SELLING 🔥✨ Selling Government & Law Enforcement Email Accounts 🔥✨ (Many countries)🔥
by Governer - 22-06-25, 01:51 AM

22-06-25, 01:51 AM (This post was last modified: 24-09-25, 07:11 AM by Governer.) #1

Governer

GOD

Posts 146
Threads 4
Joined Jun 2025
Reputation 87
4 Months

🔥✨ Selling Government & Law Enforcement Email Accounts (Many countries!) (Accounts)🔥✨

INFOSTEALERS

Monitoramento e Resposta a Incidentes

LUIZ EDUARDO SALOMÃO

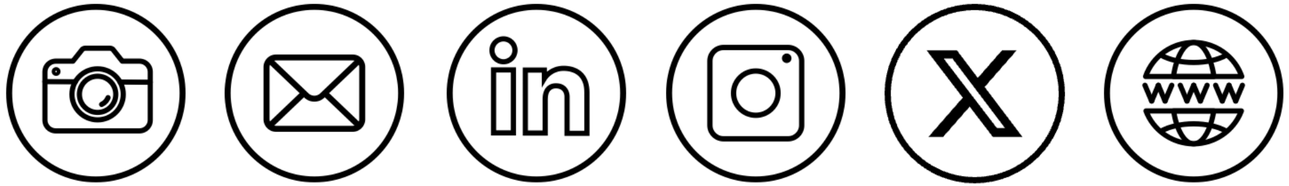
Agente de Polícia (PCDF)
Aluno Especial – Mestrado Seg. Cibernética (UNB)
Aluno – MBA em IA (IBMEC)

Especialista em segurança da informação e apaixonado por segurança cibernética, possui diversas certificações na área, como CEH, Pentest+, Privacy Manager (CIPM) e CERT Incident Response Process Professional, já tendo atuado em grandes empresas brasileiras. Atualmente, é responsável por criar, implementar e conduzir soluções de Segurança Ofensiva (Red Team/Offensive Security) e de Inteligência Cibernética (CTI), bem como é membro da equipe de resposta a incidentes (CSIRT) da Polícia Civil do Distrito Federal (PCDF) - SSTI/DITEC/DGI, atuando como analista de último nível em eventos críticos que poderiam gerar impacto na sociedade.

CERT
Incident Response Process Professional
Certificate Holder

TLP:CLEAR

NÃO HÁ LIMITES NA DIVULGAÇÃO



https://cert.br/tlp/

ATENÇÃO: No momento desta apresentação, eventuais campanhas ativas foram devidamente tarjadas.

ATENÇÃO: Este trabalho é fruto de uma análise de CTI e não representa qualquer investigação policial em curso.

Infostealer: malwares desenvolvidos para invadir sistemas e roubar dados sensíveis, como credenciais de login, detalhes financeiros, dados pessoais e informações sobre o dispositivo e sobre a rede. Uma vez instalado, extrai informações de navegadores, dos gerenciadores de senha e até mesmo do clipboard.

Kela Inside the infostealer epidemic: exposing the risks to corporate security

MALWARE-AS-SERVICE

1) AQUISIÇÃO

Official Stealer AID_Stealer Hardless · 20.02.24 2 3	Replies: 37 Views: 7K	22.10.25 VALLHAL88	V
Official Stealer LummaC2 - Стиллер, отстук 75-80%, FUD, антиразлог Google LummaStealer · 26.12.22 15 16 17	Replies: 254 Views: 38K	16.10.25 drientwintig	D
Official Stealer OLYMP BOTNET - ЛУЧШИЙ FUD MASS LOADER НА РЫНКЕ | 0\72 VT, FUD | ASSEMBLY LANGUAGE | STEALER FullyUnDetectable · 08.06.25	Replies: 5 Views: 906	22.06.25 FullyUnDetectable	
Official Stealer Mint Stealer | #1 STEALER - GAMES, BROWSERS, WALLET... | SEMI -FUD | UHQ ArtemFromNights · 15.02.25 2	Replies: 16 Views: 2K	14.06.25 HustleTrafficBHF	H
Official Stealer BLACKNOTE | STEALER BlackLoad · 01.09.24 2	Replies: 18 Views: 4K	06.03.25 да просто обычный	Д
Official Stealer Mint Stealer | #1 STEALER - GAMES, BROWSERS, WALLET... | SEMI -FUD | UHQ ArtemFromNights · 29.09.23	Replies: 1 Views: 1K	04.02.25 D	
Verified Official Stealer Phoenix Native Stealer [C/C++ | 30 KB Build] $Phoenix$ · 02.07.22 2	Replies: 16 Views: 6K	21.03.24 $Phoenix$	
Official Stealer ObserverStealer - BETA - [Rent] ObserverStealer · 16.05.23	Replies: 7 Views: 1K	13.01.25 Tomas_Shelby	T
Official Stealer Extractor Stealer - лучший Native стиллер | Хороший крипт | FUD | Отстук ~95% | RunPe | Не оставляет следов | AntiVM | AntiBrute | Красивая панель reaper_official · 10.10.23 2	Replies: 21 Views: 4K	15.11.24 georgelkardan	G
Official Stealer Ailurophile Stealer | FUD Every Day | Passwords - Cookies - History - Credit Card | Chromium-Based Gecko-Based Browsers | Managed via our Panel Ailurophile · 05.11.24	Replies: 2 Views: 1K	21.11.24 Ailurophile	
Official Stealer ACR Stealer	Replies: 12	21.06.24	

https://vidar[redacted]

EN RU

VIDAR

THE SILENT GOD

The Birth of Destiny

Vidar is a god from the Aesir family of gods. He is the son of the chief of those gods, Odin. **Vidar was born to avenge his father.**

In the Voluspa, it tells of a coming final battle where the gods will fight their enemies, the giants. One of the enemies is a wolf called Fenrir. This wolf will, according to the prediction, swallow Odin.

The Conspiracy

Odin is a clever fellow. Knowing his fate, he conspired to make
work in the future. He sought out the correct mother for this p
be Vidar's job to destroy Fenrir.

The Gift of Foresight

Vidar grew quickly. His strength became as great as the strong
warrior and learned his trade fast. But there is more to him.

Because he was born for the future, he had the gift of foresigh
Far-Seer. He knew the nature of the future, but he did not tell t
that he is called **Vidar the Silent**.

https://vida[redacted]/auth/login?ddosprotected=1

Login

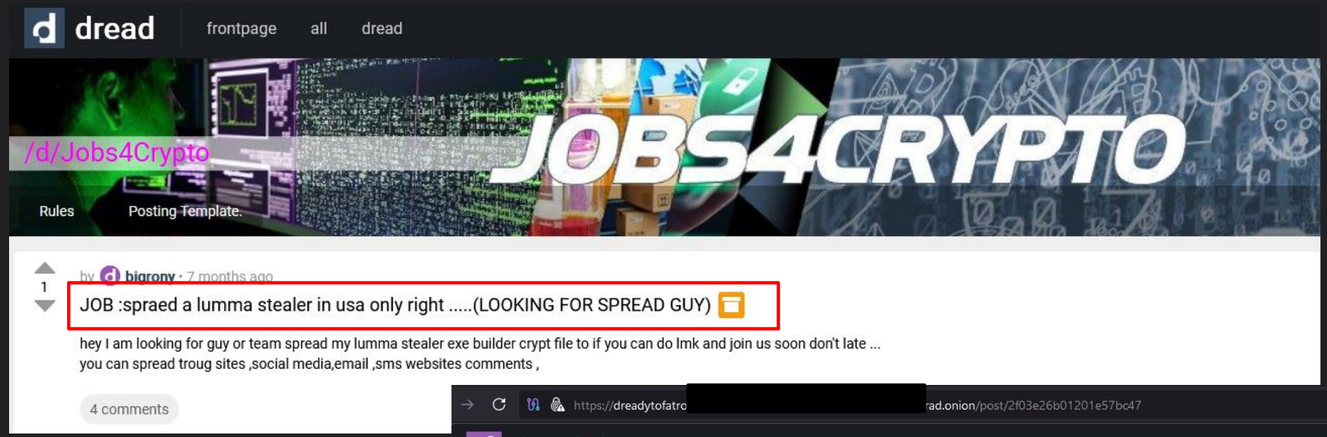
Password

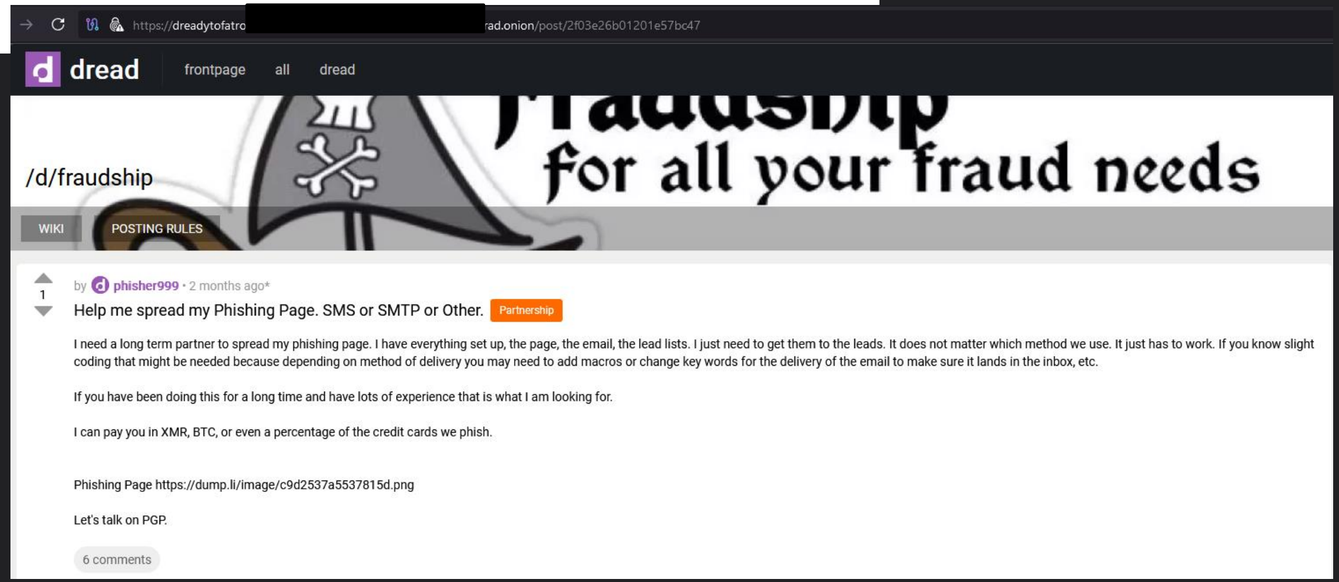
Save session Till closing the browser

Sign in

2) DISTRIBUIÇÃO

SPRAY AND PRAY


dread
frontpage
all
dread
/d/Jobs4Crypto
JOBS4CRYPTO
Rules
Posting Template
1
by bigrony • 7 months ago
JOB :spraed a lumma stealer in usa only right .....(LOOKING FOR SPREAD GUY)
hey I am looking for guy or team spread my lumma stealer exe builder crypt file to if you can do lmk and join us soon don't late ...
you can spread troug sites ,social media,email ,sms websites comments ,
4 comments


https://dreadytofatro[redacted]ad.onion/post/2f03e26b01201e57bc47
dread
frontpage
all
dread
/d/fraudship
for all your fraud needs
WIKI
POSTING RULES
1
by phisher999 • 2 months ago*
Help me spread my Phishing Page. SMS or SMTP or Other.
Partnership
I need a long term partner to spread my phishing page. I have everything set up, the page, the email, the lead lists. I just need to get them to the leads. It does not matter which method we use. It just has to work. If you know slight coding that might be needed because depending on method of delivery you may need to add macros or change key words for the delivery of the email to make sure it lands in the inbox, etc.
If you have been doing this for a long time and have lots of experience that is what I am looking for.
I can pay you in XMR, BTC, or even a percentage of the credit cards we phish.
Phishing Page https://dump.li/image/c9d2537a5537815d.png
Let's talk on PGP.
6 comments


NYPD
FREE SOFTWARE
FREE MALWARE

SC Media
A CRA Resource

CISO STORIES TOPICS TOPIC HUBS EVENTS PODCASTS RESEARCH SC AWARDS

Threat Intelligence, Malware

Infostealer malware now targets cracked software users

July 23, 2025

Share

By SC Staff

Blog da Zscaler

Receba as últimas atualizações do blog da Zscaler na sua caixa de entrada

Inscreva-se

Security Research

Making victims pay, infostealer malwares mimick pirated-software download sites

MITESH WANI, KAIVALYA KHURSALE
August 23, 2022 – 9 Min. de leitura

3) CAPTURA

https://logins.zip/ | BEST STEALER | CHROMIUM 0DAY | 12s EXECTUTION TIME
by int - 01-10-25, 07:28 AM

int

DarkForums Members

Member

01-10-25, 07:28 AM (This post was last modified: 01-10-25, 07:44 AM by int.)

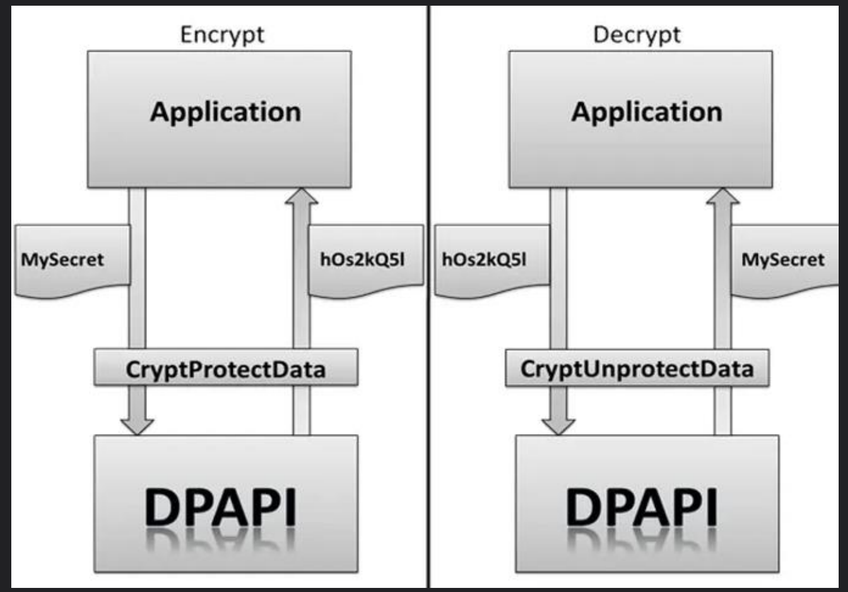
Lumma, Redline, Vidar…
All of these have one thing in common:
~~UNRELIABILITY.~~
These stealers use a single decryption technique (Windows DPAPI), which, on average, **only recovers about 43% of saved passwords and cookies**, a

Logins.zip GUARANTEES that 99% of saved credentials are decrypted and exfiltrated in under 12 seconds after a stub has been run.

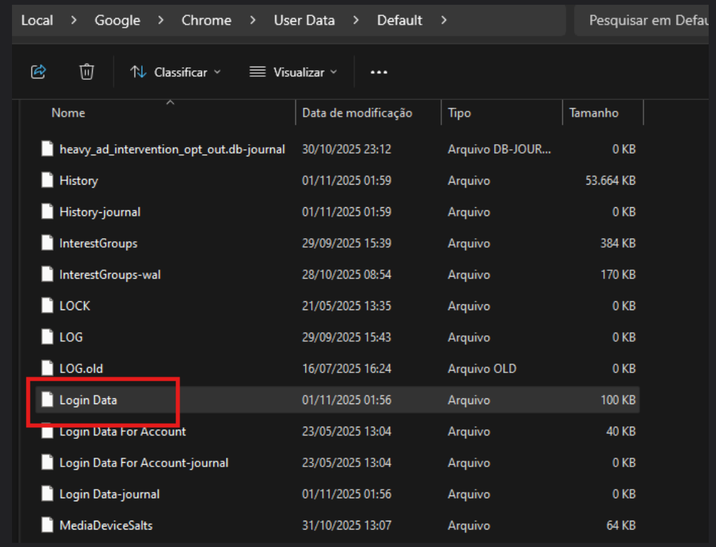
-**FULL Credential Harvesting via exploiting 2 of Chromium's security measures**, all in
-We support most browsers
-Discord token harvesting with auto checking
-Roblox cookie harvesting
-Unreal FUD Stub Sizes with polymorphic auto-obfuscation (STUB SIZES: ~150KB!)
-Advanced CC HARVESTING
The Best Web Panel Out There:
• Includes web builder

Binary analysis reveals that Vidar 2.0 implements comprehensive browser credential extraction capabilities targeting both traditional browser storage methods and Chrome's latest security protections across multiple browser platforms including Chrome, Firefox, Edge, and other Chromium-based browsers. Among its traditional credential extraction techniques, the malware employs a tiered approach that includes systematic enumeration of browser profiles and attempting to extract encryption keys from Local State files using standard DPAPI decryption.

Figure 4. Vidar initially attempts traditional credential access methods such as extracting and decryption of keys from Browser Local State files

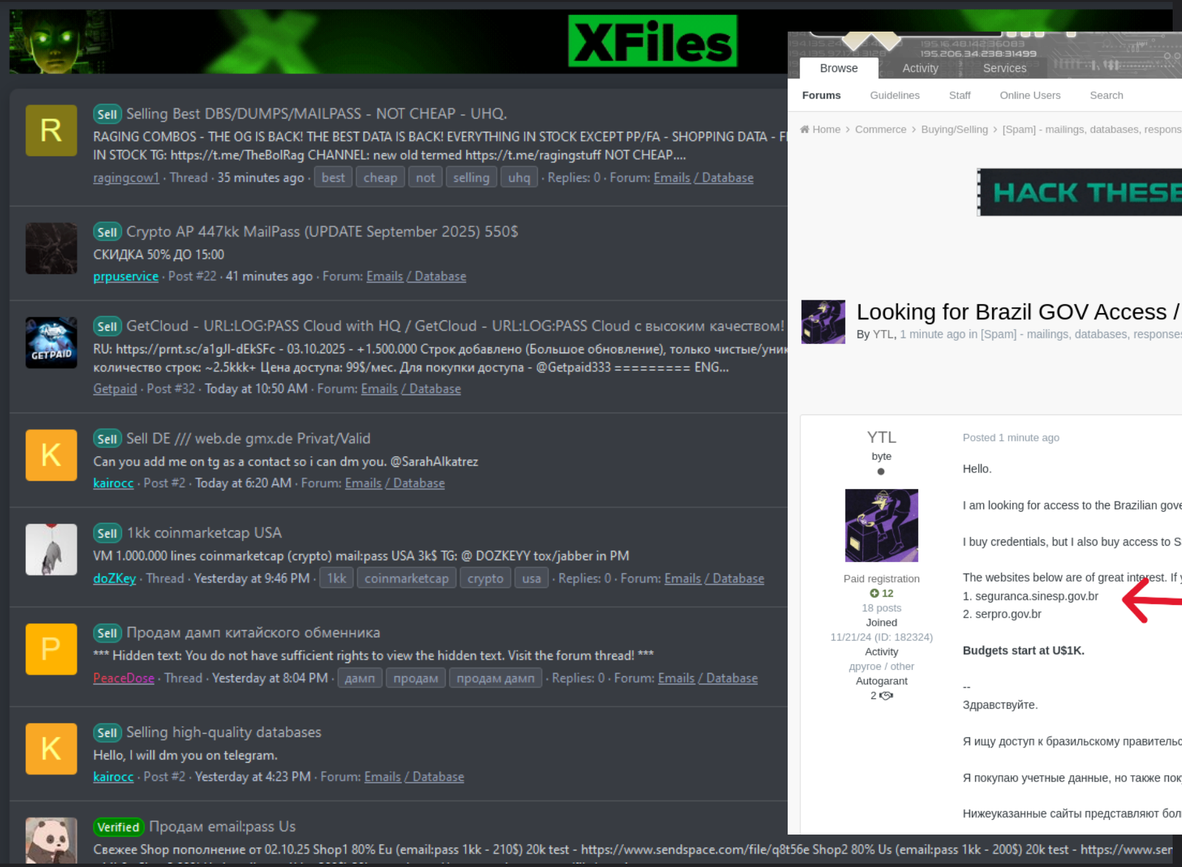


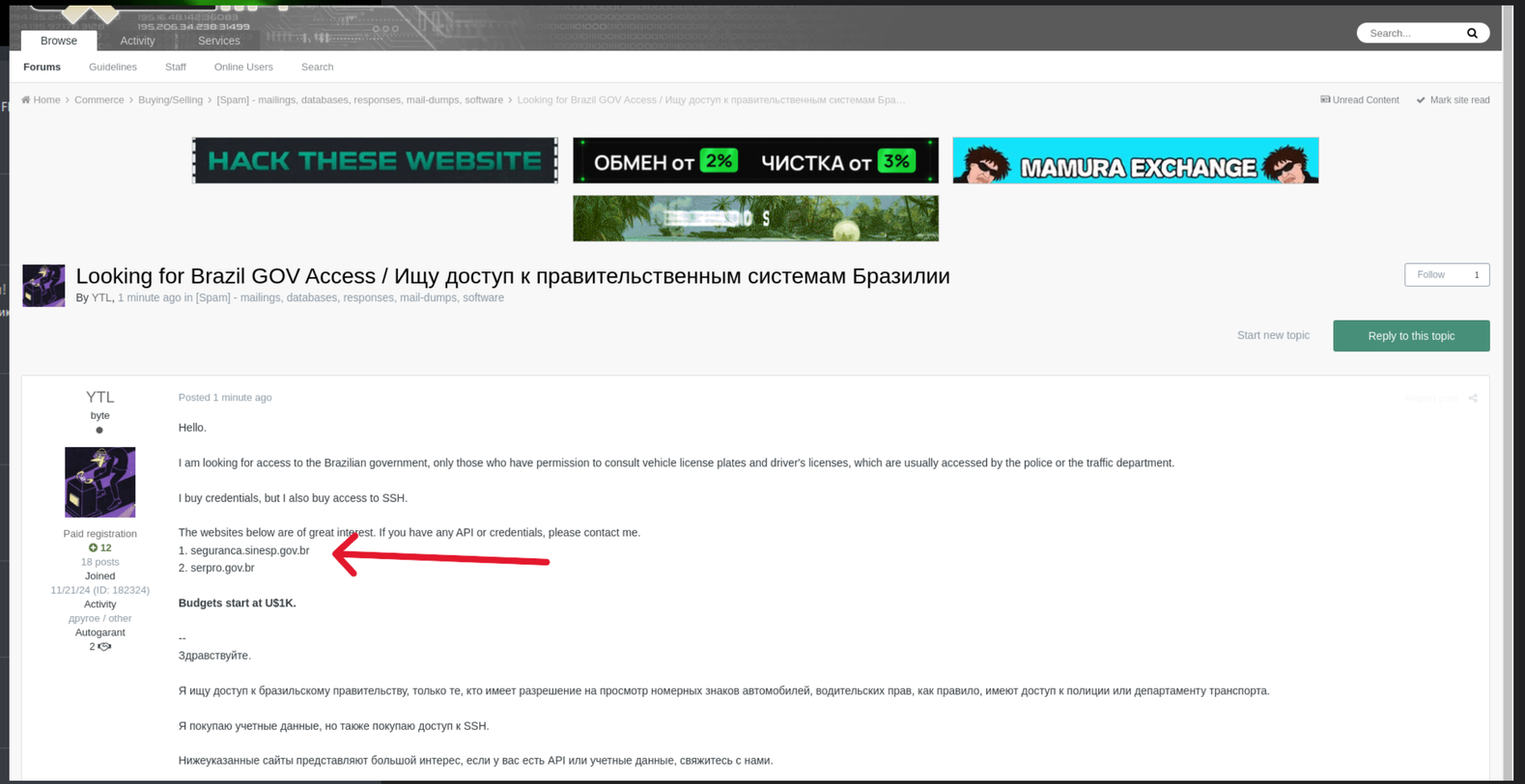
https://z3r0th.medium.com/abusing-dpapi-40b76d3ff5eb

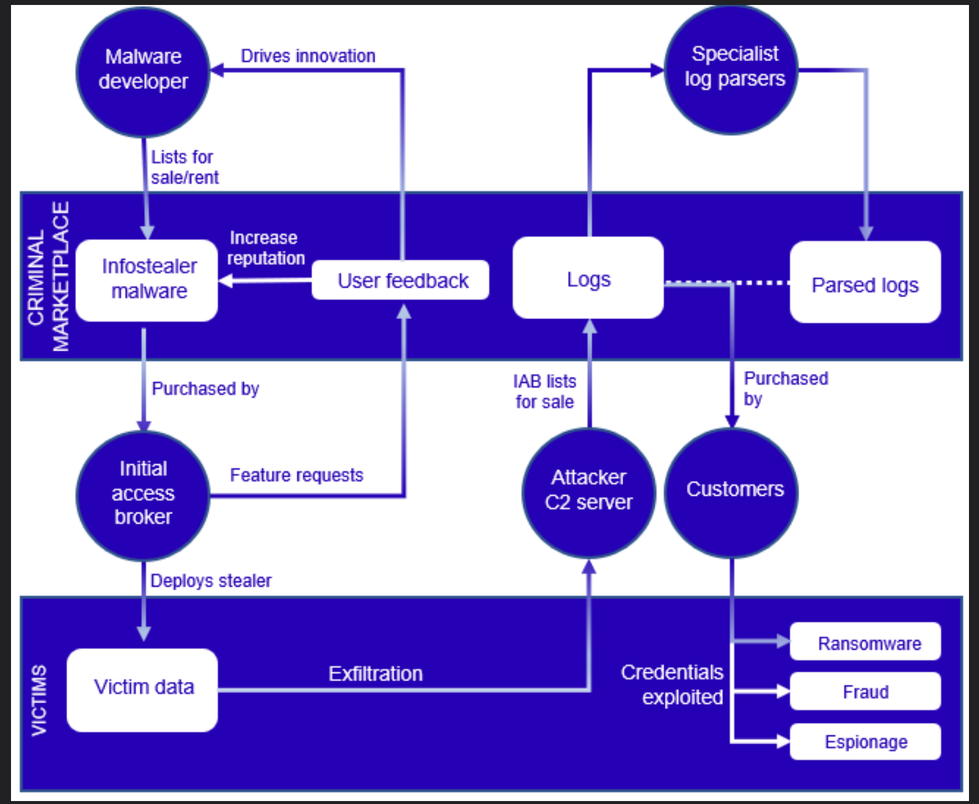


%localappdata%\Google\Chrome\User Data\Default\Login Data

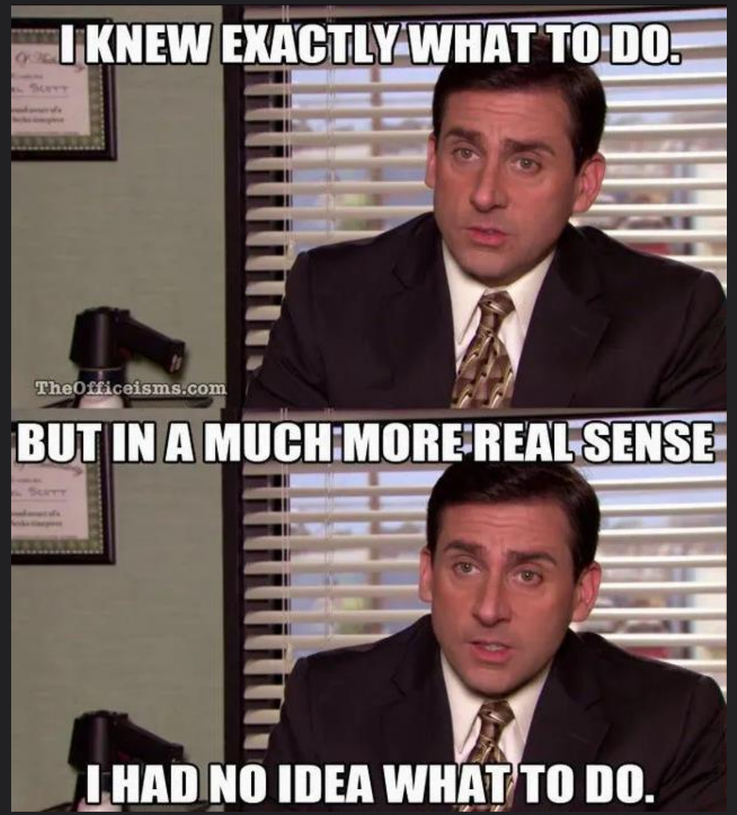
4) MONETIZAÇÃO


XFiles
Sell Selling Best DBS/DUMPS/MAILPASS - NOT CHEAP - UHQ.
RAGING COMBOS - THE OG IS BACK! THE BEST DATA IS BACK! EVERYTHING IN STOCK EXCEPT PP/FA - SHOPPING DATA - F
IN STOCK TG: https://t.me/TheBolRag CHANNEL: new old termed https://t.me/ragingstuff NOT CHEAP....
ragingcow1 · Thread · 35 minutes ago · best cheap not selling uhq · Replies: 0 · Forum: Emails / Database
Sell Crypto AP 447kk MailPass (UPDATE September 2025) 550$
СКИДКА 50% ДО 15:00
prpuservice · Post #22 · 41 minutes ago · Forum: Emails / Database
Sell GetCloud - URL:LOG:PASS Cloud with HQ / GetCloud - URL:LOG:PASS Cloud с высоким качеством!
RU: https://prnt.sc/a1gJl-dEkSFc - 03.10.2025 - +1.500.000 Строк добавлено (Большое обновление), только чистые/уни
количество строк: ~2.5kkk+ Цена доступа: 99$/мес. Для покупки доступа - @Getpaid333 ========= ENG...
Getpaid · Post #32 · Today at 10:50 AM · Forum: Emails / Database
Sell Sell DE /// web.de gmx.de Privat/Valid
Can you add me on tg as a contact so i can dm you. @SarahAlkatrez
kairocc · Post #2 · Today at 6:20 AM · Forum: Emails / Database
Sell 1kk coinmarketcap USA
VM 1.000.000 lines coinmarketcap (crypto) mail:pass USA 3k$ TG: @ DOZKEYY tox/jabber in PM
doZKey · Thread · Yesterday at 9:46 PM · 1kk coinmarketcap crypto usa · Replies: 0 · Forum: Emails / Database
Sell Продам дамп китайского обменника
*** Hidden text: You do not have sufficient rights to view the hidden text. Visit the forum thread! ***
PeaceDose · Thread · Yesterday at 8:04 PM · дамп продам продам дамп · Replies: 0 · Forum: Emails / Database
Sell Selling high-quality databases
Hello, I will dm you on telegram.
kairocc · Post #2 · Yesterday at 4:23 PM · Forum: Emails / Database
Verified Продам email:pass Us
Свежее Shop пополнение от 02.10.25 Shop1 80% Eu (email:pass 1kk - 210$) 20k test - https://www.sendspace.com/file/q8t56e Shop2 80% Us (email:pass 1kk - 200$) 20k test - https://www.ser


Browse
Activity
Services
Search...
Forums
Guidelines
Staff
Online Users
Search
Home › Commerce › Buying/Selling › [Spam] - mailings, databases, responses, mail-dumps, software › Looking for Brazil GOV Access / Ищу доступ к правительственным системам Бра...
Unread Content
Mark site read
HACK THESE WEBSITE
ОБМЕН от 2% ЧИСТКА от 3%
MAMURA EXCHANGE
Looking for Brazil GOV Access / Ищу доступ к правительственным системам Бразилии
By YTL, 1 minute ago in [Spam] - mailings, databases, responses, mail-dumps, software
Follow 1
Start new topic
Reply to this topic
YTL
byte
Paid registration
12
18 posts
Joined
11/21/24 (ID: 182324)
Activity
другое / other
Autogarant
2
Posted 1 minute ago
Hello.
I am looking for access to the Brazilian government, only those who have permission to consult vehicle license plates and driver's licenses, which are usually accessed by the police or the traffic department.
I buy credentials, but I also buy access to SSH.
The websites below are of great interest. If you have any API or credentials, please contact me.
1. seguranca.sinesp.gov.br
2. serpro.gov.br
Budgets start at U$1K.
--
Здравствуйте.
Я ищу доступ к бразильскому правительству, только те, кто имеет разрешение на просмотр номерных знаков автомобилей, водительских прав, как правило, имеют доступ к полиции или департаменту транспорта.
Я покупаю учетные данные, но также покупаю доступ к SSH.
Нижеуказанные сайты представляют большой интерес, если у вас есть API или учетные данные, свяжитесь с нами.



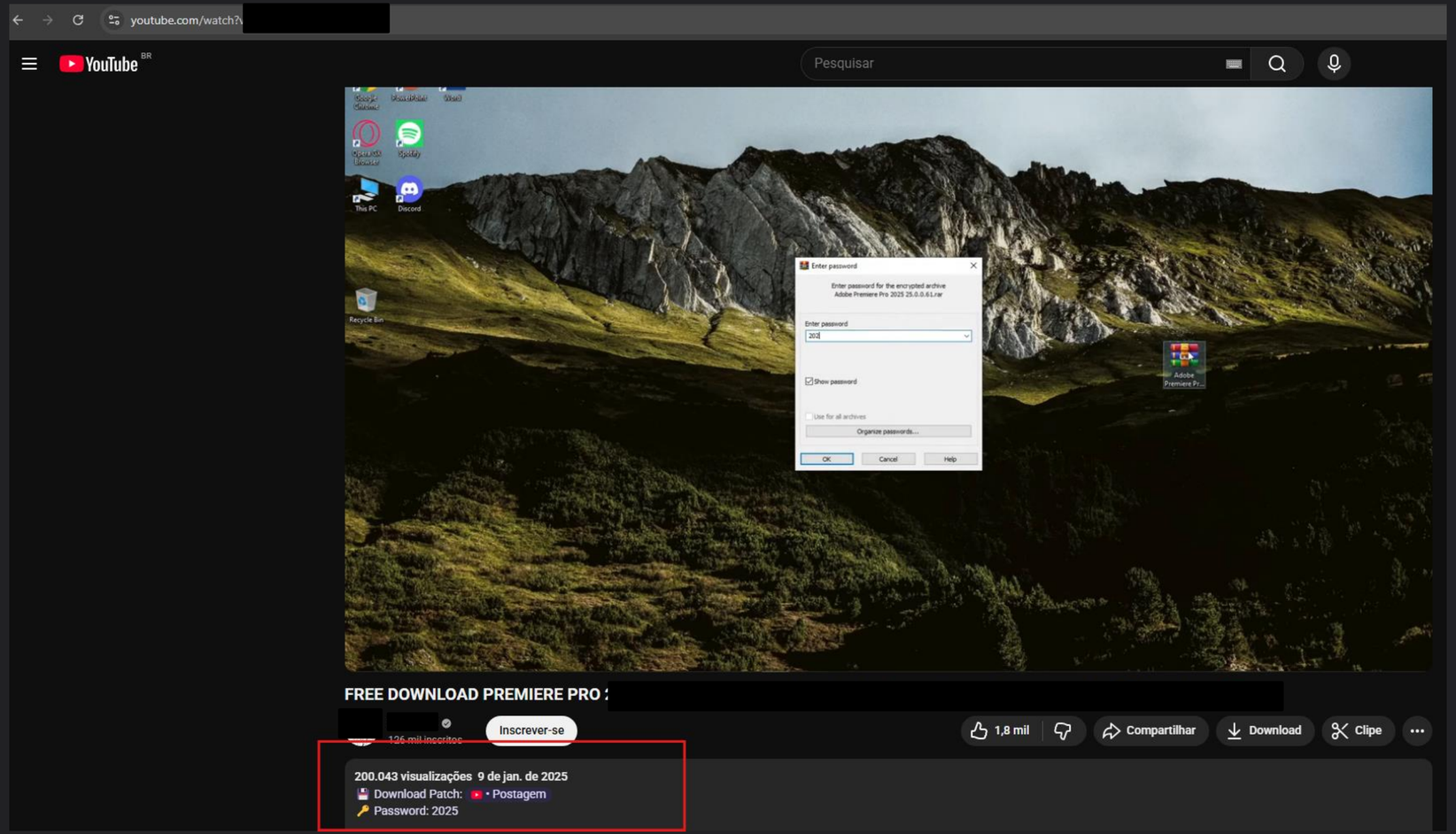
https://www.secureworks.com/research/the-growing-threat-from-infostealers

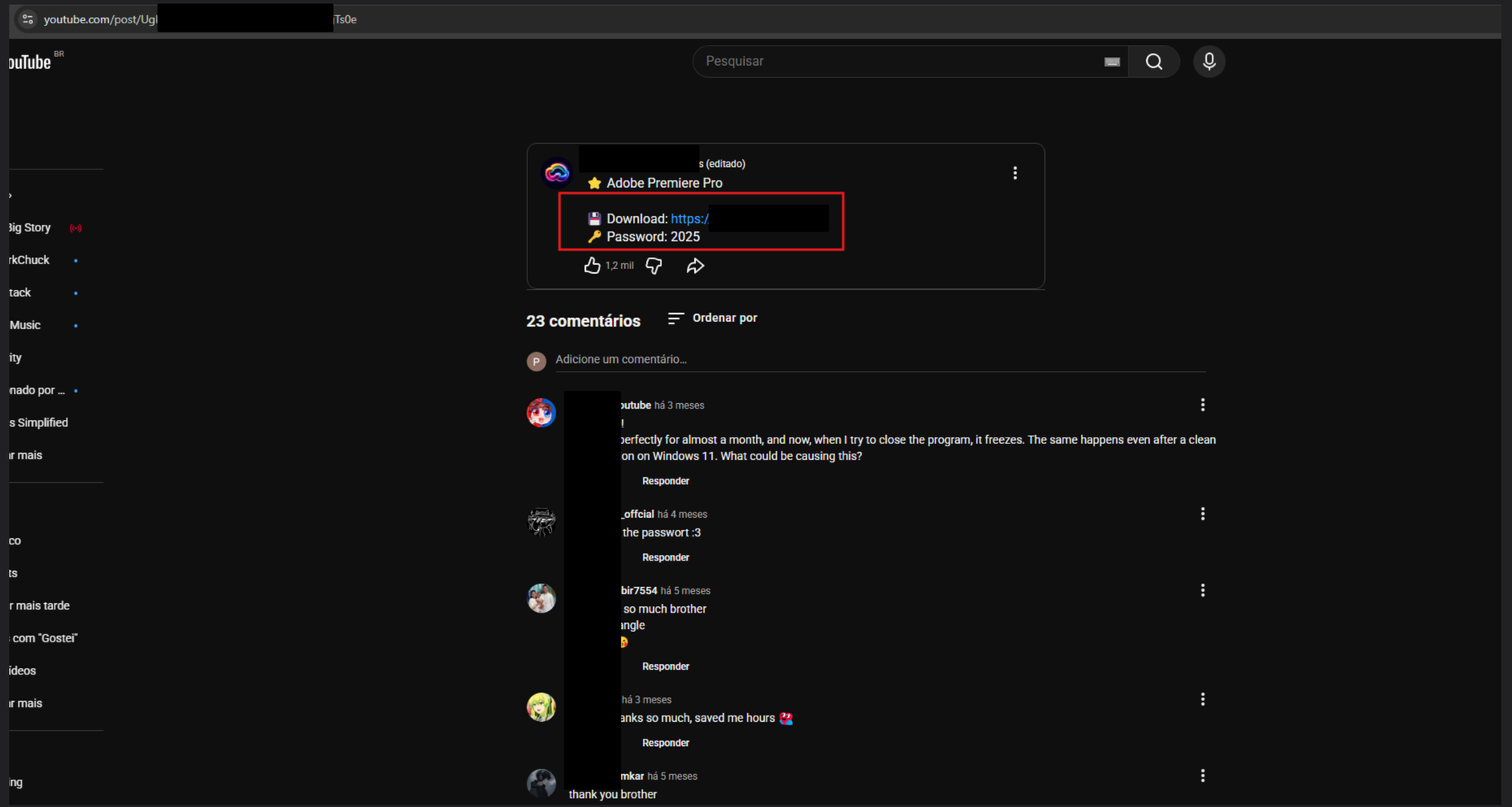

I KNEW EXACTLY WHAT TO DO.
TheOfficeisms.com
BUT IN A MUCH MORE REAL SENSE
I HAD NO IDEA WHAT TO DO.

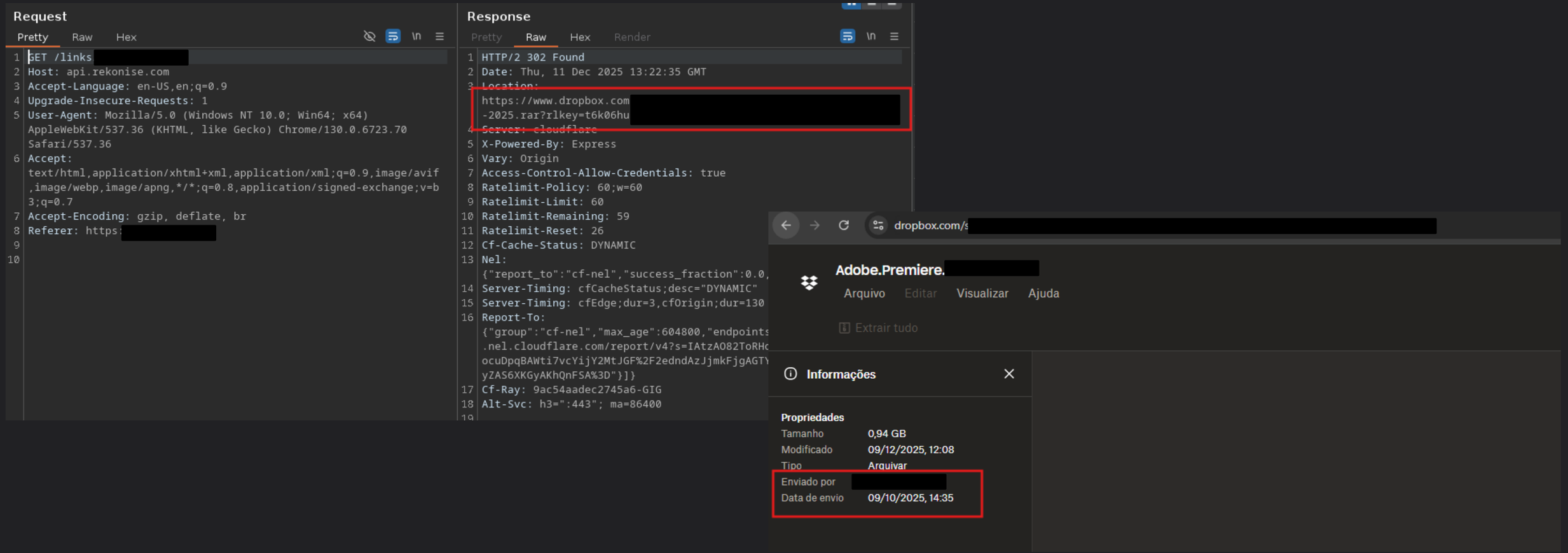
70% dos dispositivos infectados são pessoais.

Checkpoint Cyber security Report 2025

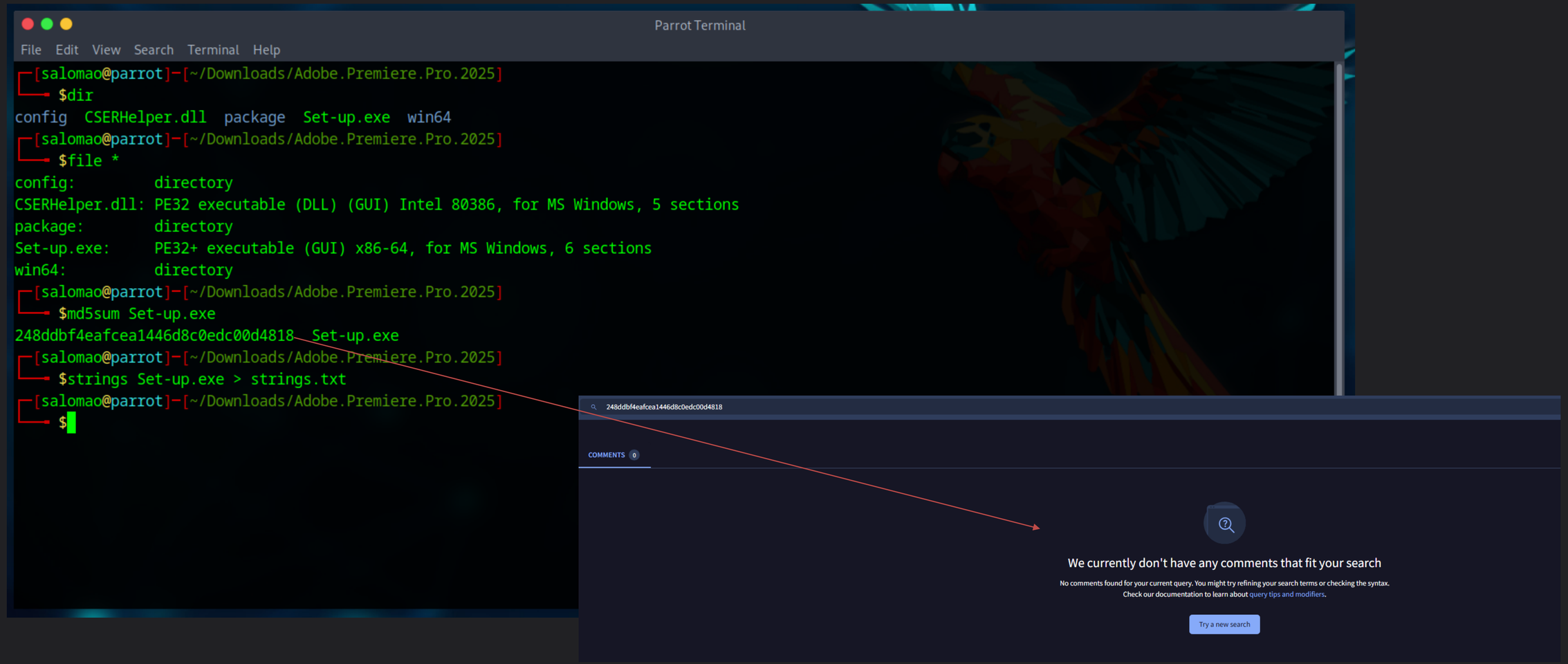
LIDANDO COM INCIDENTES

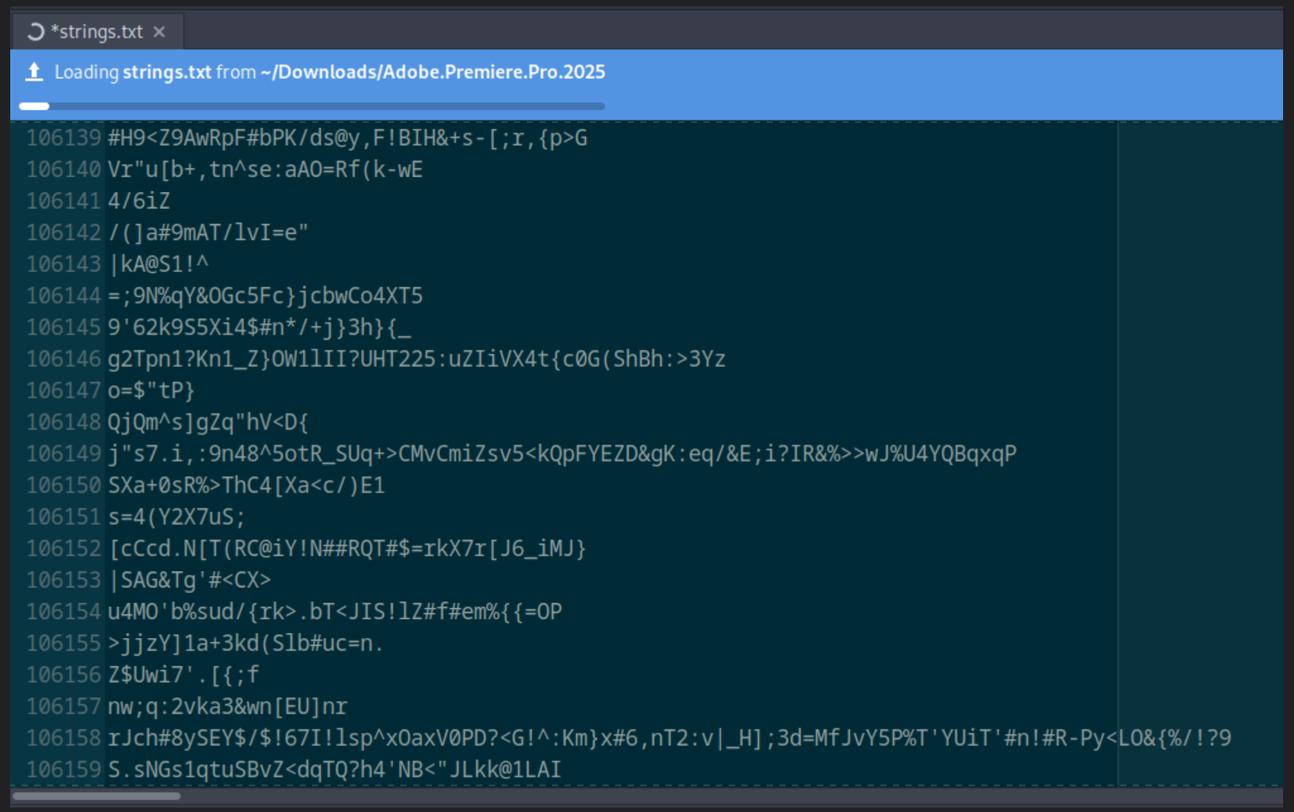

youtube.com/watch?v=[redacted]
YouTube BR
Pesquisar
Enter password
Enter password for the encrypted archive
Adobe Premiere Pro 2025 25.0.0.61.rar
Enter password
202
Show password
Use for all archives
Organize passwords...
OK
Cancel
Help
Recycle Bin
This PC
Discord
Spotify
Adobe Premiere Pr...
FREE DOWNLOAD PREMIERE PRO 2[redacted]
[redacted]
126 mil inscritos
Inscrever-se
1,8 mil
Compartilhar
Download
Clipe
200.043 visualizações 9 de jan. de 2025
Download Patch: • Postagem
Password: 2025

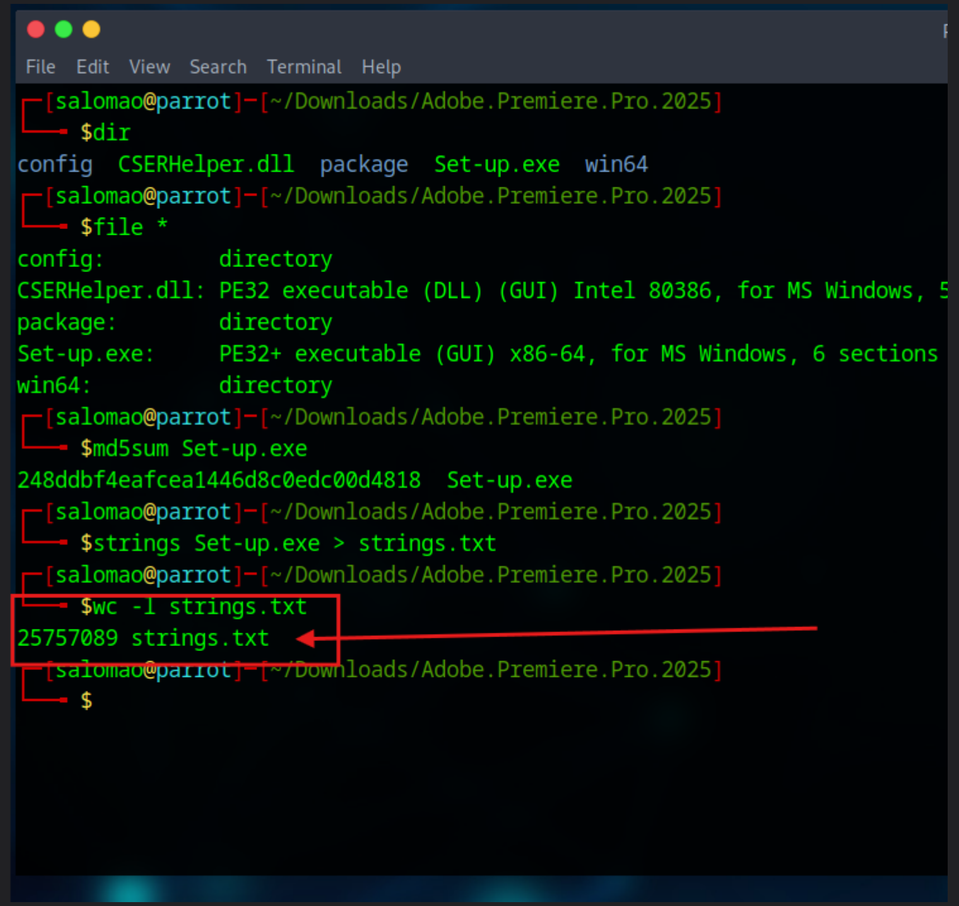

youtube.com/post/Ugl [redacted] Ts0e
Pesquisar
[redacted] s (editado)
⭐ Adobe Premiere Pro
💾 Download: https:/ [redacted]
🔑 Password: 2025
1,2 mil
23 comentários
Ordenar por
Adicione um comentário...
[redacted] utube há 3 meses
! perfectly for almost a month, and now, when I try to close the program, it freezes. The same happens even after a clean on on Windows 11. What could be causing this?
Responder
_offcial há 4 meses
the passwort :3
Responder
bir7554 há 5 meses
so much brother
ngle
Responder
há 3 meses
anks so much, saved me hours
Responder
mkar há 5 meses
thank you brother

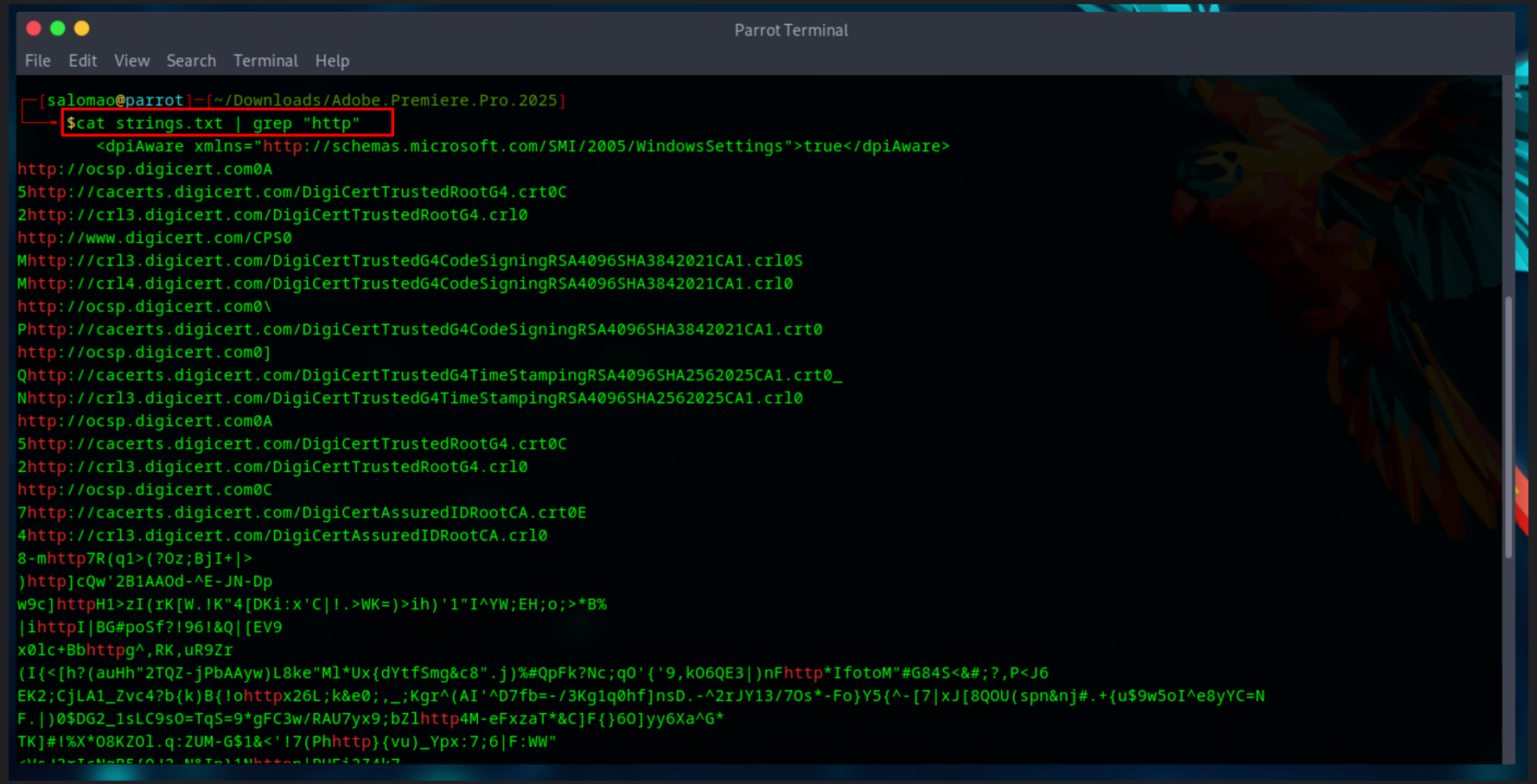


O vídeo do youtube é antigo, porém o binário é atual

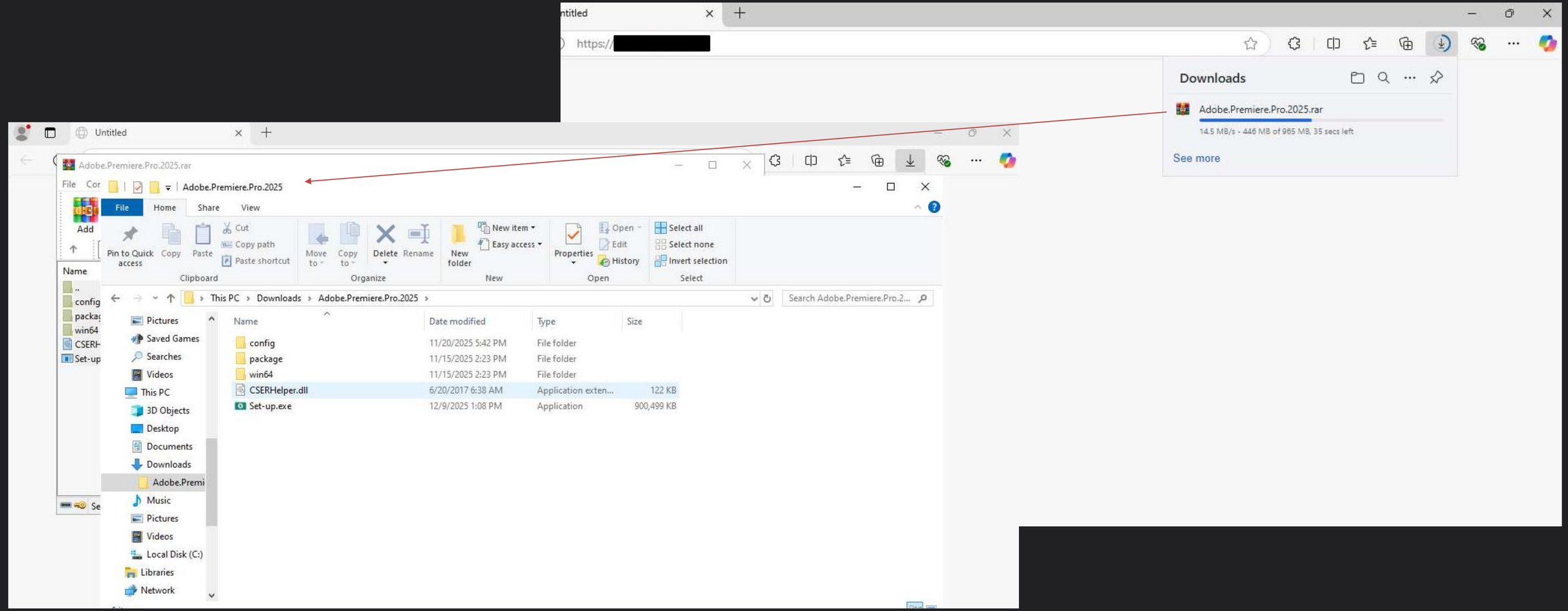

Parrot Terminal
File Edit View Search Terminal Help
[salomao@parrot]-[~/Downloads/Adobe.Premiere.Pro.2025]
$dir
config CSERHelper.dll package Set-up.exe win64
[salomao@parrot]-[~/Downloads/Adobe.Premiere.Pro.2025]
$file *
config: directory
CSERHelper.dll: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, 5 sections
package: directory
Set-up.exe: PE32+ executable (GUI) x86-64, for MS Windows, 6 sections
win64: directory
[salomao@parrot]-[~/Downloads/Adobe.Premiere.Pro.2025]
$md5sum Set-up.exe
248ddbf4eafcea1446d8c0edc00d4818 Set-up.exe
[salomao@parrot]-[~/Downloads/Adobe.Premiere.Pro.2025]
$strings Set-up.exe > strings.txt
[salomao@parrot]-[~/Downloads/Adobe.Premiere.Pro.2025]
$
248ddbf4eafcea1446d8c0edc00d4818
COMMENTS 0
We currently don't have any comments that fit your search
No comments found for your current query. You might try refining your search terms or checking the syntax.
Check our documentation to learn about query tips and modifiers.
Try a new search

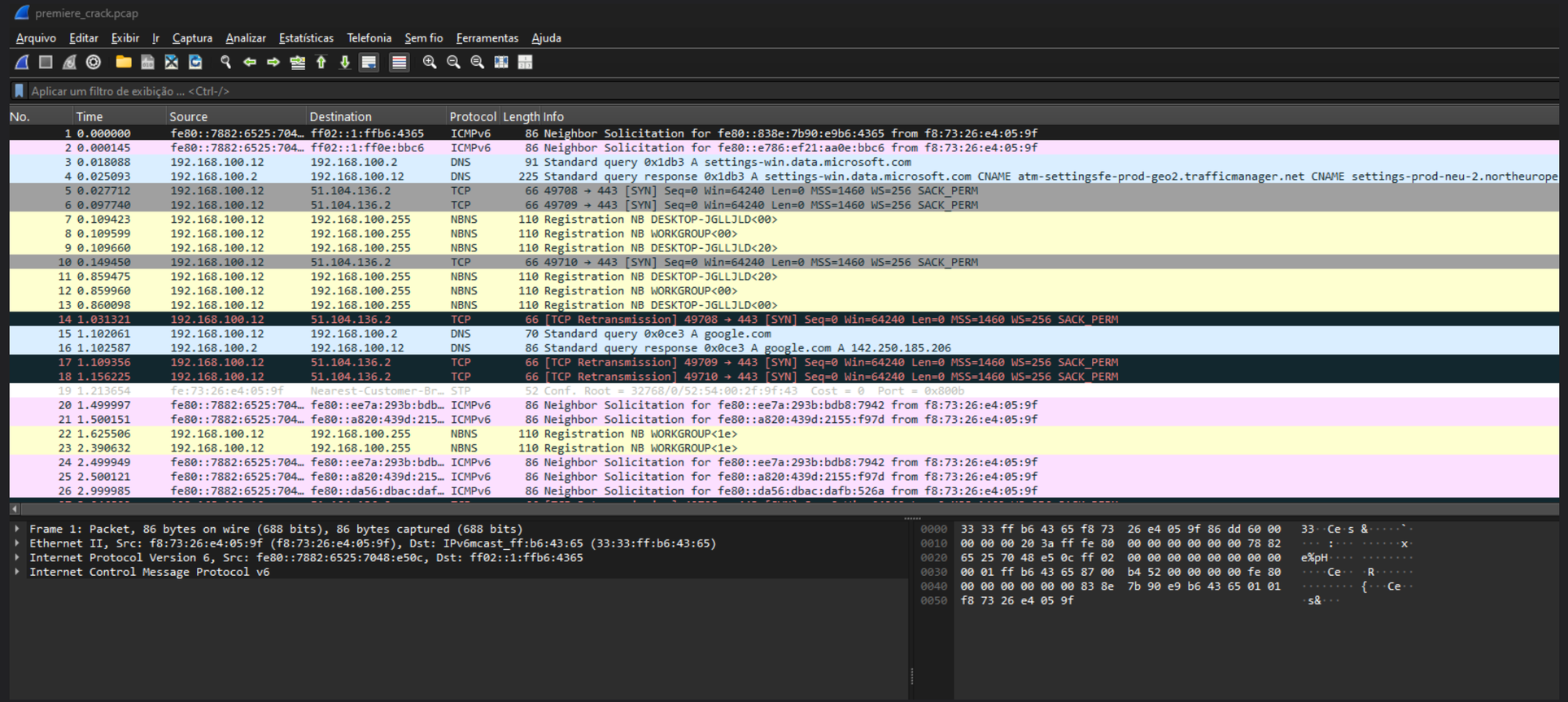

*strings.txt
Loading strings.txt from ~/Downloads/Adobe.Premiere.Pro.2025
106139 #H9<Z9AwRpF#bPK/ds@y,F!BIH&+s-[;r,{p>G
106140 Vr"u[b+,tn^se:aAO=Rf(k-wE
106141 4/6iZ
106142 /(]a#9mAT/lvI=e"
106143 |kA@S1!^
106144 =;9N%qY&OGc5Fc}jcbwCo4XT5
106145 9'62k9S5Xi4$#n*/+j}3h}{_
106146 g2Tpn1?Kn1_Z}OW1lII?UHT225:uZIiVX4t{c0G(ShBh:>3Yz
106147 o=$"tP}
106148 QjQm^s]gZq"hV<D{
106149 j"s7.i,:9n48^5otR_SUq+>CMvCmiZsv5<kQpFYEZD&gK:eq/&E;i?IR&%>>wJ%U4YQBqxqP
106150 SXa+0sR%>ThC4[Xa<c/)E1
106151 s=4(Y2X7uS;
106152 [cCcd.N[T(RC@iY!N##RQT#$=rkX7r[J6_iMJ}
106153 |SAG&Tg'#<CX>
106154 u4MO'b%sud/{rk>.bT<JIS!lZ#f#em%{{=OP
106155 >jjzY]1a+3kd(Slb#uc=n.
106156 Z$Uwi7'.[{;f
106157 nw;q:2vka3&wn[EU]nr
106158 rJch#8ySEY$/$!67I!lsp^xOaxV0PD?<G!^:Km}x#6,nT2:v|_H];3d=MfJvY5P%T'YUiT'#n!#R-Py<LO&{%/!?9
106159 S.sNGs1qtuSBvZ<dqTQ?h4'NB<"JLkk@1LAI


File Edit View Search Terminal Help
[salomao@parrot]-[~/Downloads/Adobe.Premiere.Pro.2025]
$dir
config CSERHelper.dll package Set-up.exe win64
[salomao@parrot]-[~/Downloads/Adobe.Premiere.Pro.2025]
$file *
config: directory
CSERHelper.dll: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, 5
package: directory
Set-up.exe: PE32+ executable (GUI) x86-64, for MS Windows, 6 sections
win64: directory
[salomao@parrot]-[~/Downloads/Adobe.Premiere.Pro.2025]
$md5sum Set-up.exe
248ddbf4eafcea1446d8c0edc00d4818 Set-up.exe
[salomao@parrot]-[~/Downloads/Adobe.Premiere.Pro.2025]
$strings Set-up.exe > strings.txt
[salomao@parrot]-[~/Downloads/Adobe.Premiere.Pro.2025]
$wc -l strings.txt
25757089 strings.txt
[salomao@parrot]-[~/Downloads/Adobe.Premiere.Pro.2025]
$

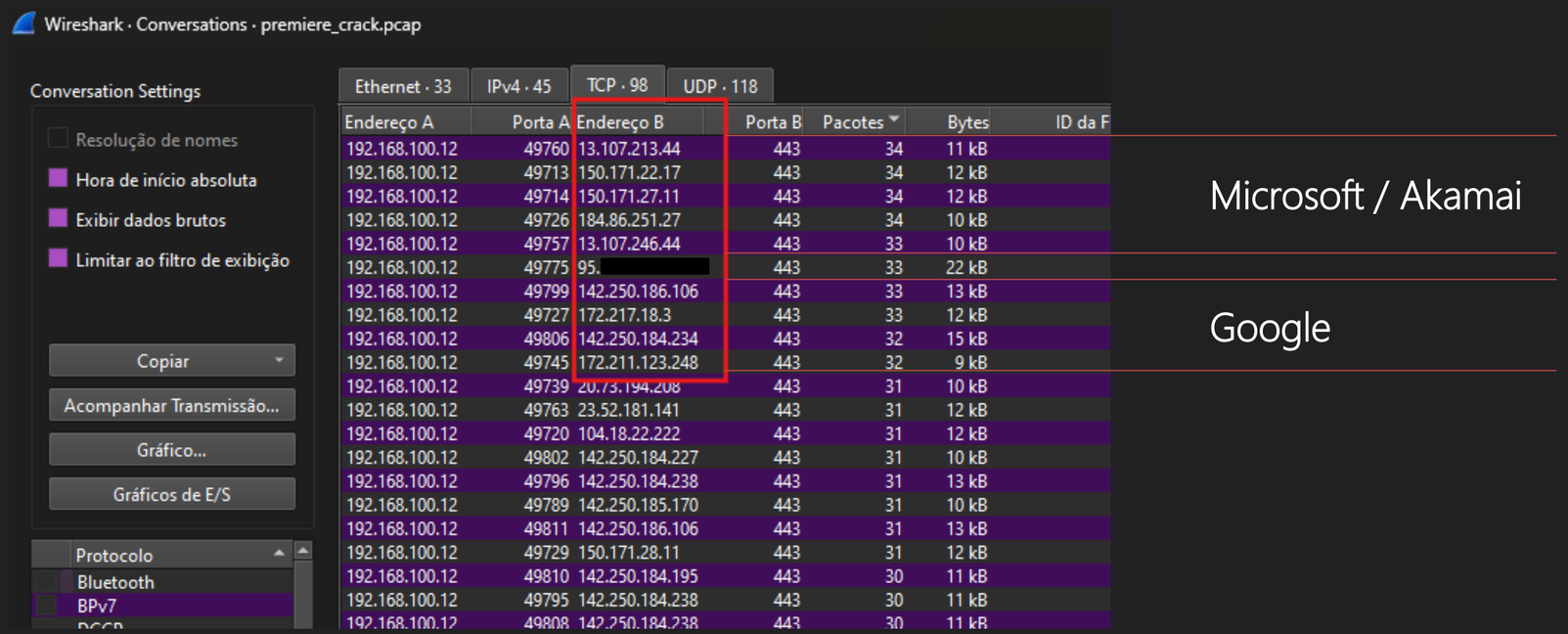

Parrot Terminal
File Edit View Search Terminal Help
[salomao@parrot]-[~/Downloads/Adobe.Premiere.Pro.2025]
$cat strings.txt | grep "http"
<dpiAware xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
http://ocsp.digicert.com0A
5http://cacerts.digicert.com/DigiCertTrustedRootG4.crt0C
2http://crl3.digicert.com/DigiCertTrustedRootG4.crl0
http://www.digicert.com/CPS0
Mhttp://crl3.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA3842021CA1.crl0S
Mhttp://crl4.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA3842021CA1.crl0
http://ocsp.digicert.com0\
Phttp://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA3842021CA1.crt0
http://ocsp.digicert.com0]
Qhttp://cacerts.digicert.com/DigiCertTrustedG4TimeStampingRSA4096SHA2562025CA1.crt0_
Nhttp://crl3.digicert.com/DigiCertTrustedG4TimeStampingRSA4096SHA2562025CA1.crl0
http://ocsp.digicert.com0A
5http://cacerts.digicert.com/DigiCertTrustedRootG4.crt0C
2http://crl3.digicert.com/DigiCertTrustedRootG4.crl0
http://ocsp.digicert.com0C
7http://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt0E
4http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl0
8-mhttp7R(q1>(?Oz;BjI+|>
)http]cQw'2B1AAOd-^E-JN-Dp
w9c]httpH1>zI(rK[W.!K"4[DKi:x'C|!.>WK=)>ih)'1"I^YW;EH;o;>*B%
|ihttpI|BG#poSf?!96!&Q|[EV9
x0lc+Bbhttpg^,RK,uR9Zr
(I{<[h?(auHh"2TQZ-jPbAAyw)L8ke"Ml*Ux{dYtfSmg&c8".j)%#QpFk?Nc;qO'{'9,kO6QE3|)nFhttp*IfotoM"#G84S<&#;?,P<J6
EK2;CjLA1_Zvc4?b{k)B{!ohttpx26L;k&e0;,_;Kgr^(AI'^D7fb=-/3Kg1q0hf]nsD.-^2rJY13/7Os*-Fo}Y5{^-[7|xJ[8QOU(spn&nj#.+{u$9w5oI^e8yYC=N
F.|)0$DG2_1sLC9sO=TqS=9*gFC3w/RAU7yx9;bZlhttp4M-eFxzaT*&C]F{}6O]yy6Xa^G*
TK]#!%X*O8KZOl.q:ZUM-G$1&<'!7(Phhttp}{vu)_Ypx:7;6|F:WW"

Mesmo extraindo mais de 25 milhões de linhas de caracteres do binário, nenhuma informação útil surgiu. Isso é exatamente o que crypters fazem, ou seja ocultam completamente C2, payload, strings e configurações. Uma forma direta de obter o conteúdo real é executando o malware em ambiente controlado e interceptando o payload. A identificação do C2, por sua vez, pode ser feita analisando as comunicações de rede.

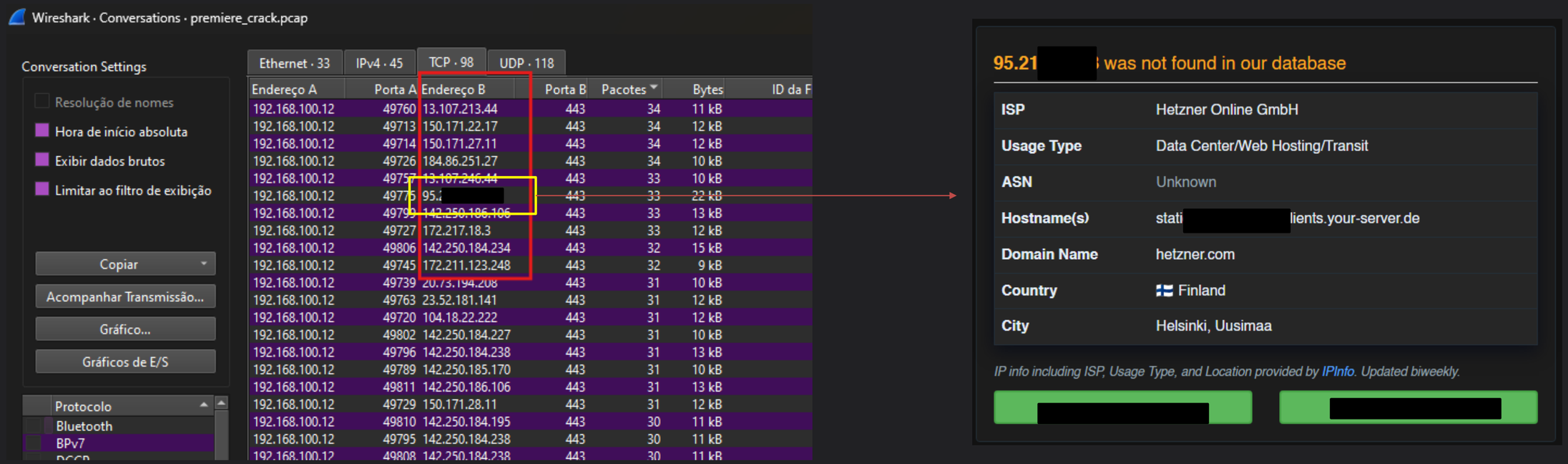

Untitled
https://[redacted]
Downloads
Adobe.Premiere.Pro.2025.rar
14.5 MB/s - 446 MB of 965 MB, 35 secs left
See more
Adobe.Premiere.Pro.2025.rar
Adobe.Premiere.Pro.2025
File
Home
Share
View
Add
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › Downloads › Adobe.Premiere.Pro.2025 ›
Search Adobe.Premiere.Pro.2...
Pictures
Saved Games
Searches
Videos
This PC
3D Objects
Desktop
Documents
Downloads
Adobe.Premi
Music
Pictures
Videos
Local Disk (C:)
Libraries
Network
Name
Date modified
Type
Size
config
11/20/2025 5:42 PM
File folder
package
11/15/2025 2:23 PM
File folder
win64
11/15/2025 2:23 PM
File folder
CSERHelper.dll
6/20/2017 6:38 AM
Application exten...
122 KB
Set-up.exe
12/9/2025 1:08 PM
Application
900,499 KB

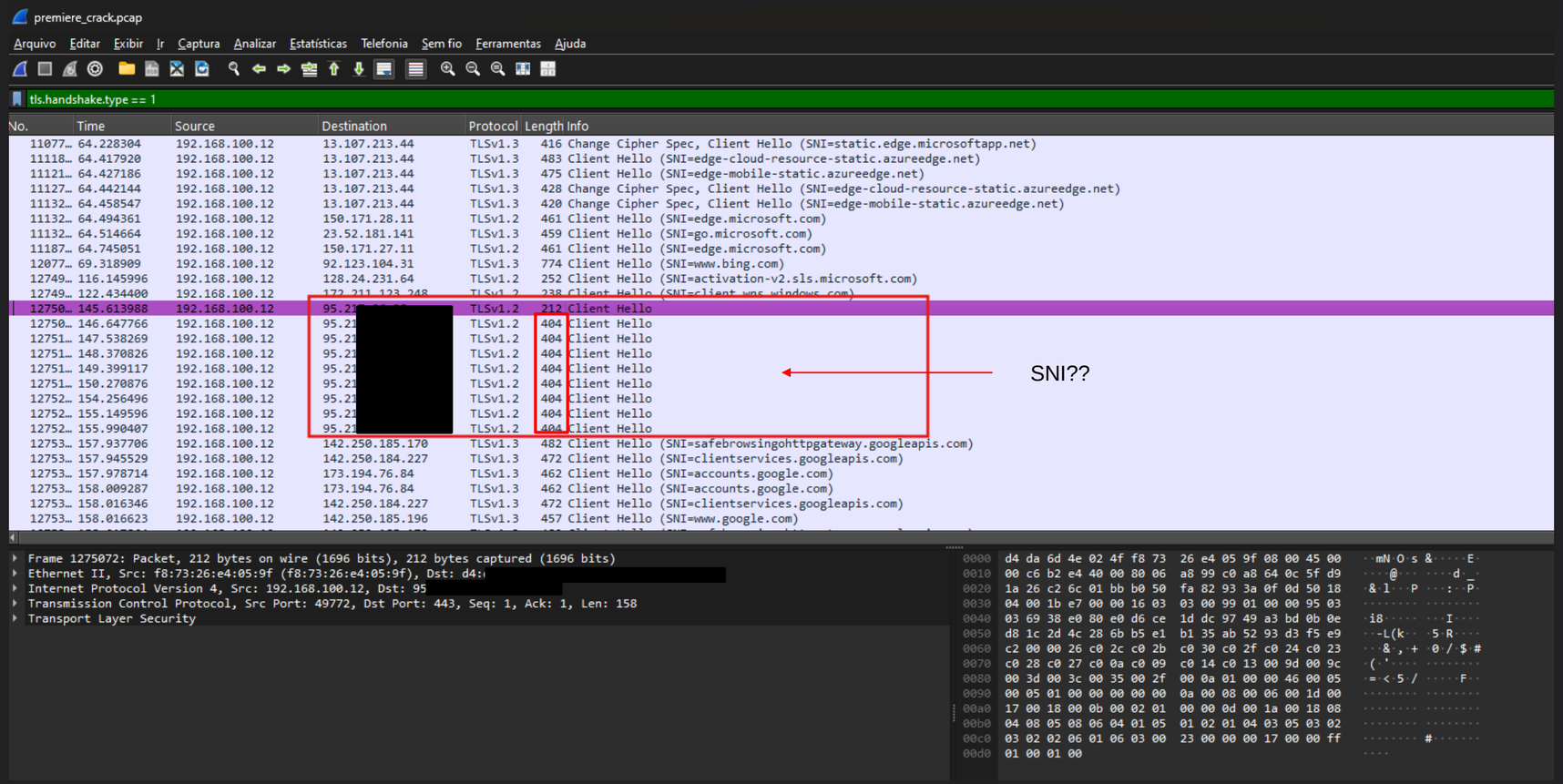


Wireshark capturou inúmeros pacotes

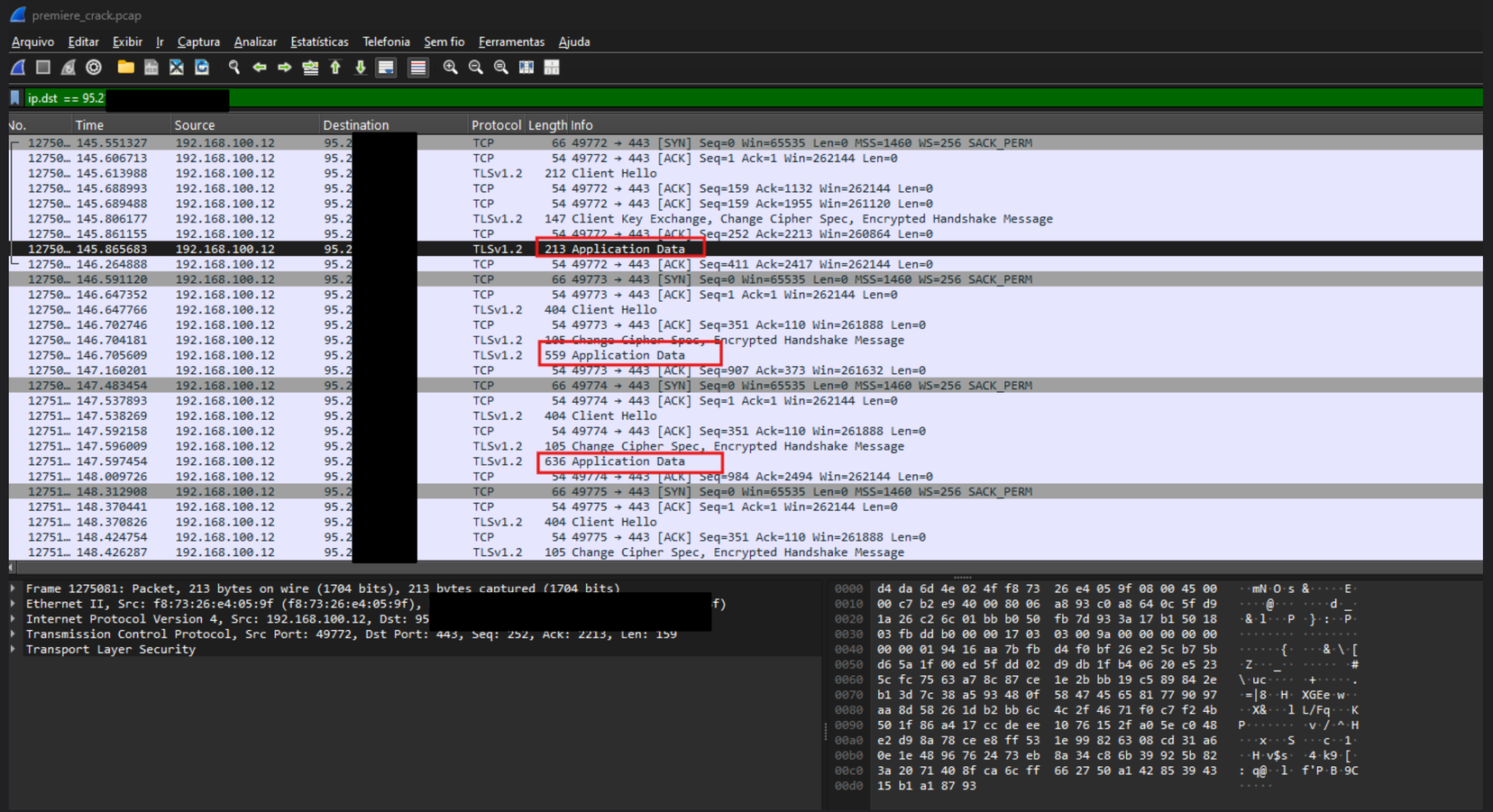


Os principais IPs pertencem a grandes empresas, com exceção a um: 95.[...]

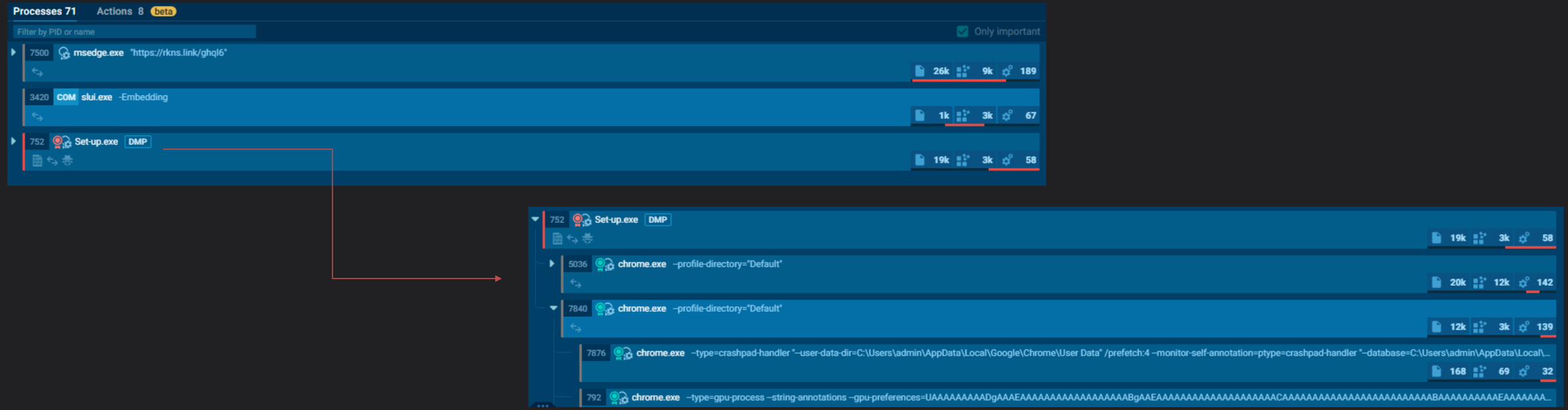

Wireshark · Conversations · premiere_crack.pcap
Conversation Settings
Resolução de nomes
Hora de início absoluta
Exibir dados brutos
Limitar ao filtro de exibição
Copiar
Acompanhar Transmissão...
Gráfico...
Gráficos de E/S
Protocolo
Bluetooth
BPv7
Ethernet · 33
IPv4 · 45
TCP · 98
UDP · 118
Endereço A Porta A Endereço B Porta B Pacotes Bytes ID da F
192.168.100.12 49760 13.107.213.44 443 34 11 kB
192.168.100.12 49713 150.171.22.17 443 34 12 kB
192.168.100.12 49714 150.171.27.11 443 34 12 kB
192.168.100.12 49726 184.86.251.27 443 34 10 kB
192.168.100.12 49757 13.107.246.44 443 33 10 kB
192.168.100.12 49776 95.[redacted] 443 33 22 kB
192.168.100.12 49799 142.250.186.106 443 33 13 kB
192.168.100.12 49727 172.217.18.3 443 33 12 kB
192.168.100.12 49806 142.250.184.234 443 32 15 kB
192.168.100.12 49745 172.211.123.248 443 32 9 kB
192.168.100.12 49739 20.73.194.208 443 31 10 kB
192.168.100.12 49763 23.52.181.141 443 31 12 kB
192.168.100.12 49720 104.18.22.222 443 31 12 kB
192.168.100.12 49802 142.250.184.227 443 31 10 kB
192.168.100.12 49796 142.250.184.238 443 31 13 kB
192.168.100.12 49789 142.250.185.170 443 31 10 kB
192.168.100.12 49811 142.250.186.106 443 31 13 kB
192.168.100.12 49729 150.171.28.11 443 31 12 kB
192.168.100.12 49810 142.250.184.195 443 30 11 kB
192.168.100.12 49795 142.250.184.238 443 30 11 kB
192.168.100.12 49808 142.250.184.238 443 30 11 kB
95.21[redacted] was not found in our database
ISP Hetzner Online GmbH
Usage Type Data Center/Web Hosting/Transit
ASN Unknown
Hostname(s) stati[redacted]lients.your-server.de
Domain Name hetzner.com
Country Finland
City Helsinki, Uusimaa
IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.



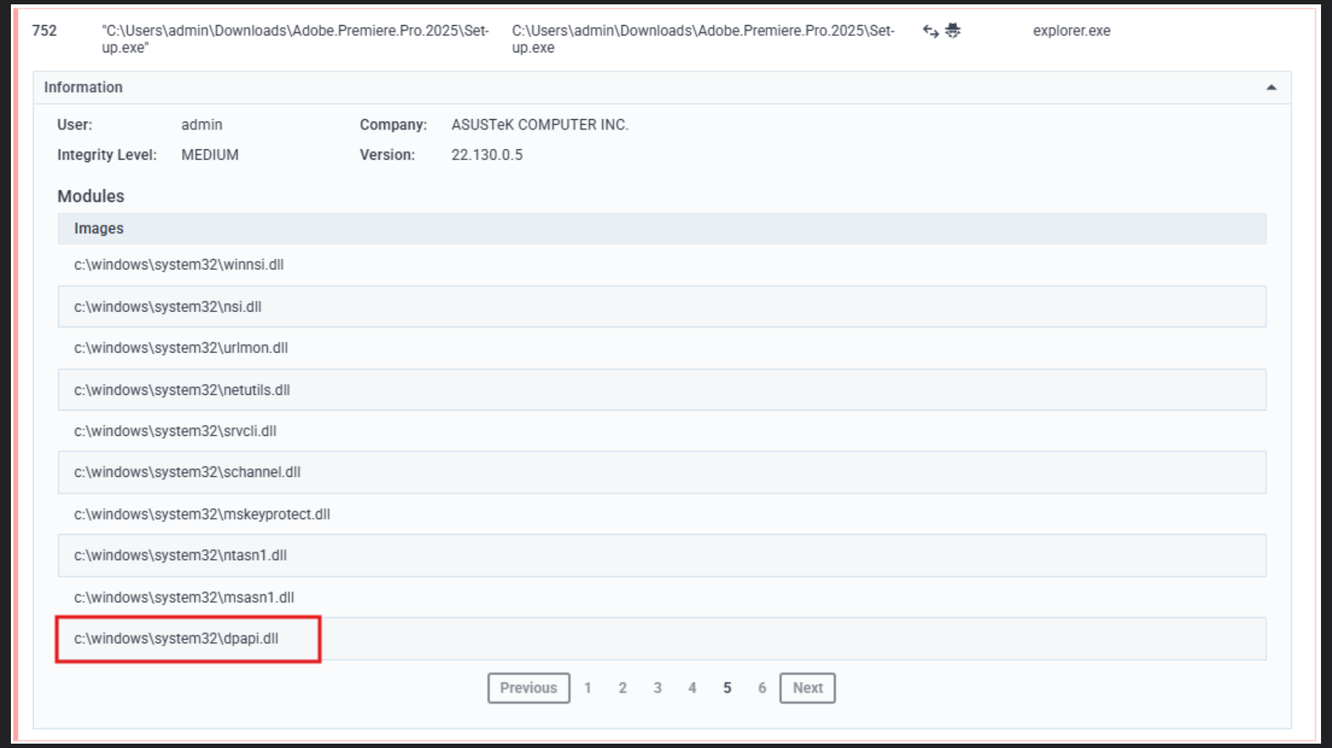
Verificando comunicações TLS sem SNI. Basicamente todo Client Hello legítimo possui a identificação do nome do host



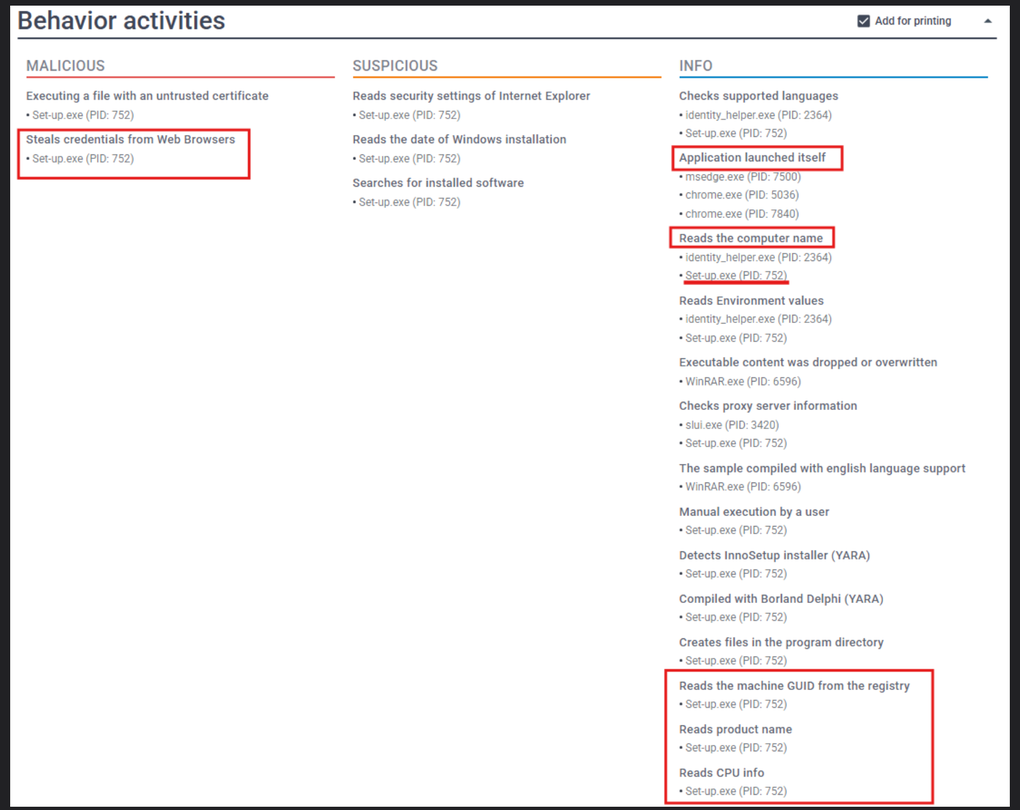
Comunicações constantes com o C2 para envio de dados



O arquivo malicioso foi baixado pelo EDGE (PID 7500). Ao executar o binário, o processo respectivo (PID 752) criou subprocessos do Chrome (PID 5036 e PID 7840)



Dentre as DLLs carregadas pelo processo, destaca-se a dpapi.dll



Análise comportamental confirma a execução de um infostealer

Regras do Suricata IPS identificaram que a comunicação HTTPS possui traços do stealer Vidar ou Stealc

11/95 security vendors flagged this IP address as malicious

Reanalyze More

95.[redacted]/15)

AS 24940 (Hetzner Online GmbH)

self-signed

FI

Last Analysis Date
1 day ago

DETECTION DETAILS RELATIONS COMMUNITY 4

Voting details (2)

NIXLovesXerneas 2 days ago	-1
JaffaCakes118 2 days ago	-11

Comments (2)

NIXLovesXerneas
2 days ago

Vidar C2 at 95.[redacted]
Geolocation: Helsinki, Uusimaa
Organization: Hetzner Online GmbH
ASN: AS24940
Country: FI

Confidence Level: 100%
IOC: https://threatfox.abuse.ch[redacted]

A identificação da infecção normalmente envolve o monitoramento de credenciais na deep/dark web e demais canais underground, bem como a análise de padrões de autenticação.

Importando Datasets

[2] ✓ 24s

```
1  base_path = '/content/drive/MyDrive/Hunt creds/'
2  autenticacoes = pd.read_excel(base_path + 'autenticacoes.xlsx')
3  breach = pd.read_excel(base_path + 'breach.xlsx')
4  sei_total = pd.read_excel(base_path + 'sei_total.xlsx')
5  print(autenticacoes.columns)
```

```
Index(['SISTEMA', 'MATR OPER', 'NOME OPER', 'IP ORIGEM', 'MENSAGEM',
       'ÓRGÃO EXERCÍCIO OPER', 'PCDF', 'DATA/HORA OPER'],
      dtype='object')
```

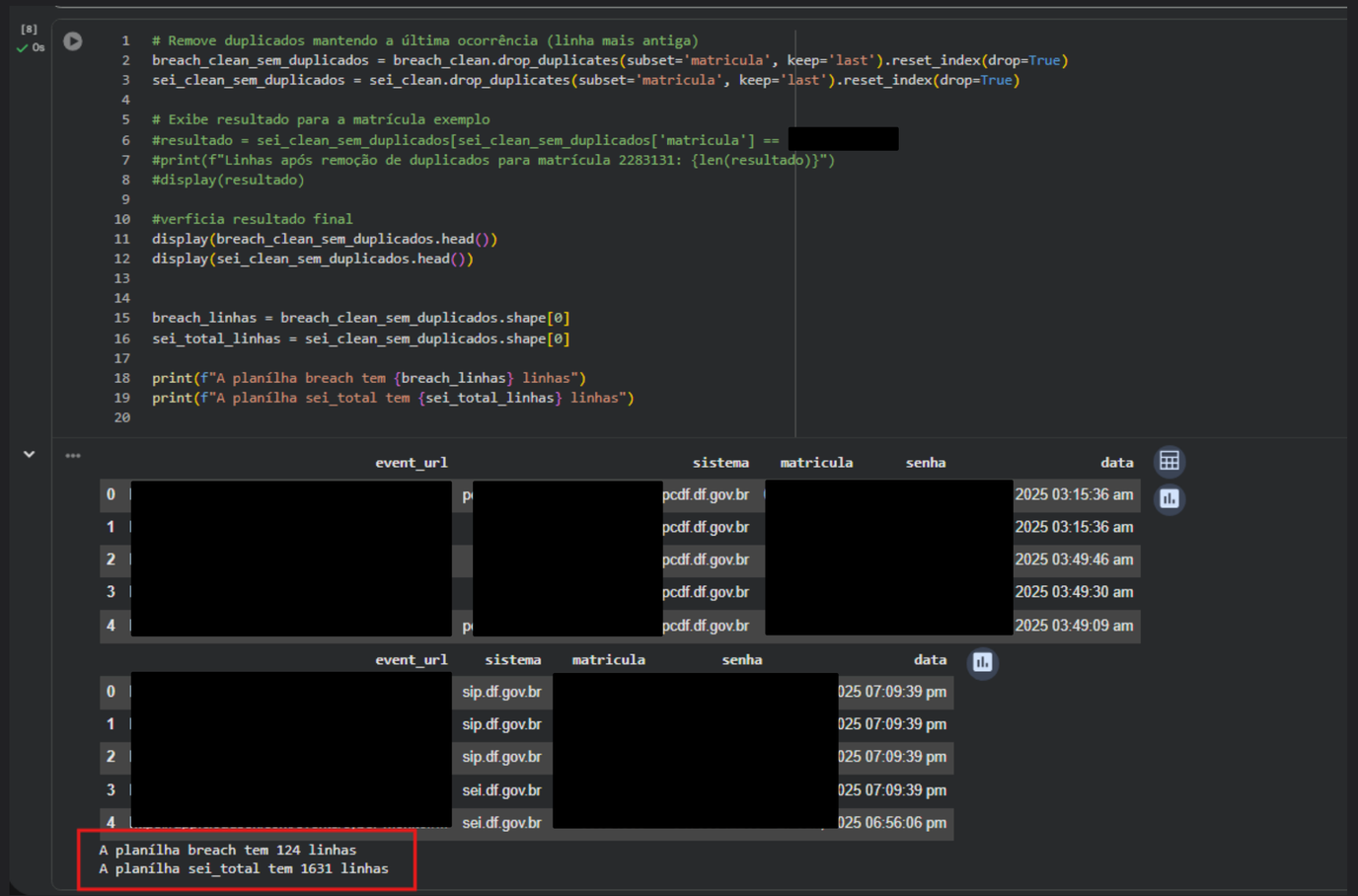
Conta linhas

[3] ✓ 0s

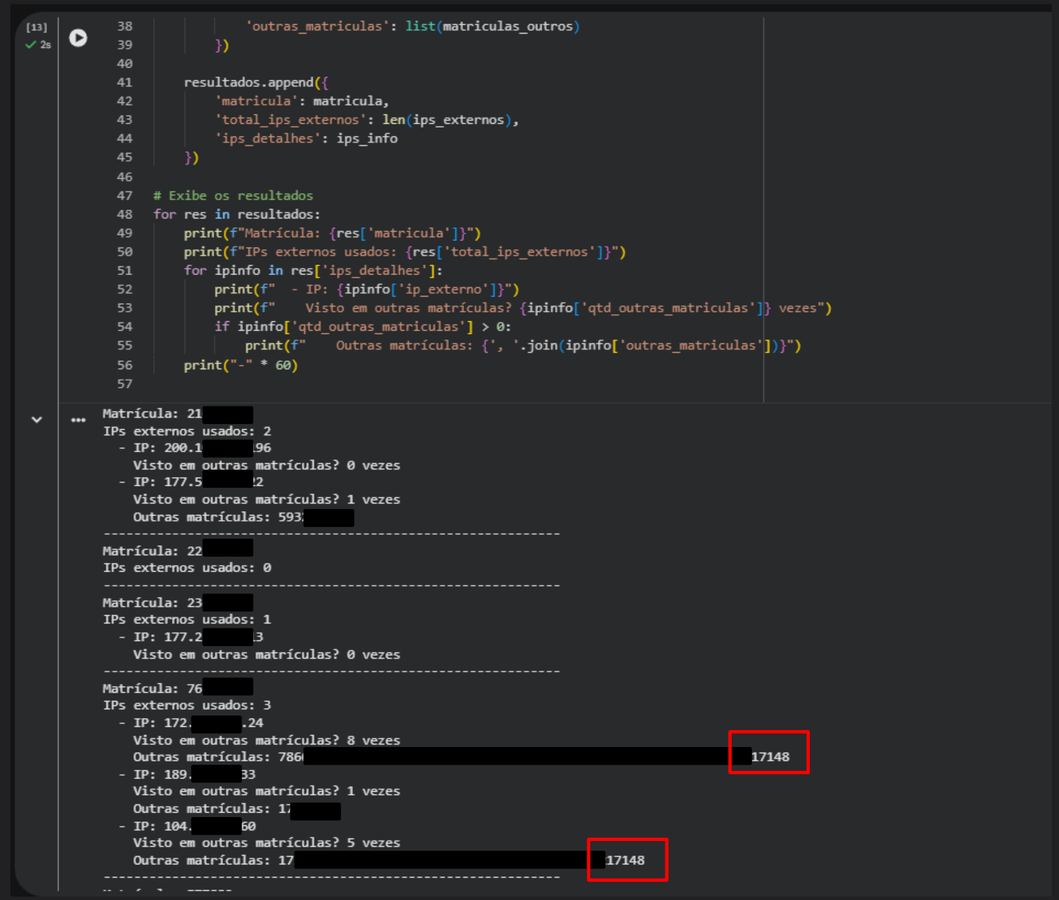
```
1  aut_linhas = autenticacoes.shape[0]
2  breach_linhas = breach.shape[0]
3  sei_total_linhas = sei_total.shape[0]
4
5  print(f"A planílha autenticacoes tem {aut_linhas} linhas")
6  print(f"A planílha breach tem {breach_linhas} linhas")
7  print(f"A planílha sei_total tem {sei_total_linhas} linhas")
```

```
A planílha autenticacoes tem 150002 linhas
A planílha breach tem 5478 linhas
A planílha sei_total tem 19220 linhas
```

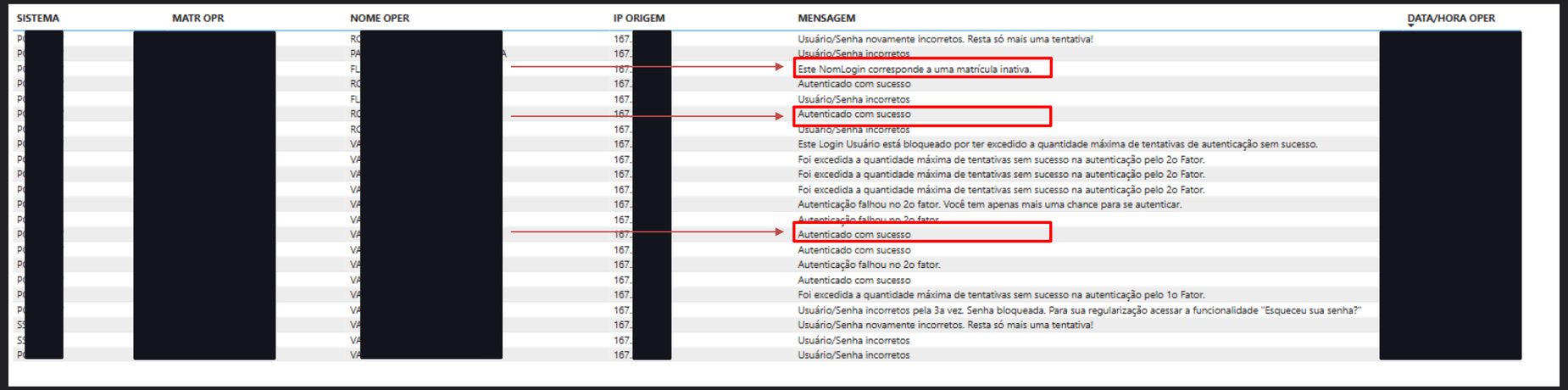
Dependendo da empresa, o recorte de menções na dark web pode ter milhares de linhas



A constante análise de eventos duplicados é essencial para redução de fadiga

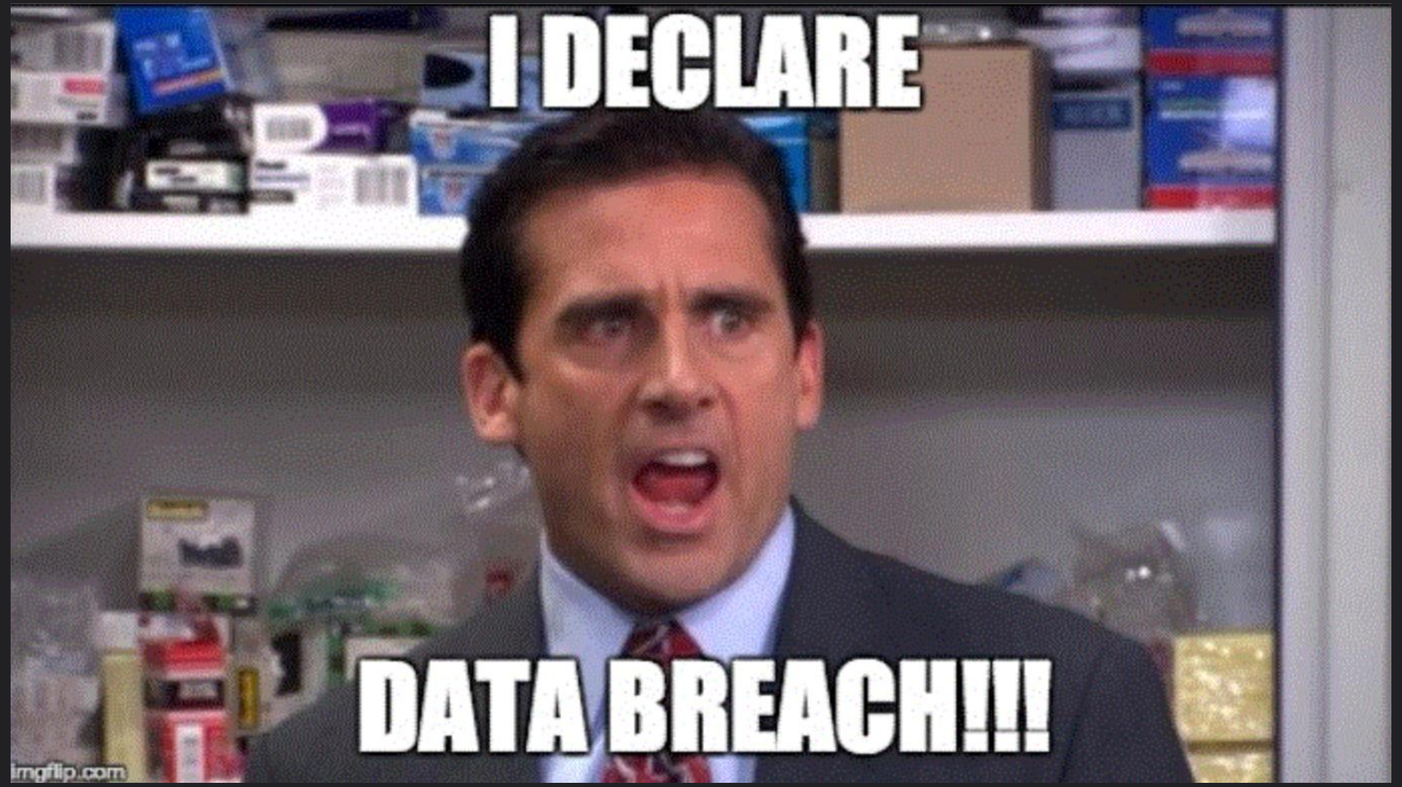


Usuários com autenticação partindo de IPs diversos merecem ser analisados



SISTEMA	MATR OPR	NOME OPER	IP ORIGEM	MENSAGEM	DATA/HORA OPER
P	[redacted]	R	167	Usuário/Senha novamente incorretos. Resta só mais uma tentativa!	[redacted]
P	[redacted]	P	167	Usuário/Senha incorretos	[redacted]
P	[redacted]	FL	167	Este NomLogin corresponde a uma matrícula inativa.	[redacted]
P	[redacted]	R	167	Autenticado com sucesso	[redacted]
P	[redacted]	FL	167	Usuário/Senha incorretos	[redacted]
P	[redacted]	R	167	Autenticado com sucesso	[redacted]
P	[redacted]	R	167	Usuário/Senha incorretos	[redacted]
P	[redacted]	VA	167	Este Login Usuário está bloqueado por ter excedido a quantidade máxima de tentativas de autenticação sem sucesso.	[redacted]
P	[redacted]	VA	167	Foi excedida a quantidade máxima de tentativas sem sucesso na autenticação pelo 2o Fator.	[redacted]
P	[redacted]	VA	167	Foi excedida a quantidade máxima de tentativas sem sucesso na autenticação pelo 2o Fator.	[redacted]
P	[redacted]	VA	167	Foi excedida a quantidade máxima de tentativas sem sucesso na autenticação pelo 2o Fator.	[redacted]
P	[redacted]	VA	167	Autenticação falhou no 2o fator. Você tem apenas mais uma chance para se autenticar.	[redacted]
P	[redacted]	VA	167	Autenticação falhou no 2o fator.	[redacted]
P	[redacted]	VA	167	Autenticado com sucesso	[redacted]
P	[redacted]	VA	167	Autenticado com sucesso	[redacted]
P	[redacted]	VA	167	Autenticação falhou no 2o fator.	[redacted]
P	[redacted]	VA	167	Autenticado com sucesso	[redacted]
P	[redacted]	VA	167	Foi excedida a quantidade máxima de tentativas sem sucesso na autenticação pelo 1o Fator.	[redacted]
P	[redacted]	VA	167	Usuário/Senha incorretos pela 3a vez. Senha bloqueada. Para sua regularização acessar a funcionalidade "Esqueceu sua senha?"	[redacted]
S	[redacted]	VA	167	Usuário/Senha novamente incorretos. Resta só mais uma tentativa!	[redacted]
S	[redacted]	VA	167	Usuário/Senha incorretos	[redacted]
P	[redacted]	VA	167	Usuário/Senha incorretos	[redacted]

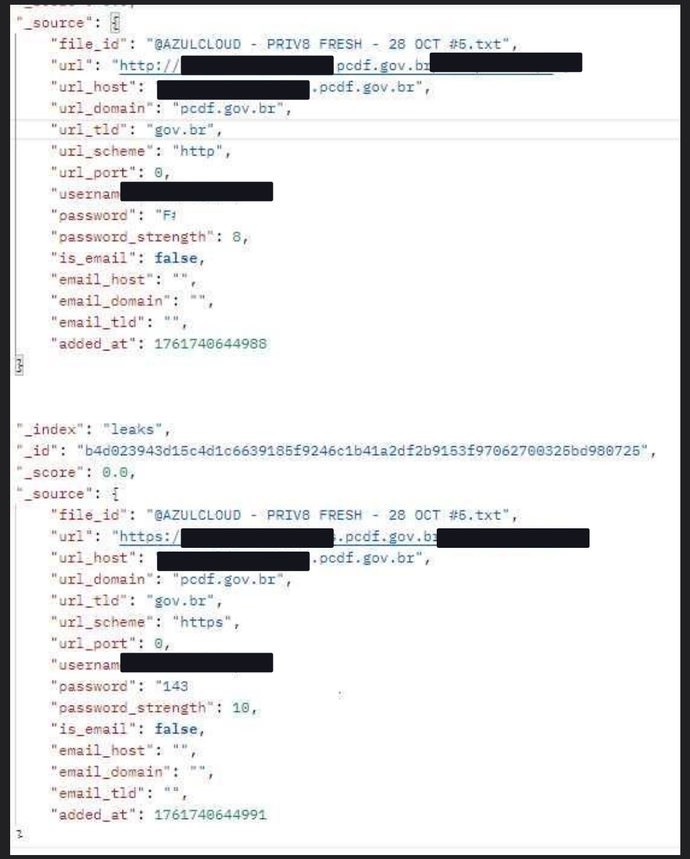
Mesmo IP de origem realizando autenticações em contas diversas em curto intervalo de tempo



É comum que o analista já pense em instaurar um incidente. Em seguida, parte imediatamente para isolamento de hosts e reset de senhas. Com o resultado do full scan, encerra o incidente encerra o incidente.

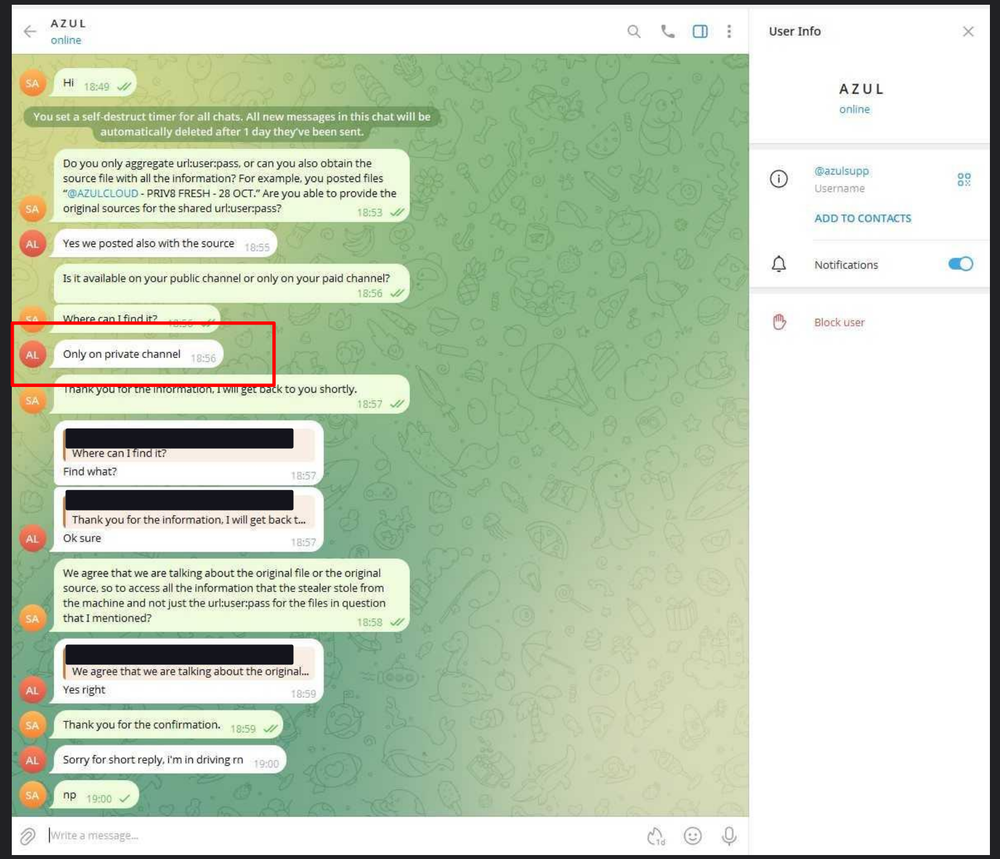
É importante analisar o contexto! Entender a origem do vazamento, se a instituição é um alvo de interesse e se há campanhas ativas voltadas para o mesmo setor. Rastrear o malware é o melhor caminho para confirmar a ausência de intrusão em rede corporativa.

A interação com o ator malicioso é importante, mas nem sempre levará a um resultado concreto.




```
"_source": {
    "file_id": "@AZULCLOUD - PRIV8 FRESH - 28 OCT #5.txt",
    "url": "http://[redacted]pcdf.gov.br[redacted]",
    "url_host": "[redacted].pcdf.gov.br",
    "url_domain": "pcdf.gov.br",
    "url_tld": "gov.br",
    "url_scheme": "http",
    "url_port": 0,
    "usernam[redacted]
    "password": "F[redacted]
    "password_strength": 8,
    "is_email": false,
    "email_host": "",
    "email_domain": "",
    "email_tld": "",
    "added_at": 1761740644988


"_index": "leaks",
"_id": "b4d023943d15c4d1c6639185f9246c1b41a2df2b9153f97062700325bd980725",
"_score": 0.0,
"_source": {
    "file_id": "@AZULCLOUD - PRIV8 FRESH - 28 OCT #5.txt",
    "url": "https:/[redacted].pcdf.gov.br[redacted]",
    "url_host": "[redacted].pcdf.gov.br",
    "url_domain": "pcdf.gov.br",
    "url_tld": "gov.br",
    "url_scheme": "https",
    "url_port": 0,
    "usernam[redacted]
    "password": "143
    "password_strength": 10,
    "is_email": false,
    "email_host": "",
    "email_domain": "",
    "email_tld": "",
    "added_at": 1761740644991
```

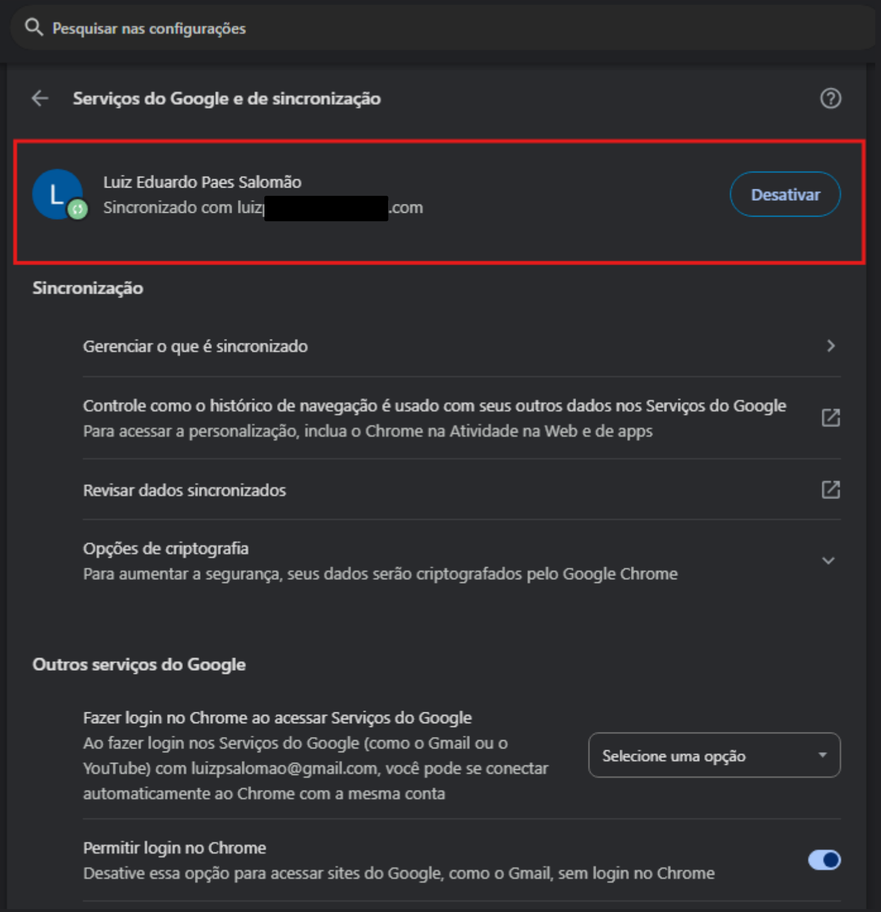



CHANNEL:t.me/+F61qGRd_ic1jZjAy ADMIN:t.me/Emirates_Cloud EMIRATES LINK:t.me/Emirates_Admin

Rhadamanthys Stealer

Install Date: 1[redacted]UTC
Traffic Name: @othertraff
HWID: 3S[redacted]
IP: 187.[redacted]
Country: BR
Time Zone: UTC-3
System Language: Portuguese
User Language: Portuguese
Keyboard Language: Portuguese
Processor: Intel(R) Core(TM) i5-9400F CPU @ 2.90GHz
Installed RAM: 24520 MB
OS: Windows 10 build 19045 (64 Bit)
Video card: NVIDIA GeForce GTX 1650
Display Resolution: 1920x1080
Computer Name: DESKTOP-21[redacted]
User Name: Usuario
Domain Name: WORKGROUP
MachineID: 569cb9c5-[redacted]
WallPaper Hash:

Se a maior parte das infecções ocorre em dispositivo pessoal, por que as empresas são afetadas?


Pesquisar nas configurações
Serviços do Google e de sincronização
Luiz Eduardo Paes Salomão
Sincronizado com luiz[redacted].com
Desativar
Sincronização
Gerenciar o que é sincronizado
Controle como o histórico de navegação é usado com seus outros dados nos Serviços do Google
Para acessar a personalização, inclua o Chrome na Atividade na Web e de apps
Revisar dados sincronizados
Opções de criptografia
Para aumentar a segurança, seus dados serão criptografados pelo Google Chrome
Outros serviços do Google
Fazer login no Chrome ao acessar Serviços do Google
Ao fazer login nos Serviços do Google (como o Gmail ou o YouTube) com luizpsalomao@gmail.com, você pode se conectar automaticamente ao Chrome com a mesma conta
Selecione uma opção
Permitir login no Chrome
Desative essa opção para acessar sites do Google, como o Gmail, sem login no Chrome

ORIENTAÇÕES FINAIS

Trate e interprete os dados: a maioria das ferramentas concentra inúmeros alertas, incluindo credenciais requentadas. Saiba interpretar o conjunto completo dos dados, identificar credenciais reais e comprometimentos concretos.

O usuário é seu amigo: a decisão se torna mais fácil ao falar com o envolvido. Quando não for possível concluir pela existência de um comprometimento, explique o processo e pergunte ao usuário.

A causa-raiz importa: rastreie a origem do vazamento. Se não existem evidências de ausência de intrusão, não é prudente encerrar o incidente com o simples reset de senha.

Interaja com o ator malicioso: esteja preparado para perguntar, com cautela.

Faça análise do malware: sempre que possível, tente identificar o binário que culminou na coleta e analisar a comunicação. Lembre-se, certos artefatos podem ser úteis para a investigação policial.

PERGUNTAS?