

SELLING 🔥🌟 **Selling Government & Law Enforcement Email Accounts** 🔥🌟 (Many countries)🔥

by Governer - 22-06-25, 01:51 AM

Pages (7): 1 2 3 4 5 ... 7 Next »

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

#1

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

👑 **Governer**



GOD



Posts 146
Threads 4
Joined Jun 2025
Reputation 87
4 Months



INFOSTEALERS

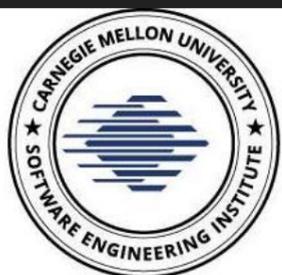
Monitoramento e Resposta a Incidentes



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.

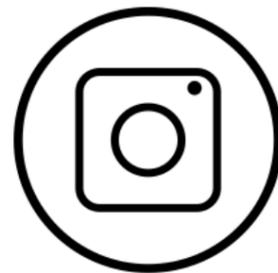
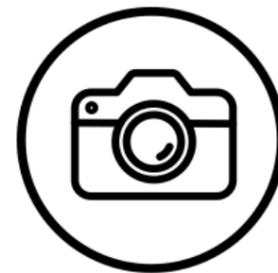


CERT
Incident Response Process Professional
Certificate Holder



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

- Rules
- Forums
- What's new
- Resources
- Members
- Guarantors
- Arbitration
- Blacklist

- Profile
- Alerts
- Settings

	Official Stealer AID_Stealer Hardless · 20.02.24 2 3		Replies: 37 Views: 7K	22.10.25 VALLHAL88	
	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	
	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	
	Official Stealer BLACKNOTE STEALER BlackLoad · 01.09.24 2		Replies: 18 Views: 4K	06.03.25 да просто обычный	
	Official Stealer Mint Stealer #1 STEALER - GAMES, BROWSERS, WALLET... SEMI -FUD UHQ ArtemFromNights · 29.09.23		Replies: 1 Views: 1K	04.02.25 	
	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	
	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	
	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	

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 purpose. **It will be Vidar's job to destroy Fenrir.**

The Gift of Foresight

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

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

Save session Till closing the browser

2) DISTRIBUIÇÃO

SPRAY AND PRAY



/d/JOBS4CRYPTO

Rules

Posting Template.



1



by [d 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

/d/fraudship

WIKI

POSTING RULES



1



by [d 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



Threat Intelligence, Malware

Infostealer malware now targets cracked software users

July 23, 2025

Share

By SC Staff

Blog da Zscaler

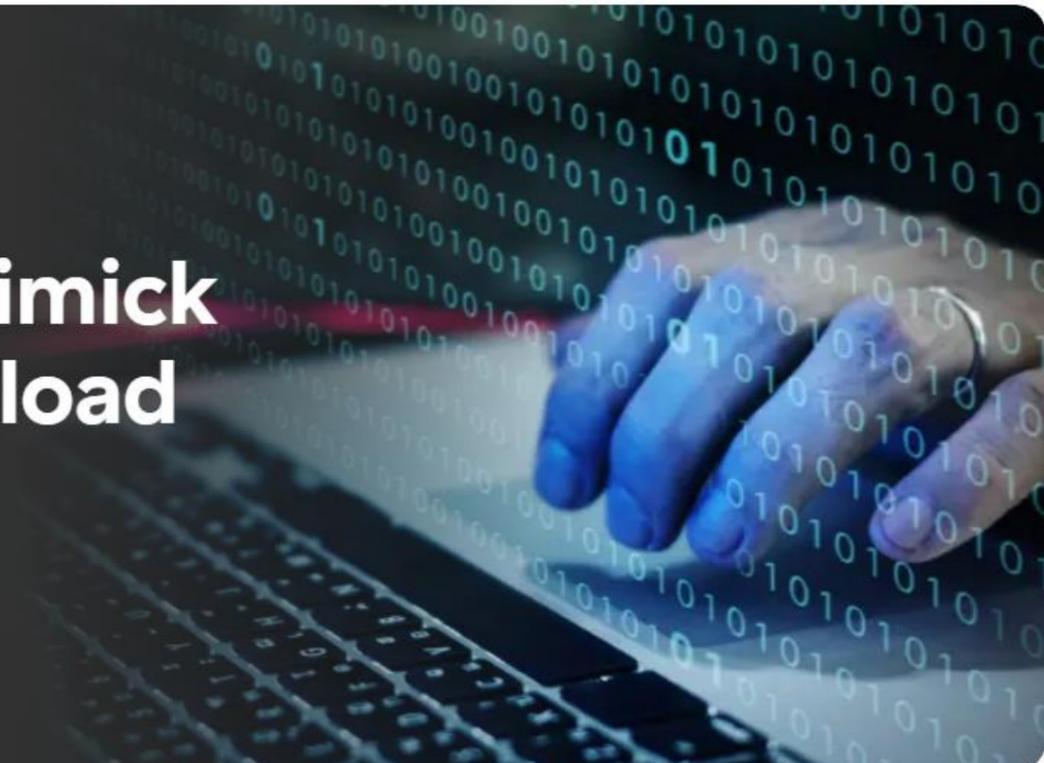
Receba as últimas atualizações do blog da Zscaler na sua caixa de entrada

[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 EXECUTION TIME

by int - 01-10-25, 07:28 AM

int



DarkForums Members



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.

```
if ( v9 == -1039207090 )
{
    v13 = mal_strcompers(a2, "Opera @");
    mal_strncpy_multiterminated((__int64)v27, 64LL, (__int64)v13);
    mal_buffer_append_cstr_bounded_return_offset((__int64)v27, 64LL, (__int64)a2);
    mal_buffer_append_cstr_bounded_return_offset((__int64)v27, 64LL, (__int64)Stable);
    v17 = v13 == 0;
    v9 = -31052990;
    if ( !v13 )
        v9 = -1671893552;
}
else
{
    mal_strncpy_multiterminated((__int64)fileName, 260LL, (__int64)v31);
    mal_buffer_append_cstr_bounded_return_offset((__int64)fileName, 260LL, (__int64)Local State);
    v11 = GetFileAttributesA(fileName) == -1;
    v9 = 1981821688;
    if ( v11 )
        v9 = 247944031;
}
```

Reads browser local state file
and locates encrypted_key

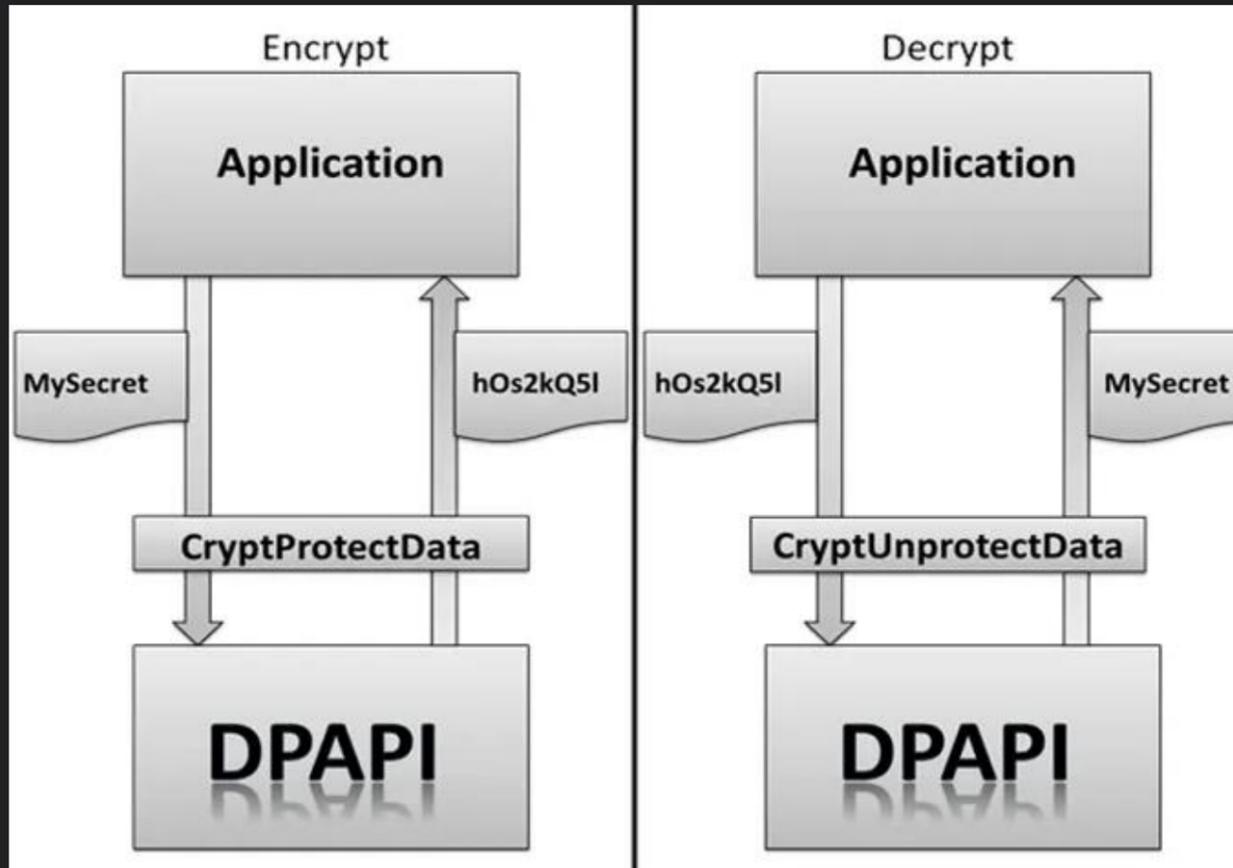
```
{
    GetLastError();
    v14 = ICryptUnprotectData(&pDataIn, 0LL, 0LL, 0LL, 0LL, 1u, &pDataOut);
    v11 = -61263044;
    if ( v14 )
        v11 = 483604784;
}
```

Attempts to decrypt payload
using CryptUnprotectData

```
mal_copybytes(v6, v10, fileSize);
*((_BYTE *)v6 + fileSize) = 0;
v27 = GetProcessHeap();
HeapFree(v27, 0, v10);
v36 = mal_findsubstring(v6, "\\encrypted_key\\.");
v11 = -1481002080;
if ( !v36 )
    v11 = -155598634;
```

©2025 TREND MICRO

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>

Local > Google > Chrome > User Data > Default > Pesquisar em Defau

Classificar Visualizar

Nome	Data de modificação	Tipo	Tamanho
heavy_ad_intervention_opt_out.db-journal	30/10/2025 23:12	Arquivo DB-JOUR...	0 KB
History	01/11/2025 01:59	Arquivo	53.664 KB
History-journal	01/11/2025 01:59	Arquivo	0 KB
InterestGroups	29/09/2025 15:39	Arquivo	384 KB
InterestGroups-wal	28/10/2025 08:54	Arquivo	170 KB
LOCK	21/05/2025 13:35	Arquivo	0 KB
LOG	29/09/2025 15:43	Arquivo	0 KB
LOG.old	16/07/2025 16:24	Arquivo OLD	0 KB
Login Data	01/11/2025 01:56	Arquivo	100 KB
Login Data For Account	23/05/2025 13:04	Arquivo	40 KB
Login Data For Account-journal	23/05/2025 13:04	Arquivo	0 KB
Login Data-journal	01/11/2025 01:56	Arquivo	0 KB
MediaDeviceSalts	31/10/2025 13:07	Arquivo	64 KB

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

4) MONETIZAÇÃO



- R** **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
prpuserice · 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/уникальные
количество строк: ~2.5kkk+ Цена доступа: 99\$/мес. Для покупки доступа - @Getpaid333 ===== ENG...
Getpaid · Post #32 · Today at 10:50 AM · Forum: [Emails / Database](#)
- K** **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](#)
- P** **Sell** Продам дампы 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 · [дампы](#) [продам](#) [продам дампы](#) · Replies: 0 · Forum: [Emails / Database](#)
- K** **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>

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

Start new topic Reply to this topic

YTL
byte
Paid registration
12 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 US1K.

--

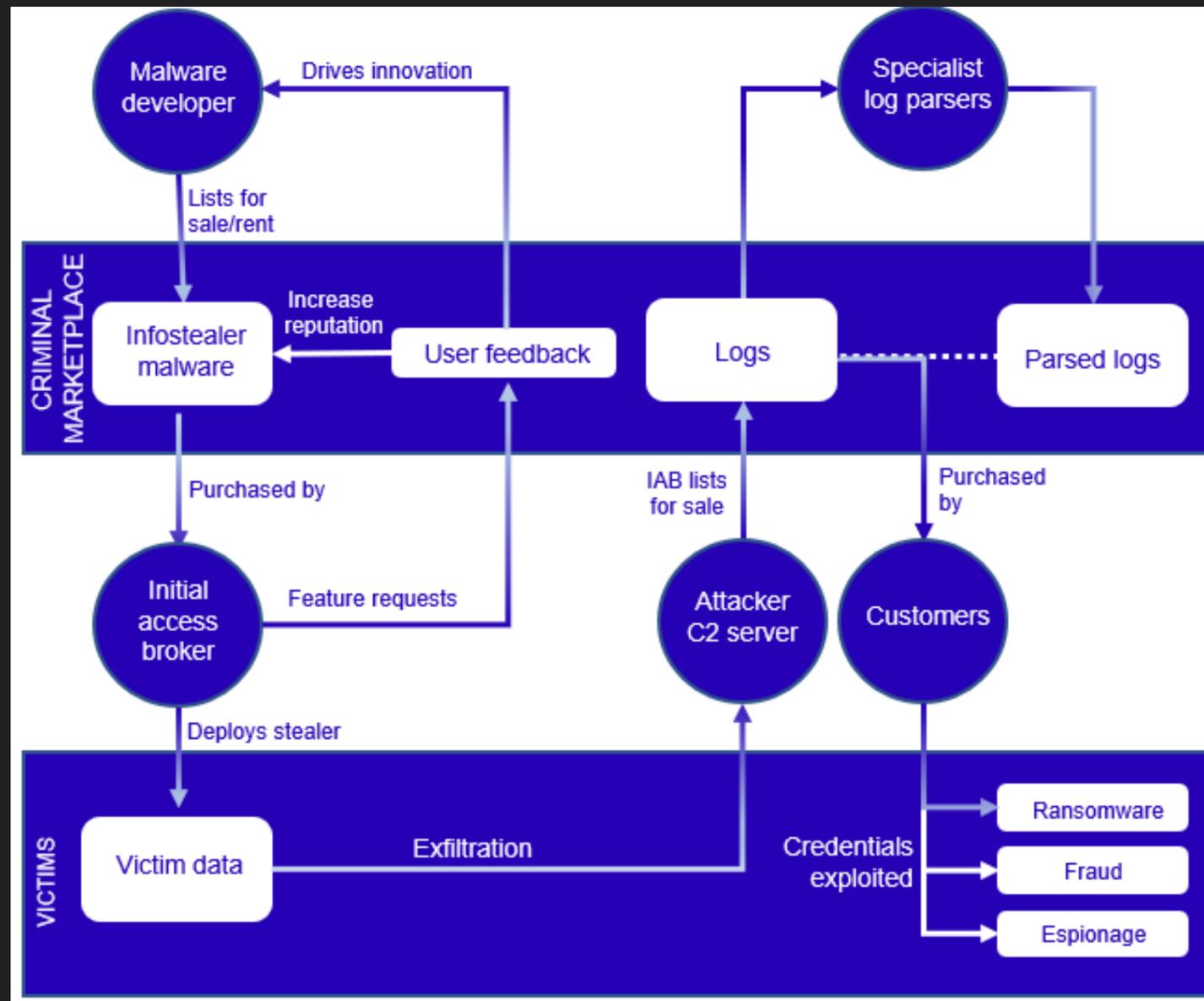
Здравствуйте.

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.





I KNEW EXACTLY WHAT TO DO.

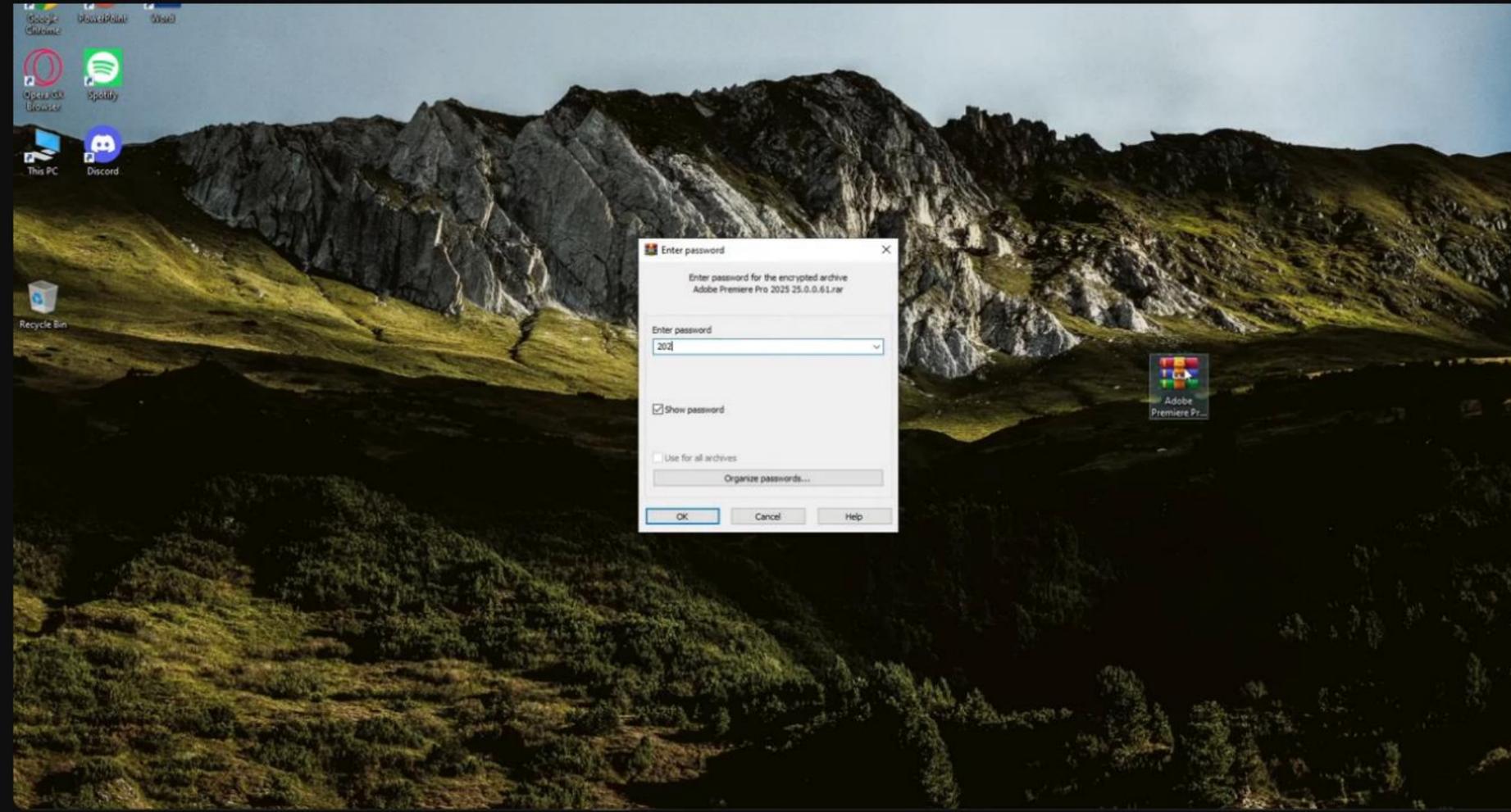
TheOfficeisms.com

BUT IN A MUCH MORE REAL SENSE

I HAD NO IDEA WHAT TO DO.

70% dos dispositivos infectados são pessoais.

LIDANDO COM INCIDENTES



FREE DOWNLOAD PREMIERE PRO :

136 mil inscritos [Inscrever-se](#)

👍 1,8 mil 🗨️ [Compartilhar](#) [Download](#) [Clipe](#) ⋮

200.043 visualizações 9 de jan. de 2025
📄 Download Patch: 📺 Postagem
🔑 Password: 2025

- Home
- Big Story 
- MrBeast
- MrBeast Gaming
- Music
- Shorts
- Watched
- Library
- History
- Playlists
- Channels
- Subscriptions
- Account

 [redacted] (editado) 

★ Adobe Premiere Pro

 Download: [https://\[redacted\]](https://[redacted])

 Password: 2025

 1,2 mil  

23 comentários  Ordenar por

 Adicione um comentário...

-  youtube 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
-  _official há 4 meses 
the passwort :3
Responder
-  bir7554 há 5 meses 
so much brother
angle

Responder
-  há 3 meses 
anks so much, saved me hours 🙏
Responder
-  mkar há 5 meses 
thank you brother

Request

Pretty Raw Hex

```
1 GET /links [redacted]
2 Host: api.rekonise.com
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
  ,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
  3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://[redacted]
9
10
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 302 Found
2 Date: Thu, 11 Dec 2025 13:22:35 GMT
3 Location:
  https://www.dropbox.com/[redacted]
  -2025.rar?rlkey=t6k06hu[redacted]
4 Server: cloudflare
5 X-Powered-By: Express
6 Vary: Origin
7 Access-Control-Allow-Credentials: true
8 Ratelimit-Policy: 60;w=60
9 Ratelimit-Limit: 60
10 Ratelimit-Remaining: 59
11 Ratelimit-Reset: 26
12 Cf-Cache-Status: DYNAMIC
13 Nel:
  {"report_to":"cf-nel","success_fraction":0.0,
14 Server-Timing: cfCacheStatus;desc="DYNAMIC"
15 Server-Timing: cfEdge;dur=3,cfOrigin;dur=130
16 Report-To:
  {"group":"cf-nel","max_age":604800,"endpoints
  .nel.cloudflare.com/report/v4?s=IAtzA082ToRHc
  ocuDpqBAWti7vcYijY2MtJGF%2F2edndAzJjmkFjgAGTY
  yZAS6XKGyAKhQnFSA%3D"}}
17 Cf-Ray: 9ac54aadec2745a6-GIG
18 Alt-Svc: h3=":443"; ma=86400
19
```

dropbox.com/s/[redacted]

Adobe.Premiere.[redacted]

Arquivo Editar Visualizar Ajuda

Extrair tudo

Informações

Propriedades	
Tamanho	0,94 GB
Modificado	09/12/2025, 12:08
Tipo	Arquivar
Enviado por	[redacted]
Data de envio	09/10/2025, 14:35

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
248ddb4eafcea1446d8c0edc00d4818 Set-up.exe
[salomao@parrot]-[~/Downloads/Adobe.Premiere.Pro.2025]
└─$ strings Set-up.exe > strings.txt
[salomao@parrot]-[~/Downloads/Adobe.Premiere.Pro.2025]
└─$
```

248ddb4eafcea1446d8c0edc00d4818

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 x
Loading strings.txt from ~/Downloads/Adobe.Premiere.Pro.2025

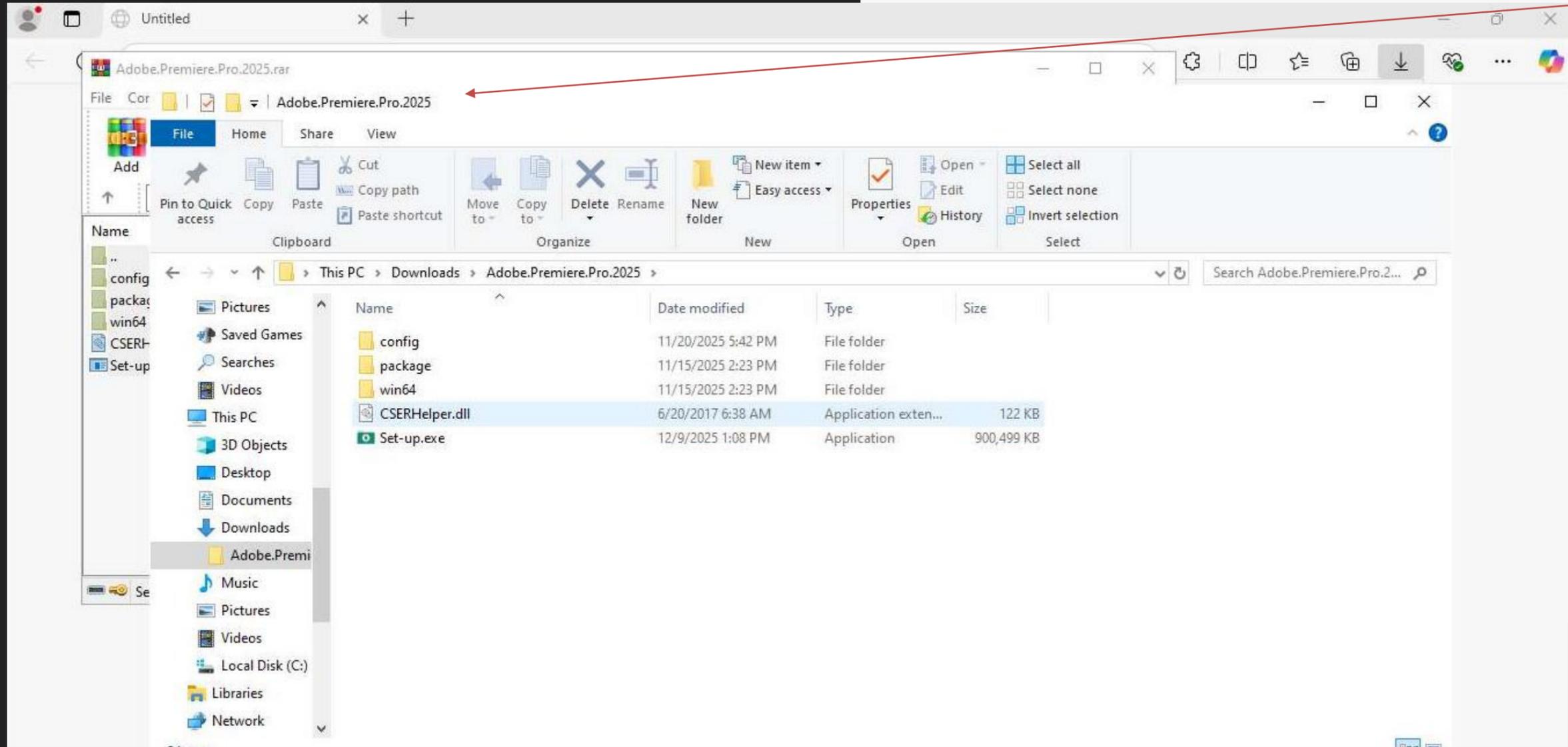
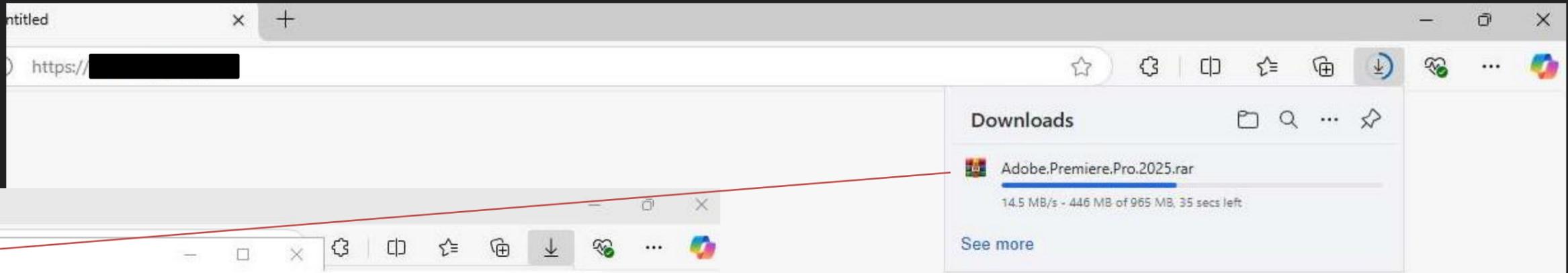
106139 #H9<Z9AwRpF#bPK/ds@y,F!BIH&+s- [ ;r, {p>G
106140 Vr"u[b+,tn^se:aA0=Rf(k-wE
106141 4/6iZ
106142 /(]a#9mAT/lvI=e"
106143 |kA@S1!^
106144 =;9N%qY&OGc5Fc}jcbwCo4XT5
106145 9'62k9S5Xi4$n*/+j}3h}{_
106146 g2Tpn1?Kn1_Z}OW1lII?UHT225:uZiivX4t{c0G(ShBh:>3Yz
106147 o=$"tP}
106148 QjQm^s}gZq"hV<D{
106149 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^x0axV0PD?<G!^:Km}x#6,nT2:v|_H];3d=MfJvY5P%T'YUiT'#n!#R-Py<L0&{%/! ?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
248ddb4eafcea1446d8c0edc00d4818 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\
Phhttp://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>( ?0z;BjI+|>
)http]cQw'2B1AA0d-^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"M1*Ux{dYtfSmg&c8" . j)%#QpFk?Nc;q0'{'9,k06QE3|)nFhttp*IfotoM"#G84S<&#;?,P<J6
EK2;CjLA1_Zvc4?b{k)B{!ohttpx26L;k&e0;,_;Kgr^(AI'^D7fb=-/3Kg1q0hf]nsD.-^2rJY13/70s*-Fo}Y5{^- [7|xJ[8Q0U(spn&nj#. +{u$9w5oI^e8yYC=N
F. |)0$DG2_1sLC9s0=TqS=9*gFC3w/RAU7yx9;bZlhttp4M-eFxzaT*&C]F{ }60]yy6Xa^G*
TK]#!%X*08KZ01.q:ZUM-G$1&<'!7(Phhttp){vu)_Ypx:7;6|F:WW"
<Vc 12>TcM>DE (0 12 M8Tc) 1Mh+>+> 1DUF: 274k7
```

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.**



premiere_crack.pcap

Arquivo Editar Exibir Ir Captura Analizar Estatísticas Telefonía Sem fio Ferramentas Ajuda

Aplicar um filtro de exibição ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::7882:6525:704...	ff02::1:ffb6:4365	ICMPv6	86	Neighbor Solicitation for fe80::838e:7b90:e9b6:4365 from f8:73:26:e4:05:9f
2	0.000145	fe80::7882:6525:704...	ff02::1:ff0e:bbc6	ICMPv6	86	Neighbor Solicitation for fe80::e786:ef21:aa0e:bbc6 from f8:73:26:e4:05:9f
3	0.018088	192.168.100.12	192.168.100.2	DNS	91	Standard query 0x1db3 A settings-win.data.microsoft.com
4	0.025093	192.168.100.2	192.168.100.12	DNS	225	Standard query response 0x1db3 A settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME settings-prod-neu-2.northeurope
5	0.027712	192.168.100.12	51.104.136.2	TCP	66	49708 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6	0.097740	192.168.100.12	51.104.136.2	TCP	66	49709 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7	0.109423	192.168.100.12	192.168.100.255	NBNS	110	Registration NB DESKTOP-JGLLJLD<00>
8	0.109599	192.168.100.12	192.168.100.255	NBNS	110	Registration NB WORKGROUP<00>
9	0.109660	192.168.100.12	192.168.100.255	NBNS	110	Registration NB DESKTOP-JGLLJLD<20>
10	0.149450	192.168.100.12	51.104.136.2	TCP	66	49710 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
11	0.859475	192.168.100.12	192.168.100.255	NBNS	110	Registration NB DESKTOP-JGLLJLD<20>
12	0.859960	192.168.100.12	192.168.100.255	NBNS	110	Registration NB WORKGROUP<00>
13	0.860098	192.168.100.12	192.168.100.255	NBNS	110	Registration NB DESKTOP-JGLLJLD<00>
14	1.031321	192.168.100.12	51.104.136.2	TCP	66	[TCP Retransmission] 49708 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
15	1.102061	192.168.100.12	192.168.100.2	DNS	70	Standard query 0x0ce3 A google.com
16	1.102587	192.168.100.2	192.168.100.12	DNS	86	Standard query response 0x0ce3 A google.com A 142.250.185.206
17	1.109356	192.168.100.12	51.104.136.2	TCP	66	[TCP Retransmission] 49709 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
18	1.156225	192.168.100.12	51.104.136.2	TCP	66	[TCP Retransmission] 49710 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
19	1.213654	fe:73:26:e4:05:9f	Nearest-Customer-Br...	STP	52	Conf. Root = 32768/0/52:54:00:2f:9f:43 Cost = 0 Port = 0x800b
20	1.499997	fe80::7882:6525:704...	fe80::ee7a:293b:bdb...	ICMPv6	86	Neighbor Solicitation for fe80::ee7a:293b:bdb8:7942 from f8:73:26:e4:05:9f
21	1.500151	fe80::7882:6525:704...	fe80::a820:439d:215...	ICMPv6	86	Neighbor Solicitation for fe80::a820:439d:2155:f97d from f8:73:26:e4:05:9f
22	1.625506	192.168.100.12	192.168.100.255	NBNS	110	Registration NB WORKGROUP<1e>
23	2.390632	192.168.100.12	192.168.100.255	NBNS	110	Registration NB WORKGROUP<1e>
24	2.499949	fe80::7882:6525:704...	fe80::ee7a:293b:bdb...	ICMPv6	86	Neighbor Solicitation for fe80::ee7a:293b:bdb8:7942 from f8:73:26:e4:05:9f
25	2.500121	fe80::7882:6525:704...	fe80::a820:439d:215...	ICMPv6	86	Neighbor Solicitation for fe80::a820:439d:2155:f97d from f8:73:26:e4:05:9f
26	2.999985	fe80::7882:6525:704...	fe80::da56:dbac:daf...	ICMPv6	86	Neighbor Solicitation for fe80::da56:dbac:dafb:526a from f8:73:26:e4:05:9f

Frame 1: Packet, 86 bytes on wire (688 bits), 86 bytes captured (688 bits)

- Ethernet II, Src: f8:73:26:e4:05:9f (f8:73:26:e4:05:9f), Dst: IPv6mcast_ff:b6:43:65 (33:33:ff:b6:43:65)
- Internet Protocol Version 6, Src: fe80::7882:6525:7048:e50c, Dst: ff02::1:ffb6:4365
- Internet Control Message Protocol v6

```

0000  33 33 ff b6 43 65 f8 73  26 e4 05 9f 86 dd 60 00  33 33 ff b6 43 65 f8 73
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 78 82  00 00 00 00 00 00 00 00
0020  65 25 70 48 e5 0c ff 02  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0030  00 01 ff b6 43 65 87 00  b4 52 00 00 00 00 fe 80  00 00 00 00 00 00 00 00
0040  00 00 00 00 00 00 83 8e  7b 90 e9 b6 43 65 01 01  00 00 00 00 00 00 00 00
0050  f8 73 26 e4 05 9f

```

Wireshark capturou inúmeros pacotes

Conversation Settings		Ethernet · 33	IPv4 · 45	TCP · 98	UDP · 118			
<input type="checkbox"/> Resolução de nomes		Endereço A	Porta A	Endereço B	Porta B	Pacotes	Bytes	ID da F
<input checked="" type="checkbox"/> Hora de início absoluta		192.168.100.12	49760	13.107.213.44	443	34	11 kB	Microsoft / Akamai
<input checked="" type="checkbox"/> Exibir dados brutos		192.168.100.12	49713	150.171.22.17	443	34	12 kB	
<input checked="" type="checkbox"/> Limitar ao filtro de exibição		192.168.100.12	49714	150.171.27.11	443	34	12 kB	
<input type="button" value="Copiar"/>		192.168.100.12	49726	184.86.251.27	443	34	10 kB	
<input type="button" value="Acompanhar Transmissão..."/>		192.168.100.12	49757	13.107.246.44	443	33	10 kB	
<input type="button" value="Gráfico..."/>		192.168.100.12	49775	95. [REDACTED]	443	33	22 kB	Google
<input type="button" value="Gráficos de E/S"/>		192.168.100.12	49799	142.250.186.106	443	33	13 kB	
<input type="button" value="Protocolo"/>		192.168.100.12	49727	172.217.18.3	443	33	12 kB	
<input type="button" value="Bluetooth"/>		192.168.100.12	49806	142.250.184.234	443	32	15 kB	
<input type="button" value="BPv7"/>		192.168.100.12	49745	172.211.123.248	443	32	9 kB	
<input type="button" value="TCP"/>		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	

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

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

IPv7

UDP

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	49775	95.1	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.

[redacted]

[redacted]

premiere_crack.pcap

Arquivo Editar Exibir Ir Captura Analizar Estatísticas Telefonía Sem fio Ferramentas Ajuda

tls.handshake.type == 1

No.	Time	Source	Destination	Protocol	Length	Info
11077...	64.228304	192.168.100.12	13.107.213.44	TLSv1.3	416	Change Cipher Spec, Client Hello (SNI=static.edge.microsoftapp.net)
11118...	64.417920	192.168.100.12	13.107.213.44	TLSv1.3	483	Client Hello (SNI=edge-cloud-resource-static.azureedge.net)
11121...	64.427186	192.168.100.12	13.107.213.44	TLSv1.3	475	Client Hello (SNI=edge-mobile-static.azureedge.net)
11127...	64.442144	192.168.100.12	13.107.213.44	TLSv1.3	428	Change Cipher Spec, Client Hello (SNI=edge-cloud-resource-static.azureedge.net)
11132...	64.458547	192.168.100.12	13.107.213.44	TLSv1.3	420	Change Cipher Spec, Client Hello (SNI=edge-mobile-static.azureedge.net)
11132...	64.494361	192.168.100.12	150.171.28.11	TLSv1.2	461	Client Hello (SNI=edge.microsoft.com)
11132...	64.514664	192.168.100.12	23.52.181.141	TLSv1.3	459	Client Hello (SNI=go.microsoft.com)
11187...	64.745051	192.168.100.12	150.171.27.11	TLSv1.2	461	Client Hello (SNI=edge.microsoft.com)
12077...	69.318909	192.168.100.12	92.123.104.31	TLSv1.3	774	Client Hello (SNI=www.bing.com)
12749...	116.145996	192.168.100.12	128.24.231.64	TLSv1.2	252	Client Hello (SNI=activation-v2.sls.microsoft.com)
12749...	122.434400	192.168.100.12	172.211.123.248	TLSv1.2	238	Client Hello (SNI=client.wps.windows.com)
12750...	145.613988	192.168.100.12	95.213.111.111	TLSv1.2	212	Client Hello
12750...	146.647766	192.168.100.12	95.213.111.111	TLSv1.2	404	Client Hello
12751...	147.538269	192.168.100.12	95.213.111.111	TLSv1.2	404	Client Hello
12751...	148.370826	192.168.100.12	95.213.111.111	TLSv1.2	404	Client Hello
12751...	149.399117	192.168.100.12	95.213.111.111	TLSv1.2	404	Client Hello
12751...	150.270876	192.168.100.12	95.213.111.111	TLSv1.2	404	Client Hello
12752...	154.256496	192.168.100.12	95.213.111.111	TLSv1.2	404	Client Hello
12752...	155.149596	192.168.100.12	95.213.111.111	TLSv1.2	404	Client Hello
12752...	155.990407	192.168.100.12	95.213.111.111	TLSv1.2	404	Client Hello
12753...	157.937706	192.168.100.12	142.250.185.170	TLSv1.3	482	Client Hello (SNI=safebrowsinghttpgateway.googleapis.com)
12753...	157.945529	192.168.100.12	142.250.184.227	TLSv1.3	472	Client Hello (SNI=clientservices.googleapis.com)
12753...	157.978714	192.168.100.12	173.194.76.84	TLSv1.3	462	Client Hello (SNI=accounts.google.com)
12753...	158.009287	192.168.100.12	173.194.76.84	TLSv1.3	462	Client Hello (SNI=accounts.google.com)
12753...	158.016346	192.168.100.12	142.250.184.227	TLSv1.3	472	Client Hello (SNI=clientservices.googleapis.com)
12753...	158.016623	192.168.100.12	142.250.185.196	TLSv1.3	457	Client Hello (SNI=www.google.com)

SNI?? ←

```

Frame 1275072: Packet, 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits)
Ethernet II, Src: f8:73:26:e4:05:9f (f8:73:26:e4:05:9f), Dst: d4:11:11:11:11:11
Internet Protocol Version 4, Src: 192.168.100.12, Dst: 95.213.111.111
Transmission Control Protocol, Src Port: 49772, Dst Port: 443, Seq: 1, Ack: 1, Len: 158
Transport Layer Security
0000 d4 da 6d 4e 02 4f f8 73 26 e4 05 9f 08 00 45 00  ..mN.O.s &.....E
0010 00 c6 b2 e4 40 00 80 06 a8 99 c0 a8 64 0c 5f d9  ....@.....d...
0020 1a 26 c2 6c 01 bb b0 50 fa 82 93 3a 0f 0d 50 18  &1...P...:..P
0030 04 00 1b e7 00 00 16 03 03 00 99 01 00 00 95 03  ....
0040 03 69 38 e0 80 e0 d6 ce 1d dc 97 49 a3 bd 0b 0e  i8.....I....
0050 d8 1c 2d 4c 28 6b b5 e1 b1 35 ab 52 93 d3 f5 e9  ...L(k...5R...
0060 c2 00 00 26 c0 2c c0 2b c0 30 c0 2f c0 24 c0 23  ...&,+0/$#
0070 c0 28 c0 27 c0 0a c0 09 c0 14 c0 13 00 9d 00 9c  (.....
0080 00 3d 00 3c 00 35 00 2f 00 0a 01 00 00 46 00 05  =<5/.....F..
0090 00 05 01 00 00 00 00 00 0a 00 08 00 06 00 1d 00  ....
00a0 17 00 18 00 0b 00 02 01 00 00 0d 00 1a 00 18 08  ....
00b0 04 08 05 08 06 04 01 05 01 02 01 04 03 05 03 02  ....
00c0 03 02 02 06 01 06 03 00 23 00 00 00 17 00 00 ff  ....#.....
00d0 01 00 01 00

```

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

premiere_crack.pcap

Arquivo Editar Exibir Ir Captura Analizar Estatísticas Telefonias Sem fio Ferramentas Ajuda

ip.dst == 95.2

No.	Time	Source	Destination	Protocol	Length	Info
12750...	145.551327	192.168.100.12	95.2...	TCP	66	49772 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
12750...	145.606713	192.168.100.12	95.2...	TCP	54	49772 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
12750...	145.613988	192.168.100.12	95.2...	TLSv1.2	212	Client Hello
12750...	145.688993	192.168.100.12	95.2...	TCP	54	49772 → 443 [ACK] Seq=159 Ack=1132 Win=262144 Len=0
12750...	145.689488	192.168.100.12	95.2...	TCP	54	49772 → 443 [ACK] Seq=159 Ack=1955 Win=261120 Len=0
12750...	145.806177	192.168.100.12	95.2...	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
12750...	145.861155	192.168.100.12	95.2...	TCP	54	49772 → 443 [ACK] Seq=252 Ack=2213 Win=260864 Len=0
12750...	145.865683	192.168.100.12	95.2...	TLSv1.2	213	Application Data
12750...	146.264888	192.168.100.12	95.2...	TCP	54	49772 → 443 [ACK] Seq=411 Ack=2417 Win=262144 Len=0
12750...	146.591120	192.168.100.12	95.2...	TCP	66	49773 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
12750...	146.647352	192.168.100.12	95.2...	TCP	54	49773 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
12750...	146.647766	192.168.100.12	95.2...	TLSv1.2	404	Client Hello
12750...	146.702746	192.168.100.12	95.2...	TCP	54	49773 → 443 [ACK] Seq=351 Ack=110 Win=261888 Len=0
12750...	146.704181	192.168.100.12	95.2...	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
12750...	146.705609	192.168.100.12	95.2...	TLSv1.2	559	Application Data
12750...	147.160201	192.168.100.12	95.2...	TCP	54	49773 → 443 [ACK] Seq=907 Ack=373 Win=261632 Len=0
12750...	147.483454	192.168.100.12	95.2...	TCP	66	49774 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
12751...	147.537893	192.168.100.12	95.2...	TCP	54	49774 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
12751...	147.538269	192.168.100.12	95.2...	TLSv1.2	404	Client Hello
12751...	147.592158	192.168.100.12	95.2...	TCP	54	49774 → 443 [ACK] Seq=351 Ack=110 Win=261888 Len=0
12751...	147.596009	192.168.100.12	95.2...	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
12751...	147.597454	192.168.100.12	95.2...	TLSv1.2	636	Application Data
12751...	148.009726	192.168.100.12	95.2...	TCP	54	49774 → 443 [ACK] Seq=984 Ack=2494 Win=262144 Len=0
12751...	148.312908	192.168.100.12	95.2...	TCP	66	49775 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
12751...	148.370441	192.168.100.12	95.2...	TCP	54	49775 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
12751...	148.370826	192.168.100.12	95.2...	TLSv1.2	404	Client Hello
12751...	148.424754	192.168.100.12	95.2...	TCP	54	49775 → 443 [ACK] Seq=351 Ack=110 Win=261888 Len=0
12751...	148.426287	192.168.100.12	95.2...	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message

Frame 1275081: Packet, 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits) on interface f)

- Ethernet II, Src: f8:73:26:e4:05:9f (f8:73:26:e4:05:9f), Dst: 95.2...
- Internet Protocol Version 4, Src: 192.168.100.12, Dst: 95.2...
- Transmission Control Protocol, Src Port: 49772, Dst Port: 443, Seq: 252, Ack: 2213, Len: 159
- Transport Layer Security

```

0000  d4 da 6d 4e 02 4f f8 73 26 e4 05 9f 08 00 45 00  ..mN.O.s &....E.
0010  00 c7 b2 e9 40 00 80 06 a8 93 c0 a8 64 0c 5f d9  ....@.....d...
0020  1a 26 c2 6c 01 bb b0 50 fb 7d 93 3a 17 b1 50 18  ..&.l...P...}...P.
0030  03 fb dd b0 00 00 17 03 03 00 9a 00 00 00 00 00  .....
0040  00 00 01 94 16 aa 7b fb d4 f0 bf 26 e2 5c b7 5b  .....{...&.\.[
0050  d6 5a 1f 00 ed 5f dd 02 d9 db 1f b4 06 20 e5 23  ..Z.....#
0060  5c fc 75 63 a7 8c 87 ce 1e 2b bb 19 c5 89 84 2e  \uc...+.....
0070  b1 3d 7c 38 a5 93 48 0f 58 47 45 65 81 77 90 97  ..=|8..H.XGEe.w...
0080  aa 8d 58 26 1d b2 bb 6c 4c 2f 46 71 f0 c7 f2 4b  ..X&...l L/Fq...K
0090  50 1f 86 a4 17 cc de ee 10 76 15 2f a0 5e c0 48  P.....v./..^H
00a0  e2 d9 8a 78 ce e8 ff 53 1e 99 82 63 08 cd 31 a6  ...x...S...c..1.
00b0  0e 1e 48 96 76 24 73 eb 8a 34 c8 6b 39 92 5b 82  ..H.v$s...4.k9.[
00c0  3a 20 71 40 8f ca 6c ff 66 27 50 a1 42 85 39 43  : q@..l'f'P'B'9C
00d0  15 b1 a1 87 93  .....

```

Comunicações constantes com o C2 para envio de dados

Processes 71 Actions 8 **beta**

Filter by PID or name Only important

7500	msedge.exe	"https://rkns.link/ghql6"	26k	9k	189
3420	COM slui.exe	-Embedding	1k	3k	67
752	Set-up.exe	DMP	19k	3k	58

752 Set-up.exe DMP

5036	chrome.exe	-profile-directory="Default"	20k	12k	142
7840	chrome.exe	-profile-directory="Default"	12k	3k	139
7876	chrome.exe	-type=crashpad-handler *-user-data-dir=C:\Users\admin\AppData\Local\Google\Chrome\User Data* /prefetch:4 -monitor-self-annotation=ptype=crashpad-handler *-database=C:\Users\admin\AppData\Local\...	168	69	32
792	chrome.exe	-type=gpu-process -string-annotations -gpu-preferences=UAAAAAAAAADgAAAEAAAAAAAAAAAAAAAAABgAAEAAAAAAAAAAAAAAAAACAAAAAAAAAAAAAAAAABAAAAAAAAAEAAAAAA...			

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)

752 "C:\Users\admin\Downloads\Adobe.Premiere.Pro.2025\Set-up.exe" C:\Users\admin\Downloads\Adobe.Premiere.Pro.2025\Set-up.exe explorer.exe

Information

User:	admin	Company:	ASUSTeK COMPUTER INC.
Integrity Level:	MEDIUM	Version:	22.130.0.5

Modules

Images

- c:\windows\system32\winnsi.dll
- c:\windows\system32\nsi.dll
- c:\windows\system32\urlmon.dll
- c:\windows\system32\netutils.dll
- c:\windows\system32\svcli.dll
- c:\windows\system32\schannel.dll
- c:\windows\system32\mskeyprotect.dll
- c:\windows\system32\ntasn1.dll
- c:\windows\system32\msasn1.dll
- c:\windows\system32\dpapi.dll**

Previous 1 2 3 4 5 6 Next

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

Behavior activities ☑ Add for printing ▲

MALICIOUS	SUSPICIOUS	INFO
Executing a file with an untrusted certificate <ul style="list-style-type: none">• Set-up.exe (PID: 752)	Reads security settings of Internet Explorer <ul style="list-style-type: none">• Set-up.exe (PID: 752)	Checks supported languages <ul style="list-style-type: none">• identity_helper.exe (PID: 2364)• Set-up.exe (PID: 752)
Steals credentials from Web Browsers <ul style="list-style-type: none">• Set-up.exe (PID: 752)	Reads the date of Windows installation <ul style="list-style-type: none">• Set-up.exe (PID: 752)	Application launched itself <ul style="list-style-type: none">• msedge.exe (PID: 7500)• chrome.exe (PID: 5036)• chrome.exe (PID: 7840)
	Searches for installed software <ul style="list-style-type: none">• Set-up.exe (PID: 752)	Reads the computer name <ul style="list-style-type: none">• identity_helper.exe (PID: 2364)• Set-up.exe (PID: 752)
		Reads Environment values <ul style="list-style-type: none">• identity_helper.exe (PID: 2364)• Set-up.exe (PID: 752)
		Executable content was dropped or overwritten <ul style="list-style-type: none">• WinRAR.exe (PID: 6596)
		Checks proxy server information <ul style="list-style-type: none">• slui.exe (PID: 3420)• Set-up.exe (PID: 752)
		The sample compiled with english language support <ul style="list-style-type: none">• WinRAR.exe (PID: 6596)
		Manual execution by a user <ul style="list-style-type: none">• Set-up.exe (PID: 752)
		Detects InnoSetup installer (YARA) <ul style="list-style-type: none">• Set-up.exe (PID: 752)
		Compiled with Borland Delphi (YARA) <ul style="list-style-type: none">• Set-up.exe (PID: 752)
		Creates files in the program directory <ul style="list-style-type: none">• Set-up.exe (PID: 752)
		Reads the machine GUID from the registry <ul style="list-style-type: none">• Set-up.exe (PID: 752)
		Reads product name <ul style="list-style-type: none">• Set-up.exe (PID: 752)
		Reads CPU info <ul style="list-style-type: none">• Set-up.exe (PID: 752)

Análise comportamental confirma a execução de um infostealer

General Info

Add for printing

URL: [https://r\[REDACTED\]](https://r[REDACTED])

Full analysis: [https://app.any.run/tasks/\[REDACTED\]](https://app.any.run/tasks/[REDACTED])

Verdict: **Malicious activity**

Threats: **Stealc** Stealc Stealer Vidar

Stealc is a stealer malware that targets victims' sensitive data, which it exfiltrates from browsers, messaging apps, and other software. The malware is equipped with advanced features, including fingerprinting, control panel, evasion mechanisms, string obfuscation, etc. Stealc establishes persistence and communicates with its C2 server through HTTP POST requests.

[Malware Trends Tracker >>>](#)

Analysis date: December 09, 2025 at 23:50:21

OS: Windows 10 Professional (build: 19044, 64 bit)

Tags: [delphi](#) [inno](#) [installer](#) [stealer](#) [stealc](#) [vidar](#)

Indicators:   

MD5: EAB9EE512AFDAB389DCF9F5CE90BEA7E

SHA1: B52380B0CD1F8FEAA5AAFF71D74F7DE4BD2C4B41

SHA256: 2EAF2AE82423C9D7C8327F8D8C365C0EE0B89FCB38727BBEAEDB7D9E4CA989A9

SSDEEP: 3:N8exhOQT:2ghOQT

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

11
/ 95
Community Score -12

11/95 security vendors flagged this IP address as malicious

95.2 [redacted] /15
AS 24940 (Hetzner Online GmbH)
self-signed

FI Last Analysis Date 1 day ago

Reanalyze More

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.

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 planilha autenticacoes tem {aut_linhas} linhas")
6 print(f"A planilha breach tem {breach_linhas} linhas")
7 print(f"A planilha sei_total tem {sei_total_linhas} linhas")
```

A planilha autenticacoes tem 150002 linhas
A planilha breach tem 5478 linhas
A planilha sei_total tem 19220 linhas

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

```
[8]
✓ Os
1 # Remove duplicados mantendo a última ocorrência (linha mais antiga)
2 breach_clean_sem_duplicados = breach_clean.drop_duplicates(subset='matricula', keep='last').reset_index(drop=True)
3 sei_clean_sem_duplicados = sei_clean.drop_duplicates(subset='matricula', keep='last').reset_index(drop=True)
4
5 # Exibe resultado para a matrícula exemplo
6 #resultado = sei_clean_sem_duplicados[sei_clean_sem_duplicados['matricula'] == ██████████]
7 #print(f"Linhas após remoção de duplicados para matrícula 2283131: {len(resultado)}")
8 #display(resultado)
9
10 #verficia resultado final
11 display(breach_clean_sem_duplicados.head())
12 display(sei_clean_sem_duplicados.head())
13
14
15 breach_linhas = breach_clean_sem_duplicados.shape[0]
16 sei_total_linhas = sei_clean_sem_duplicados.shape[0]
17
18 print(f"A planilha breach tem {breach_linhas} linhas")
19 print(f"A planilha sei_total tem {sei_total_linhas} linhas")
20
```

	event_url	matricula	senha	data
0	██████████	██████████	██████████	2025 03:15:36 am
1	██████████	██████████	██████████	2025 03:15:36 am
2	██████████	██████████	██████████	2025 03:49:46 am
3	██████████	██████████	██████████	2025 03:49:30 am
4	██████████	██████████	██████████	2025 03:49:09 am

	event_url	matricula	senha	data
0	██████████	██████████	██████████	2025 07:09:39 pm
1	██████████	██████████	██████████	2025 07:09:39 pm
2	██████████	██████████	██████████	2025 07:09:39 pm
3	██████████	██████████	██████████	2025 07:09:39 pm
4	██████████	██████████	██████████	2025 06:56:06 pm

A planilha breach tem 124 linhas
A planilha sei_total tem 1631 linhas

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

```
[13] 38         'outras_matriculas': list(matriculas_outros)
✓ 2s 39     })
40
41     resultados.append({
42         'matricula': matricula,
43         'total_ips_externos': len(ips_externos),
44         'ips_detalhes': ips_info
45     })
46
47     # Exibe os resultados
48     for res in resultados:
49         print(f"Matrícula: {res['matricula']}")
50         print(f"IPs externos usados: {res['total_ips_externos']}")
51         for ipinfo in res['ips_detalhes']:
52             print(f" - IP: {ipinfo['ip_externo']}")
53             print(f"   Visto em outras matrículas? {ipinfo['qtd_outras_matriculas']} vezes")
54             if ipinfo['qtd_outras_matriculas'] > 0:
55                 print(f"   Outras matrículas: {', '.join(ipinfo['outras_matriculas'])}")
56     print("-" * 60)
57
```

```
Matrícula: 21 ██████████
IPs externos usados: 2
- IP: 200.1 ██████████.96
  Visto em outras matrículas? 0 vezes
- IP: 177.5 ██████████.2
  Visto em outras matrículas? 1 vezes
  Outras matrículas: 593 ██████████
-----
Matrícula: 22 ██████████
IPs externos usados: 0
-----
Matrícula: 23 ██████████
IPs externos usados: 1
- IP: 177.2 ██████████.3
  Visto em outras matrículas? 0 vezes
-----
Matrícula: 76 ██████████
IPs externos usados: 3
- IP: 172. ██████████.24
  Visto em outras matrículas? 8 vezes
  Outras matrículas: 786 ██████████ 17148
- IP: 189. ██████████.33
  Visto em outras matrículas? 1 vezes
  Outras matrículas: 17 ██████████
- IP: 104. ██████████.60
  Visto em outras matrículas? 5 vezes
  Outras matrículas: 17 ██████████ 17148
-----
```

Usuários com autenticação partindo de IPs diversos merecem ser analisados

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

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.

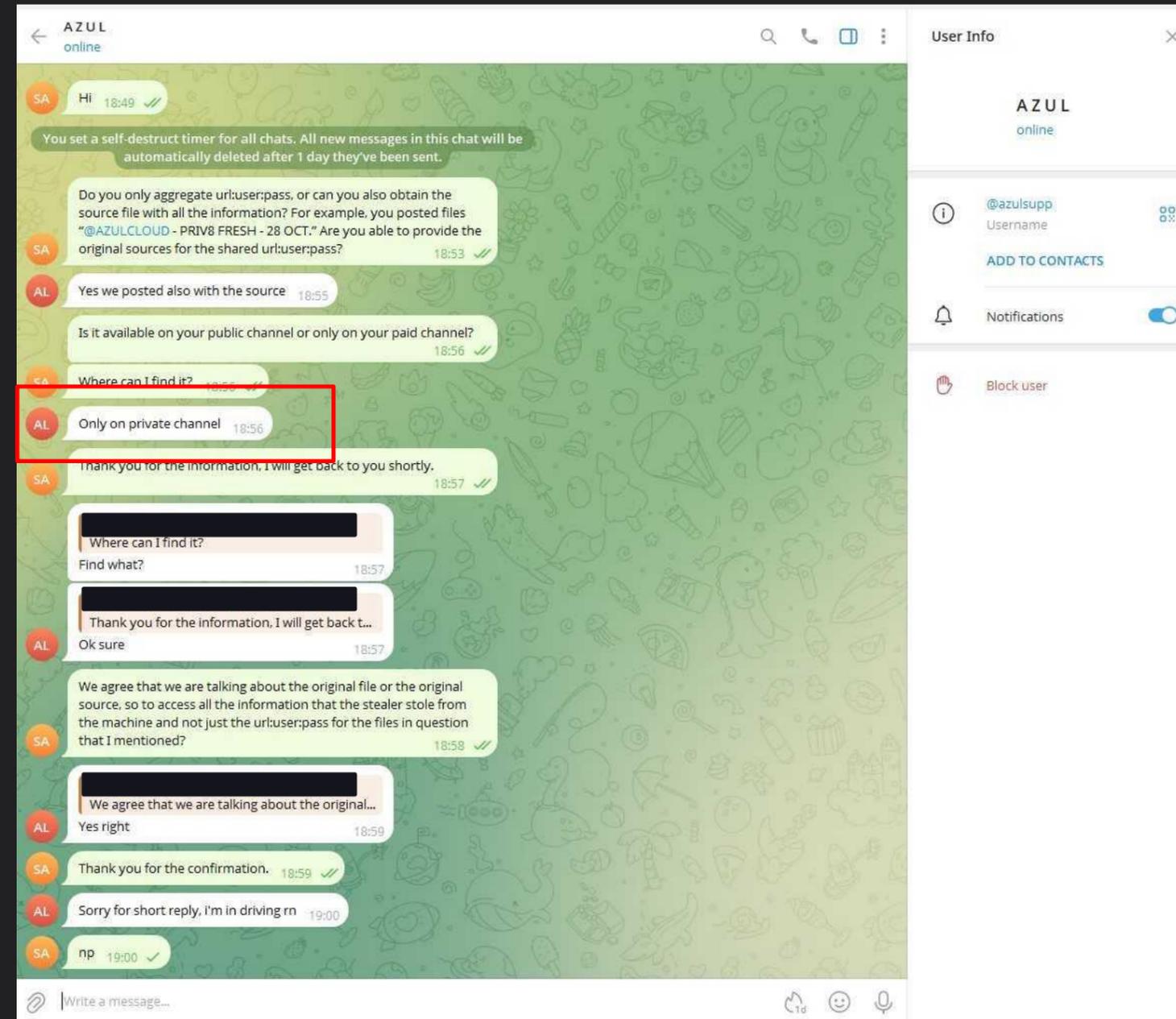
A interação com o ator malicioso é importante, mas nem sempre levará a um resultado concreto.

```

"_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,
  "username": "[REDACTED]",
  "password": "F",
  "password_strength": 8,
  "is_email": false,
  "email_host": "",
  "email_domain": "",
  "email_tld": "",
  "added_at": 1761740644988
}

"_index": "leaks",
"_id": "b4d023943d15c4d1c6639185f9246c1b41a2df2b9153f97062700326bd980725",
"_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,
  "username": "[REDACTED]",
  "password": "143",
  "password_strength": 10,
  "is_email": false,
  "email_host": "",
  "email_domain": "",
  "email_tld": "",
  "added_at": 1761740644991
}

```



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 requeentadas. 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?