

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



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



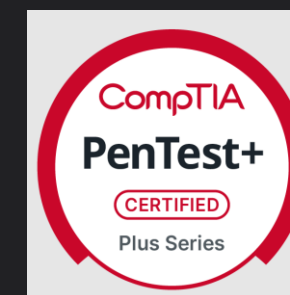
LUIZ EDUARDO SALOMÃO

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.

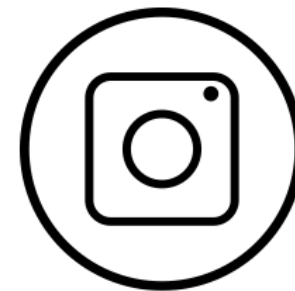
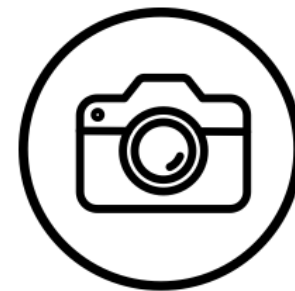


CERT
Incident Response Process Professional
Certificate Holder



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

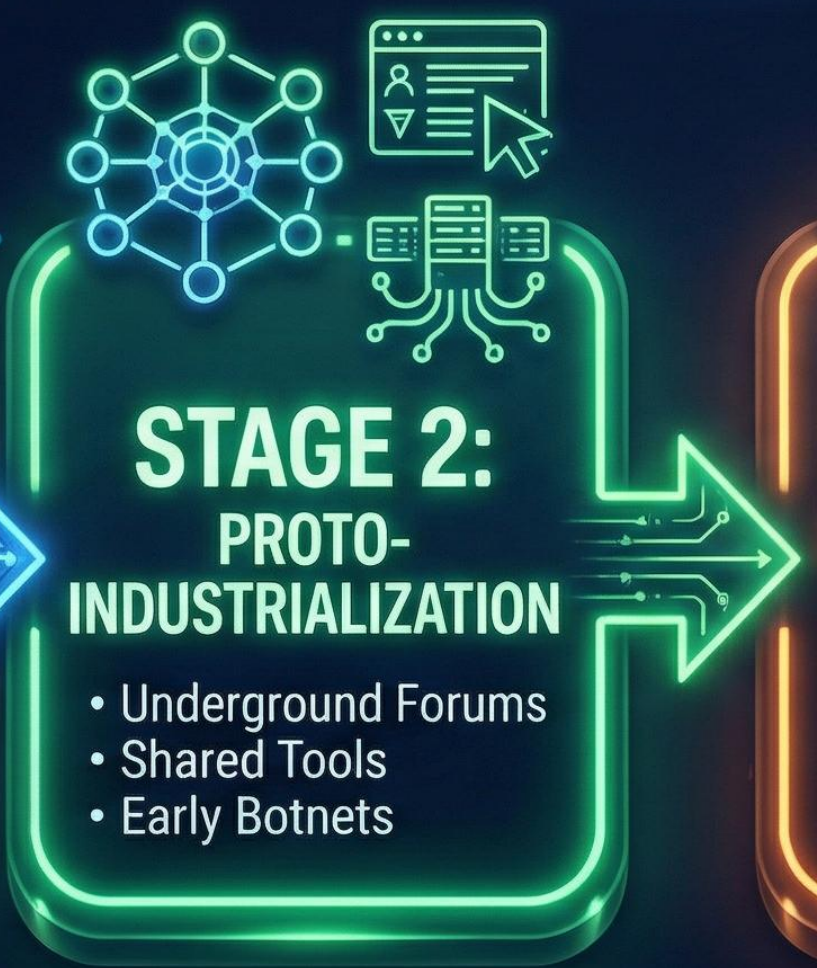


010110 011010
010110 101010
010101 101011
010001 101001
01011 01010
010 110
01

**STAGE 1:
ISOLATED
HACKERS**

- High Expertise
- Generalists
- Low Scale

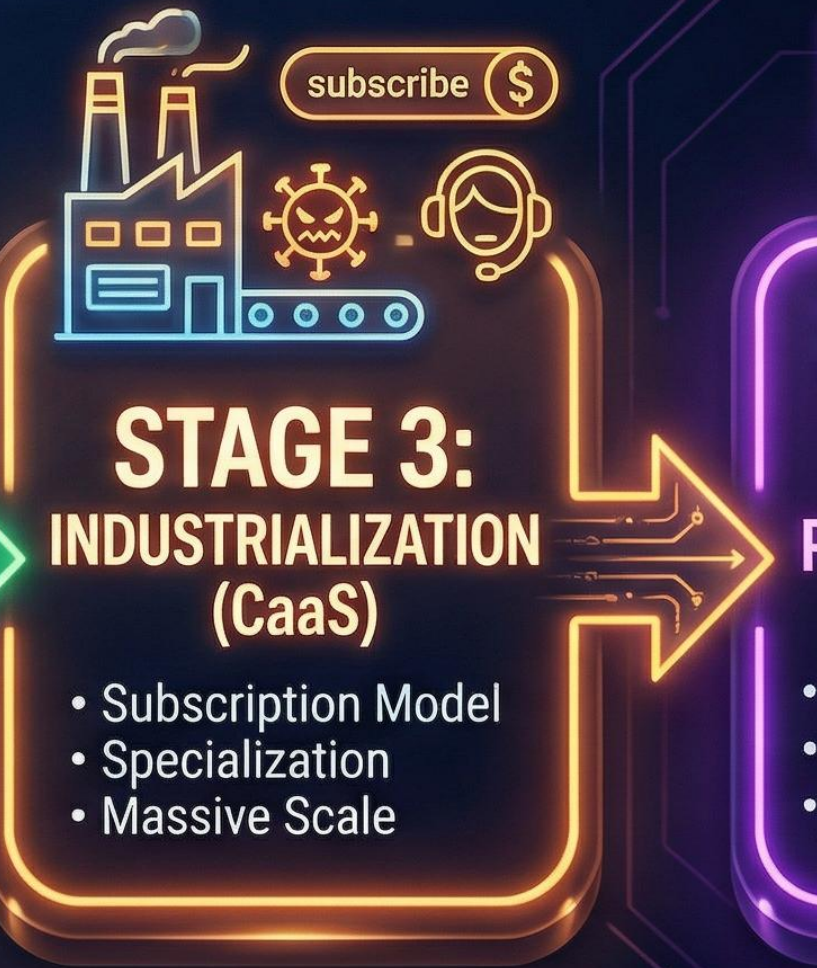
Icon: A hooded hacker sitting at a laptop with binary code floating around.



**STAGE 2:
PROTO-
INDUSTRIALIZATION**

- Underground Forums
- Shared Tools
- Early Botnets

Icon: A network diagram, a web browser window, and a server rack.



**STAGE 3:
INDUSTRIALIZATION
(CaaS)**

- Subscription Model
- Specialization
- Massive Scale

Icon: A factory with smokestacks, a "subscribe" button with a dollar sign, a virus icon, and a headset.



**STAGE 4:
PLATFORMIZATION**

- Integrated Ecosystems
- End-to-End Automation
- IAB + Ransomware

Icon: A stack of blocks labeled "IAB", "Stearler", and "Ransomware", with "Data APIs" labels and a crown on top.

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







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]
Replies: 35 Views: 37K
Thursday at 7:49 PM

- 
Official Stealer
AURA Stealer - Вам это не нужно (Шучу. Нужно. Срочно!)
Replies: 26 Views: 6K
01.02.26

- 
Official Stealer
[XILLEN STEALER V5] HVNC • Keylogger • Crypto Clipper • Wallet Bruteforce | \$200/мес (акция)
Replies: 3 Views: 663
18.01.26


NORMAL THREADS

- 
Official Stealer
Misericorde Stealer(C++ stub) - USER-HOST PANEL / v10&v20 decrypt / FOR ALL 79\$+
Replies: 4 Views: 946
14.01.26

- 
Official Stealer
The Void Stealer - | 80%+ отстук | V20 обход | 20+ браузеров | 100+ расширений | приватный морфер
Replies: 4 Views: 301
Friday at 7:03 AM

- 
Official Stealer
AID_Stealer
Replies: 42 Views: 2K
11.01.26


Santa Stealer - A modern information stealer

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

 **SantaStealer**



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://\[redacted\]](https://[redacted])
For a full list of features, product information and detailed module information visit [https://\[redacted\]](https://[redacted])

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

Santa Stealer

Your #1 Premium Quality Stealer

SantaStealer is a modern information stealer designed to extract every piece of **valuable information** from infected devices at an **affordable price**.

[Purchase Now](#)

[Contact Us](#)



 **General Features** (Included with any plan)

Central de Atendimento

Trabalhamos para você em caráter permanente.



Inscrição

Cadastre-se em nosso portal.



Autorização

Link de autorização



Telegrama

Serviço de suporte.



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 time help is appreciated

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

93bmxvYwQgcm9ibG94IGV4ZWV1dG9y

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



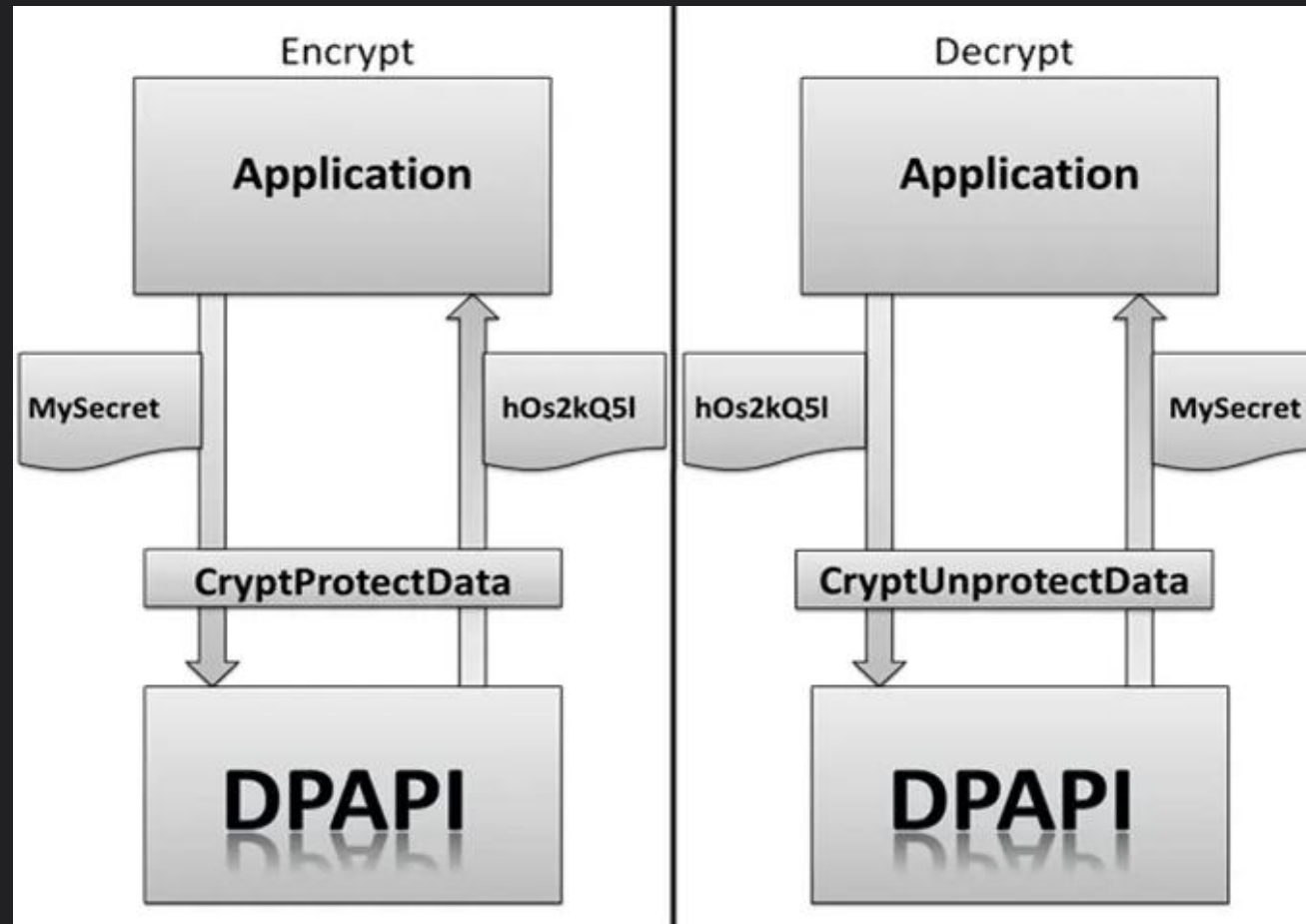
Free Download Adobe Acrobat | Adobe Acrobat Free Download | How To Free Download Adobe Acrobat

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>

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

DEAD DROP RESOLVER

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 +	binary
				44 b ↓	binary
https://hungry-pixel.com/					
+26248 ms	H1 POST 200: OK	? Unknown	United States	96 b +	binary
				44 b ↓	binary
https://hungry-pixel.com/					
+26316 ms	H1 POST 200: OK	? Unknown	United States	160 b +	binary
				44 b ↓	binary
https://hungry-pixel.com/					
+26439 ms	H1 POST 200: OK	? Unknown	United States	176 b +	binary



pixel

1 subscriber

angry-toaster.com

[VIEW IN TELEGRAM](#)

Preview channel



pixel

1 subscriber

seall-vernous.com

[VIEW IN TELEGRAM](#)

Preview channel

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
 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/уники
 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
 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.

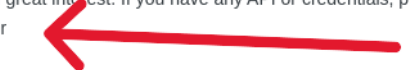
--

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.




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

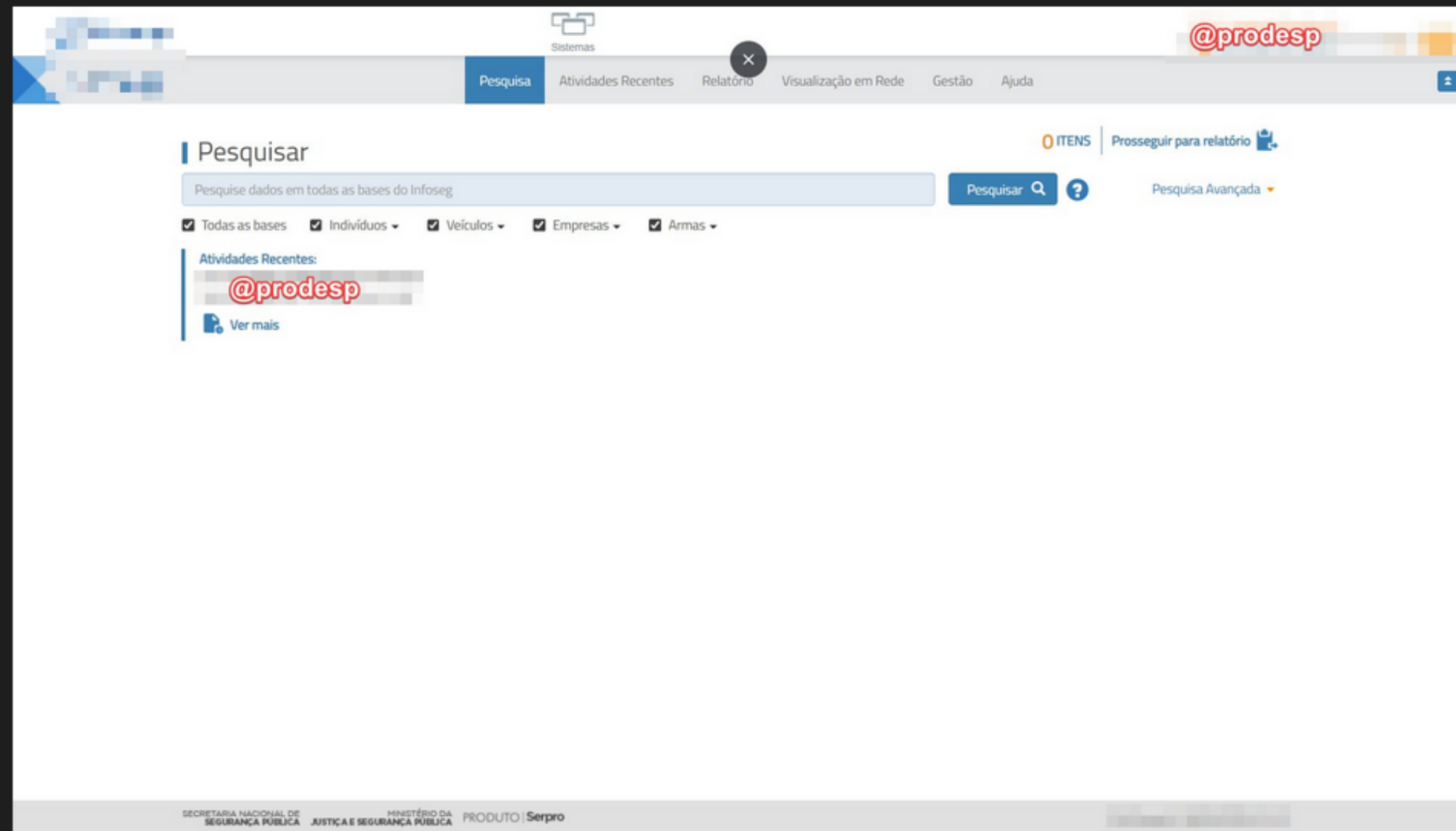


DarkForums Members

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


- Home
- Big Story 
- MrBeast
- MrBeast Gaming
- Music
- Shorts
- Subscriptions
- Library
- History
- Watch later
- Liked videos
- Playlists
- Channels
- Settings
- Help
- Account

 [redacted] (editado) 

★ Adobe Premiere Pro












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

 Password: 2025

 1,2 mil  

23 comentários  Ordenar por

 Adicione um comentário...

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

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

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
- DCCP

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.██████████	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		

Microsoft / Akamai

Google

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

BPv7

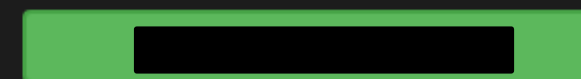
CCP

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.



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	95.213.123.123	TLSv1.2	212	Client Hello
12750...	146.647766	192.168.100.12	95.213.123.123	TLSv1.2	404	Client Hello
12751...	147.538269	192.168.100.12	95.213.123.123	TLSv1.2	404	Client Hello
12751...	148.370826	192.168.100.12	95.213.123.123	TLSv1.2	404	Client Hello
12751...	149.399117	192.168.100.12	95.213.123.123	TLSv1.2	404	Client Hello
12751...	150.270876	192.168.100.12	95.213.123.123	TLSv1.2	404	Client Hello
12752...	154.256496	192.168.100.12	95.213.123.123	TLSv1.2	404	Client Hello
12752...	155.149596	192.168.100.12	95.213.123.123	TLSv1.2	404	Client Hello
12752...	155.990407	192.168.100.12	95.213.123.123	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: d4:1:1:P
 Internet Protocol Version 4, Src: 192.168.100.12, Dst: 95
 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/ghq16"	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

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]

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

NOME OPER	IP ORIGEM	MENSAGEM
VA	187.121.149.114	<i>Autenticado com sucesso</i>
VA	187.121.149.114	<i>Autenticado com sucesso</i>
VA	187.121.149.114	<i>Autenticado com sucesso</i>
VA	187.121.149.114	<i>Autenticado com sucesso</i>
VA	187.121.149.114	<i>Autenticado com sucesso</i>
VA	187.121.149.114	<i>Autenticado com sucesso</i>

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?