SELLING [Brazil] 300K Photos of People from the Federal District

by NikoCorp - 15-02-26, 10:43 AM

15-02-26, 10:43 AM #1

NikoCorp

DarkForums Members

Member

Posts	3
Threads	1
Joined	Feb 2026
Reputation	0

3 Weeks

Hi everyone!
I am selling a database with approximately **300,000 people** from the **Federal District**, a state in **Brazil**. The data was extracted at the end of **2025** from a police system, with all photos originating from **national driver's licenses (Detran)**. This is a **private database**, meaning very few people possess it.

Lines / Rows: 298.743
Format: CSV
Size: 7.8GB
Year: 2025

Price: **$480** USD (**R$2,500** BRL)

Field Header

Code:

```
cpf;imagem_base64
```

What is this data?

cpf: Individual's national registration number
imagem_base64: Photo of the person encoded in base64

PRECISAMOS FALAR SOBRE INFOSTEALERS

como o ecossistema de Cybercrime-as-a-Service (CaaS) impacta a reputação e a operação das redes

LUIZ EDUARDO SALOMÃO

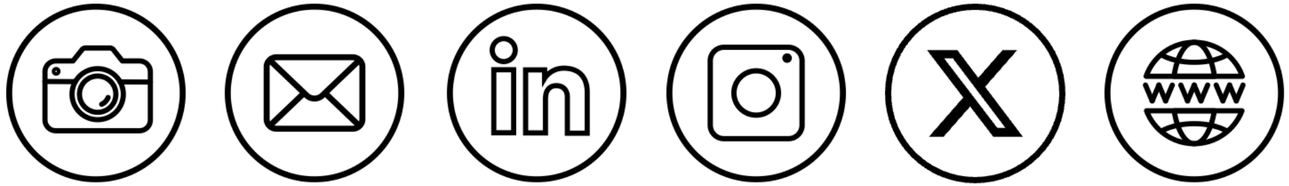
Agente de Polícia (PCDF)
Aluno Especial – Mestrado Seg. Cibernética (UNB)
Aluno – MBA em IA (IBMEC)

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.

Infostealers: 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.

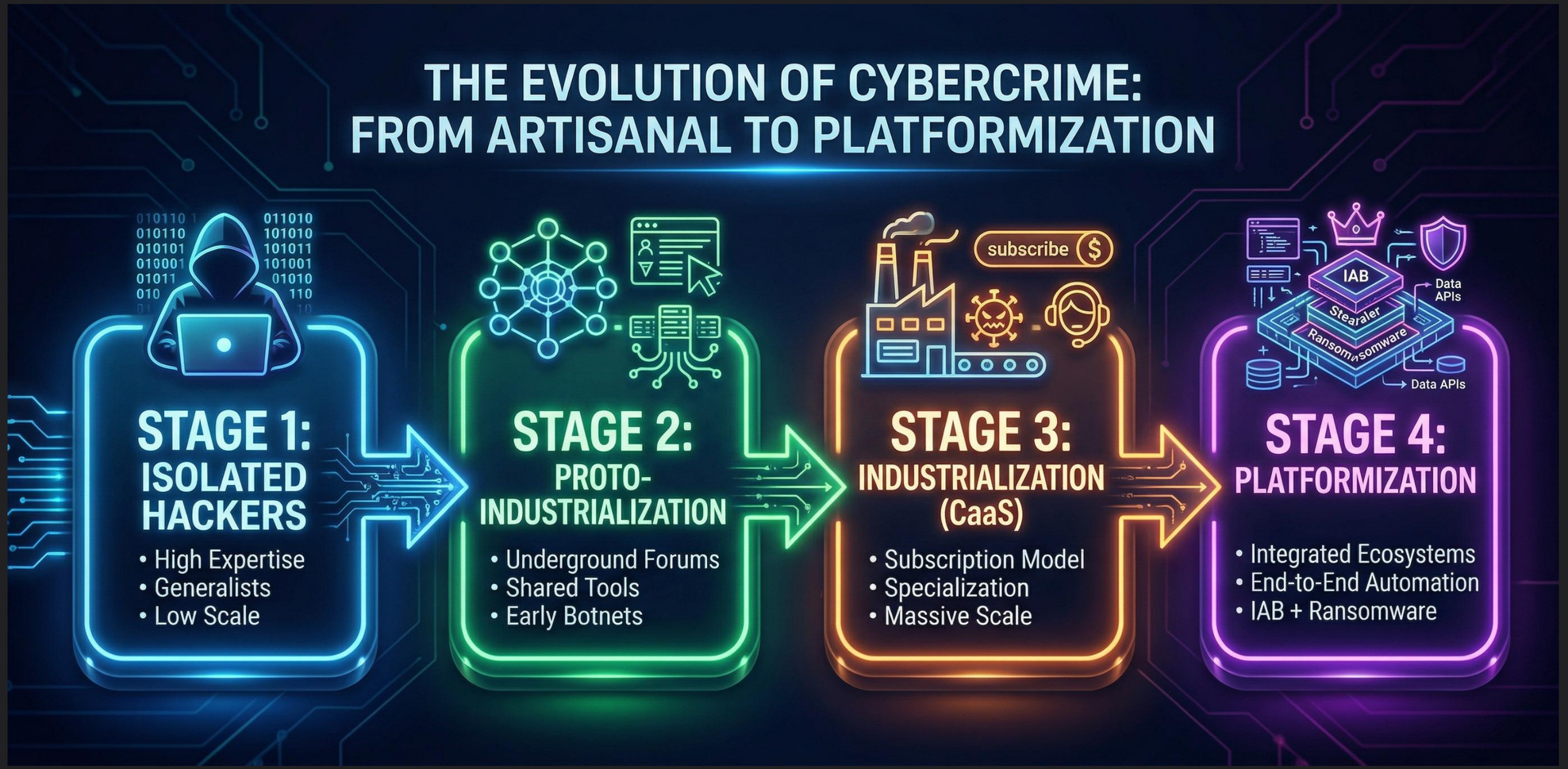
Kela Inside the infostealer epidemic: exposing the risks to corporate security

70% dos dispositivos infectados são **pessoais**.

Checkpoint Cyber security Report 2025

CYBERCRIME-AS-SERVICE

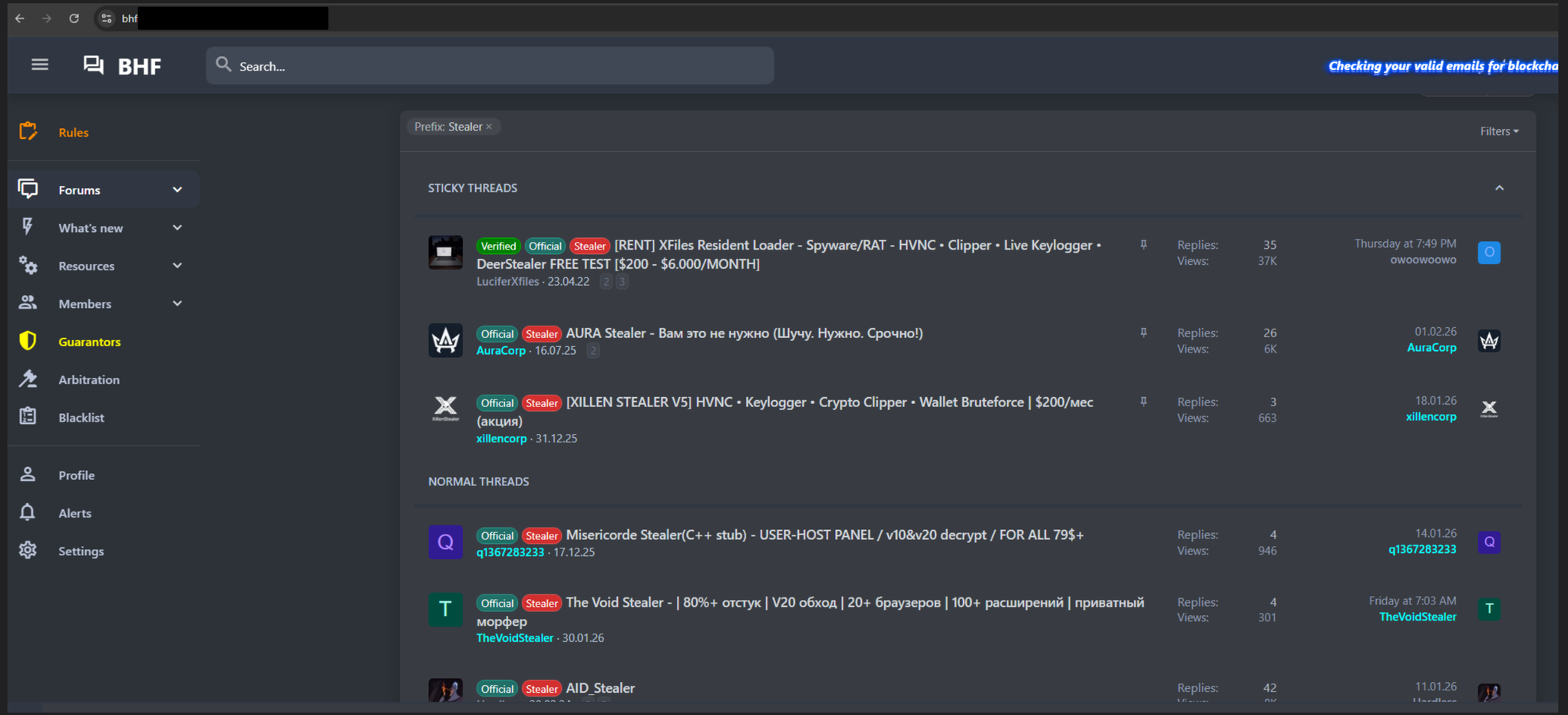
THE EVOLUTION OF CYBERCRIME: FROM ARTISANAL TO PLATFORMIZATION



Malware-as-a-Service: modelo de negócio em que programadores de software malicioso alugam a sua infraestrutura, código e ferramentas para outros criminosos mediante o pagamento de uma assinatura ou comissão sobre os lucros. Essa estrutura promove a democratização do crime: um atacante já não precisa saber programar ou gerir servidores complexos; ele apenas "contrata" o serviço e foca-se na distribuição do ataque.

PATSAKIS, Constantinos; ARROYO, David; CASINO, Fran. The Malware as a Service ecosystem. arXiv, 2024.

1) AQUISIÇÃO


bhf
BHF
Search...
Checking your valid emails for blockcha
Rules
Forums
What's new
Resources
Members
Guarantors
Arbitration
Blacklist
Profile
Alerts
Settings
Prefix: Stealer ×
Filters
STICKY THREADS
Verified Official Stealer [RENT] XFiles Resident Loader - Spyware/RAT - HVNC • Clipper • Live Keylogger • DeerStealer FREE TEST [$200 - $6.000/MONTH]
LuciferXfiles · 23.04.22
Replies: 35
Views: 37K
Thursday at 7:49 PM
owoowoowo
Official Stealer AURA Stealer - Вам это не нужно (Шучу. Нужно. Срочно!)
AuraCorp · 16.07.25
Replies: 26
Views: 6K
01.02.26
AuraCorp
Official Stealer [XILLEN STEALER V5] HVNC • Keylogger • Crypto Clipper • Wallet Bruteforce | $200/мес (акция)
xillencorp · 31.12.25
Replies: 3
Views: 663
18.01.26
xillencorp
NORMAL THREADS
Official Stealer Misericorde Stealer(C++ stub) - USER-HOST PANEL / v10&v20 decrypt / FOR ALL 79$+
q1367283233 · 17.12.25
Replies: 4
Views: 946
14.01.26
q1367283233
Official Stealer The Void Stealer - | 80%+ отстук | V20 обход | 20+ браузеров | 100+ расширений | приватный морфер
TheVoidStealer · 30.01.26
Replies: 4
Views: 301
Friday at 7:03 AM
TheVoidStealer
Official Stealer AID_Stealer
Replies: 42
11.01.26

https://br[redacted]mation-stealer

BreachForums › Marketplace › Services › **Santa Stealer - A modern information stealer**

Mark all as read

Santa Stealer - A modern information stealer

by SantaStealer - Sunday December 28, 2025 at 06:08 AM

SantaStealer

[redacted]

GOD

Posts: 8
Threads: 2
Joined: Dec 2025
Reputation: 60

12-28-2025, 06:08 AM (This post was last modified: 01-08-2026, 11:59 AM by SantaStealer. Edited 1 time in total.)

Santa Stealer is a Windows based stealer developed in C, it works without dependencies fully standalone. The stealer works on any Windows machine from 7 to 11.

- We have a Web Panel ([redacted]or creating, managing and editing builds. Logs can be configured to be sent to a Telegram group or chat
- You can configure modules to take certain data and choose which modules to use. The stealer is designed to extract every piece of valuable information from infected devices at an affordable price.

You can **generate** and purchase a plan in **less than 1 minute** - https:/[redacted]
For a full list of features, product information and detailed module information visit https://[redacted]

Basic - $200/month
Premium - $300/month
Lifetime (Premium) - $1000/lifetime


reg.vidar
Central de Atendimento
Trabalhamos para você em caráter permanente.
Inscrição
Cadastre-se em nosso portal.
Autorização
Link de autorização
Telegrama
Serviço de suporte.
© 2018-2025. Todos os direitos reservados.
RU
EN

2) DISTRIBUIÇÃO

SPRAY AND PRAY

ATIVADORES E CHEATS

1

by xxbnoxx • 1 week ago

spreading malware

hello how can i spread my malware to more people? rn im just dming random people on discord who are in some cheat servers but most of the ti
help is appriciated

10 comments

Comments

Sort comments by Top

brokemf 2 points 1 week ago

Post "cheat tutorials" (or anything else) on social media.

Reply Permalink

repent 1 points 3 days ago

even then you would need footage of u using the cheat so ppl dont get sus abt it, where would u get that

Reply Permalink

rizuken 1 points 1 week ago

you can try SE, like making friends then sending them malware, takes a bit more time though

Reply Permalink

realbct 1 points 1 week ago

create a YT channel and post tutorials and in the description put link with the software with malware

Reply Permalink

download roblox executor

✅HOW TO DOWNLOAD DELTA EXECUTOR FOR PC AND INSTALL SCRIPT INTO ROBLOX WITHOUT A KEY - UPDATED! DI...
4,9 mil visualizações • há 3 dias
Poison Scripts
🔸 Mumu Player: https://www.poisonscripts.com/post/mumu-player-oficial 🔸 Delta: https://www.poisonscripts.com/post/delta-v67
Novo
7 capítulos INICIO | BAIXANDO DELTA E MUMU | INSTALANDO MUMU | CONFIGURANDO MUMU | INSTALANDO...

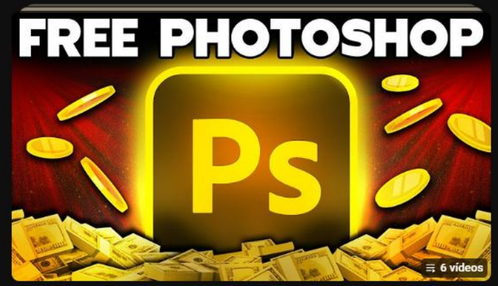
✅LINK DIRETO! COMO BAIXAR Executor RONIX ATUALIZADO + SCRIPT no ROBLOX CELULAR/MOBILE MEDIAFIRE 2026
16 mil visualizações • há 2 dias
PEDRIN TRAVAS OFC
LINK DIRETO! COMO BAIXAR Executor RONIX ATUALIZADO e SCRIPT blox fruits para celular, Script Roube Um Brainrot, Script ...
Novo

[100% UNC] Exploit sem chave "Velocity" do Roblox Executor funcionando em 2026
19 mil visualizações • há 1 dia
Aira Winterland
#Roblox #ExploraçãoDeRoblox #ScriptsRoblox #Byfron #ByfronBypass 📌 TODOS OS LINKS NOS COMENTÁRIOS ‼️ ...
Novo 4K

93bmxvYWQgcm9ibG94IGV4ZWN1dG9y

download adobe crack

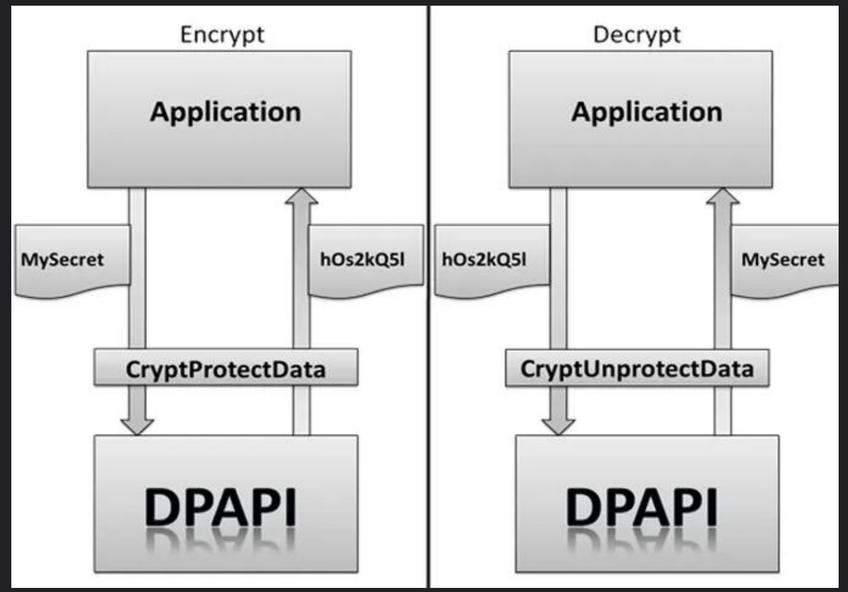
✅ ADOBE PHOTOSHOP FREE DOWNLOAD / PHOTOSHOP CRACK 2026 / PHOTOSHOP FOR PC & MAC / WITH AI
713 visualizações • há 1 dia
Under The Hood
📁Download(CLICK POST):http://youtube.com/post/Ugkxv9Ox_qhfzG9FoCeghSMCDH42yIjgEYub 🔐Password:1885 ⛔ IF YOU HAV
Novo
4 capítulos What will be in the video today | Creative Cloud new | How to download Photoshop 2026 | "Trial period"...



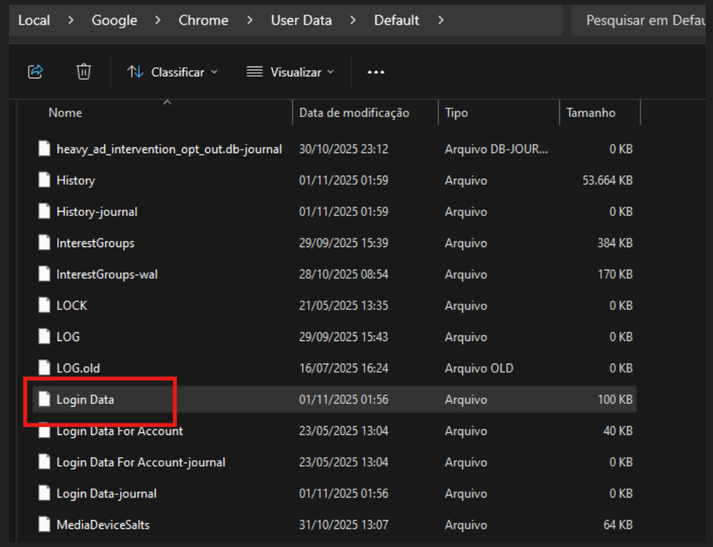
Free Download Adobe Photoshop | Adobe Photoshop Crack | Adobe Photoshop Free Download
Rihan Abbasi • Playlist • Atualizado hoje
G1 · 3:09
30 seconds me skin Finer plugin with photoshop 2020-skin Finer #photoshopplugin #short #plugin · 0:33
Ver playlist completa

Free Download Adobe Acrobat | Adobe Acrobat Free Download | How To Free Download Adobe Acrobat
ROLEX XG • Playlist • Atualizado hoje
G1 · 1:45
How to Download Adobe Acrobat Pro for FREE on PC, LAPTOP & MAC (2025) · 0:46

3) CAPTURA



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



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

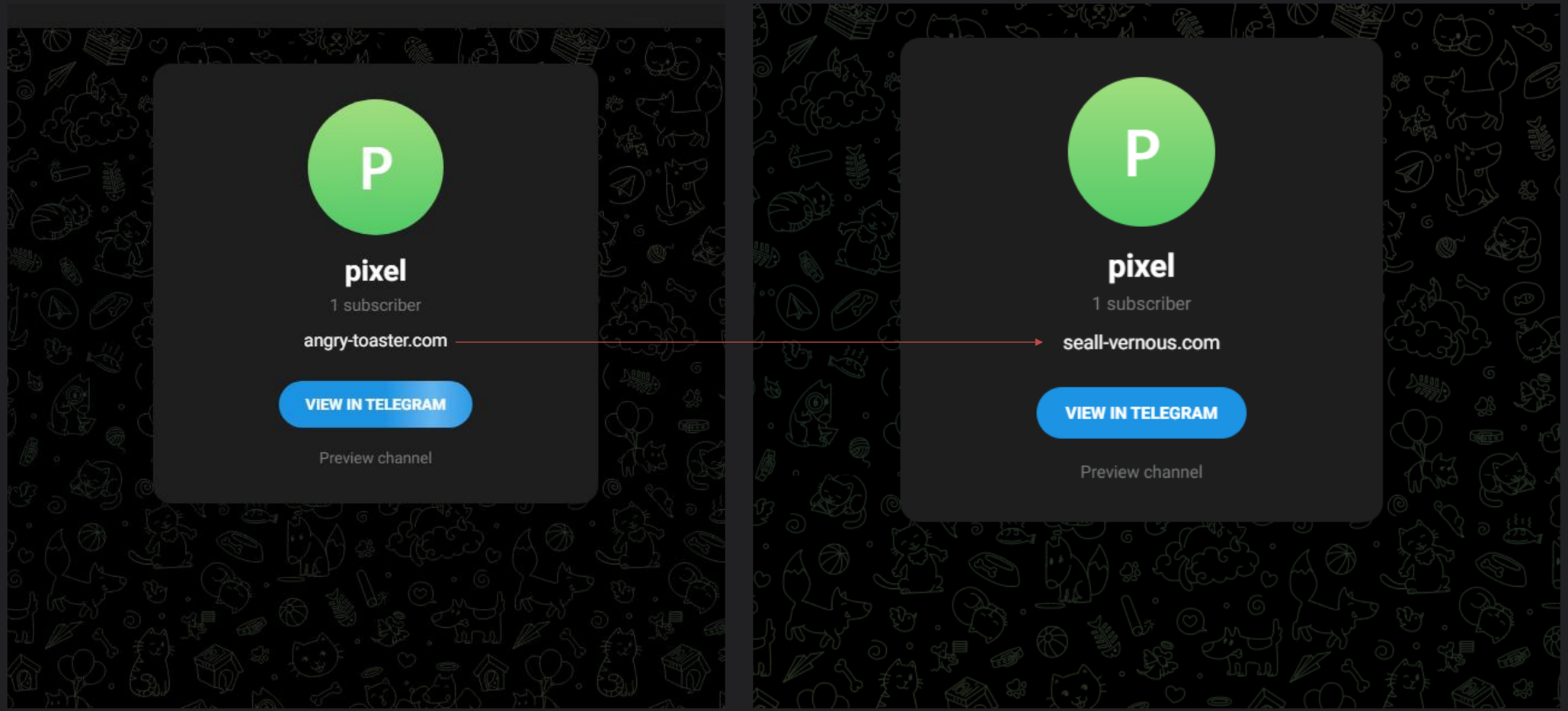
DEAD DROP RESOLVER

[1932] **executavel_temporario.exe** C:\Users\admin\AppData\Local\qiGArqvuPK\executavel_temporario.exe

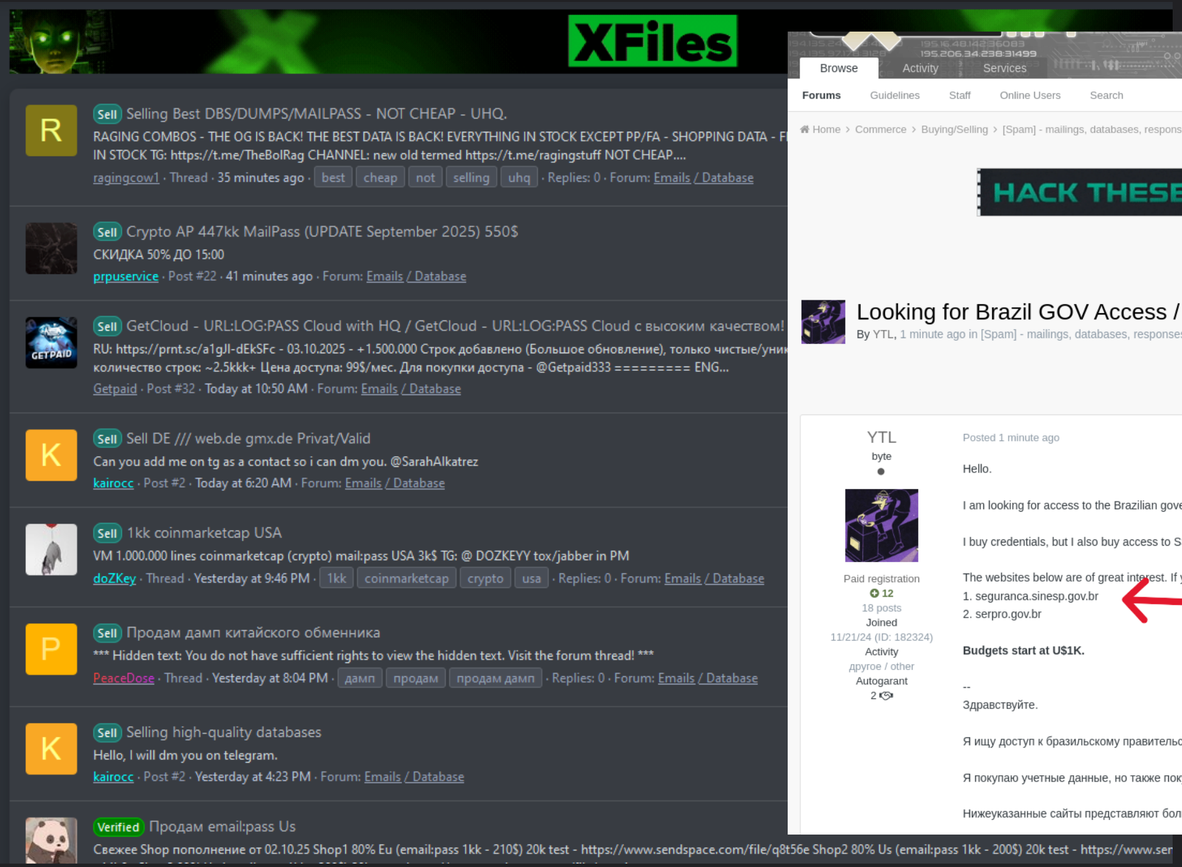
Put the slider in the desired position or select the desired segment by yourself

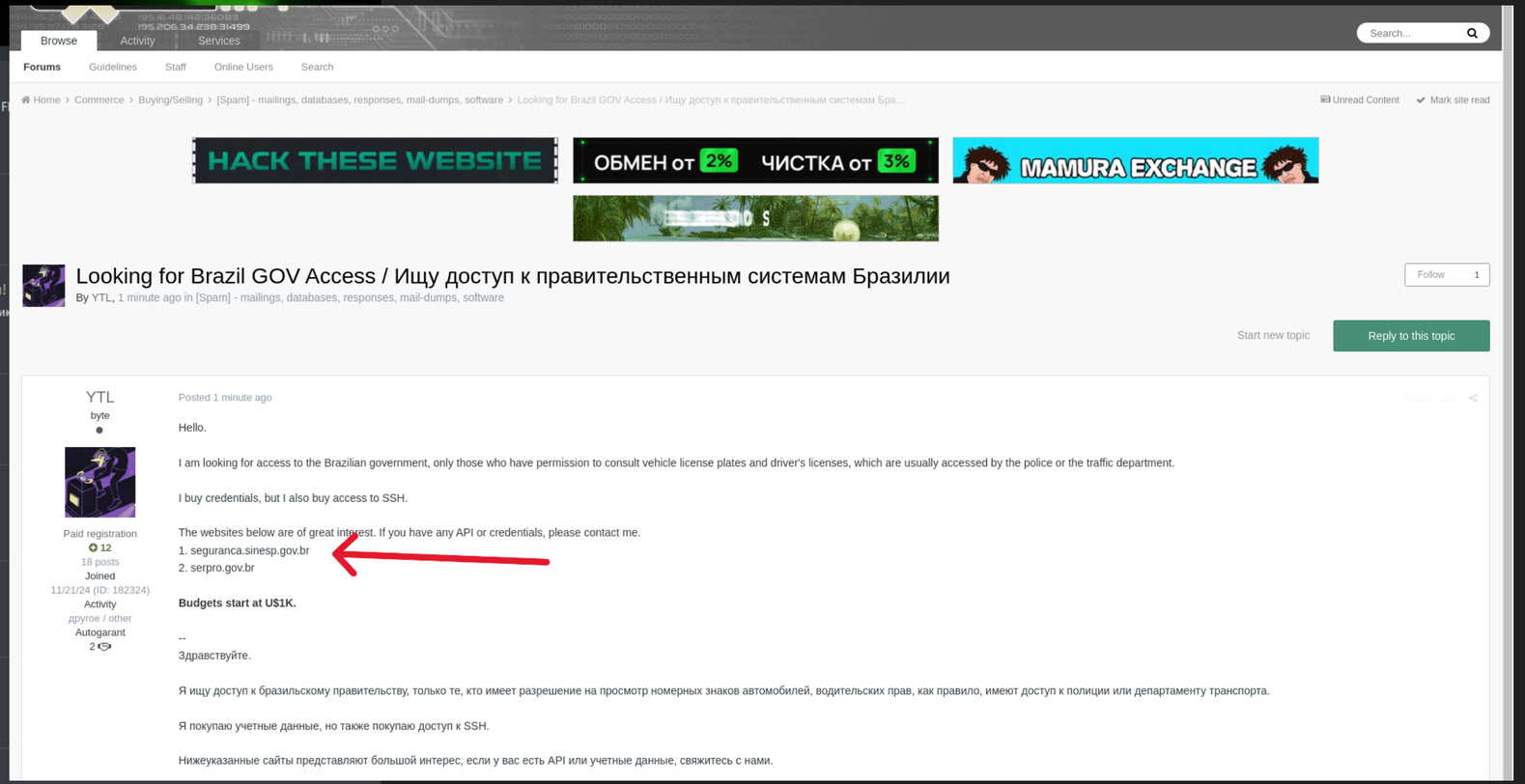
31.275 s

Time	HTTP headers	Reputation	Country	Content	Type
https://t.me/pixel_sunset					
+3555 ms	H1 GET 200: OK	? Unknown	Virgin Islands, British	12 Kb ↓	html
https://hungry-pixel.com/					
+4287 ms	H1 POST No Response	? Unknown	United States		
https://hungry-pixel.com/					
+25077 ms	H1 POST 200: OK	? Unknown	United States	128 Kb ↑ 44 b ↓	binary binary
https://hungry-pixel.com/					
+26248 ms	H1 POST 200: OK	? Unknown	United States	96 b ↑ 44 b ↓	binary binary
https://hungry-pixel.com/					
+26316 ms	H1 POST 200: OK	? Unknown	United States	160 b ↑ 44 b ↓	binary binary
https://hungry-pixel.com/					
+26439 ms	H1 POST 200: OK	? Unknown	United States	176 b ↑	binary


P
pixel
1 subscriber
angry-toaster.com
VIEW IN TELEGRAM
Preview channel
P
pixel
1 subscriber
seall-vernous.com
VIEW IN TELEGRAM
Preview channel

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.

SELLING Brazil National Police Panel Login – LE Account + OTP | Full Country Ac

by potafr - 22-03-26, 11:35 PM

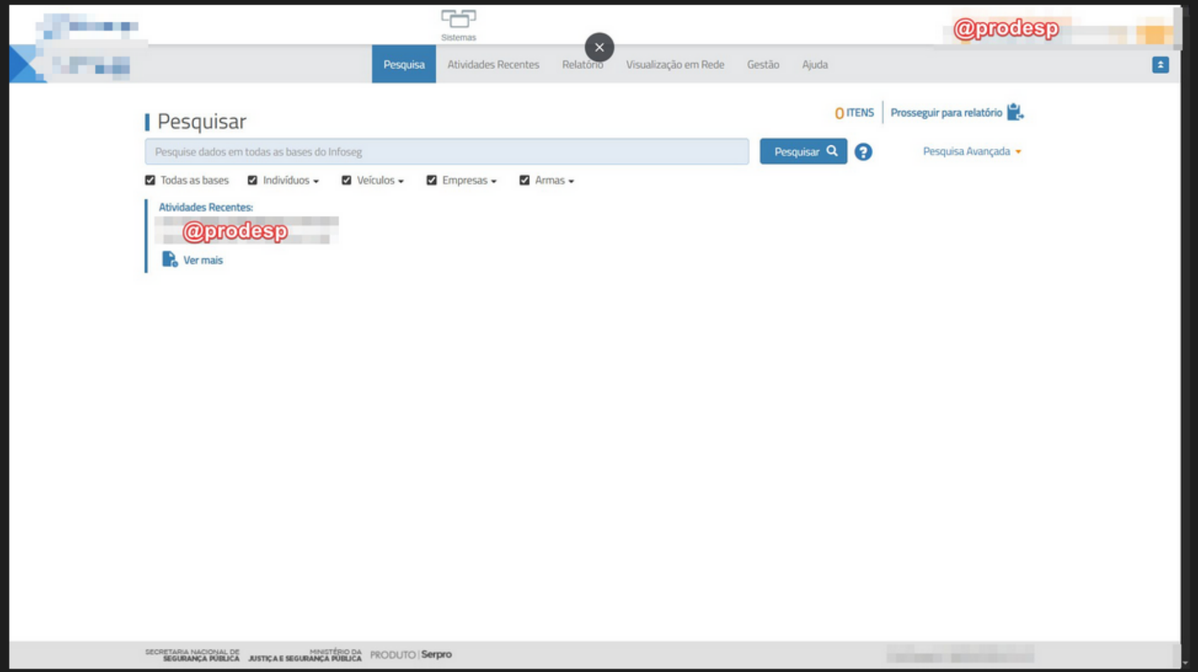
22-03-26, 11:35 PM

potafr

DarkForums Members

Member

Posts 1
Threads 1
Joined Mar 2026
Reputation 0
1 days



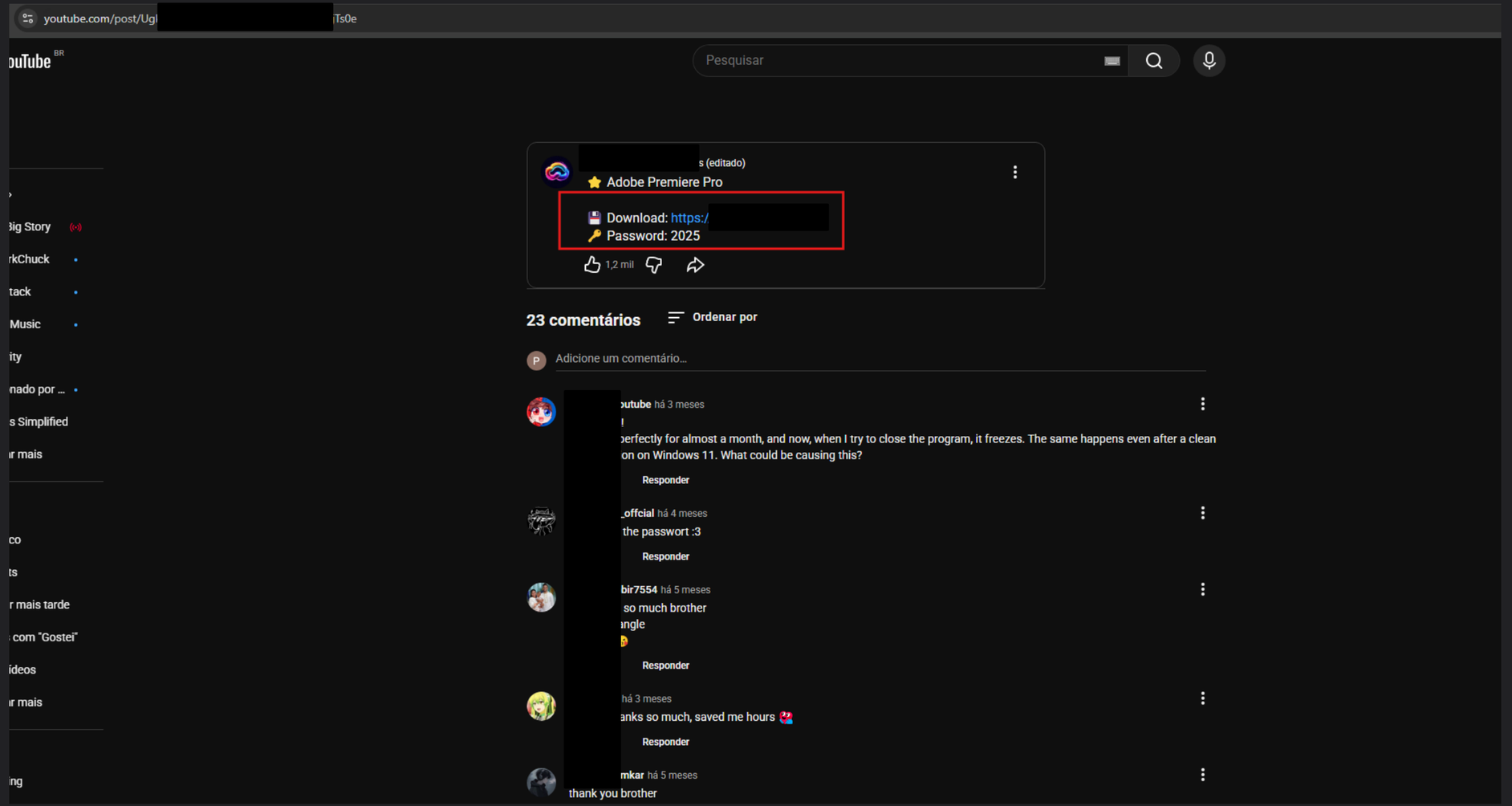
Selling one fresh, active police-level login for Brazil's national restricted LE database panel (used by Federal Police, Civil Police, Military Police, Highway Police, etc.).

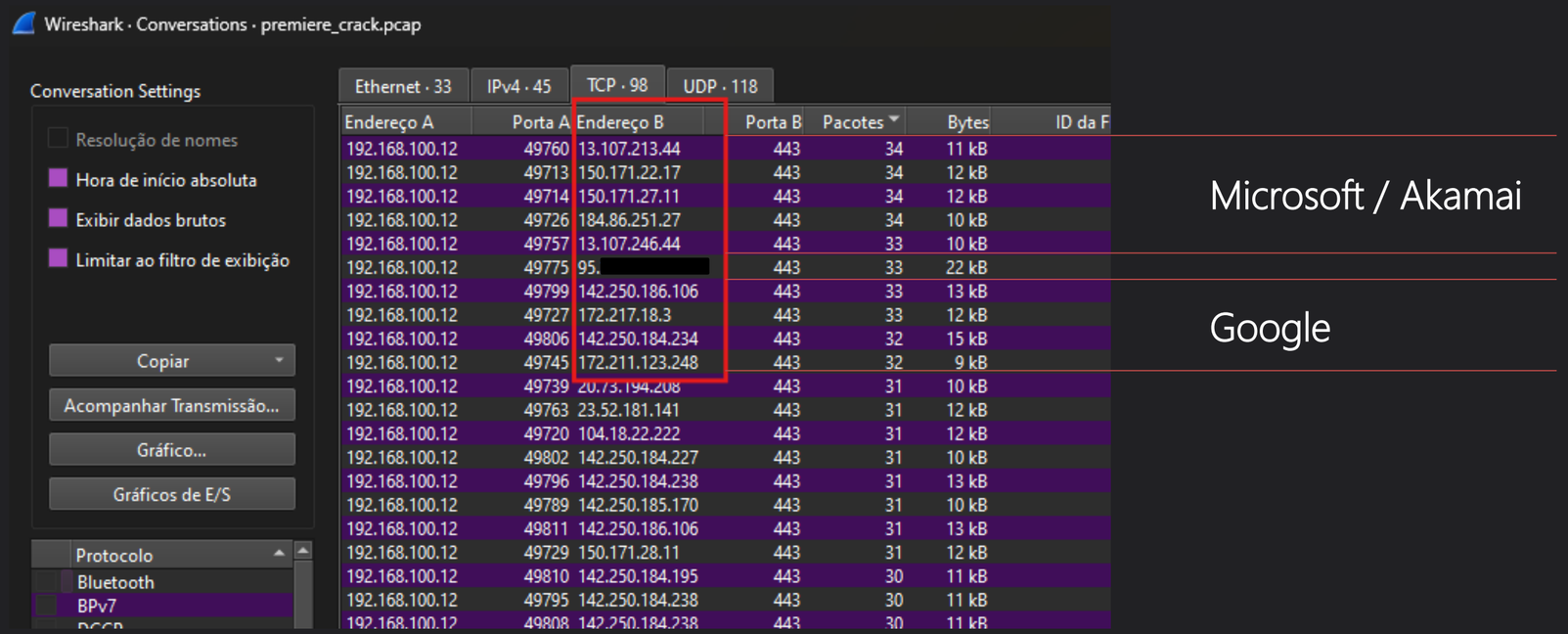
Gets the real CNH driver's license photo (face shot) of literally anyone in Brazil. Nationwide facial pull.

Includes:

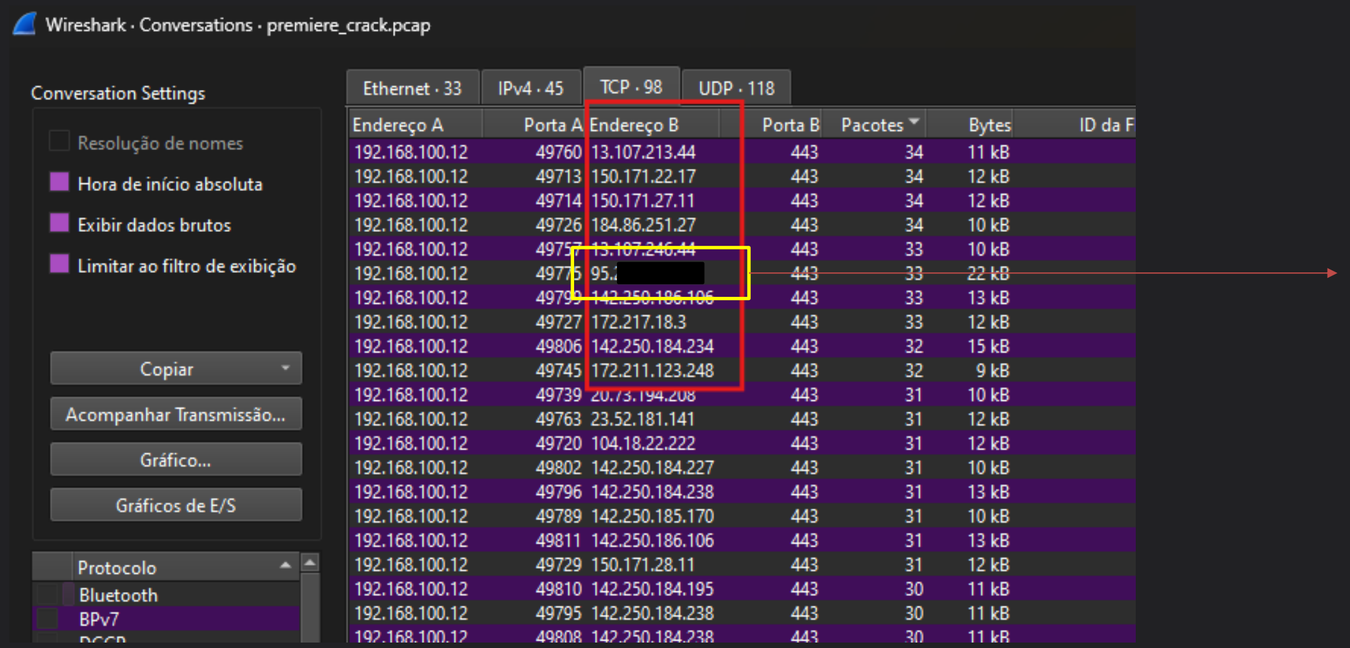
- Full police dashboard
- All integrated national databases (screenshots of the Bases Integradas panel attached – dozens of federal and state sources)
- High query limits
- OTP / 2FA credentials handed over (seed + current code)

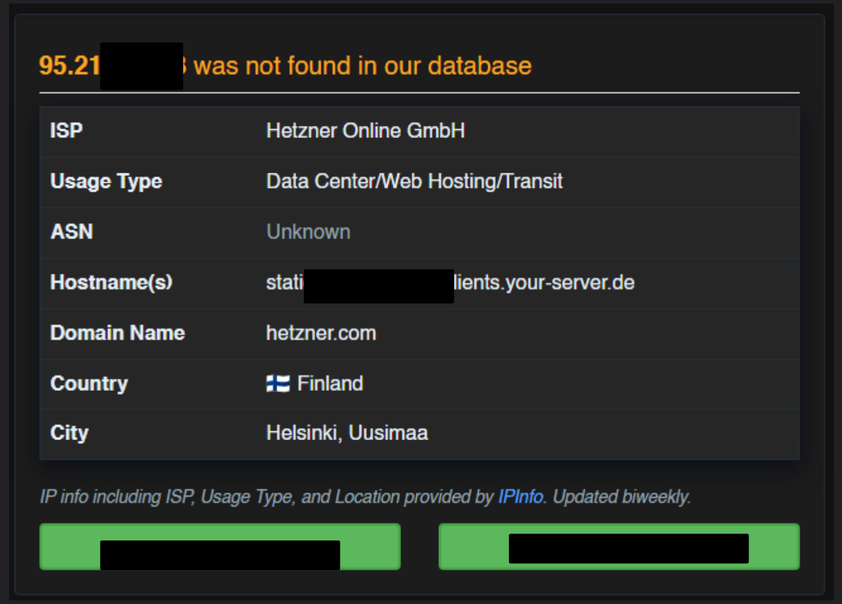
INCIDENTES E O PROBLEMA DA REPUTAÇÃO

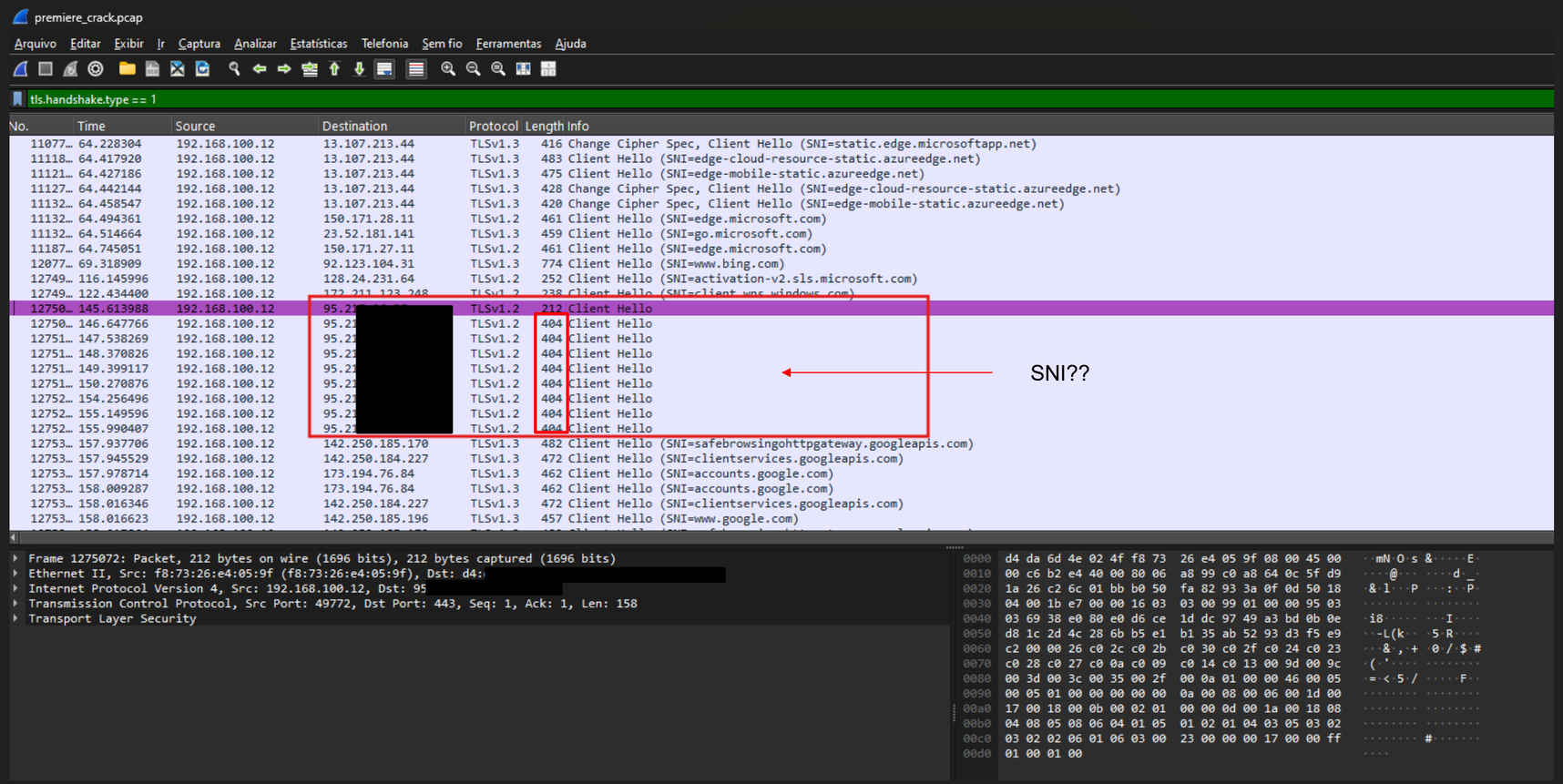

youtube.com/post/Ug
Ts0e
Pesquisar
s (editado)
Adobe Premiere Pro
Download: https:/
Password: 2025
1,2 mil
23 comentários
Ordenar por
Adicione um comentário...
utube há 3 meses
perfectly for almost a month, and now, when I try to close the program, it freezes. The same happens even after a clean
on on 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



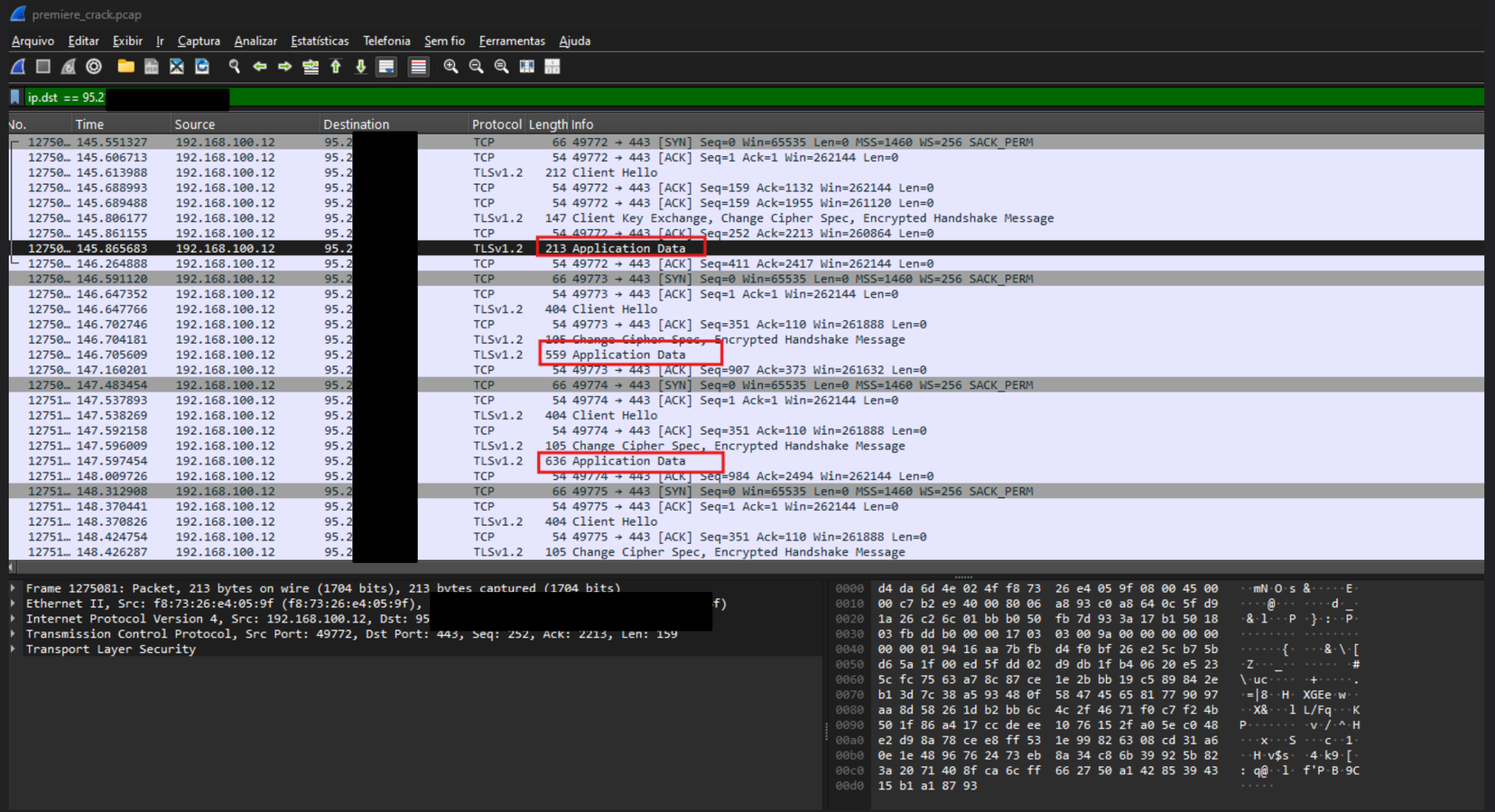
Os principais IPs pertencem a grandes empresas, com exceção a um: 95.[...]


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 | 49775 | 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

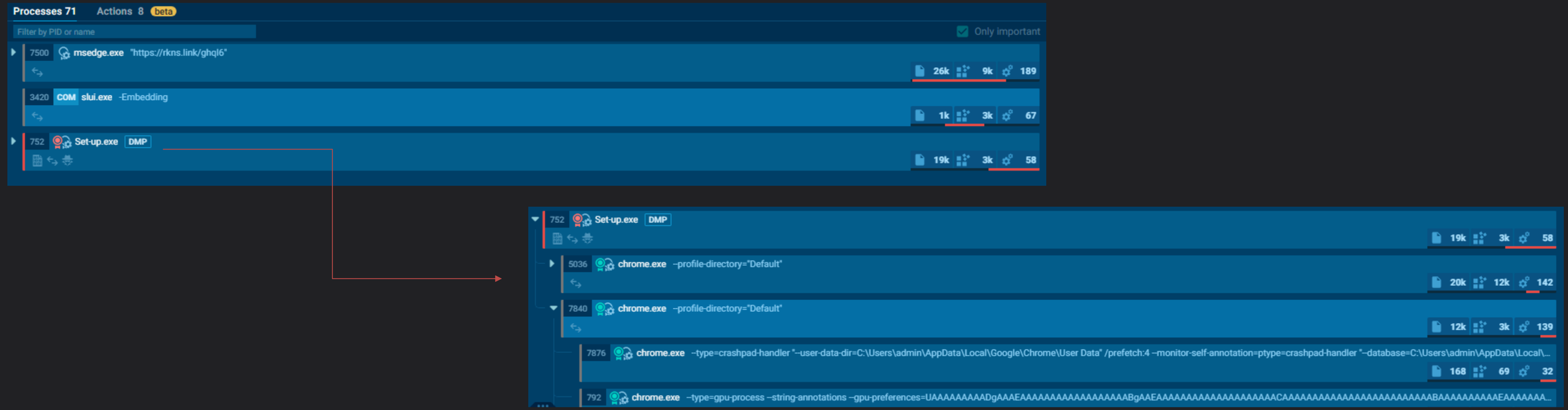

95.21[redacted] was not found in our database
ISP
Hetzner Online GmbH
Usage Type
Data Center/Web Hosting/Transit
ASN
Unknown
Hostname(s)
stati[redacted]lients.your-server.de
Domain Name
hetzner.com
Country
Finland
City
Helsinki, Uusimaa
IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.
[redacted]
[redacted]



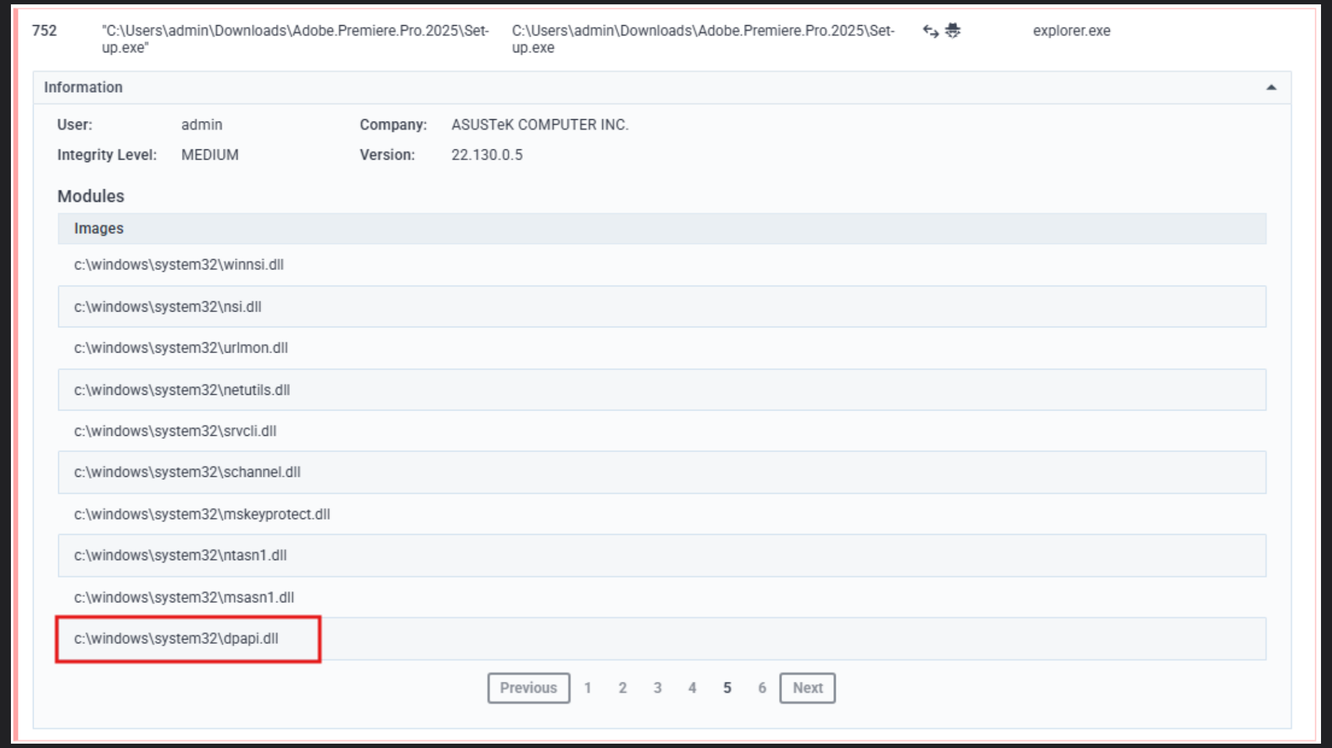
Verificando comunicações TLS sem SNI. Basicamente todo Client Hello legítimo possui a identificação do nome do host



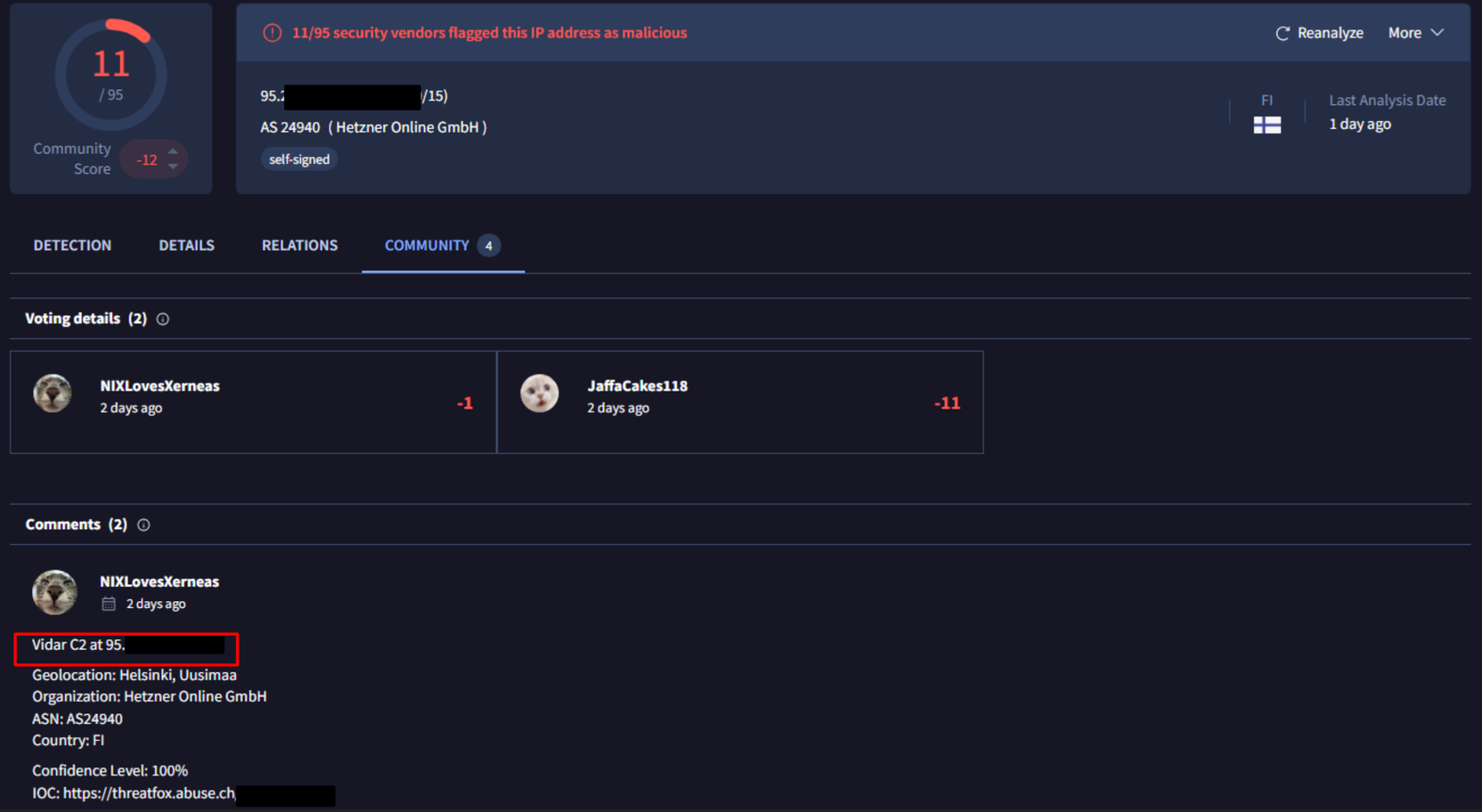
Comunicações constantes com o C2 para envio de dados

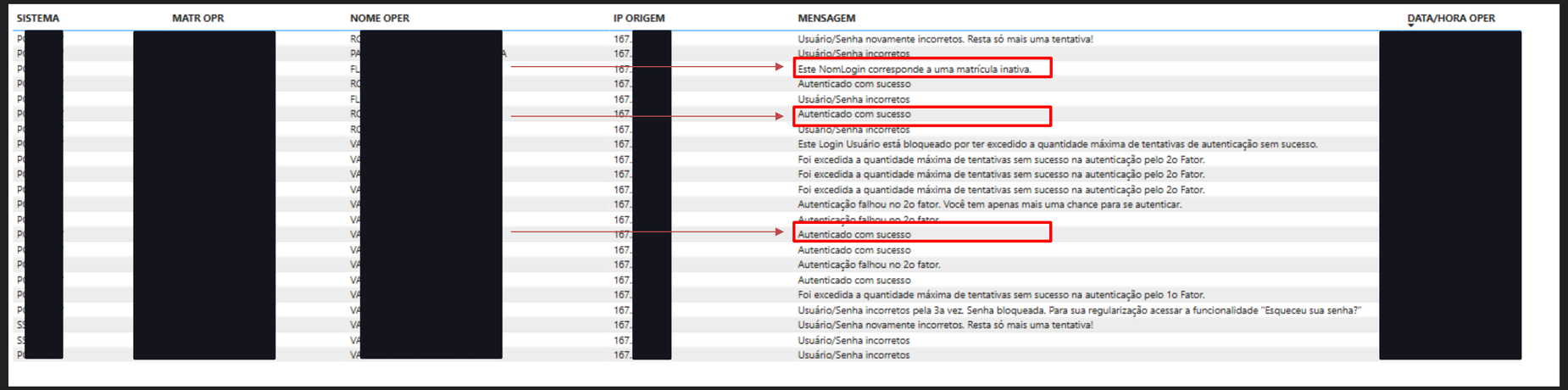


O arquivo malicioso foi baixado pelo EDGE (PID 7500). Ao executar o binário, o processo respectivo (PID 752) criou subprocessos do Chrome (PID 5036 e PID 7840)



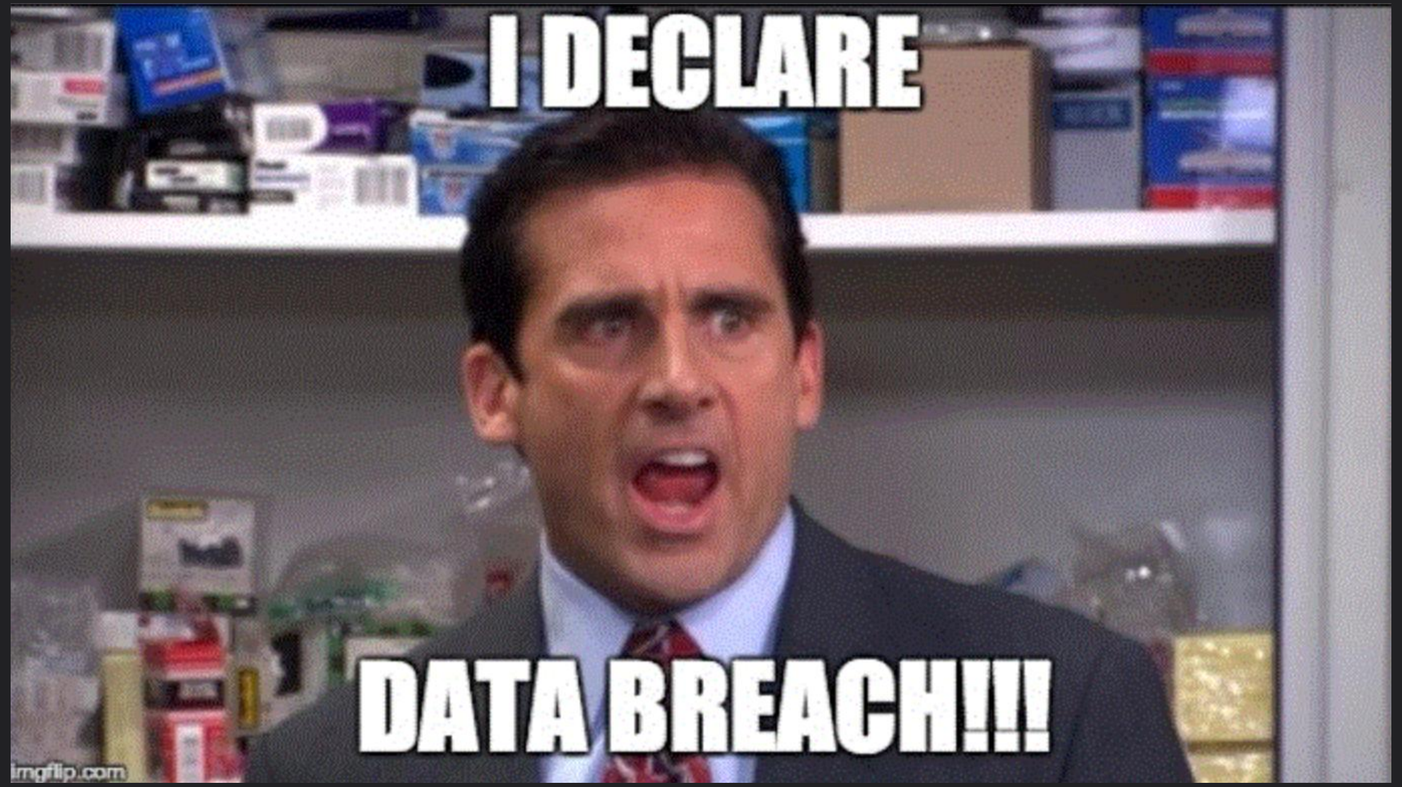
Dentre as DLLs carregadas pelo processo, destaca-se a dpapi.dll


11
/ 95
Community Score
-12
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]



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]	PA	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.

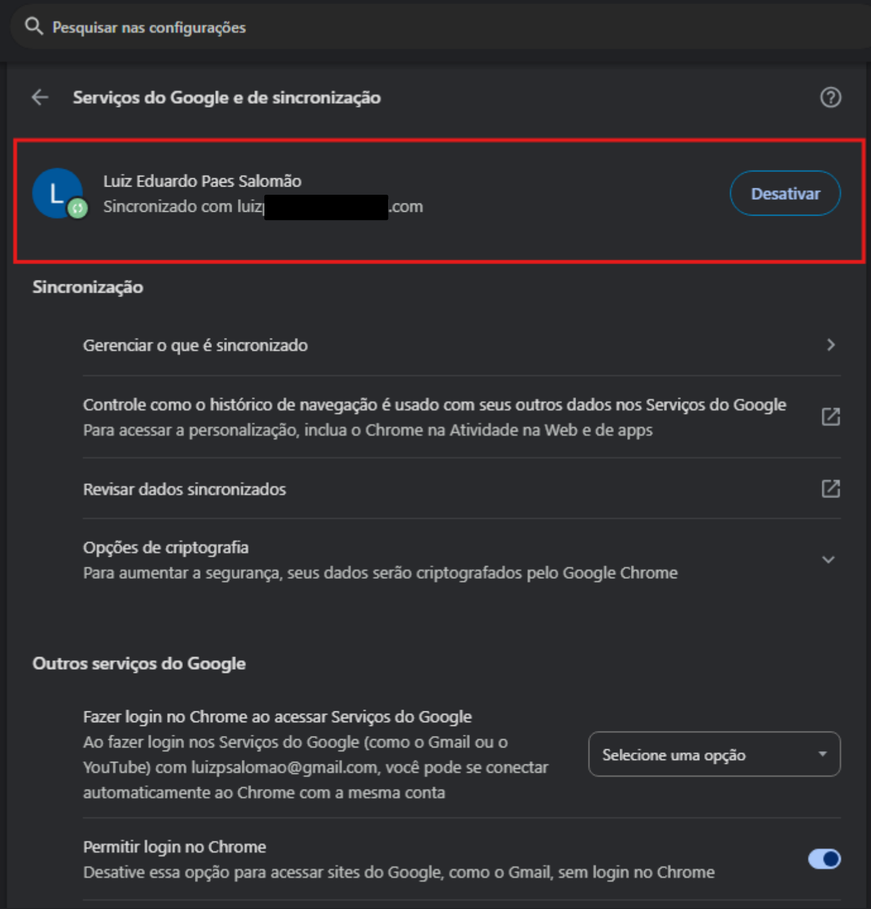
CHANNEL:t.me/+F61qGRd_ic1jZjAy ADMIN:t.me/Emirates_Cloud EMIRATES LINK:t.me/Emirates_Admin

Rhadamanthys Stealer

Install Date: 1[redacted]UTC
Traffic Name: @othertraff
HWID: 3S[redacted]XT
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:

NOME OPER	IP ORIGEM	MENSAGEM
VA[redacted]A	187.121.149.114	Autenticado com sucesso
VA[redacted]A	187.121.149.114	Autenticado com sucesso
VA[redacted]A	187.121.149.114	Autenticado com sucesso
VA[redacted]A	187.121.149.114	Autenticado com sucesso
VA[redacted]A	187.121.149.114	Autenticado com sucesso
VA[redacted]A	187.121.149.114	Autenticado com sucesso

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

CONCLUSÕES

Infostealers modernos frequentemente burlam soluções de antimalware em dispositivos pessoais, mas a exfiltração de dados gera padrões de rede identificáveis (ex: conexões TLS para IPs sem SNI ou domínios de Dead Drop Resolvers)

Plataformas legítimas são frequentemente abusadas para fins ilícitos

Uma rede infestada de dispositivos com infostealers acaba em blacklists globais

Em ambientes de CGNAT, o comportamento malicioso de um único dispositivo infectado pode comprometer a reputação de centenas de usuários que compartilham o mesmo IP público.

PERGUNTAS?