Ransomware en Iberoamérica

Un clic, una catástrofe: así empieza el ransomware.

Por: David Ramos

MistiHack 2025

$whoami

David Ramos Rodriguez (Aka. D0V0)

Digital Forensics Specialist at Lazarus Technology

Coordinador CiberSecUNI
CPTE | CTIA | DFE | eJPT | SC-900 | ISO | SSYB | SFC
Systems Engineering - UNI (⏳)

- 🌎 Advance CTF Ekoparty 2025 - Buenos Aires, Argentina - 2do Puesto
- 🌎 International Cybersecurity Challenge 2024 - Santiago de Chile - 6to Puesto.
- 🌎 CyberChallenge 2024 OEA - San José, Costa Rica - 2do Puesto.
- 🌎 CTF Pacifico Seguros Prima AFP - Lima, Perú - 1er Puesto.
- 🌎 International Cybersecurity Challenge 2023 - San Diego, USA - 6to Puesto.
- 🌎 OEA CyberChallenge 2023 - Santiago de Chile - 2do Puesto.
- 🌎 CTF Metared Internacional - Perú 2022 | 2023 | 2024 - 1er Puesto.
- 🚃 Entre otros

Participant in OAS Cybersecurity Program
HackTheBox #Top10 Perú

HACKTHEBOX

<CIBERSEC> UNI

“El hacking descubre la grieta en el sistema; el forense reconstruye la historia que intentaron borrar.”

Contenido

Instructor: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

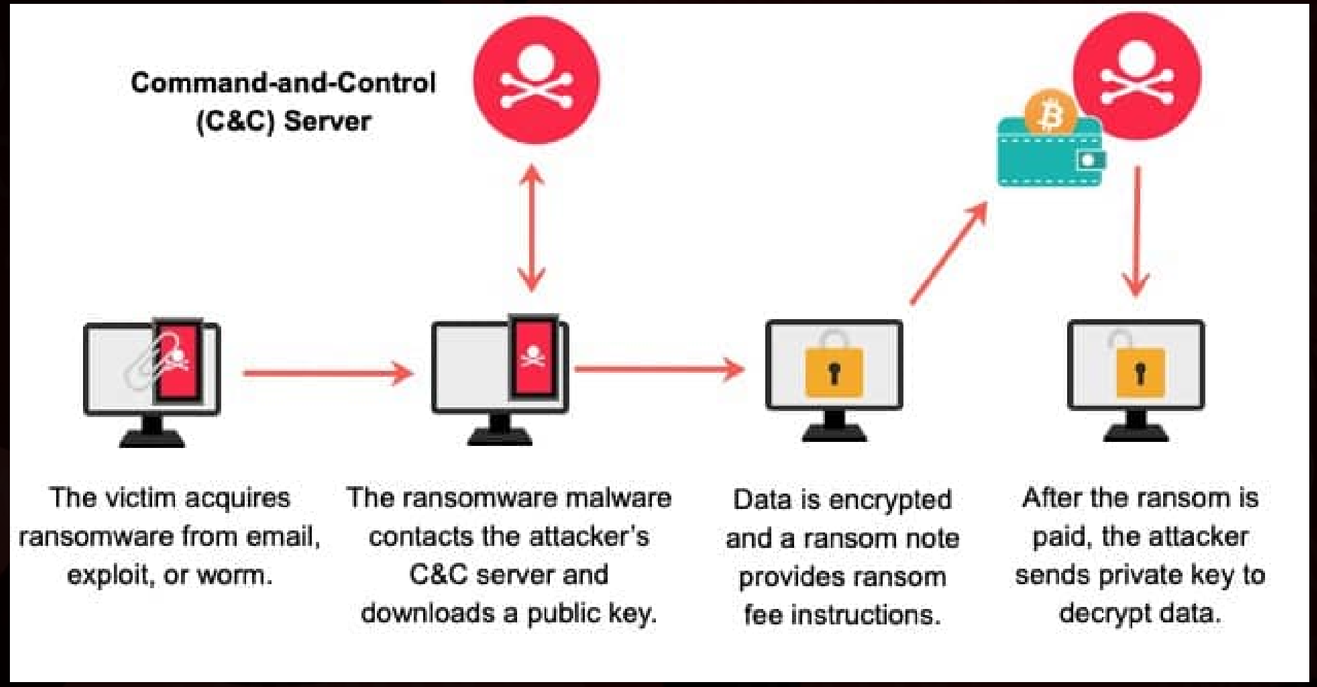
¿Qué es un Ransomware?

No es una amenaza futura; es la epidemia digital de hoy.

Instructor: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

El ransomware es un tipo de software malicioso que bloquea el acceso a archivos o sistemas mediante cifrado, y exige un pago (ransom) para liberarlos.

- **Infección:** El ransomware llega a través de phishing, descargas maliciosas, vulnerabilidades, etc.
- **Ejecución:** El malware se instala, se propaga por la red y espera el mejor momento.
- **Cifrado:** Archivos y sistemas quedan inaccesibles; la víctima pierde control total.
- **Nota de rescate:** Aparece un mensaje exigiendo un pago, generalmente en criptomonedas.
- **Amenazas adicionales**: Muchos grupos también roban datos y amenazan con publicarlos si no se paga (doble o triple extorsión).



Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

El Ransomware en cifras

Los números no mienten: el ransomware ya es una industria criminal multimillonaria.

Instructor: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Crowdstrike - LATAM Regional Threat Landscape Report

Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Crowdstrike - LATAM Regional Threat Landscape Report

Ponente: David Ramos
https://www.linkedin.com/in/david-ramos-rodriguez/

Principales vectores de entrada

Stealers

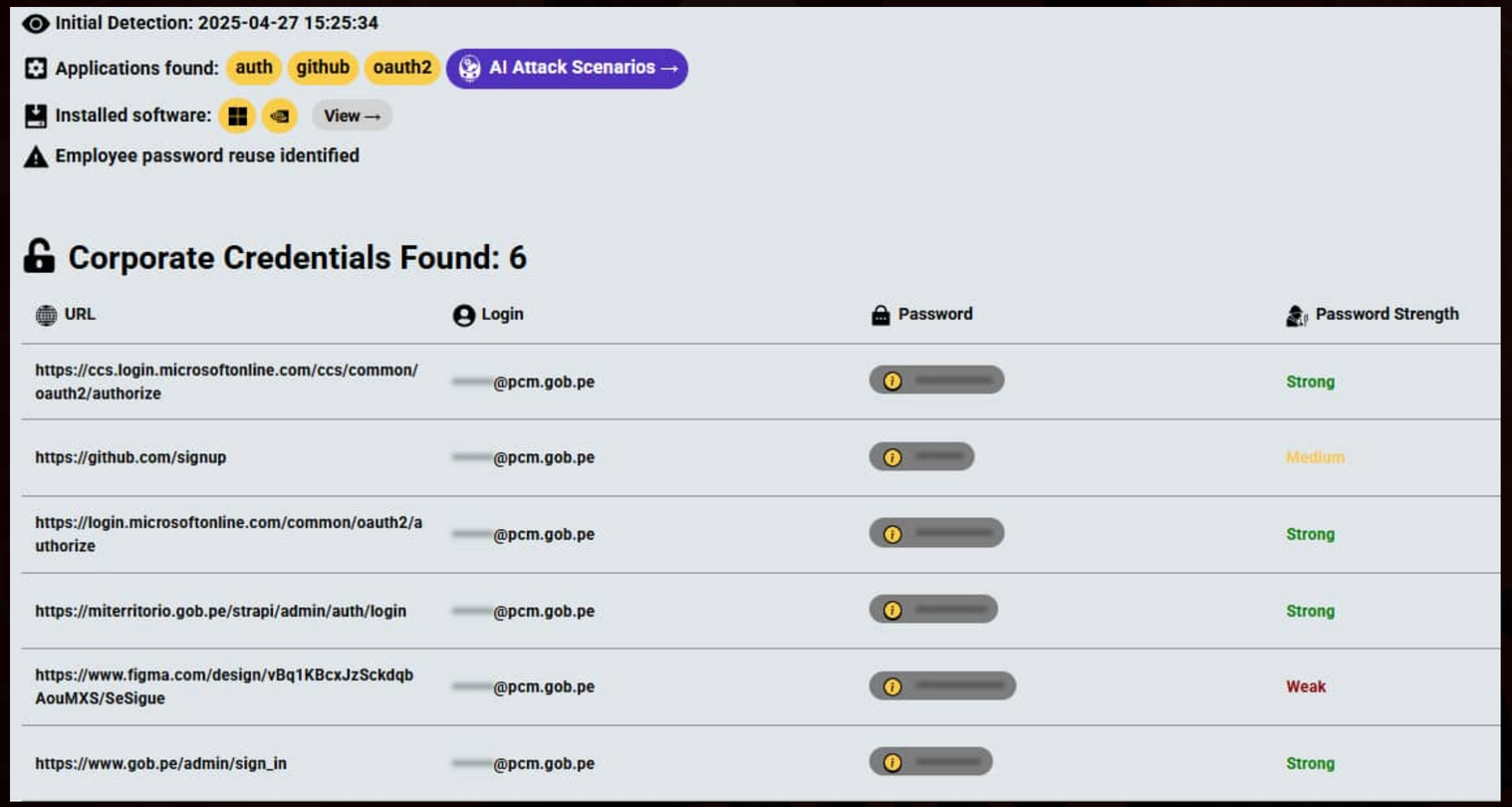
- *Cuentas VPN.*
- *Cuentas RDP.*

0DayExploits

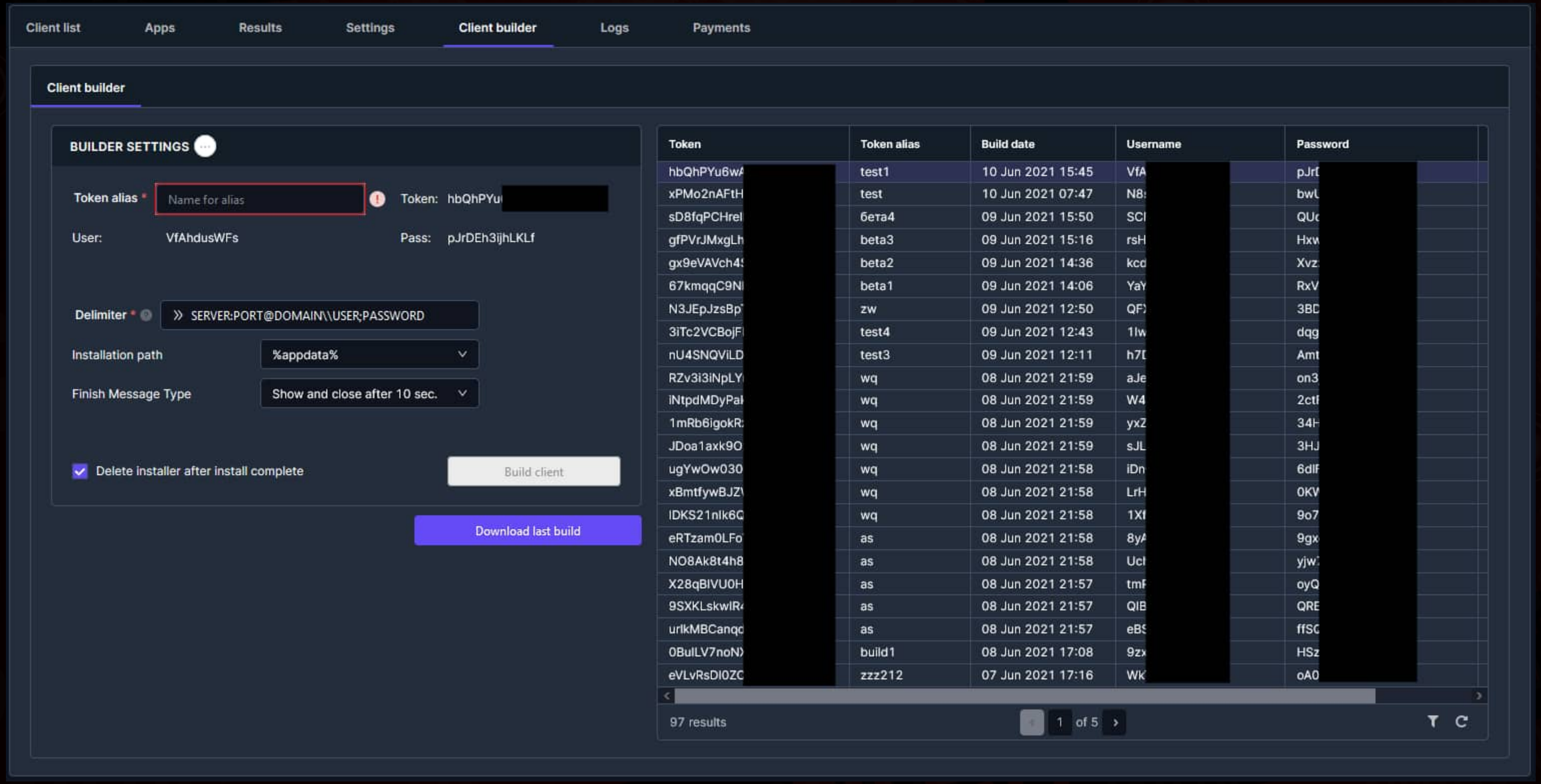
- *Firewalls (Fortinet, Citrix, etc.)*
- *VMware ESXi.*

Phishing

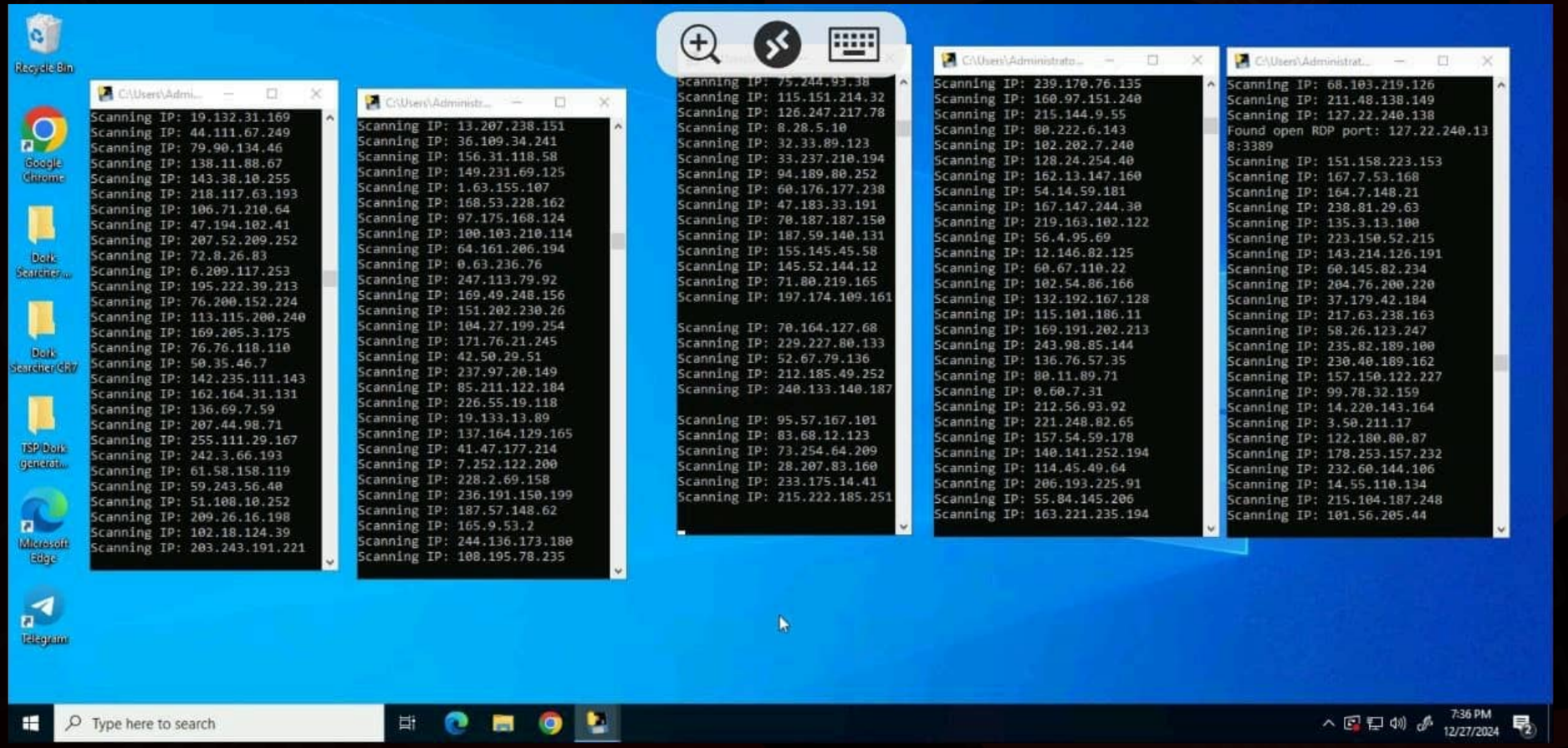
- *SpearPhishing.*
- *Sitios de descarga.*

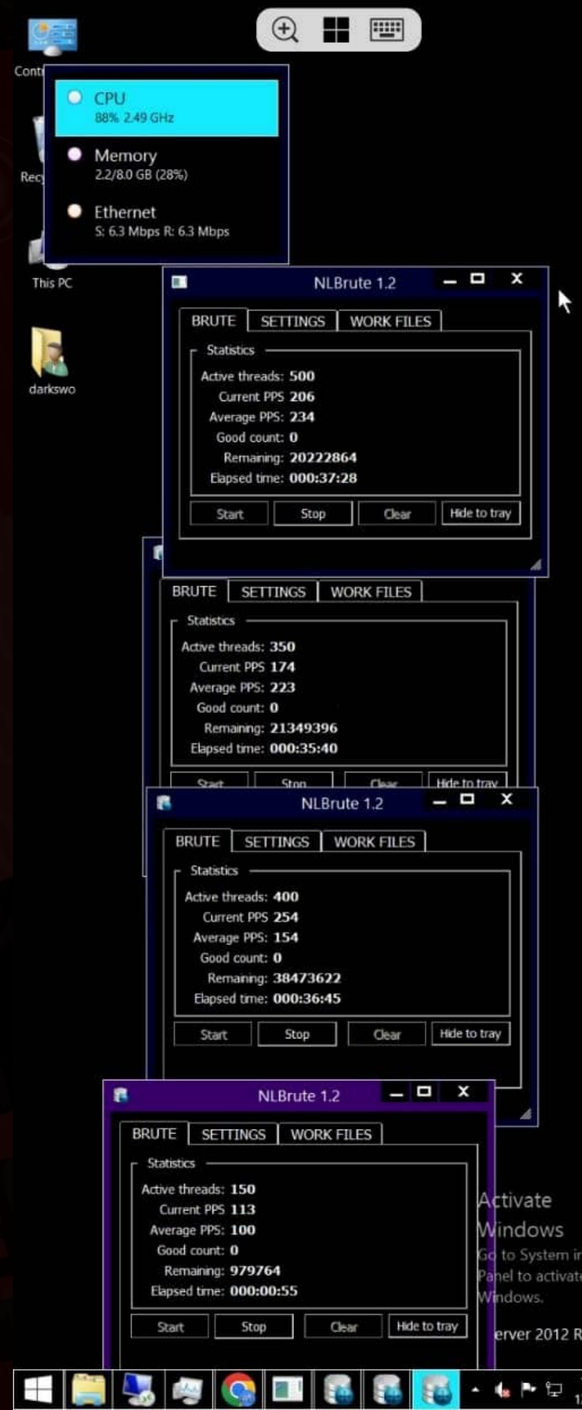


NLBrute 1.2

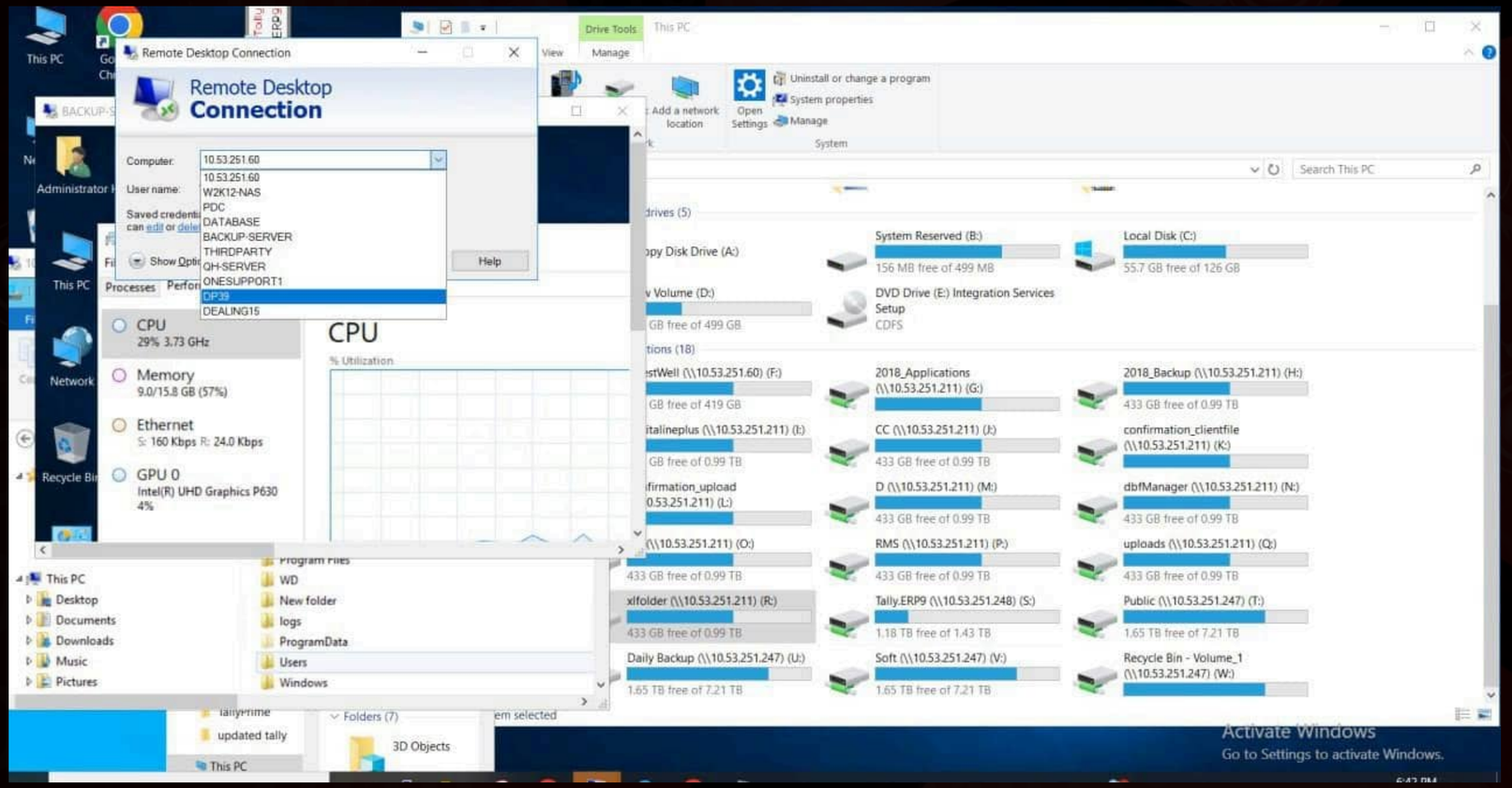

Client list
Apps
Results
Settings
Client builder
Logs
Payments
Client builder
BUILDER SETTINGS
Token alias *
Name for alias
Token: hbQhPYu
User: VfAhdusWFs
Pass: pJrDEh3ijhLKLf
Delimiter *
» SERVER:PORT@DOMAIN\\USER;PASSWORD
Installation path
%appdata%
Finish Message Type
Show and close after 10 sec.
Delete installer after install complete
Build client
Download last build
Token
Token alias
Build date
Username
Password
test1 10 Jun 2021 15:45
test 10 Jun 2021 07:47
бета4 09 Jun 2021 15:50
beta3 09 Jun 2021 15:16
beta2 09 Jun 2021 14:36
beta1 09 Jun 2021 14:06
zw 09 Jun 2021 12:50
test4 09 Jun 2021 12:43
test3 09 Jun 2021 12:11
wq 08 Jun 2021 21:59
wq 08 Jun 2021 21:59
wq 08 Jun 2021 21:59
wq 08 Jun 2021 21:59
wq 08 Jun 2021 21:58
wq 08 Jun 2021 21:58
wq 08 Jun 2021 21:58
as 08 Jun 2021 21:58
as 08 Jun 2021 21:58
as 08 Jun 2021 21:57
as 08 Jun 2021 21:57
as 08 Jun 2021 21:57
build1 08 Jun 2021 17:08
zzz212 07 Jun 2021 17:16
97 results
1 of 5

NLBrute 1.2


Recycle Bin
Google Chrome
Dork Searcher ...
Dork Searcher CR7
TSP Dork generat...
Microsoft Edge
Telegram
Scanning IP: 19.132.31.169
Scanning IP: 44.111.67.249
Scanning IP: 79.90.134.46
Scanning IP: 138.11.88.67
Scanning IP: 143.38.10.255
Scanning IP: 218.117.63.193
Scanning IP: 106.71.210.64
Scanning IP: 47.194.102.41
Scanning IP: 207.52.209.252
Scanning IP: 72.8.26.83
Scanning IP: 6.209.117.253
Scanning IP: 195.222.39.213
Scanning IP: 76.200.152.224
Scanning IP: 113.115.200.240
Scanning IP: 169.205.3.175
Scanning IP: 76.76.118.110
Scanning IP: 50.35.46.7
Scanning IP: 142.235.111.143
Scanning IP: 162.164.31.131
Scanning IP: 136.69.7.59
Scanning IP: 207.44.98.71
Scanning IP: 255.111.29.167
Scanning IP: 242.3.66.193
Scanning IP: 61.58.158.119
Scanning IP: 59.243.56.40
Scanning IP: 51.108.10.252
Scanning IP: 209.26.16.198
Scanning IP: 102.18.124.39
Scanning IP: 203.243.191.221
Scanning IP: 13.207.238.151
Scanning IP: 36.109.34.241
Scanning IP: 156.31.118.58
Scanning IP: 149.231.69.125
Scanning IP: 1.63.155.107
Scanning IP: 168.53.228.162
Scanning IP: 97.175.168.124
Scanning IP: 100.103.210.114
Scanning IP: 64.161.206.194
Scanning IP: 0.63.236.76
Scanning IP: 247.113.79.92
Scanning IP: 169.49.248.156
Scanning IP: 151.202.230.26
Scanning IP: 104.27.199.254
Scanning IP: 171.76.21.245
Scanning IP: 42.50.29.51
Scanning IP: 237.97.20.149
Scanning IP: 85.211.122.184
Scanning IP: 226.55.19.118
Scanning IP: 19.133.13.89
Scanning IP: 137.164.129.165
Scanning IP: 41.47.177.214
Scanning IP: 7.252.122.200
Scanning IP: 228.2.69.158
Scanning IP: 236.191.150.199
Scanning IP: 187.57.148.62
Scanning IP: 165.9.53.2
Scanning IP: 244.136.173.180
Scanning IP: 108.195.78.235
Scanning IP: 115.151.214.32
Scanning IP: 126.247.217.78
Scanning IP: 8.28.5.10
Scanning IP: 32.33.89.123
Scanning IP: 33.237.210.194
Scanning IP: 94.189.80.252
Scanning IP: 60.176.177.238
Scanning IP: 47.183.33.191
Scanning IP: 70.187.187.150
Scanning IP: 187.59.140.131
Scanning IP: 155.145.45.58
Scanning IP: 145.52.144.12
Scanning IP: 71.80.219.165
Scanning IP: 197.174.109.161
Scanning IP: 70.164.127.68
Scanning IP: 229.227.80.133
Scanning IP: 52.67.79.136
Scanning IP: 212.185.49.252
Scanning IP: 240.133.140.187
Scanning IP: 95.57.167.101
Scanning IP: 83.68.12.123
Scanning IP: 73.254.64.209
Scanning IP: 28.207.83.160
Scanning IP: 233.175.14.41
Scanning IP: 215.222.185.251
Scanning IP: 239.170.76.135
Scanning IP: 160.97.151.240
Scanning IP: 215.144.9.55
Scanning IP: 80.222.6.143
Scanning IP: 102.202.7.240
Scanning IP: 128.24.254.40
Scanning IP: 162.13.147.160
Scanning IP: 54.14.59.181
Scanning IP: 167.147.244.30
Scanning IP: 219.163.102.122
Scanning IP: 56.4.95.69
Scanning IP: 12.146.82.125
Scanning IP: 60.67.110.22
Scanning IP: 102.54.86.166
Scanning IP: 132.192.167.128
Scanning IP: 115.101.186.11
Scanning IP: 169.191.202.213
Scanning IP: 243.98.85.144
Scanning IP: 136.76.57.35
Scanning IP: 80.11.89.71
Scanning IP: 0.60.7.31
Scanning IP: 212.56.93.92
Scanning IP: 221.248.82.65
Scanning IP: 157.54.59.178
Scanning IP: 140.141.252.194
Scanning IP: 114.45.49.64
Scanning IP: 206.193.225.91
Scanning IP: 55.84.145.206
Scanning IP: 163.221.235.194
Scanning IP: 68.103.219.126
Scanning IP: 211.48.138.149
Scanning IP: 127.22.240.138
Found open RDP port: 127.22.240.138:3389
Scanning IP: 151.158.223.153
Scanning IP: 167.7.53.168
Scanning IP: 164.7.148.21
Scanning IP: 238.81.29.63
Scanning IP: 135.3.13.100
Scanning IP: 223.150.52.215
Scanning IP: 143.214.126.191
Scanning IP: 60.145.82.234
Scanning IP: 204.76.200.220
Scanning IP: 37.179.42.184
Scanning IP: 217.63.238.163
Scanning IP: 58.26.123.247
Scanning IP: 235.82.189.100
Scanning IP: 230.40.189.162
Scanning IP: 157.150.122.227
Scanning IP: 99.78.32.159
Scanning IP: 14.220.143.164
Scanning IP: 3.50.211.17
Scanning IP: 122.180.80.87
Scanning IP: 178.253.157.232
Scanning IP: 232.60.144.106
Scanning IP: 14.55.110.134
Scanning IP: 215.104.187.248
Scanning IP: 101.56.205.44
Type here to search
7:36 PM
12/27/2024

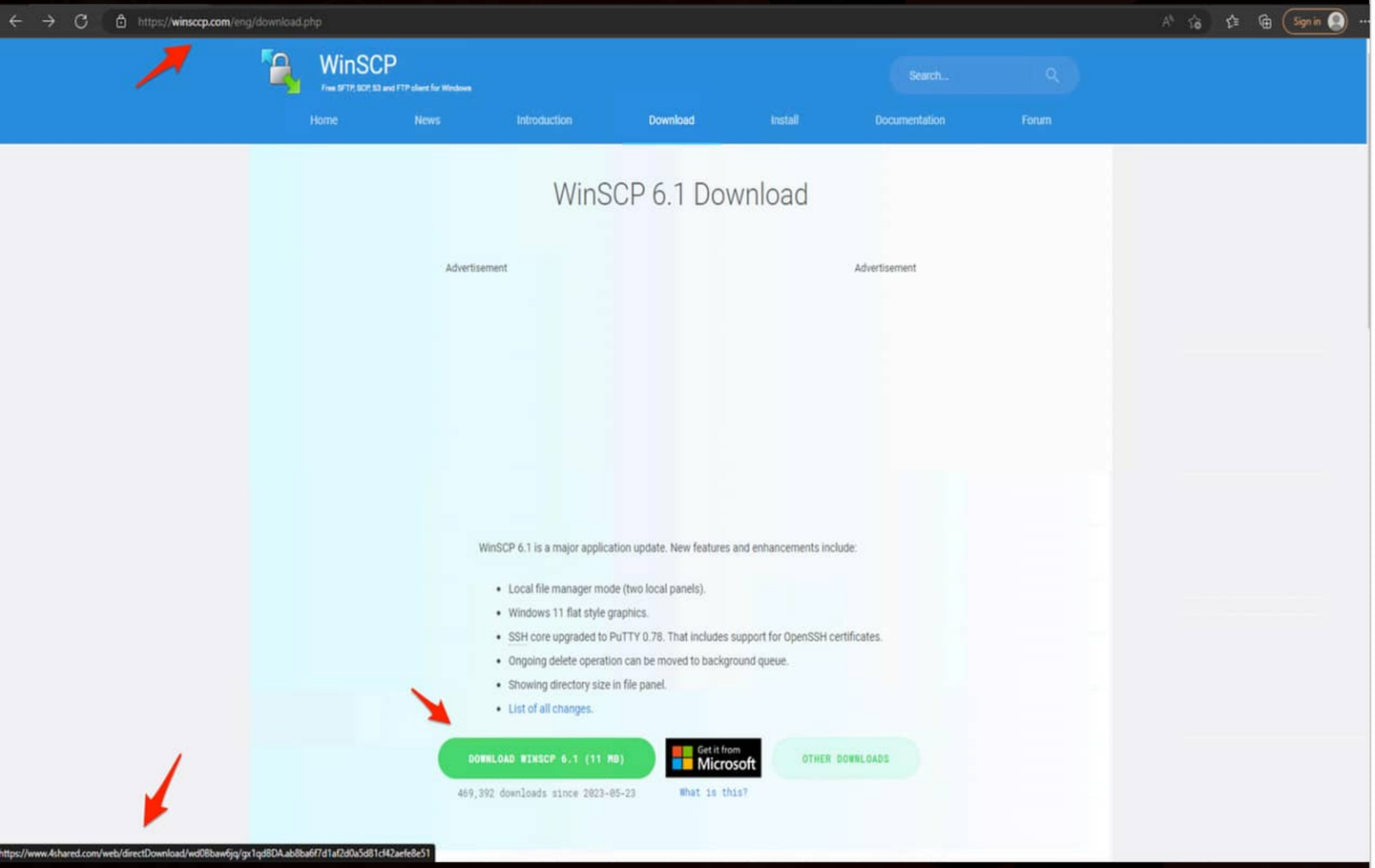

CPU
88% 2.49 GHz
Memory
2.2/8.0 GB (28%)
Ethernet
S: 6.3 Mbps R: 6.3 Mbps
This PC
darkswo
NLBrute 1.2
BRUTE
SETTINGS
WORK FILES
Statistics
Active threads: 500
Current PPS 206
Average PPS: 234
Good count: 0
Remaining: 20222864
Elapsed time: 000:37:28
Start
Stop
Clear
Hide to tray
Active threads: 350
Current PPS 174
Average PPS: 223
Good count: 0
Remaining: 21349396
Elapsed time: 000:35:40
Active threads: 400
Current PPS 254
Average PPS: 154
Good count: 0
Remaining: 38473622
Elapsed time: 000:36:45
Active threads: 150
Current PPS 113
Average PPS: 100
Good count: 0
Remaining: 979764
Elapsed time: 000:00:55
Activate Windows
Go to System in Control Panel to activate Windows.
erver 2012 R2 Standard
Build 9600
10:43 AM
12/23/2024

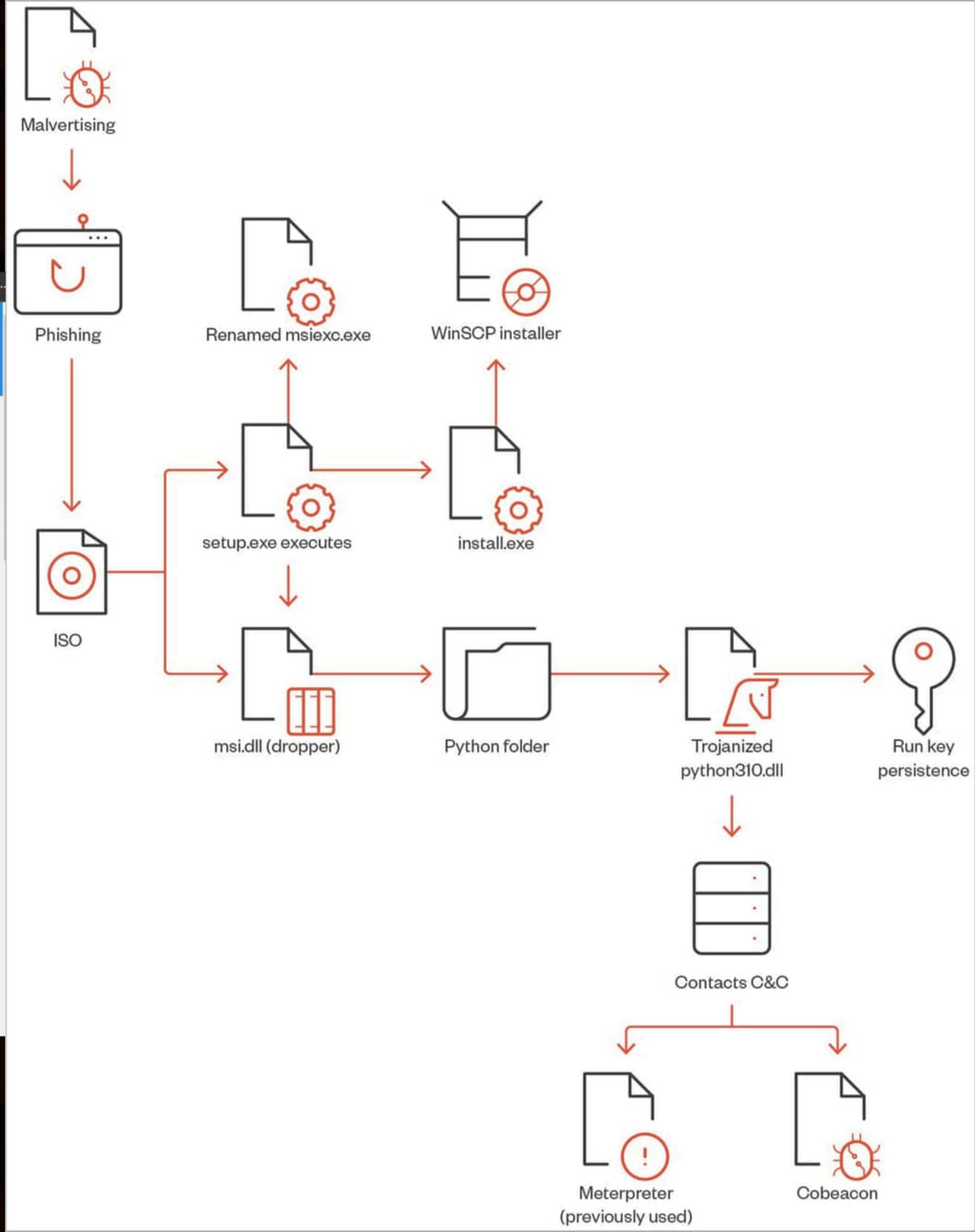
NLBrute 1.2


Remote Desktop Connection
Remote Desktop Connection
Computer:
10.53.251.60
User name:
W2K12-NAS
PDC
DATABASE
BACKUP-SERVER
THIRDPARTY
QH-SERVER
ONESUPPORT1
DP39
DEALING15
Help
CPU
29% 3.73 GHz
Memory
9.0/15.8 GB (57%)
Ethernet
S: 160 Kbps R: 24.0 Kbps
GPU 0
Intel(R) UHD Graphics P630
4%
Drive Tools
This PC
Search This PC
System Reserved (B:)
156 MB free of 499 MB
Local Disk (C:)
55.7 GB free of 126 GB
DVD Drive (E:) Integration Services Setup
CDFS
2018_Applications (\\10.53.251.211) (G:)
433 GB free of 0.99 TB
2018_Backup (\\10.53.251.211) (H:)
433 GB free of 0.99 TB
CC (\\10.53.251.211) (J:)
433 GB free of 0.99 TB
confirmation_clientfile (\\10.53.251.211) (K:)
433 GB free of 0.99 TB
D (\\10.53.251.211) (M:)
433 GB free of 0.99 TB
dbfManager (\\10.53.251.211) (N:)
433 GB free of 0.99 TB
RMS (\\10.53.251.211) (P:)
433 GB free of 0.99 TB
uploads (\\10.53.251.211) (Q:)
433 GB free of 0.99 TB
xlfolder (\\10.53.251.211) (R:)
433 GB free of 0.99 TB
Tally.ERP9 (\\10.53.251.248) (S:)
1.18 TB free of 1.43 TB
Public (\\10.53.251.247) (T:)
1.65 TB free of 7.21 TB
Daily Backup (\\10.53.251.247) (U:)
1.65 TB free of 7.21 TB
Soft (\\10.53.251.247) (V:)
1.65 TB free of 7.21 TB
Recycle Bin - Volume_1 (\\10.53.251.247) (W:)
1.65 TB free of 7.21 TB
Activate Windows
Go to Settings to activate Windows.


Windows 任务管理器
文件(F) 选项(O) 查看(V) 帮助(H)
应用程序 进程 服务 性能 联网 用户
CPU 使用率
CPU 使用记录
内存
物理内存使用记录
物理内存(MB)
总数 16383
已缓存 1589
可用 13629
空闲 12327
系统
句柄数 20023
线程数 1089
进程数 65
开机时间 3:06:17:42
提交(GB) 2 / 31
核心内存(MB)
分页数 118
未分页 66
资源监视器(R)...
进程数: 65
CPU 使用率: 0%
物理内存: 16%
计算机
网络
回收站
ARM2000
火绒安全软件
火绒应用商店
向日葵远程控制
360安全浏览器
U31客户端
U31控制台
开始
21:50
2024/12/25

Phishing WinSCP – BlackCat – ALPHV Ransom





Phishing

https://www.bing.com/search?q=winscp+download	winscp download - Suchen	
ftp-winscp.org	first_site_storage_time	
https://www.bing.com/	WinSCP :: Official Site :: Download	
https://winscp-net-dow	WinSCP :: Official Site :: Download	
https://ftp-winscp.org/	WinSCP :: Official Site :: Download	
https://ftp-winscp.org/eng/download.php	WinSCP :: Official Site :: Download	
https://[*.]ftp-winscp.org,*	cookie_controls_metadata [in Pr	{'la
ftp-winscp.org	last_site_storage_time	
static.xx.fbcdn.net	HSTS observed	{'ex
ftp-winscp.org	first_user_interaction_time	
www.youtube.com	HSTS observed	{'ex
https://ghaithana.com/wp-includes/assets/WinSCP-6.3.6-Setup.zip	Complete - 100% [12362033/12	\\r
ftp-winscp.org	last_user_interaction_time	
https://ftp-winscp.org:443,*	media_engagement [in Preferen	{'ex
ftp-winscp.org	Status: Live	last

www.youtube.com

2607:f8b0:4006:806::200e Public Scan

Lookup Go To Rescan

Add Verdict Report

Submitted URL: http://ftp-winscp.org/
Effective URL: https://www.youtube.com/watch?v=dQw4w9WgXcQ
Submission: On February 27 via manual (February 27th 2025, 3:01:46 am UTC) from IN — Scanned from US

Summary HTTP 211 Redirects Links 2 Behaviour Indicators Similar DOM Content API Verdicts

Summary

This website contacted **20 IPs** in **2 countries** across **9 domains** to perform **211 HTTP transactions**. The main IP is 2607:f8b0:4006:806::200e, located in **United States** and belongs to GOOGLE, US. The main domain is **www.youtube.com**. The Cisco Umbrella rank of the primary domain is **83**.
TLS certificate: Issued by *WR2* on February 3rd 2025. Valid for: 3 months.

www.youtube.com scanned **10000+ times** on urlscan.io Show Scans 10000+

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *www.youtube.com*
Current DNS A record: 216.58.206.46 (AS15169 - GOOGLE, US)
Domain created: February 15th 2005, 05:13:12 (UTC)
Domain registrar: MarkMonitor, Inc.

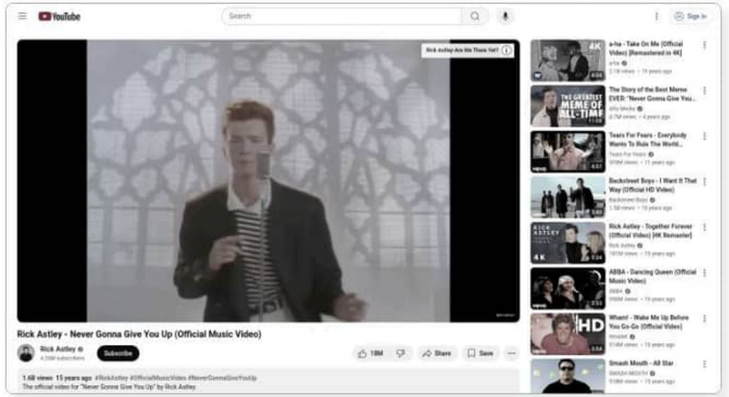
Domain & IP information

IP/ASNs | IP Detail | Domains | Domain Tree | Links | Certs | Frames

	IP Address	AS Autonomous System
1 → 1	23.227.196.13	29802 (HVC-AS)
17	2607:f8b0:4006:806::200e	15169 (GOOGLE)
7	2607:f8b0:4006:821::2016	15169 (GOOGLE)
3	2607:f8b0:4006:809::200a	15169 (GOOGLE)

Screenshot

Live screenshot Full Image



Page Title

Rick Astley - Never Gonna Give You Up (Official Music Video) - YouTube

Page URL History

Show full URLs

1. http://ftp-winscp.org/ HTTP 307
   https://ftp-winscp.org/ HTTP 302
   https://www.youtube.com/watch?v=dQw4w9WgXcQ Page URL

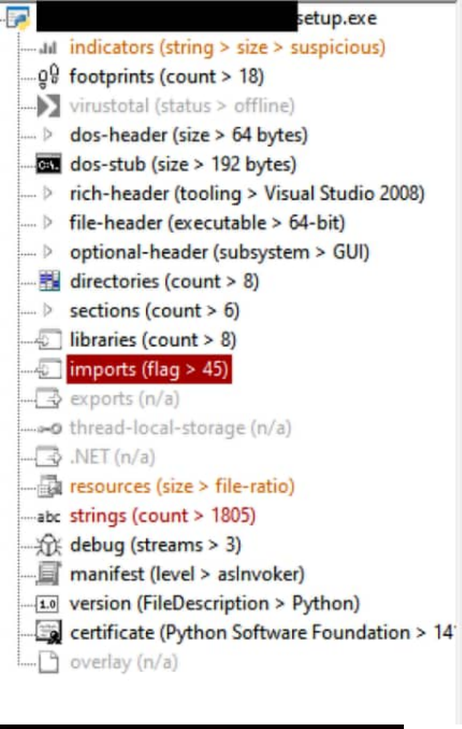
Page Statistics

211	98 %	45 %	9	18
Requests	HTTPS	IPv6	Domains	Subdomains

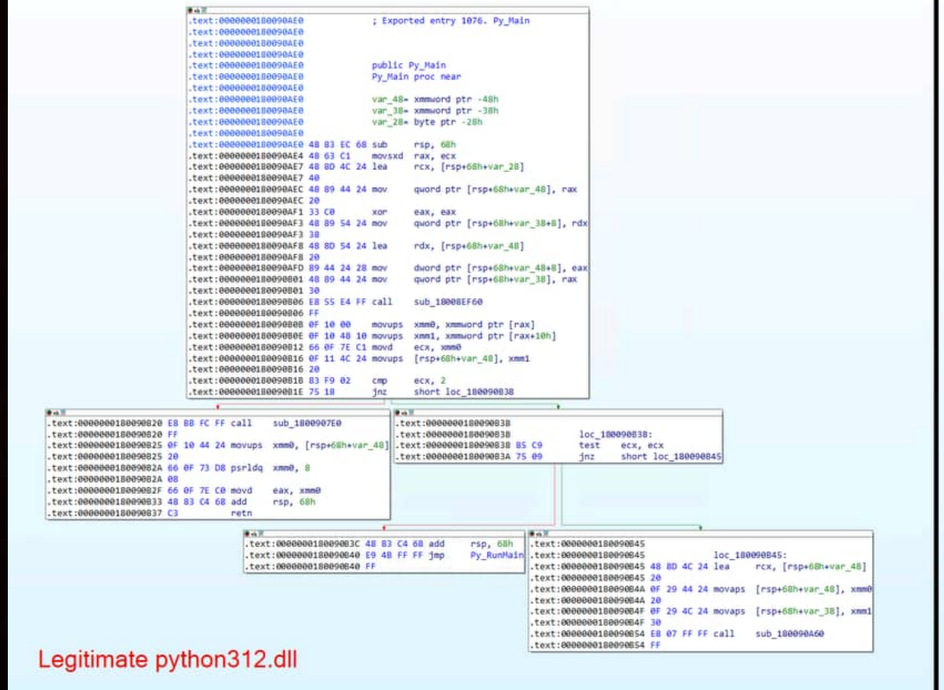
20534

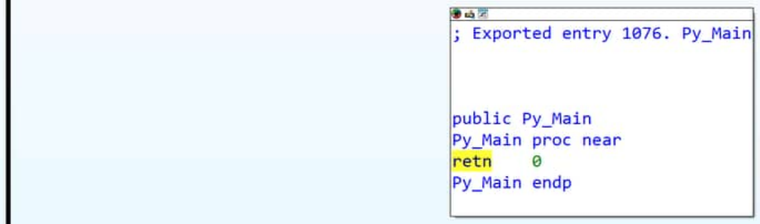
Created0x10 | Parent Sequence N… | Enter text to search… | Find

Line	Tag	Entry Number	Sequenc…	Parent …	In Use	Parent Path	File Name	u Sec Zeros	Copied	Extension
=	■	=	=	=	■	[redacted]		■	■	.exe
23…	☐	2271	768	151518	☑	.\Program Files\Intel\WiFi\Docs	Intel64.exe	☐	☐	.exe
Parent Sequence Number: 4 (Count=8)										
31…	☐	296448	21	295676	☑	.\Program Files\WindowsApps\Microsoft.Deskto…	winget.exe	☐	☐	.exe
31…	☐	296409	19	295676	☑	.\Program Files\WindowsApps\Microsoft.Deskto…	WindowsPackageManagerServer.exe	☐	☐	.exe
14…	☐	120748	74	125330	☑	.\Intel	tcpp.exe	☐	☐	.exe
84…	☐	62845	34	125330	☑	.\Intel	IntelGup.exe	☐	☐	.exe
31…	☐	296369	20	295676	☑	.\Program Files\WindowsApps\Microsoft.Deskto…	AuthenticationManager.exe	☐	☐	.exe
31…	☐	296366	21	295676	☑	.\Program Files\WindowsApps\Microsoft.Deskto…	AppInstallerPythonRedirector.exe	☐	☐	.exe
31…	☐	296361	4	295676	☑	.\Program Files\WindowsApps\Microsoft.Deskto…	AppInstallerFullTrustAppServiceClient.exe	☐	☐	.exe
31…	☐	296343	13	295676	☑	.\Program Files\WindowsApps\Microsoft.Deskto…	AppInstaller.exe	☐	☐	.exe
Parent Sequence Number: 8 (Count=1)										
Parent Sequence Number: 17 (Count=1)										
14…	☐	112347	16	112056	☑	[redacted]\AppData\Local\Downloads	WinSCP-6.1.2-Setup.exe	☐	☐	.exe
Parent Sequence Number: 19 (Count=3)										
Parent Sequence Number: 28 (Count=1)										
12…	☐	99459	7	72394	☑	[redacted]WinSCP-6.3.6-Setup	setup.exe	☐	☑	.exe
Parent Sequence Number: 45 (Count=2)										
22…	☐	203796	48	203777	☑	.\Program Files (x86)\WinSCP\PuTTY	puttygen.exe	☑	☑	.exe
22…	☐	203793	79	203777	☑	.\Program Files (x86)\WinSCP\PuTTY	pageant.exe	☑	☑	.exe



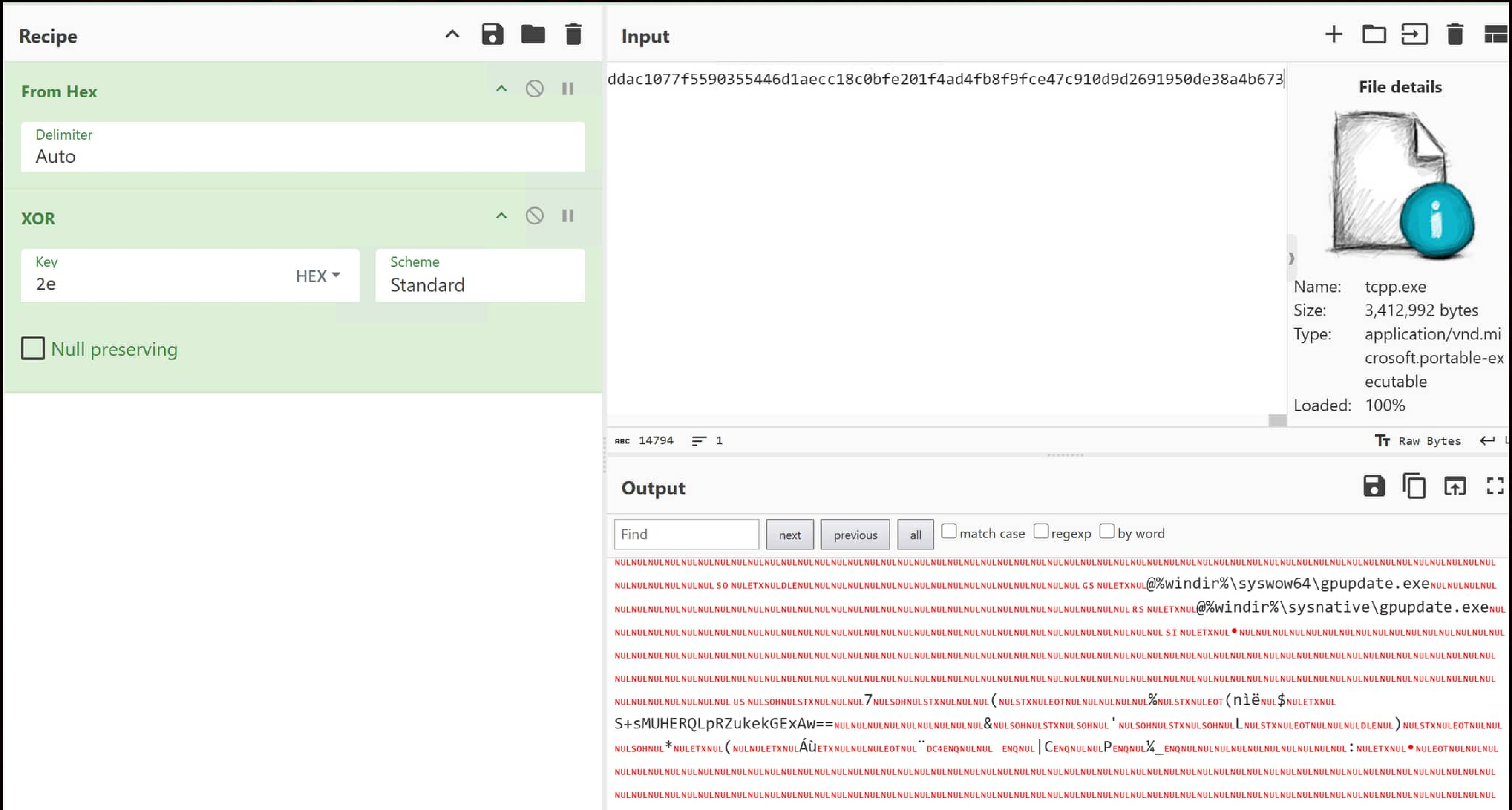
imports (45)	flag (5)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (7)	technique (3)	type (1)	ordinal (1)	library (0)
Py_Main	-	0x0000000000002B18	0x0000000000002B18	1075 (0x0433)	-	-	implicit	-	python312.dll
__p__commode	-	0x0000000000002CE4	0x0000000000002CE4	1 (0x0001)	-	-	implicit	-	api-ms-win-crt-st...
_set_fmode	-	0x0000000000002C6E	0x0000000000002C6E	84 (0x0054)	-	-	implicit	-	api-ms-win-crt-st...
_initialize_onexit_table	-	0x0000000000002CF4	0x0000000000002CF4	52 (0x0034)	-	-	implicit	-	api-ms-win-crt-ru...
_register_onexit_function	-	0x0000000000002D10	0x0000000000002D10	60 (0x003C)	-	-	implicit	-	api-ms-win-crt-ru...
_crt_atexit	-	0x0000000000002D2C	0x0000000000002D2C	30 (0x001E)	-	-	implicit	-	api-ms-win-crt-ru...
terminate	-	0x0000000000002D3A	0x0000000000002D3A	103 (0x0067)	-	-	implicit	-	api-ms-win-crt-ru...
_configure_wide_argv	-	0x0000000000002BEA	0x0000000000002BEA	25 (0x0019)	-	-	implicit	-	api-ms-win-crt-ru...
_register_thread_local_exe_at...	-	0x0000000000002C90	0x0000000000002C90	61 (0x003D)	-	-	implicit	-	api-ms-win-crt-ru...
_initialize_wide_environment	-	0x0000000000002C02	0x0000000000002C02	53 (0x0035)	-	-	implicit	-	api-ms-win-crt-ru...
_set_app_type	-	0x0000000000002BC6	0x0000000000002BC6	66 (0x0042)	-	-	implicit	-	api-ms-win-crt-ru...
_seh_filter_exe	-	0x0000000000002BB4	0x0000000000002BB4	64 (0x0040)	-	-	implicit	-	api-ms-win-crt-ru...
__p__argc	-	0x0000000000002BA6	0x0000000000002BA6	4 (0x0004)	-	-	implicit	-	api-ms-win-crt-ru...
__p__wargv	-	0x0000000000002B98	0x0000000000002B98	6 (0x0006)	-	-	implicit	-	api-ms-win-crt-ru...
_c_exit	-	0x0000000000002C86	0x0000000000002C86	21 (0x0015)	-	-	implicit	-	api-ms-win-crt-ru...
_cexit	-	0x0000000000002C7C	0x0000000000002C7C	22 (0x0016)	-	-	implicit	-	api-ms-win-crt-ru...
_get_wide_winmain_comma...	-	0x0000000000002C22	0x0000000000002C22	47 (0x002F)	-	-	implicit	-	api-ms-win-crt-ru...
_exit	-	0x0000000000002C66	0x0000000000002C66	35 (0x0023)	-	-	implicit	-	api-ms-win-crt-ru...
exit	-	0x0000000000002C5E	0x0000000000002C5E	85 (0x0055)	-	-	implicit	-	api-ms-win-crt-ru...
_initterm_e	-	0x0000000000002C50	0x0000000000002C50	55 (0x0037)	-	-	implicit	-	api-ms-win-crt-ru...
_initterm	-	0x0000000000002C44	0x0000000000002C44	54 (0x0036)	-	-	implicit	-	api-ms-win-crt-ru...
__setusermatherr	-	0x0000000000002BD6	0x0000000000002BD6	9 (0x0009)	-	-	implicit	-	api-ms-win-crt-m...





tcpp.exe

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	20	21	22	23	Decoded text
001791A8	38	62	34	65	32	39	34	37	37	34	31	39	62	65	61	62	33	66	65	64	38	61	33	39	32	34	63	30	36	62	65	38	30	36	34	63	8b4e29477419beab3fed8a3924c06be8064c
001791CC	39	64	31	61	32	61	31	38	64	34	65	62	65	63	32	30	39	30	38	63	31	61	33	63	38	39	39	62	30	65	38	39	31	31	32	37	9d1a2a18d4ebec20908c1a3c899b0e891127
001791F0	65	62	31	62	31	62	39	38	33	64	66	61	30	37	61	61	31	37	37	62	61	37	32	38	30	32	65	64	61	32	38	61	39	38	36	32	eb1b1b983dfa07aa177ba72802eda28a9862
00179214	30	32	61	37	32	30	39	64	39	30	61	36	65	31	30	64	63	64	31	38	66	62	30	65	61	62	33	33	30	30	38	35	30	61	34	34	02a7209d90a6e10dcd18fb0eab3300850a44
00179238	39	37	37	32	61	31	64	30	38	33	35	33	65	34	38	61	30	63	39	31	32	62	30	33	64	65	36	61	32	61	30	36	39	61	33	66	9772a1d08353e48a0c912b03de6a2a069a3f
0017925C	61	34	30	39	36	31	31	30	32	62	38	30	63	61	36	62	37	64	33	38	30	35	30	61	66	62	35	63	33	62	34	36	34	65	65	62	a40961102b80ca6b7d38050afb5c3b464eeb
00179280	38	64	65	32	31	62	39	63	32	65	32	66	32	65	32	66	32	65	32	63	32	65	32	61	32	65	32	63	32	65	32	66	32	65	32	63	8de21b9c2e2f2e2f2e2c2e2a2e2c2e2f2e2c
001792A4	33	64	61	36	32	65	32	64	32	65	32	63	32	65	32	61	32	65	32	65	30	39	33	65	32	65	32	61	32	65	32	63	32	65	32	61	3da62e2d2e2c2e2a2e2e093e2e2a2e2c2e2a
001792C8	32	65	38	65	32	65	32	65	32	65	32	62	32	65	32	66	32	65	32	63	32	65	32	65	32	65	32	38	32	65	32	66	32	65	32	63	2e8e2e2e2e2b2e2f2e2c2e2e2e282e2f2e2c
001792EC	32	65	32	65	32	65	32	39	32	65	32	64	32	66	32	65	31	65	61	66	62	31	31	65	32	33	32	38	32	37	30	34	61	38	36	36	2e2e2e292e2d2f2eleafb11e23282704a866
00179310	61	38	64	39	32	33	32	66	32	66	32	66	32	62	32	65	32	64	61	66	61	33	32	65	31	65	61	66	61	37	32	63	61	66	61	66	a8d9232f2f2f2b2e2dafa32eleafa72cafaf
00179334	32	65	38	34	66	35	66	37	64	34	62	66	62	34	34	35	30	30	35	62	32	63	65	64	62	66	34	66	63	63	62	66	36	64	36	32	2e84f5f7d4bfb445005b2cedbf4fccbf6d62
00179358	37	38	61	39	33	37	31	32	35	66	64	31	30	61	33	35	66	63	33	30	66	65	64	65	66	36	33	30	37	66	37	30	65	66	36	63	78a937125fd10a35fc30fedef6307f70ef6c
0017937C	66	36	31	62	33	39	38	32	39	64	33	62	61	39	63	38	39	63	36	33	61	39	64	61	32	63	63	37	34	36	36	63	64	30	33	34	f61b39829d3ba9c89c63a9da2cc7466cd034
001793A0	32	32	65	35	32	37	63	38	34	30	32	34	62	66	37	62	38	39	34	62	62	65	36	62	37	63	65	66	33	65	35	64	33	31	62	32	22e527c84024bf7b894bbe6b7cef3e5d31b2
001793C4	37	30	66	62	62	65	35	33	38	34	62	66	33	32	31	36	62	38	33	35	61	62	36	33	30	37	33	39	35	34	34	38	33	65	65	33	70fbbe5384bf3216b835ab63073954483ee3
001793E8	[redacted]																																				fb619132a4d582e9e676f25e93e74b86b0ff
0017940C																																					[redacted]
00179430																																					
00179454	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e
00179478	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e
0017949C	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e
001794C0	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e
001794E4	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	36	32	65	32	64	32	66	32	65	[redacted]
00179508	[redacted]																																				
0017952C	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e
00179550	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e
00179574	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e
00179598	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e
001795BC	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e
001795E0	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e
00179604	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e
00179628	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e
0017964C	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	32	65	2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e2e


Recipe
From Hex
Delimiter
Auto
XOR
Key
2e
HEX
Scheme
Standard
Null preserving
Input
ddac1077f5590355446d1aecc18c0bfe201f4ad4fb8f9fce47c910d9d2691950de38a4b673
File details
Name: tcpp.exe
Size: 3,412,992 bytes
Type: application/vnd.microsoft.portable-executable
Loaded: 100%
14794
1
Raw Bytes
Output
Find
next
previous
all
match case
regexp
by word
@%windir%\syswow64\gpupdate.exe
@%windir%\sysnative\gpupdate.exe
S+sMUHERQLpRZukekGExAw==

```
(venv) FLARE-VM 04/12/2025 15:08:59
PS C:\Tools\CobaltStrikeParser > python .\parse_beacon_config.py 'C:\Users\                    .dat'
BeaconType                      - TCP
Port                            - 5000
SleepTime                       - 10000
MaxGetSize                      - 10485760
Jitter                          - 0
MaxDNS                          - 0
PublicKey_MD5                   -
C2Server                        - 192.168.101.
UserAgent                       -
HttpPostUri                     -
Malleable_C2_Instructions       - Empty
PipeName                        -
DNS_Idle                        - Not Found
DNS_Sleep                       - Not Found
SSH_Host                        - Not Found
SSH_Port                        - Not Found
SSH_Username                    - Not Found
SSH_Password_Plaintext          - Not Found
SSH_Password_Pubkey             - Not Found
SSH_Banner                      - Not Found
HttpGet_Verb                    - Not Found
HttpPost_Verb                   - Not Found
HttpPostChunk                   - Not Found
Spawnto_x86                     - %windir%\syswow64\gpupdate.exe
Spawnto_x64                     - %windir%\sysnative\gpupdate.exe
CryptoScheme                    - 0
Proxy_Config                    - Not Found
Proxy_User                      - Not Found
Proxy_Password                  - Not Found
Proxy_Behavior                  - Not Found
Watermark_Hash                  - S+sMUHERQLpRZukekGExAw==
Watermark                       - 678358251
bStageCleanup                   - True
bCFGCaution                     - True
KillDate                        - 0
bProcInject_StartRWX            - False
bProcInject_UseRWX              - False
bProcInject_MinAllocSize        - 18191
ProcInject_PrependAppend_x86    -

ProcInject_PrependAppend_x64    -
                                  Empty
ProcInject_Execute              - ntdll.dll:RtlUserThreadStart
                                  NtQueueApcThread-s
                                  SetThreadContext
                                  CreateRemoteThread
                                  kernel32.dll:LoadLibraryA
                                  RtlCreateUserThread
ProcInject_AllocationMethod     - NtMapViewOfSection
```

DFIR

Contención

- *Aislamiento de equipos afectados.*
- *Restablecimiento de accesos, etc.*

Recuperación

- *Validar integridad de copias de seguridad.*
- *Validar estado de continuidad de negocio.*

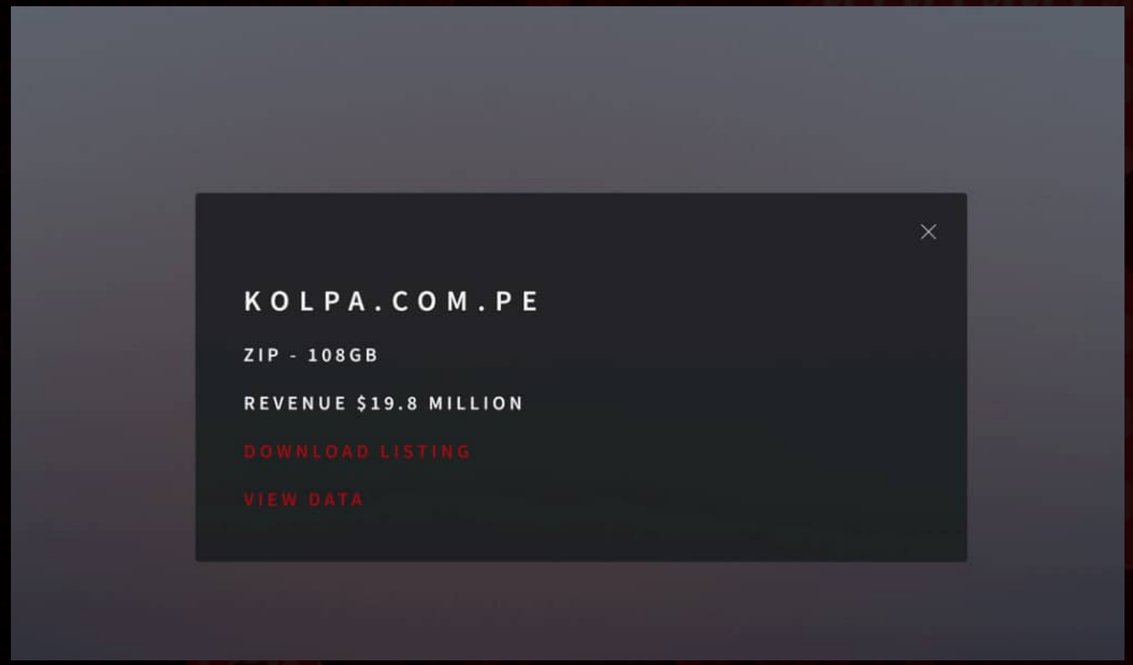
Forense

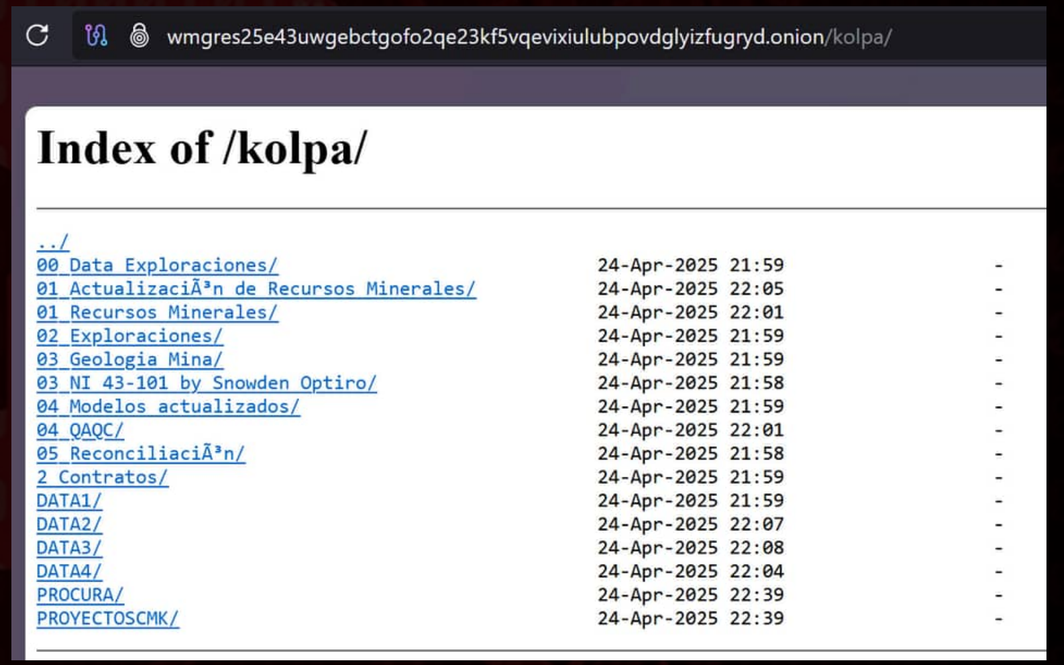
- *Recolección de evidencias.*
- *Comunicación con el TA:*
  - *Lista de exfiltración*
  - *Pruebas de vida.*
  - *Pruebas de descifrado.*

Actores de Amenaza


como se
pone el arroba

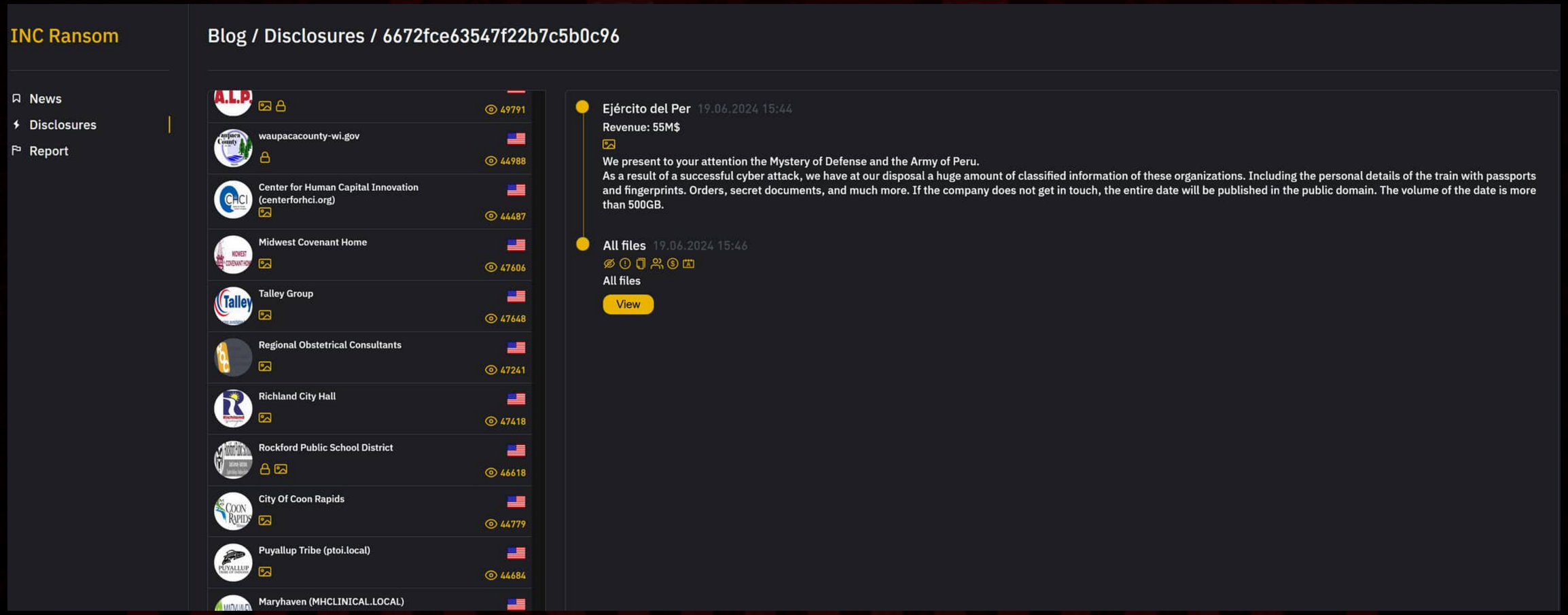
KOLPA





Ransomware

EJERCITO DEL PERÚ



Fuero Militar Policial - FMP

Movistar

AJE

hxxps[://]akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion/

hxxps[://]akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion/

Qilin

Log In

SORTING CREATED AT ↓ NAME

MHMLAWGROUP.COM

COMPANY URL | MAY 29, 2025

5 photos | 0 files | 246.00 GB

Learn More

All data of this company will be available for download on 10.06.2025. MHM Law Group is one of the fastest growing law firms in California. The firm handles all personal injury, immigration, and criminal defense matters. 1.The document is a ...



+ 2 more

HALLMARKNAMEPLATE.COM

COMPANY URL | MAY 29, 2025

5 photos | 0 files | 44.00 GB

Learn More

All data of this company will be available for download on 14.06.2025.Hallmark Nameplate is located in a 30,000 square foot manufacturing facility in the heart of Central Florida. Since 1957, our

WikileaksV2

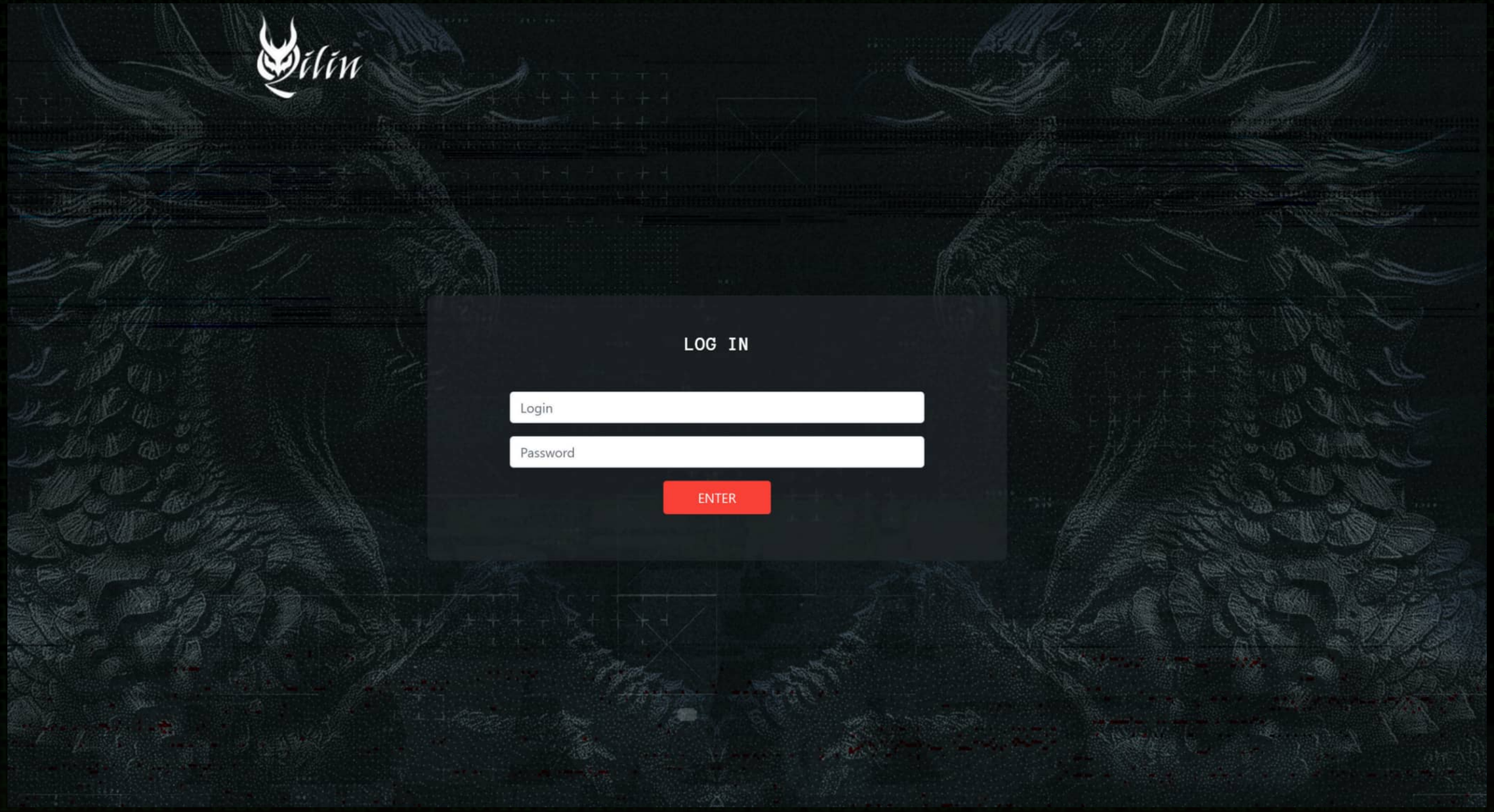
jabber: qilin@exploit.im

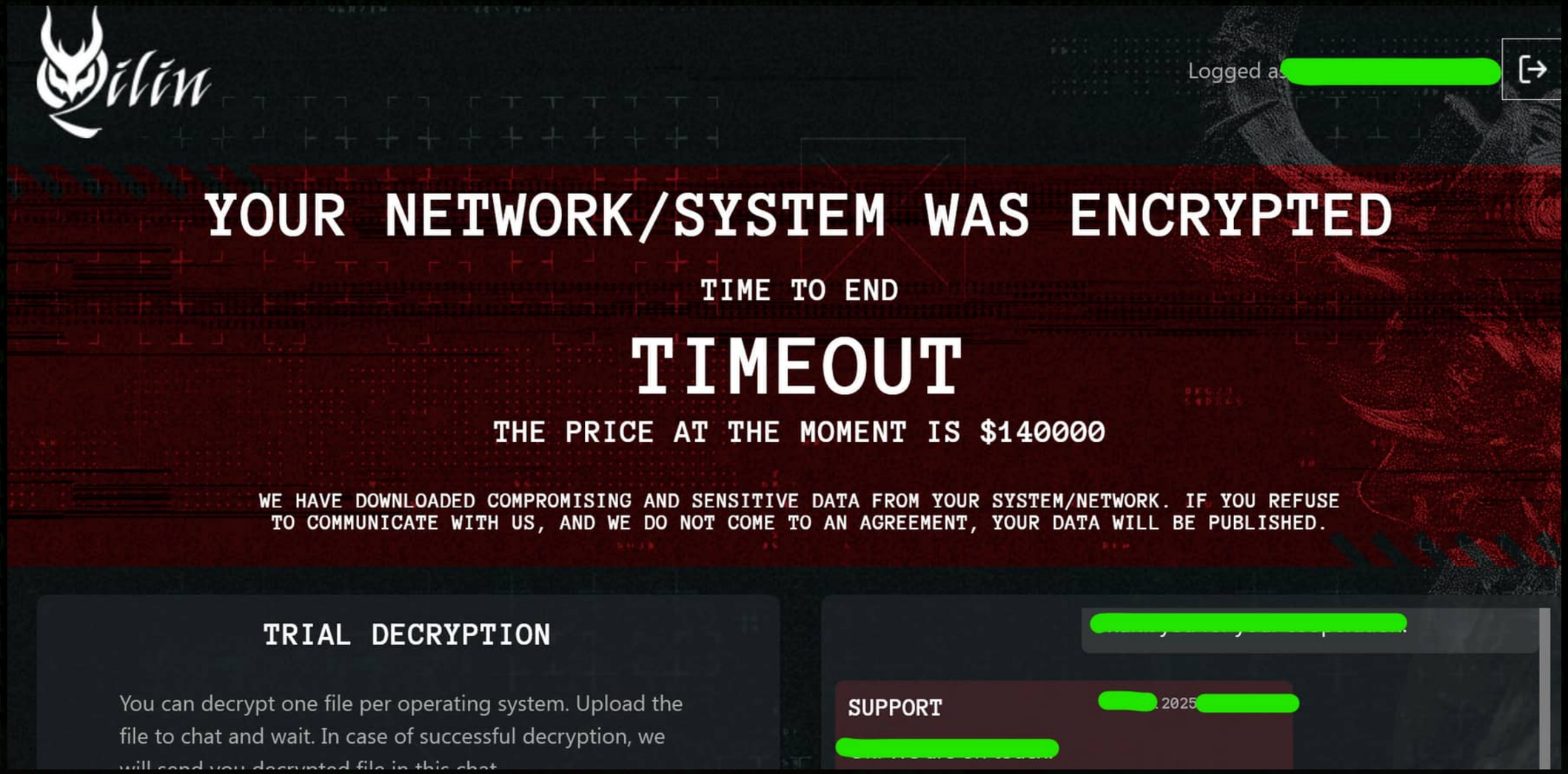
TOX: 7C35408411AEEBD53CDBCEBAB167D7B22F1E66614E89DFCB62EE835416F60E1BCD6995152B68

ftp://dataShare:nX4aJxu3rYUMiLjCMtuJYTKS@185.208.156.157

ftp://dataShare:2bTWYKNn7aK7Rqp9mnv3@185.196.10.19

hxxp[://]ijzn3sicrcy7guixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvqd[.]onion


Qilin
LOG IN
Login
Password
ENTER


Logged as [redacted]
YOUR NETWORK/SYSTEM WAS ENCRYPTED
TIME TO END
TIMEOUT
THE PRICE AT THE MOMENT IS $140000
WE HAVE DOWNLOADED COMPROMISING AND SENSITIVE DATA FROM YOUR SYSTEM/NETWORK. IF YOU REFUSE TO COMMUNICATE WITH US, AND WE DO NOT COME TO AN AGREEMENT, YOUR DATA WILL BE PUBLISHED.
TRIAL DECRYPTION
You can decrypt one file per operating system. Upload the file to chat and wait. In case of successful decryption, we
SUPPORT
[redacted] 2025 [redacted]


Demo
Ransomware

Muchas Gracias

Datos de contacto:

contact.pastime903@passmail.net

in/david-ramos-rodriguez/