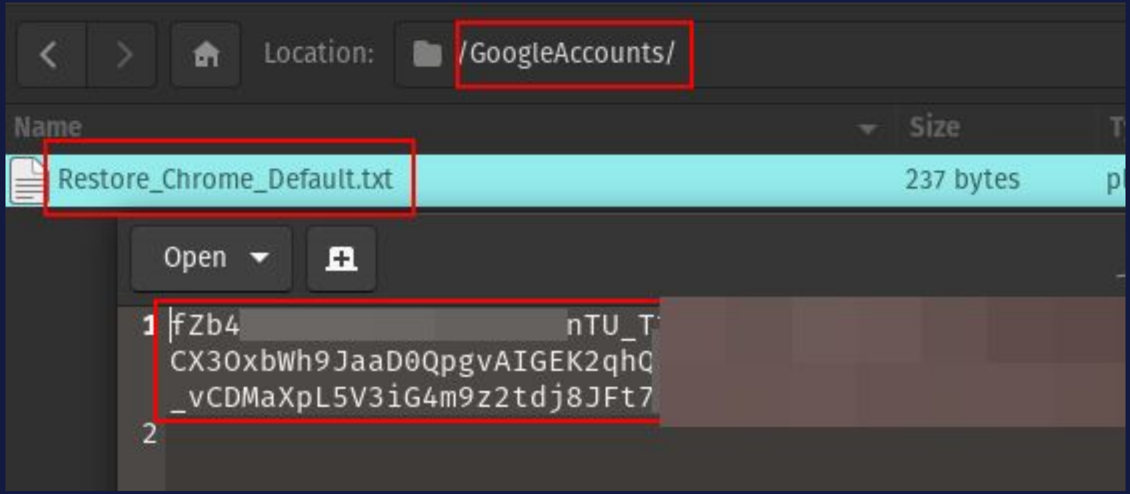
Name	Size
metamask.txt	72 bytes
Password.kdbx	4.3 kB

Cracking tooling exists (john, hashcat)



```
obilodeau@sparkle ~/f/r/p/24-q4_stealerlogs-password-vaults> ~/Documents/src/john/run/keepass2john e630/Im
portant\ Files/Profile/Documents/Password.kdbx > extracted-keepassh-hash.key
obilodeau@sparkle ~/f/r/p/24-q4_stealerlogs-password-vaults> cat extracted-keepassh-hash.key
Password:$keepass$*2*60000*0*fd005ae18f[redacted]0a9f*744e[redacted]e
ecd[redacted]998cbf5d5c92e12[redacted]1b40fc1ea[redacted]8
8c5[redacted]02ba0d92da790323[redacted]32eecc0f3[redacted]9
0f4
```

Google Master Cookies?

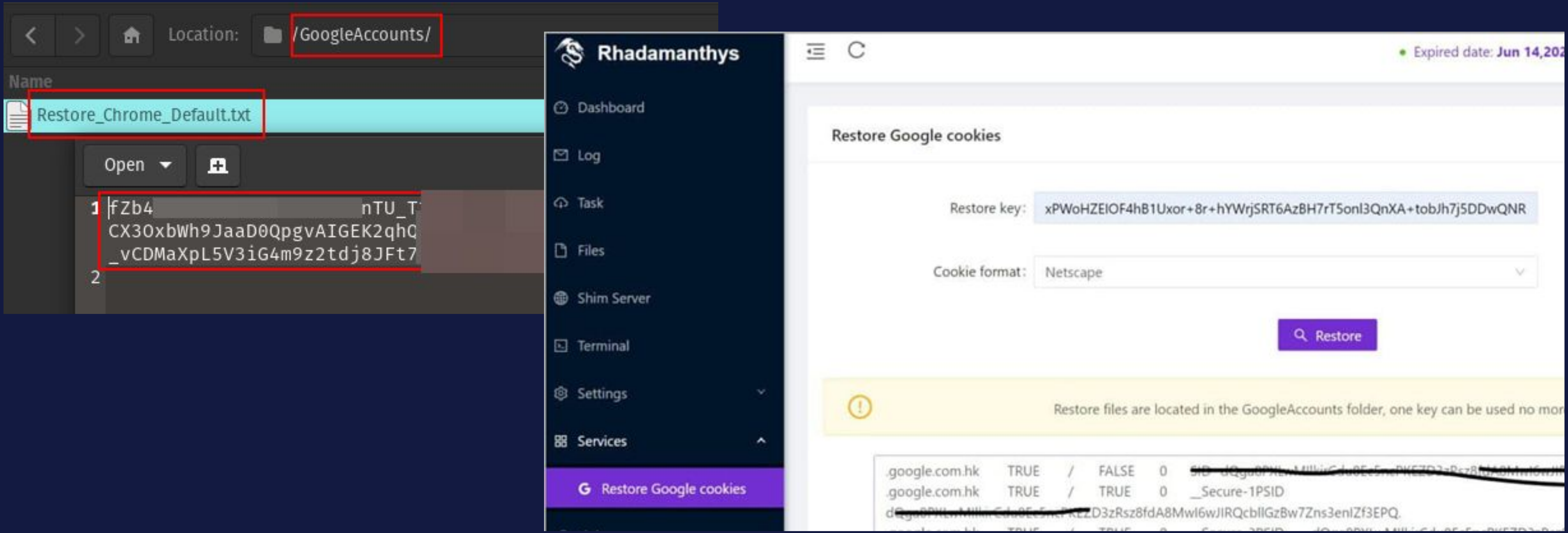


/GoogleAccounts/

Restore_Chrome_Default.txt 237 bytes p

```
fZb4 [redacted] nTU_T [redacted]
CX3OxbWh9JaaD0QpgvAIGEK2qhQ
_vCDMaXpL5V3iG4m9z2tdj8JFt7
```

Google Master Cookies?



```
1 fZb4[redacted]nTU_T
  CX3OxbWh9JaaD0QpgvAIGEK2qhQ
  _vCDMaXpL5V3iG4m9z2tdj8JFt7
2
```

Expired date: Jun 14,202

Restore Google cookies

Restore key: xPWoHZEIOF4hB1Uxor+8r+hYWrjSRT6AzBH7rT5onl3QnXA+tobJh7j5DDwQNR

Cookie format: Netscape

Restore

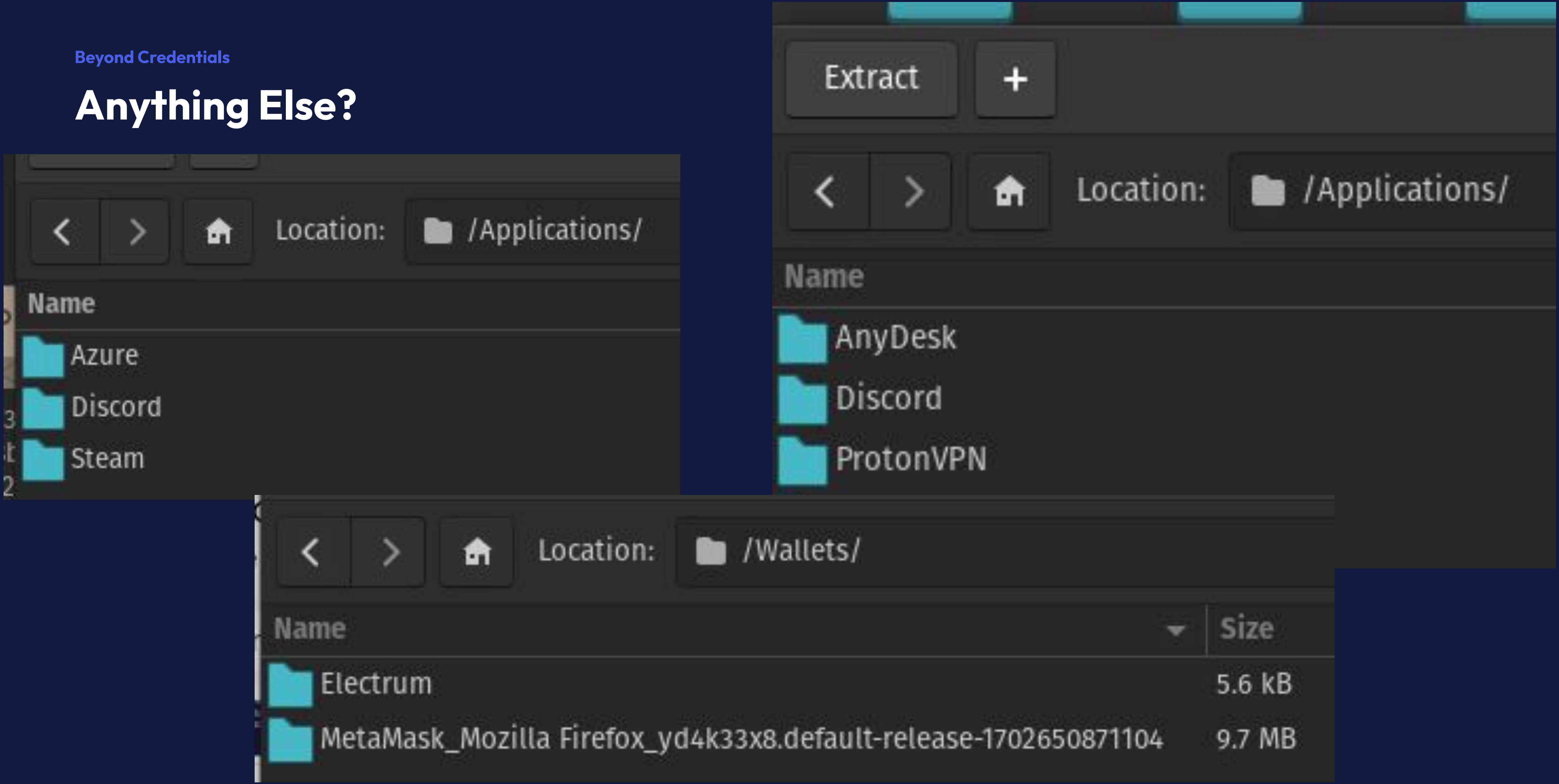
Restore files are located in the GoogleAccounts folder, one key can be used no mor

```
.google.com.hk    TRUE    /    FALSE    0    [redacted]
.google.com.hk    TRUE    /    TRUE     0    _Secure-1PSID
d[redacted]D3zRsz8fdA8Mwl6wJIRQcbllGzBw7Zns3enlZf3EPQ.
```

Lumma Tool Screenshot from

https://fieldeffect.com/blog/infostealers-restore-expired-google-cookies

Anything Else?



Location: /Applications/

Name
Azure
Discord
Steam

Location: /Applications/

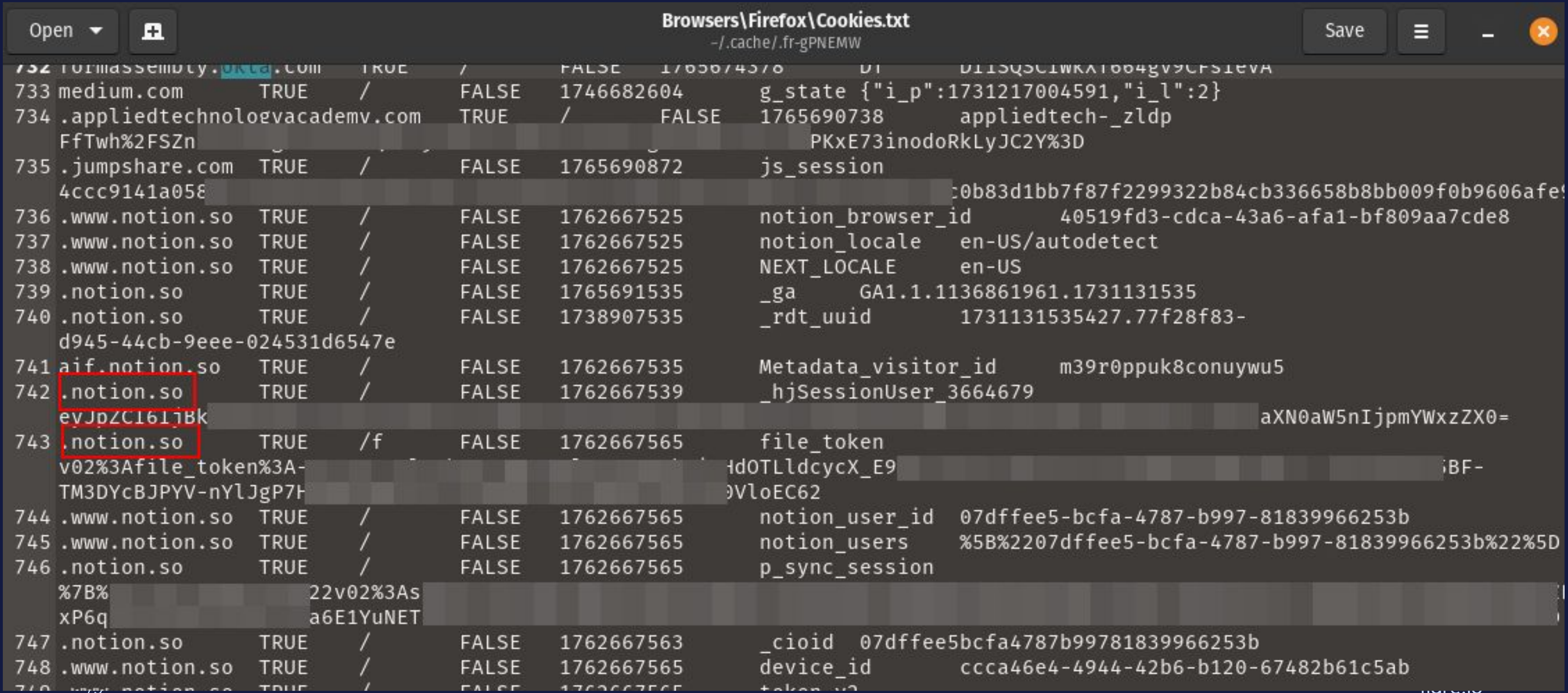
Name
AnyDesk
Discord
ProtonVPN

Location: /Wallets/

Name	Size
Electrum	5.6 kB
MetaMask_Mozilla Firefox_yd4k33x8.default-release-1702650871104	9.7 MB

and OpenVPN files (.ovpn), FileZilla, Binance, Phantom, XDEFI Wallet, etc.

But also Cookies!

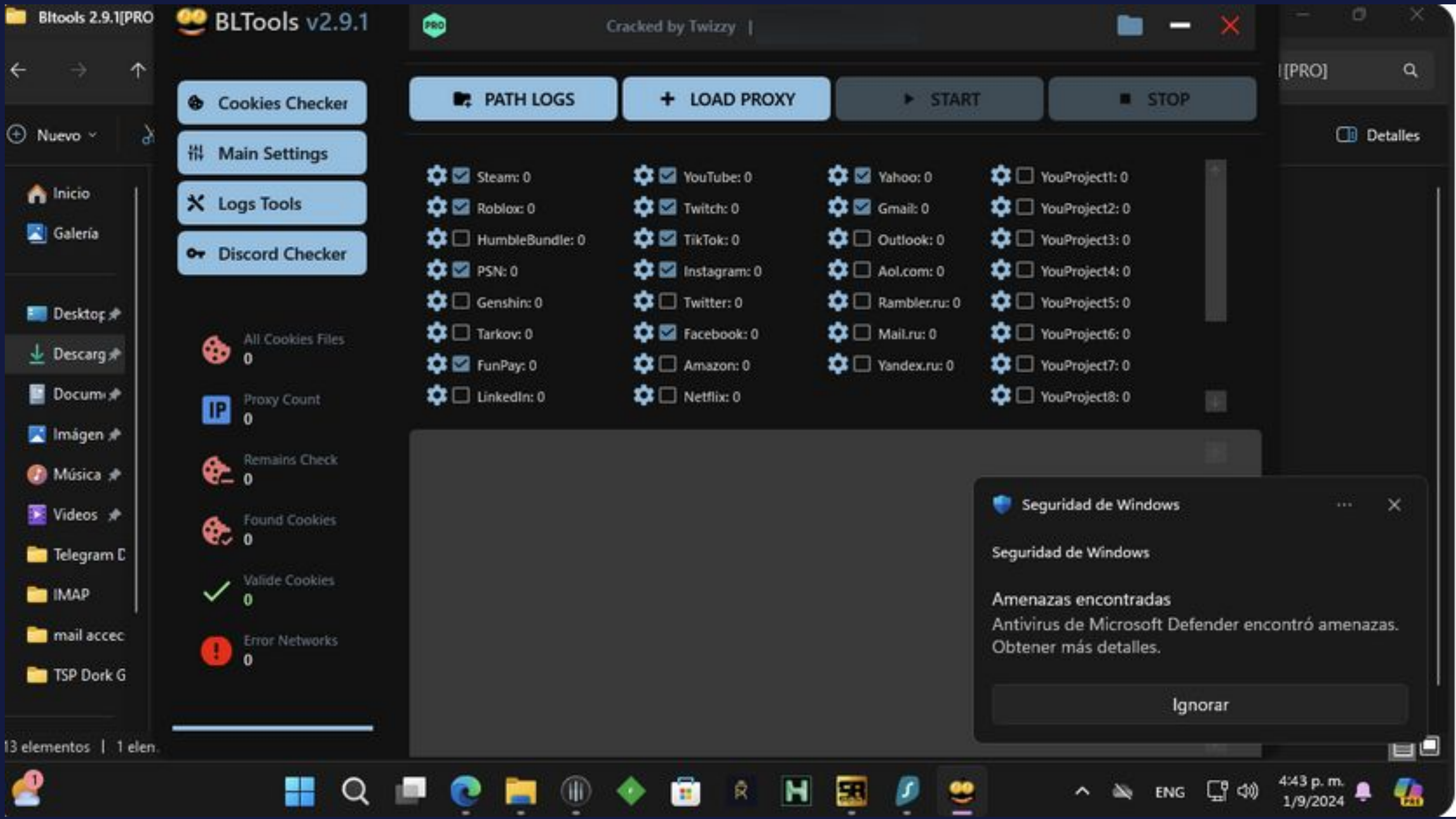


```
formassembly.okta.com   TRUE    /       FALSE   1765674378      DT      DI1SQSC1WkXT664gV9CFSIevA
medium.com      TRUE    /       FALSE   1746682604      g_state {"i_p":1731217004591,"i_l":2}
.appliedtechnologyacademy.com   TRUE    /       FALSE   1765690738      appliedtech-_zldp
FfTwh%2FSZn[redacted]PKxE73inodoRkLyJC2Y%3D
.jumpshare.com  TRUE    /       FALSE   1765690872      js_session
4ccc9141a058[redacted]c0b83d1bb7f87f2299322b84cb336658b8bb009f0b9606afe
.www.notion.so  TRUE    /       FALSE   1762667525      notion_browser_id       40519fd3-cdca-43a6-afa1-bf809aa7cde8
.www.notion.so  TRUE    /       FALSE   1762667525      notion_locale   en-US/autodetect
.www.notion.so  TRUE    /       FALSE   1762667525      NEXT_LOCALE     en-US
.notion.so      TRUE    /       FALSE   1765691535      _ga     GA1.1.1136861961.1731131535
.notion.so      TRUE    /       FALSE   1738907535      _rdt_uuid       1731131535427.77f28f83-
d945-44cb-9eee-024531d6547e
aif.notion.so   TRUE    /       FALSE   1762667535      Metadata_visitor_id     m39r0ppuk8conuywu5
.notion.so      TRUE    /       FALSE   1762667539      _hjSessionUser_3664679
eyJpZCI6IjBk[redacted]aXN0aW5nIjpmYWxzZX0=
.notion.so      TRUE    /f      FALSE   1762667565      file_token
v02%3Afile_token%3A-[redacted]HdOTLldcycX_E9[redacted]BF-
TM3DYcBJPYV-nYlJgP7H[redacted]0VloEC62
.www.notion.so  TRUE    /       FALSE   1762667565      notion_user_id  07dffee5-bcfa-4787-b997-81839966253b
.www.notion.so  TRUE    /       FALSE   1762667565      notion_users    %5B%2207dffee5-bcfa-4787-b997-81839966253b%22%5D
.notion.so      TRUE    /       FALSE   1762667565      p_sync_session
%7B%[redacted]22v02%3As[redacted]
xP6q[redacted]a6E1YuNET[redacted]
.notion.so      TRUE    /       FALSE   1762667563      _cioid  07dffee5bcfa4787b99781839966253b
.www.notion.so  TRUE    /       FALSE   1762667565      device_id       ccca46e4-4944-42b6-b120-67482b61c5ab
.www.notion.so  TRUE    /       FALSE   1762667565      token_v2
```

How about the Cookies?

“Checkers”

- Used to identify valid session cookies for particular applications in stealer logs.
- Usually sold similar to malware on a MaaS licensing scheme.
- Flare identified a threat actor that seeded a cracked checker with infostealers, infecting stealer log “users”
- Hundreds of cybercriminals downloaded it and were subsequently infected.



All Cookies Files 0

Proxy Count 0

Remains Check 0

Found Cookies 0

Valide Cookies 0

Error Networks 0

☑ Steam: 0
☑ Roblox: 0
□ HumbleBundle: 0
☑ PSN: 0
□ Genshin: 0
□ Tarkov: 0
☑ FunPay: 0
□ LinkedIn: 0

☑ YouTube: 0
☑ Twitch: 0
☑ TikTok: 0
☑ Instagram: 0
□ Twitter: 0
☑ Facebook: 0
□ Amazon: 0
□ Netflix: 0

☑ Yahoo: 0
☑ Gmail: 0
□ Outlook: 0
□ Aol.com: 0
□ Rambler.ru: 0
□ Mail.ru: 0
□ Yandex.ru: 0

□ YouProject1: 0
□ YouProject2: 0
□ YouProject3: 0
□ YouProject4: 0
□ YouProject5: 0
□ YouProject6: 0
□ YouProject7: 0
□ YouProject8: 0

Seguridad de Windows

Seguridad de Windows

Amenazas encontradas
Antivirus de Microsoft Defender encontró amenazas. Obtener más detalles.

Ignorar

4:43 p. m.
1/9/2024

flare

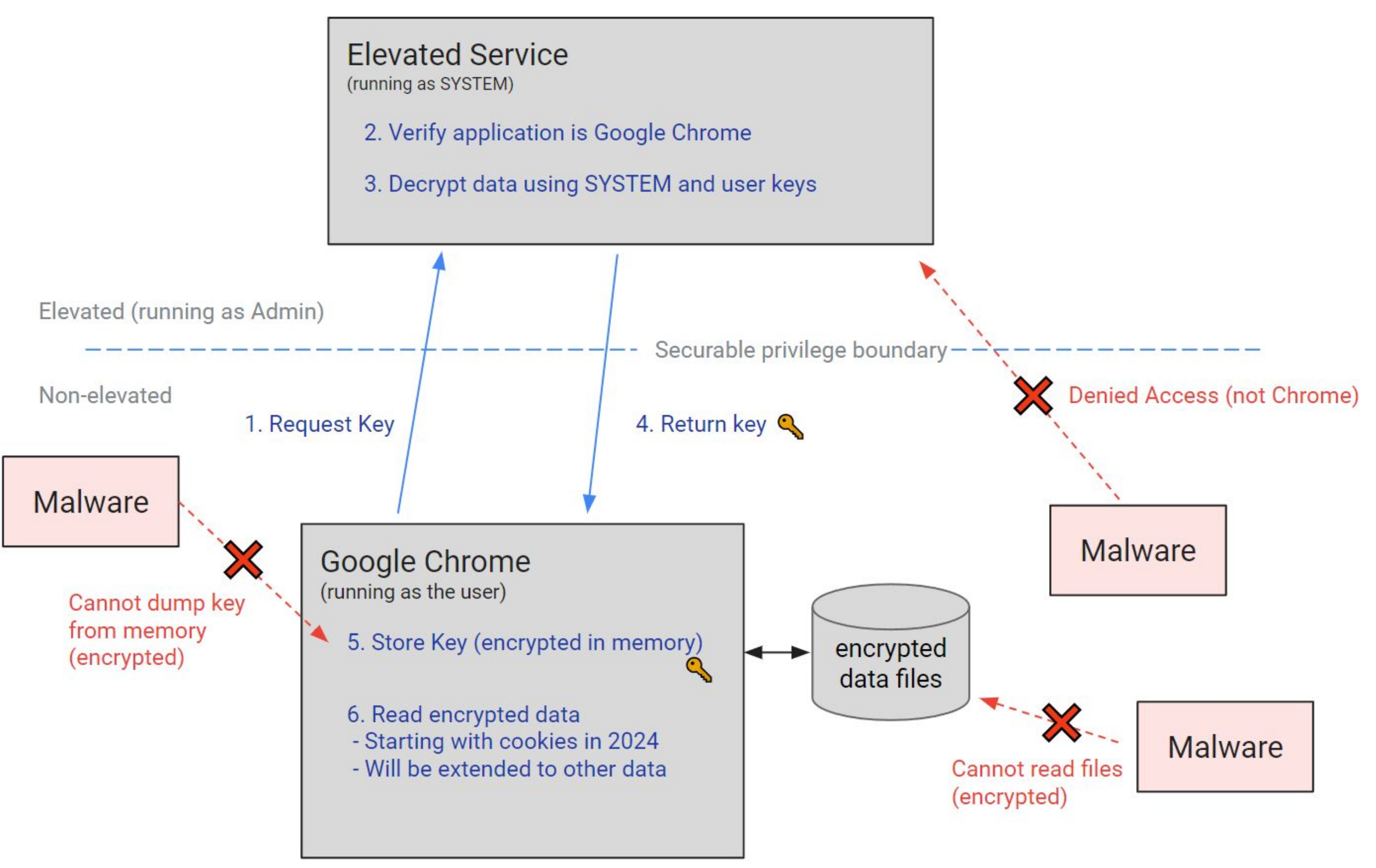
What Now?

Defense and Mitigation Strategies

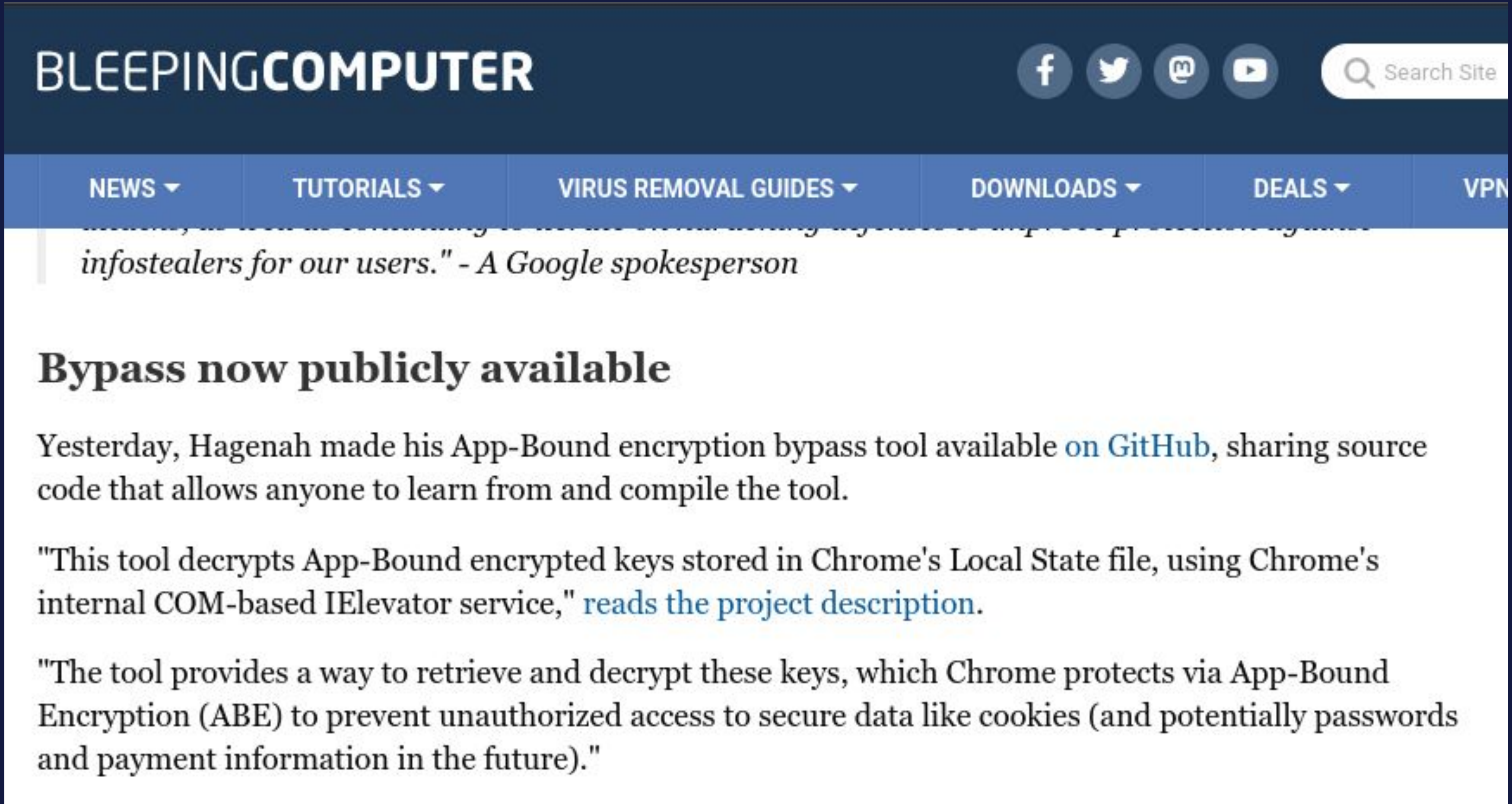
Defensive Mechanism: Application Bound Encryption

A defense in depth feature for Chrome and Chromium-based Browsers

- Data files are encrypted
  - Cookies, passwords, etc.
- A privileged service protects the data


Elevated Service
(running as SYSTEM)
2. Verify application is Google Chrome
3. Decrypt data using SYSTEM and user keys
Elevated (running as Admin)
Securable privilege boundary
Non-elevated
1. Request Key
4. Return key
Denied Access (not Chrome)
Malware
Cannot dump key from memory (encrypted)
Google Chrome
(running as the user)
5. Store Key (encrypted in memory)
6. Read encrypted data
- Starting with cookies in 2024
- Will be extended to other data
encrypted data files
Malware
Malware
Cannot read files (encrypted)

Application Bound Encryption Bypassed



> *infostealers for our users." - A Google spokesperson*

Bypass now publicly available

Yesterday, Hagenah made his App-Bound encryption bypass tool available on GitHub, sharing source code that allows anyone to learn from and compile the tool.

"This tool decrypts App-Bound encrypted keys stored in Chrome's Local State file, using Chrome's internal COM-based IElevator service," reads the project description.

"The tool provides a way to retrieve and decrypt these keys, which Chrome protects via App-Bound Encryption (ABE) to prevent unauthorized access to secure data like cookies (and potentially passwords and payment information in the future)."

October 28th 2024

Application Bound Encryption (ABE) Bypassed

Bypass Techniques

- Launch a headless Chrome with Remote Debugging
- Dumping memory
- Interacting with Elevated Service using COM objects impersonating Chrome
- Disabling ABE Registry Keys

https://redcanary.com/blog/threat-intelligence/google-chrome-app-bound-encryption/

https://www.elastic.co/security-labs/katz-and-mouse-game

ABE Bypassed: Doesn’t Matter

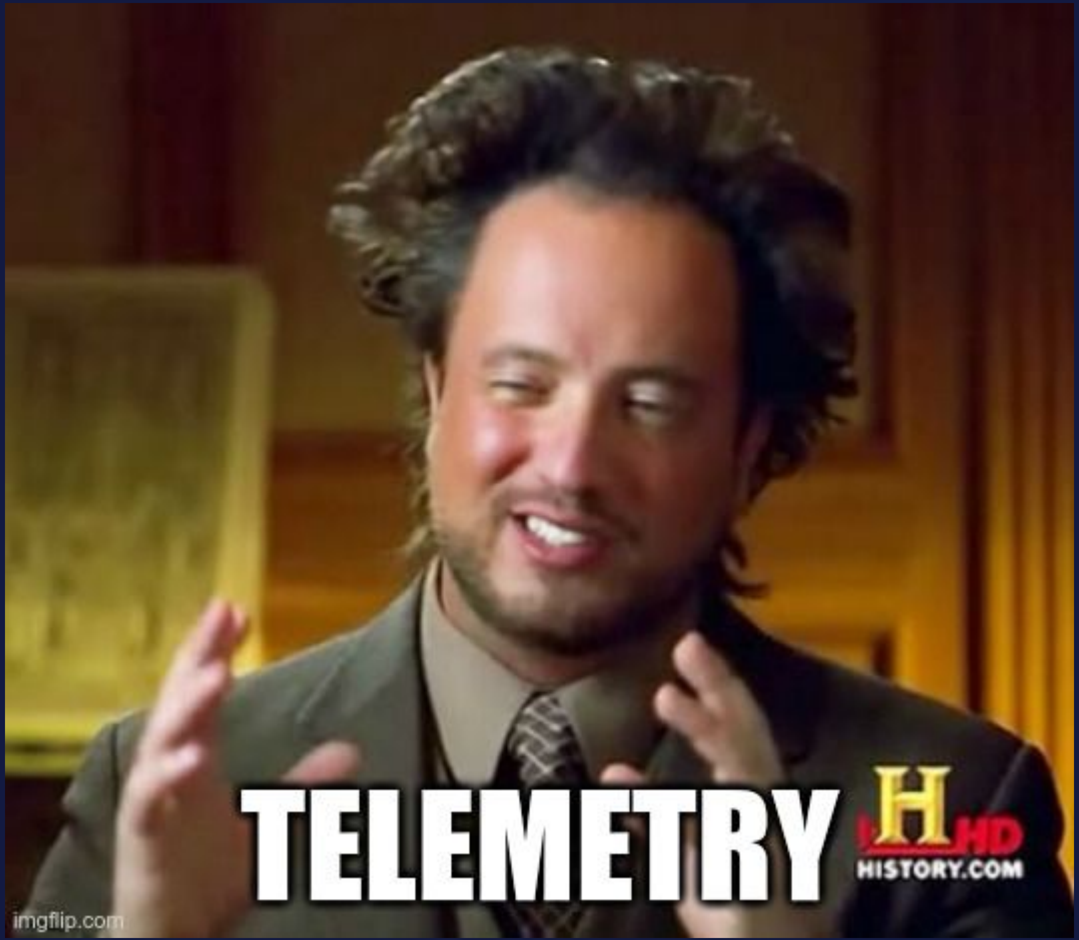
- Requires Admin

  or

- More Detectable than File I/O

  or

- Brittle (relying on frequently changing things like memory offsets)



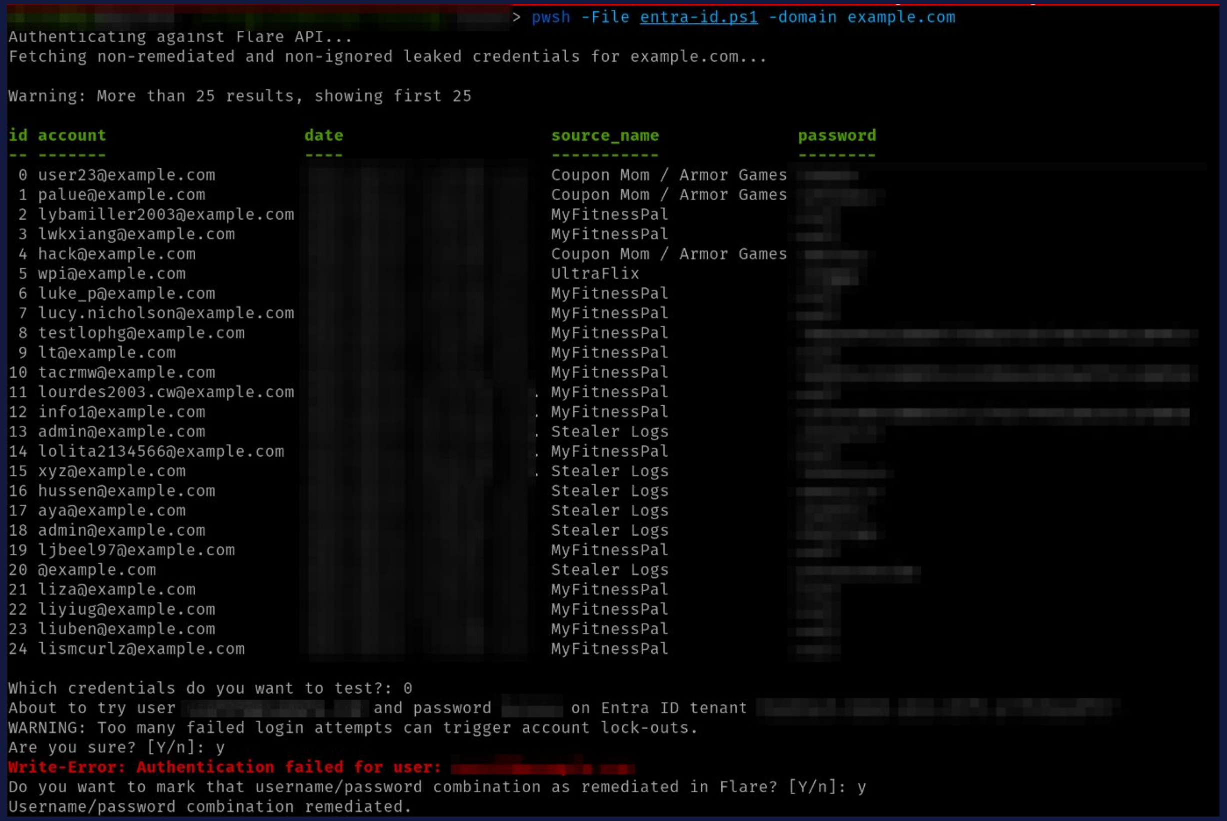
Defense: Testing Credential

All credible credentials should be tested

Force a reset on next login if its valid

Be Aware

- Generates logs that can trigger the Blue Teams
- Avoid account lockouts



```
[redacted] > pwsh -File entra-id.ps1 -domain example.com
Authenticating against Flare API...
Fetching non-remediated and non-ignored leaked credentials for example.com...

Warning: More than 25 results, showing first 25

id account                      date                      source_name              password
-- -------                      ----                      -----------              --------
 0 user23@example.com           [redacted]                Coupon Mom / Armor Games [redacted]
 1 palue@example.com            [redacted]                Coupon Mom / Armor Games [redacted]
 2 lybamiller2003@example.com   [redacted]                MyFitnessPal             [redacted]
 3 lwkxiang@example.com         [redacted]                MyFitnessPal             [redacted]
 4 hack@example.com             [redacted]                Coupon Mom / Armor Games [redacted]
 5 wpi@example.com              [redacted]                UltraFlix                [redacted]
 6 luke_p@example.com           [redacted]                MyFitnessPal             [redacted]
 7 lucy.nicholson@example.com   [redacted]                MyFitnessPal             [redacted]
 8 testlophg@example.com        [redacted]                MyFitnessPal             [redacted]
 9 lt@example.com               [redacted]                MyFitnessPal             [redacted]
10 tacrmw@example.com           [redacted]                MyFitnessPal             [redacted]
11 lourdes2003.cw@example.com   [redacted]              . MyFitnessPal             [redacted]
12 info1@example.com            [redacted]              . MyFitnessPal             [redacted]
13 admin@example.com            [redacted]              . Stealer Logs             [redacted]
14 lolita2134566@example.com    [redacted]              . MyFitnessPal             [redacted]
15 xyz@example.com              [redacted]              . Stealer Logs             [redacted]
16 hussen@example.com           [redacted]                Stealer Logs             [redacted]
17 aya@example.com              [redacted]                Stealer Logs             [redacted]
18 admin@example.com            [redacted]                Stealer Logs             [redacted]
19 ljbeel97@example.com         [redacted]                MyFitnessPal             [redacted]
20 @example.com                 [redacted]                Stealer Logs             [redacted]
21 liza@example.com             [redacted]                MyFitnessPal             [redacted]
22 liyiug@example.com           [redacted]                MyFitnessPal             [redacted]
23 liuben@example.com           [redacted]                MyFitnessPal             [redacted]
24 lismcurlz@example.com        [redacted]                MyFitnessPal             [redacted]

Which credentials do you want to test?: 0
About to try user [redacted] and password [redacted] on Entra ID tenant [redacted]
WARNING: Too many failed login attempts can trigger account lock-outs.
Are you sure? [Y/n]: y
Write-Error: Authentication failed for user: [redacted]
Do you want to mark that username/password combination as remediated in Flare? [Y/n]: y
Username/password combination remediated.
```

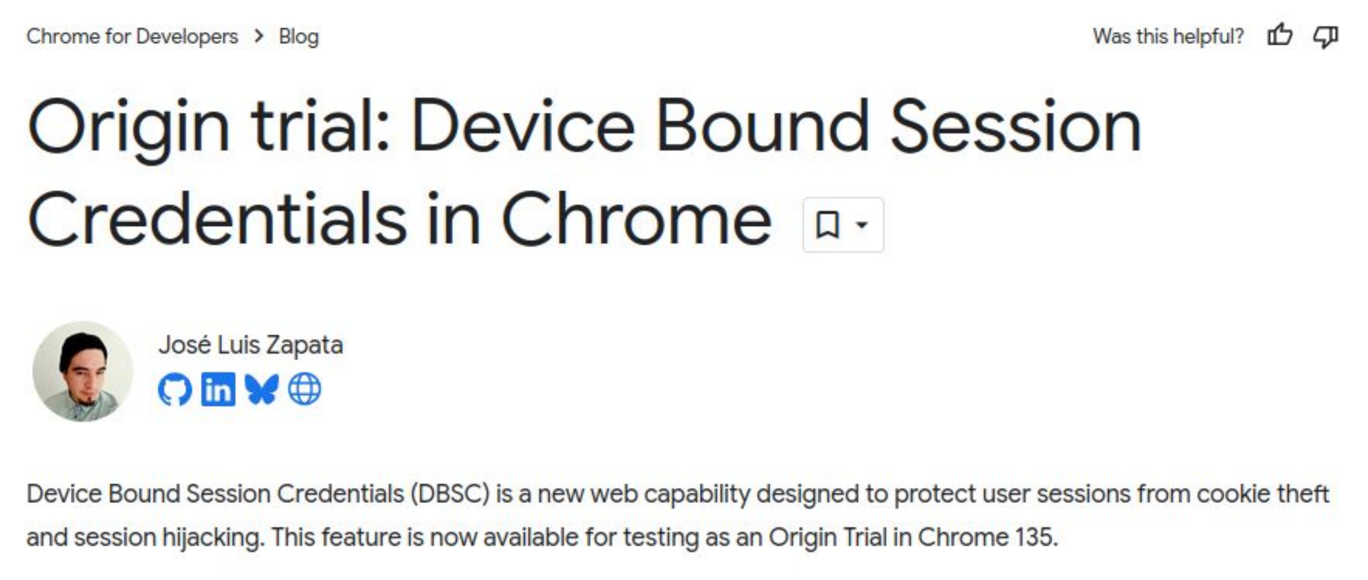
Defense: More is coming!

Announced two months ago!

- New API for short-lived sessions
- Crypto is bound to TPM
- Requires a new HTTP Header

Time will tell if it will catch up…

https://developer.chrome.com/blog/dbsc-origin-trial



Chrome for Developers > Blog

Was this helpful?

Origin trial: Device Bound Session Credentials in Chrome

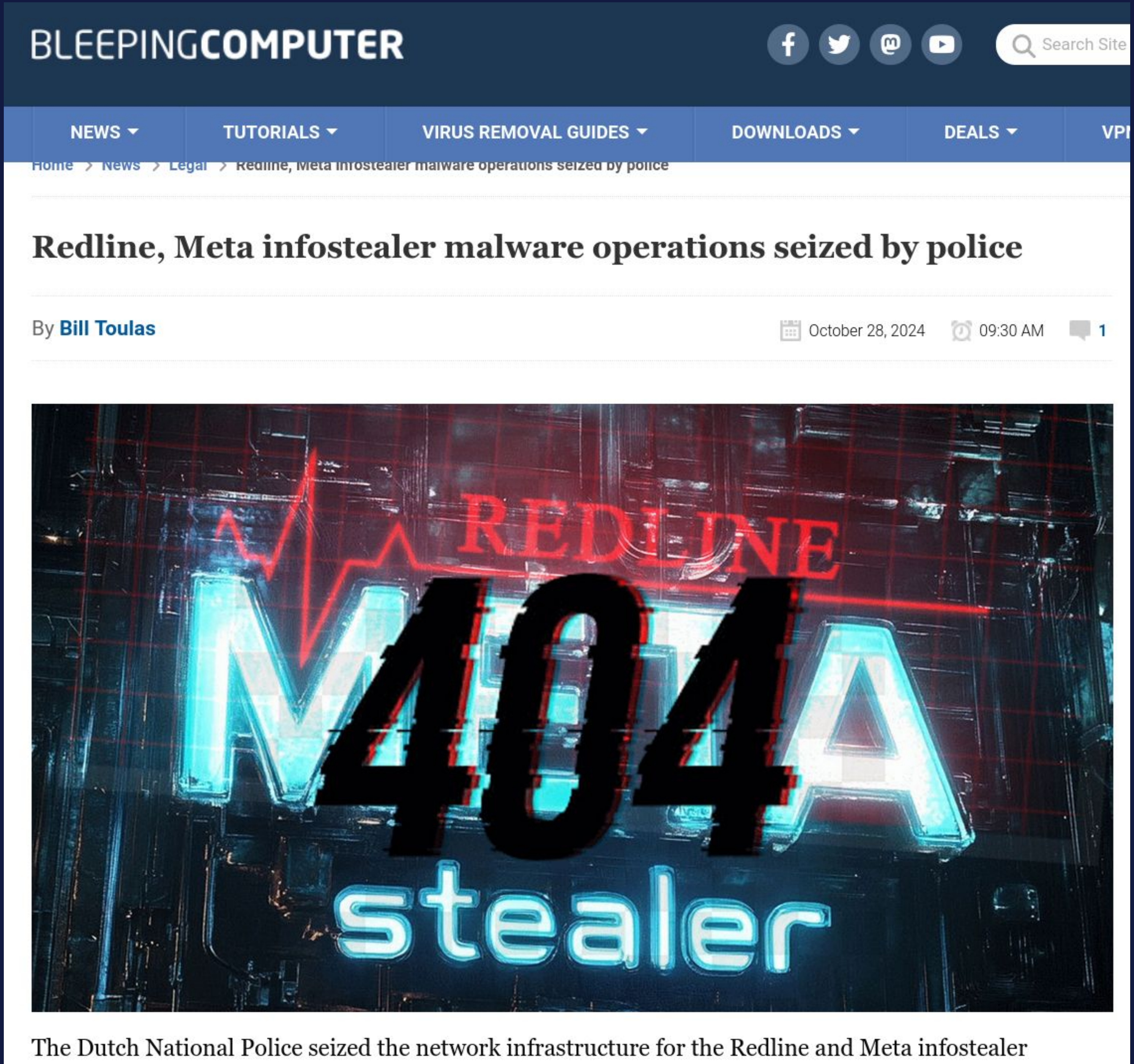
José Luis Zapata

Device Bound Session Credentials (DBSC) is a new web capability designed to protect user sessions from cookie theft and session hijacking. This feature is now available for testing as an Origin Trial in Chrome 135.

The Redline/META Takedown

Redline - Meta

In October 2024



Home > News > Legal > Redline, Meta infostealer malware operations seized by police

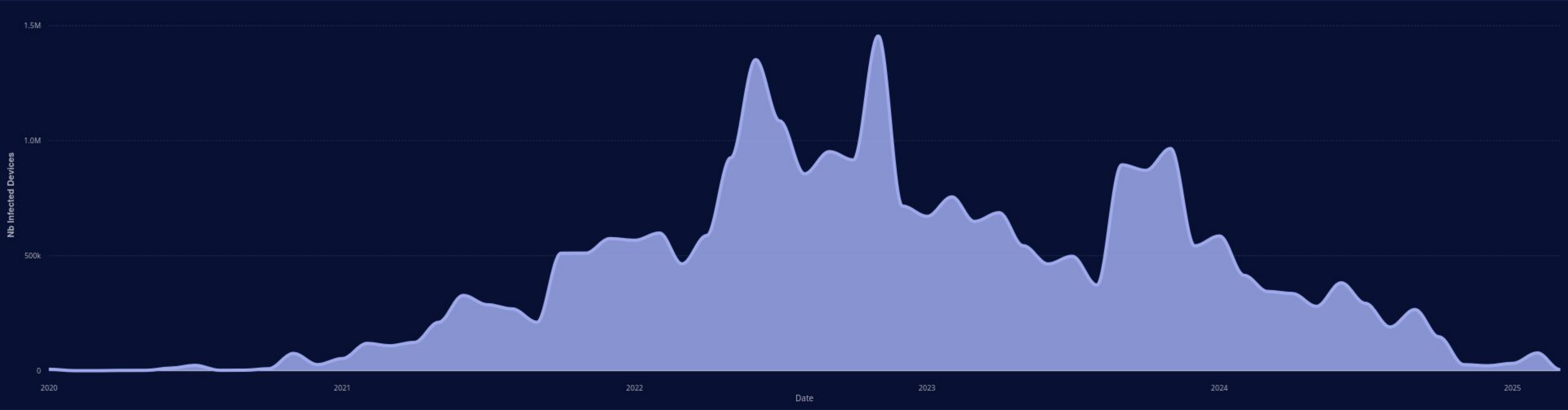
Redline, Meta infostealer malware operations seized by police

By Bill Toulas

October 28, 2024 09:30 AM 1

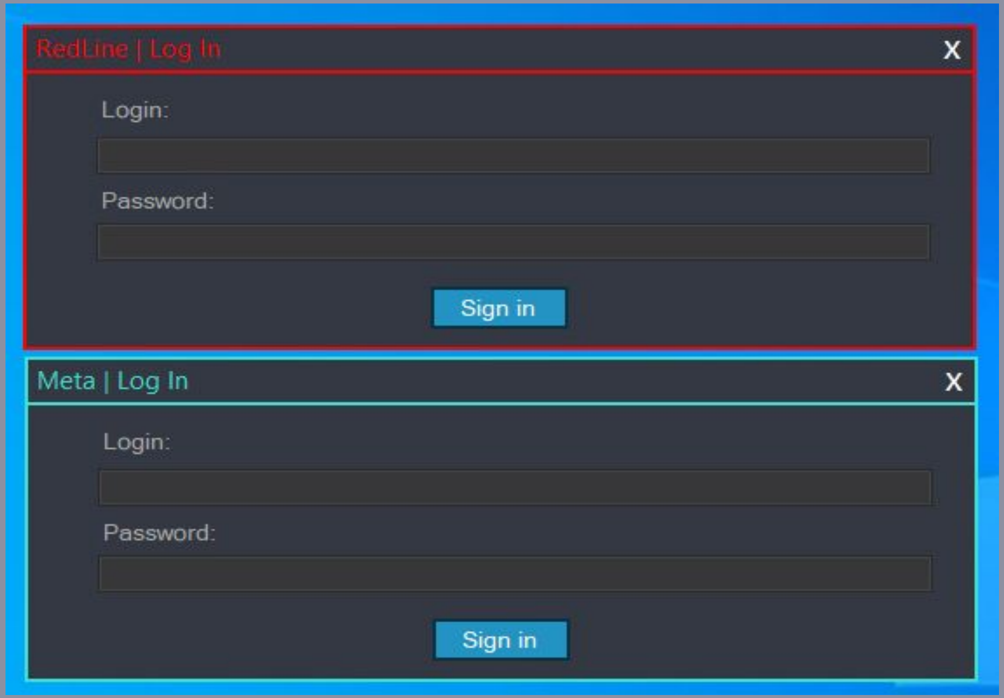
The Dutch National Police seized the network infrastructure for the Redline and Meta infostealer

Redline/Meta's Infections Through Time



They are the same...

~~RedLine~~ META Stealer



RedLine | Log In

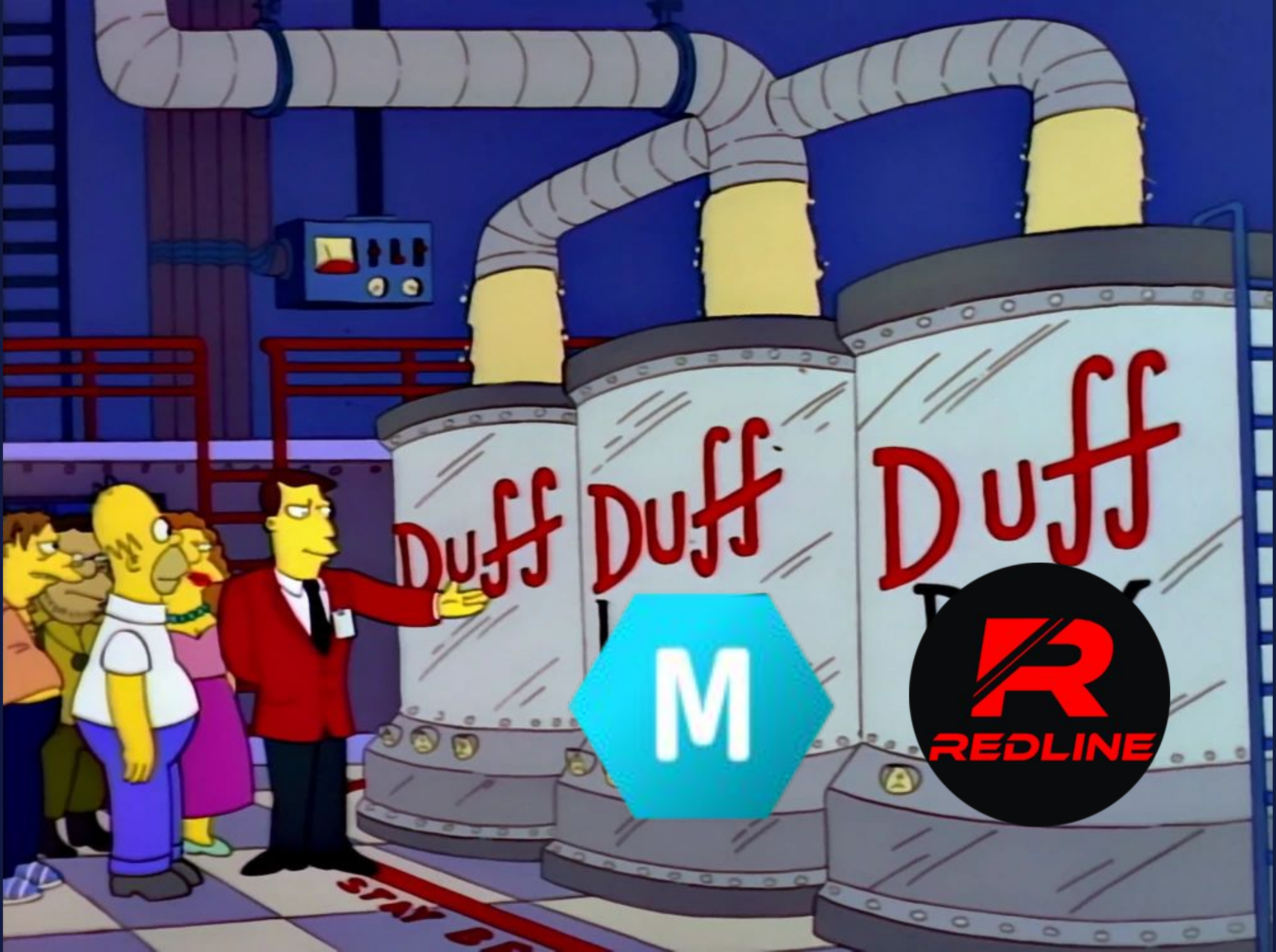
Login:

Password:

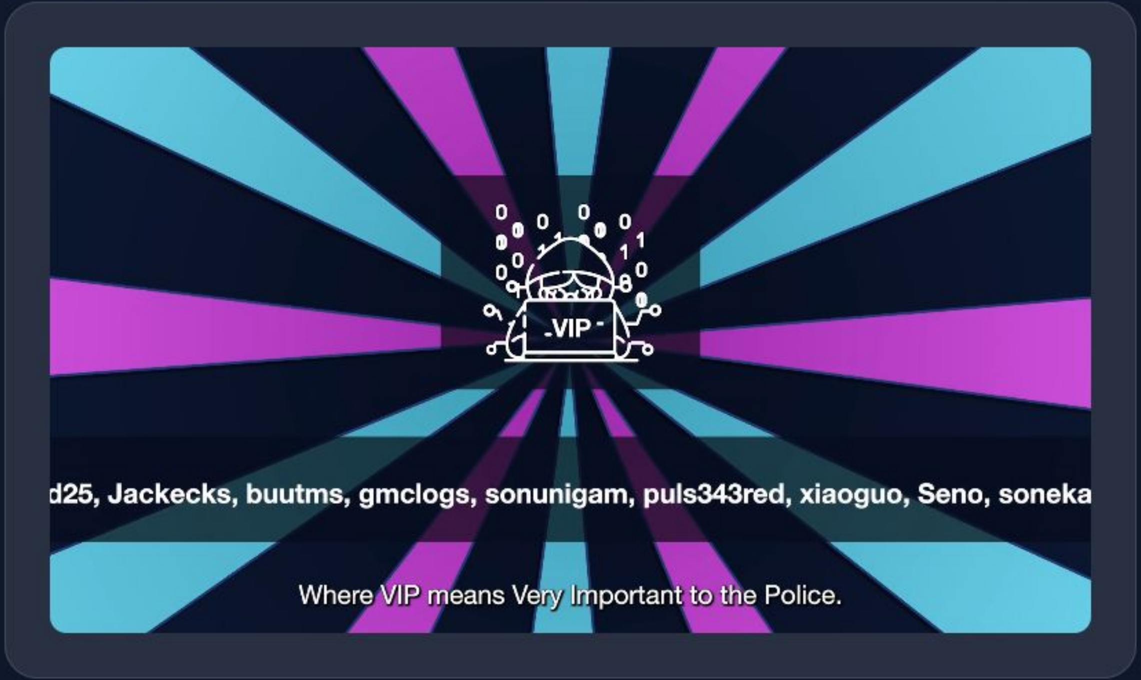
Meta | Log In

Login:

Password:


Duff
Duff
Duff
M
REDLINE
STAY B

From Flare & ESET to Takedown - a 2 year process



d25, Jackecks, buutms, gmclogs, sonunigam, puls343red, xiaoguo, Seno, soneka

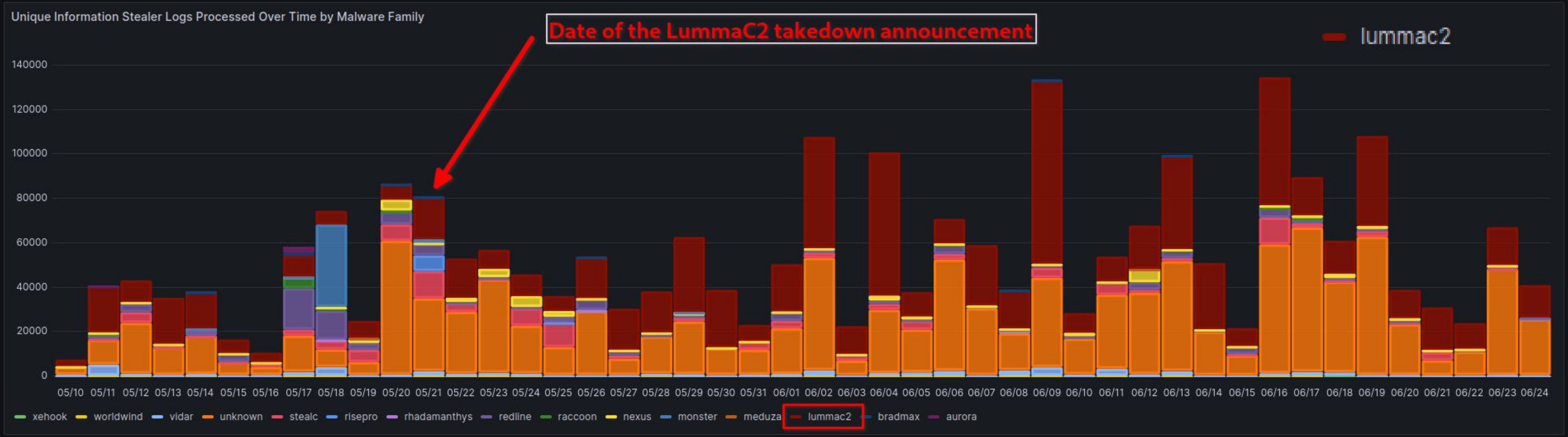
Where VIP means Very Important to the Police.

POLITIE NCIS IRS-CI Federal Police NCA National Crime Agency

POLÍCIA JUDICIÁRIA OPENBAAR MINISTERIE EUROJUST

But Do Takedowns Actually Work?

LummaC2



Date of the LummaC2 takedown announcement

- Domains seized but fallback C2 is Telegram
- Is it worth all the trouble? Open to discuss!

Wrapping Up

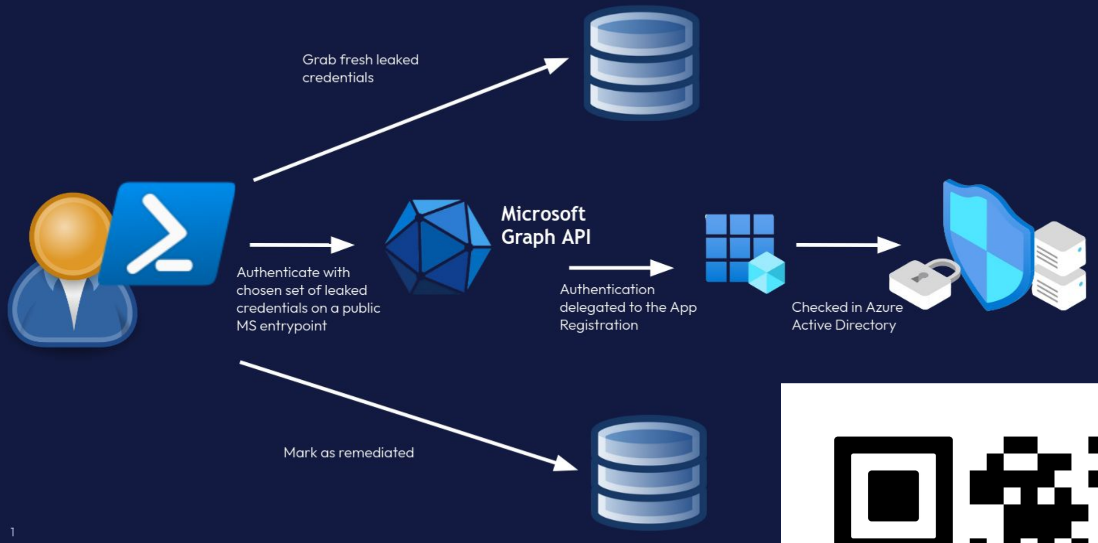
and community contributions!

Community Contributions

flare

1. Credential Testing Script

Test credentials against Entra-ID (Azure AD)



Grab fresh leaked credentials

Microsoft Graph API

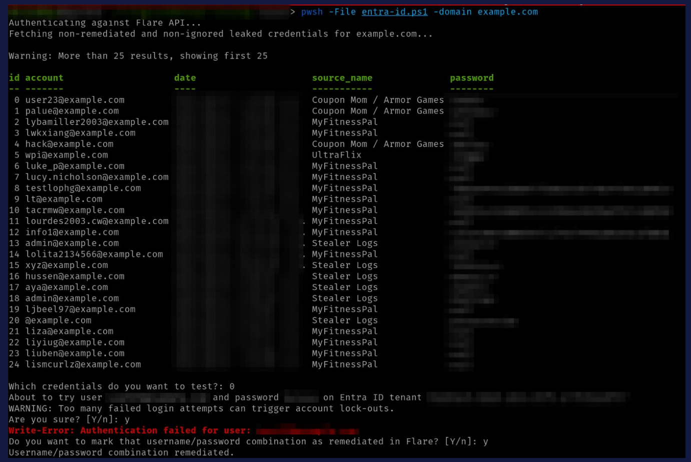
Authenticate with chosen set of leaked credentials on a public MS entrypoint

Authentication delegated to the App Registration

Checked in Azure Active Directory

Mark as remediated

1

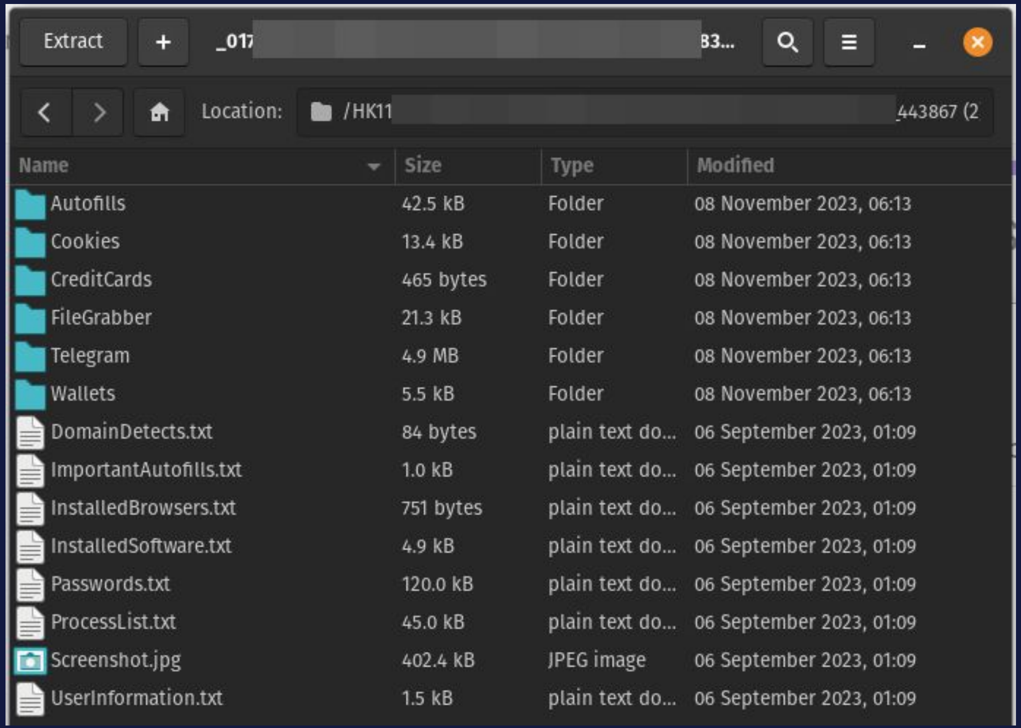


```
[redacted] > pwsh -File entra-id.ps1 -domain example.com
Authenticating against Flare API...
Fetching non-remediated and non-ignored leaked credentials for example.com...

Warning: More than 25 results, showing first 25

id account                      date                        source_name           password
-- -------                      ----                        -----------           --------
 0 user23@example.com           [redacted]                  Coupon Mom / Armor Games [redacted]
 1 palue@example.com                                        Coupon Mom / Armor Games
 2 lybamiller2003@example.com                               MyFitnessPal
 3 lwkxiang@example.com                                     MyFitnessPal
 4 hack@example.com                                         Coupon Mom / Armor Games
 5 wpi@example.com                                          UltraFlix
 6 luke_p@example.com                                       MyFitnessPal
 7 lucy.nicholson@example.com                               MyFitnessPal
 8 testlophg@example.com                                    MyFitnessPal
 9 lt@example.com                                           MyFitnessPal
10 tacrmw@example.com                                       MyFitnessPal
11 lourdes2003.cw@example.com                             . MyFitnessPal
12 info1@example.com                                      . MyFitnessPal
13 admin@example.com                                      . Stealer Logs
14 lolita2134566@example.com                              . MyFitnessPal
15 xyz@example.com                                        . Stealer Logs
16 hussen@example.com                                       Stealer Logs
17 aya@example.com                                          Stealer Logs
18 admin@example.com                                        Stealer Logs
19 ljbeel97@example.com                                     MyFitnessPal
20 @example.com                                             Stealer Logs
21 liza@example.com                                         MyFitnessPal
22 liyiug@example.com                                       MyFitnessPal
23 liuben@example.com                                       MyFitnessPal
24 lismcurlz@example.com                                    MyFitnessPal

Which credentials do you want to test?: 0
About to try user [redacted] and password [redacted] on Entra ID tenant [redacted]
WARNING: Too many failed login attempts can trigger account lock-outs.
Are you sure? [Y/n]: y
Write-Error: Authentication failed for user: [redacted]
Do you want to mark that username/password combination as remediated in Flare? [Y/n]: y
Username/password combination remediated.
```

2. A Sample Set of Stealer Logs

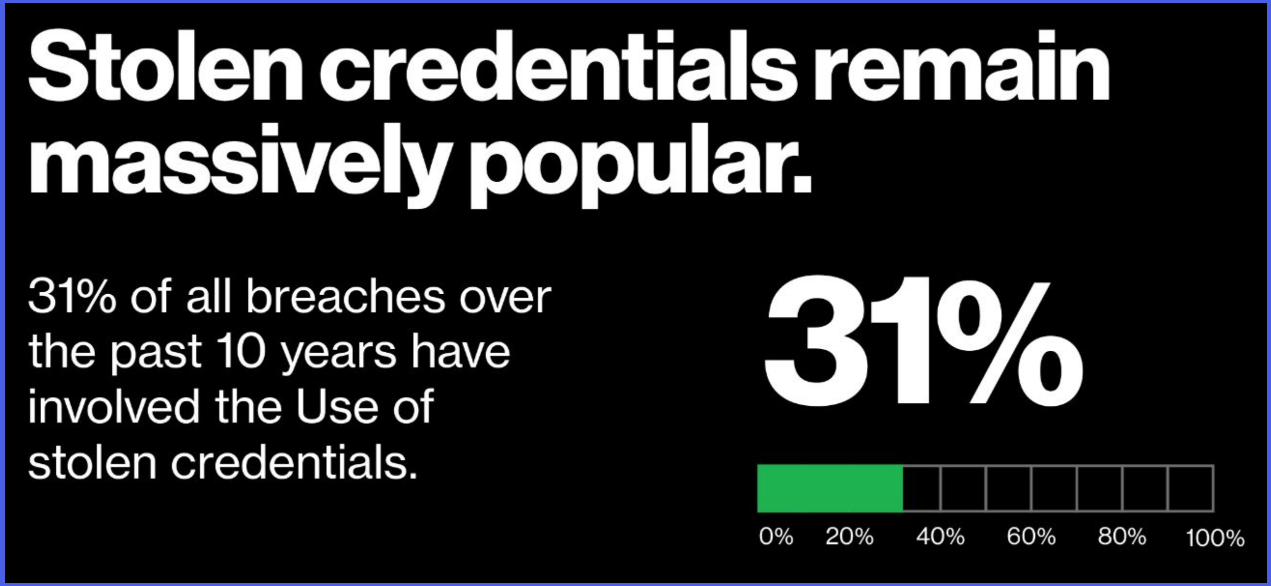
Get intimate with what they are and what they contain.

To adequately defend: Knowledge is Power



Name	Size	Type	Modified
Autofills	42.5 kB	Folder	08 November 2023, 06:13
Cookies	13.4 kB	Folder	08 November 2023, 06:13
CreditCards	465 bytes	Folder	08 November 2023, 06:13
FileGrabber	21.3 kB	Folder	08 November 2023, 06:13
Telegram	4.9 MB	Folder	08 November 2023, 06:13
Wallets	5.5 kB	Folder	08 November 2023, 06:13
DomainDetects.txt	84 bytes	plain text do...	06 September 2023, 01:09
ImportantAutofills.txt	1.0 kB	plain text do...	06 September 2023, 01:09
InstalledBrowsers.txt	751 bytes	plain text do...	06 September 2023, 01:09
InstalledSoftware.txt	4.9 kB	plain text do...	06 September 2023, 01:09
Passwords.txt	120.0 kB	plain text do...	06 September 2023, 01:09
ProcessList.txt	45.0 kB	plain text do...	06 September 2023, 01:09
Screenshot.jpg	402.4 kB	JPEG image	06 September 2023, 01:09
UserInformation.txt	1.5 kB	plain text do...	06 September 2023, 01:09

Conclusion



Stolen credentials remain massively popular.

31% of all breaches over the past 10 years have involved the Use of stolen credentials.

31%

from the Verizon 2024 DBIR Report

1. **Understand/Educate**
2. **Protect**
3. **Remediate**

Understand/Educate

- Administrative rights NOT required
- Comes via
  - Cracked software!
  - Malicious ads
  - Free robux YouTube videos
  - Fake updates
  - Free PDFs
- There is rarely a reason to disable your A/V
- Don’t share work computers with family members
- Not limited to passwords: MFA, wallets, etc.
- Study the provided stealer logs to understand them

Protect

- Password managers are still effective
- Windows SmartScreen is effective against files pretending to be something else*
- AdBlock like uBlock Origin

Remediate

- Search through Stealer Log databases from your favorite Threat Exposure Vendor ;)
- Make sure the credentials found are not working
- Find and manage shadow IT services used by your compromised users

Questions?

the good stuff is here!

Olivier Bilodeau

- Email: olivier.bilodeau@flare.io
- Other Hat: https://nsec.io
- Social: @obilodeau.bsky.social

First to ask a question will get a NorthSec 2024 badge!

Come and see us at our booth!
(I have more hw badges!)