This slide deck is from a security presentation by Steve Stasiukonis from SNT. If you would like to schedule a live web presentation of this material, please reach out to

Jim Ockenden
(315) 949-2803

Secure Network

2025

CYBER SECURITY OUTLOOK

SECURE NETWORK-WHO WE ARE…

PROFESSIONAL WHITE HAT HACKERS
TESTING NETWORK SECURITY

RESPOND TO SECURITY INCIDENTS
AKA:COMPANIES WHO WERE HACKED

MORE NATION STATE SPONSORED THREAT ACTORS

WHO ARE THE HACKERS

Secure Network

THE ADVANCED PERSISTENT THREAT

FOREIGN NATIONALS

HACKTIVISTS / ANARCHISTS

ORGANIZED CYBER CRIMINALS

DARk$ide REvil

Carbon Spyder

TENSIONS WITH CHINA

Xi Jinping

HAFNIUM

Microsoft

DEEP PANDA

GOVERNMENT & INFRASTRUCTURE

BRONZE STAR LIGHT

ANYONE

TA428

GOVERNMENT & BUSINESSES

VOLT TYPHOON

ANYONE

TENSIONS WITH NORTH KOREA

Secure Network

Kim Jong Un

KIMSUKY

FINANCIAL SERVICES

TEMP/HERMIT

FINANCIAL SERVICES

LAZARUS

GOVERNMENT
INFRASTRUCTURE
FINANCIAL SERVICES
HI-TECH
ANYONE
ANYTHING

TENSIONS WITH IRAN

HANDALA

GOVERNMENT

CHARMING KITTEN

ANYONE

ILLUSIVE

GOVERNMENT DEFENSE CONTRACTORS

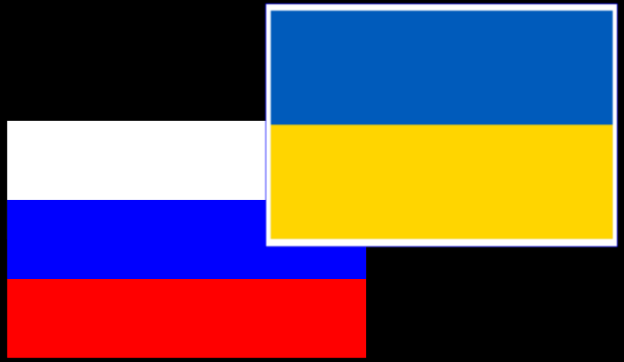
POLONIUM

ANYONE

#1 THREAT ACTOR COUNTRY
RUSSIA

TENSIONS WITH RUSSIA

GEOPOLITICAL ISSUES



30+ COUNTRIES IMPOSED RUSSIAN SANCTIONS

GLOBAL FINANCIAL PLAYERS CUT OFF RUSSIAN ACCESS

SWI
STARBUCKS COFFEE
VISA
MasterCard
McDonald's

RUSSIAN APT'S GROWING

Alexander Lukashenko

- FANCY BEAR
- COZY BEAR
- BERSERK
- CONTI
- CLOP
- VENOMOUS BEAR
- SANDWORM
- FIN7
- LIST GETS BIGGER

Secure Network

PUTINS CYBER PLAN

INCREASE IN THREAT ACTOR GROUPS

TARGETING VERTICAL MARKETS

LOGISTICS
FOOD INDUSTRY
PETROLEUM COMPANIES
ANYTHING ESSENTIAL

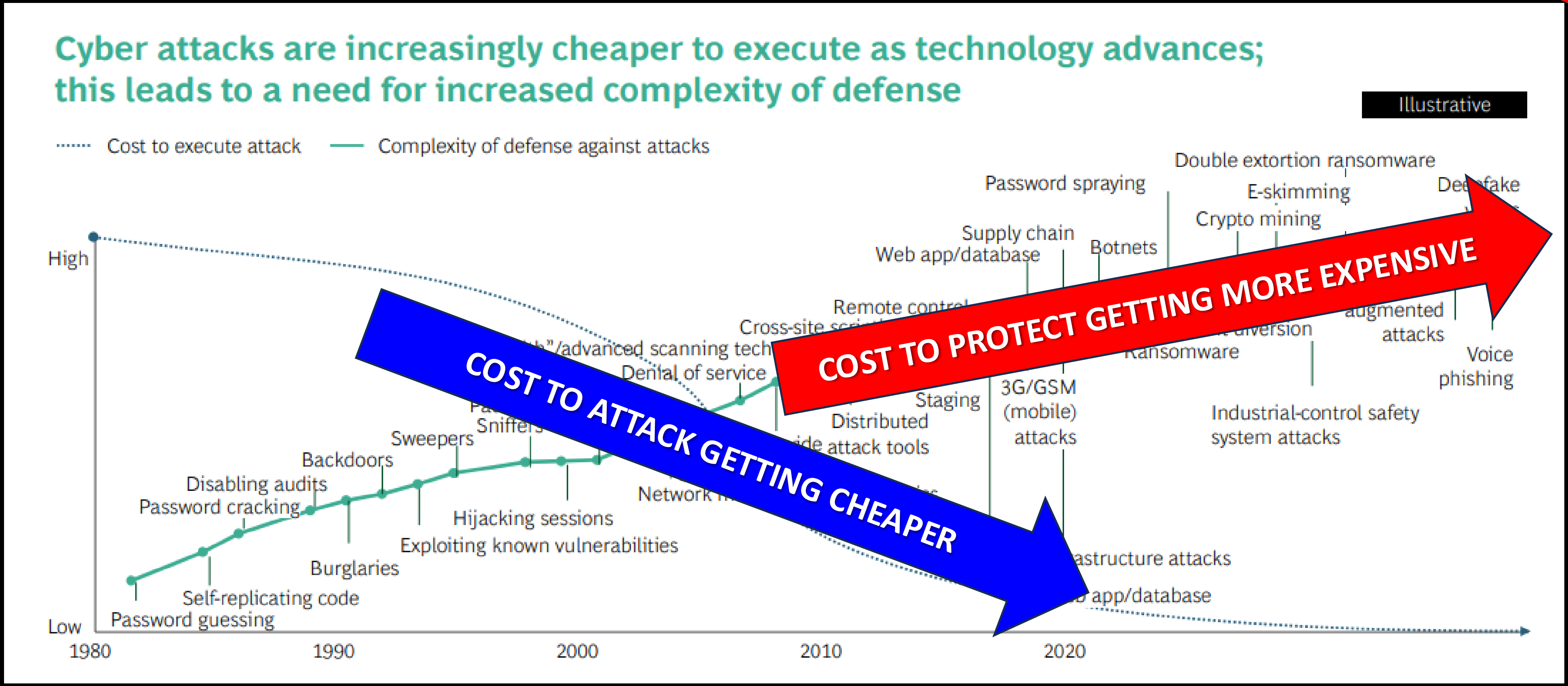
NO SIZE RESTRICTIONS ON VICTIMS

LARGE
MEDIUM
SMALL

HACKING VS PROTECTING

COST TO ATTACK DECREASES

Secure Network



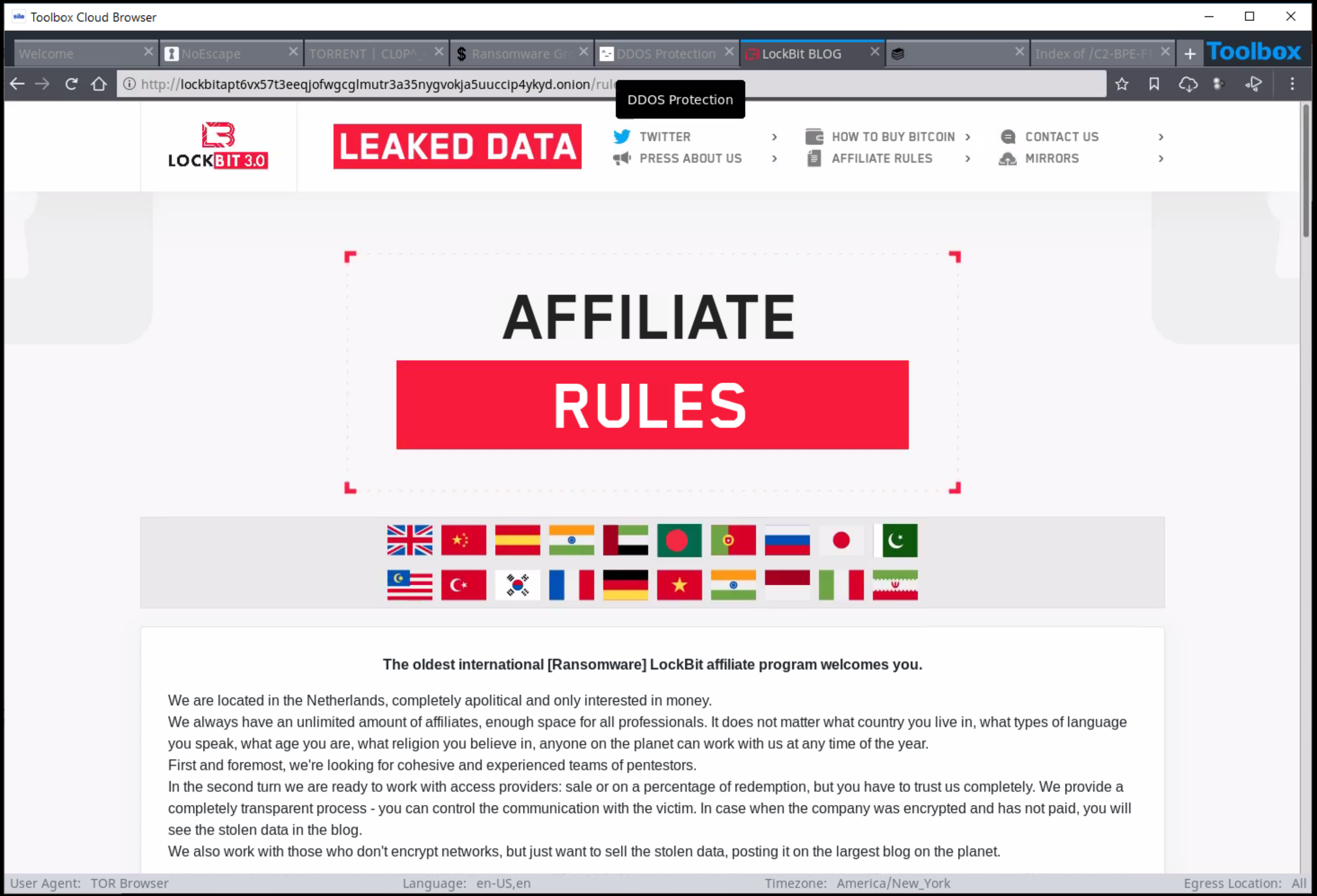
Cyber attacks are increasingly cheaper to execute as technology advances; this leads to a need for increased complexity of defense

COST TO PROTECT INCREASES

THREAT ACTORS EXPANDING

FRANCHISED HACKERS

Secure Network



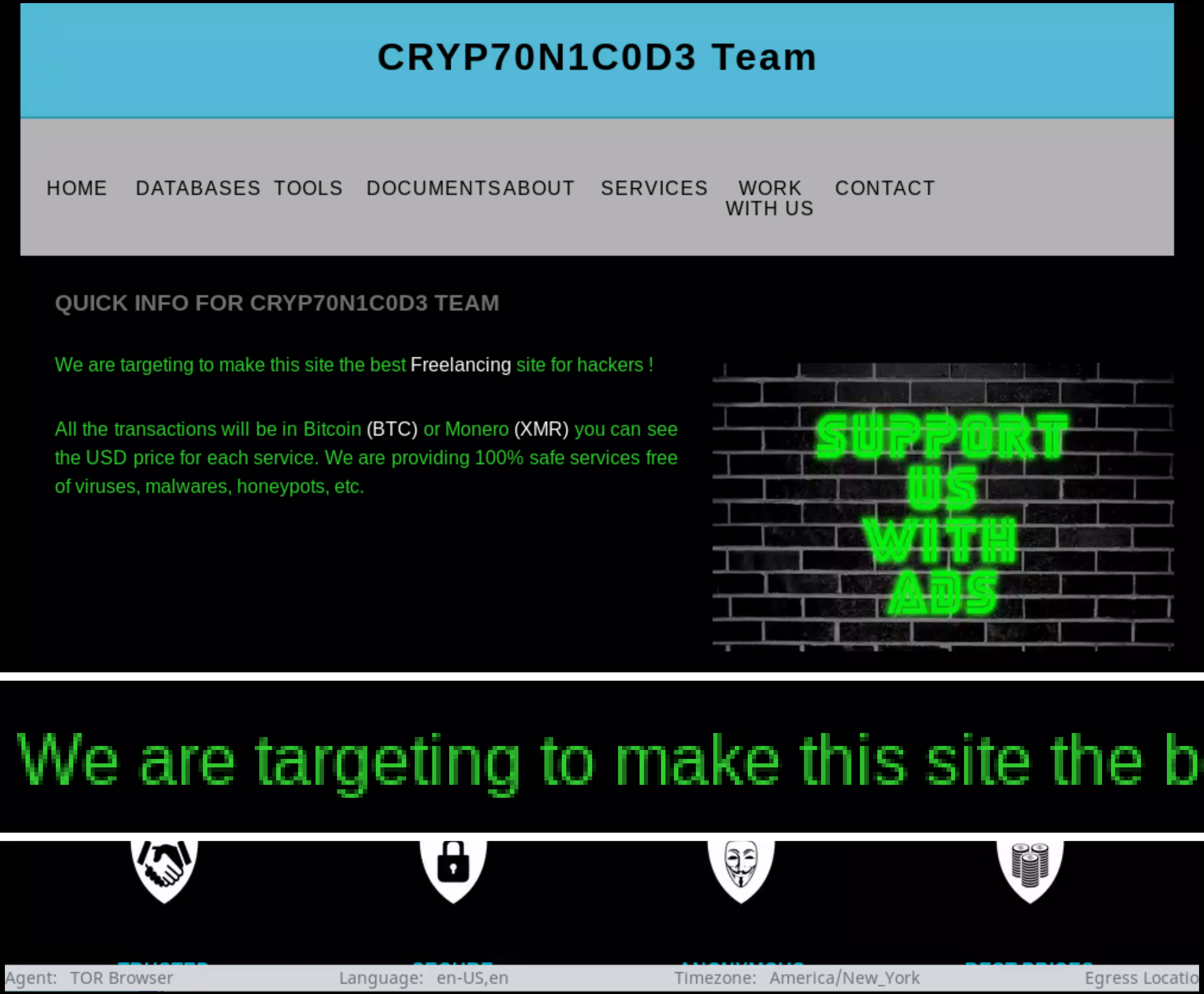
AFFILIATE RULES

The oldest international [Ransomware] LockBit affiliate program welcomes you.

We are located in the Netherlands, completely apolitical and only interested in money.
We always have an unlimited amount of affiliates, enough space for all professionals. It does not matter what country you live in, what types of language you speak, what age you are, what religion you believe in, anyone on the planet can work with us at any time of the year.
First and foremost, we're looking for cohesive and experienced teams of pentestors.
In the second turn we are ready to work with access providers: sale or on a percentage of redemption, but you have to trust us completely. We provide a completely transparent process - you can control the communication with the victim. In case when the company was encrypted and has not paid, you will see the stolen data in the blog.
We also work with those who don't encrypt networks, but just want to sell the stolen data, posting it on the largest blog on the planet.

10-30%

FREELANCE SERVICES



CRYP70N1C0D3 Team

QUICK INFO FOR CRYP70N1C0D3 TEAM

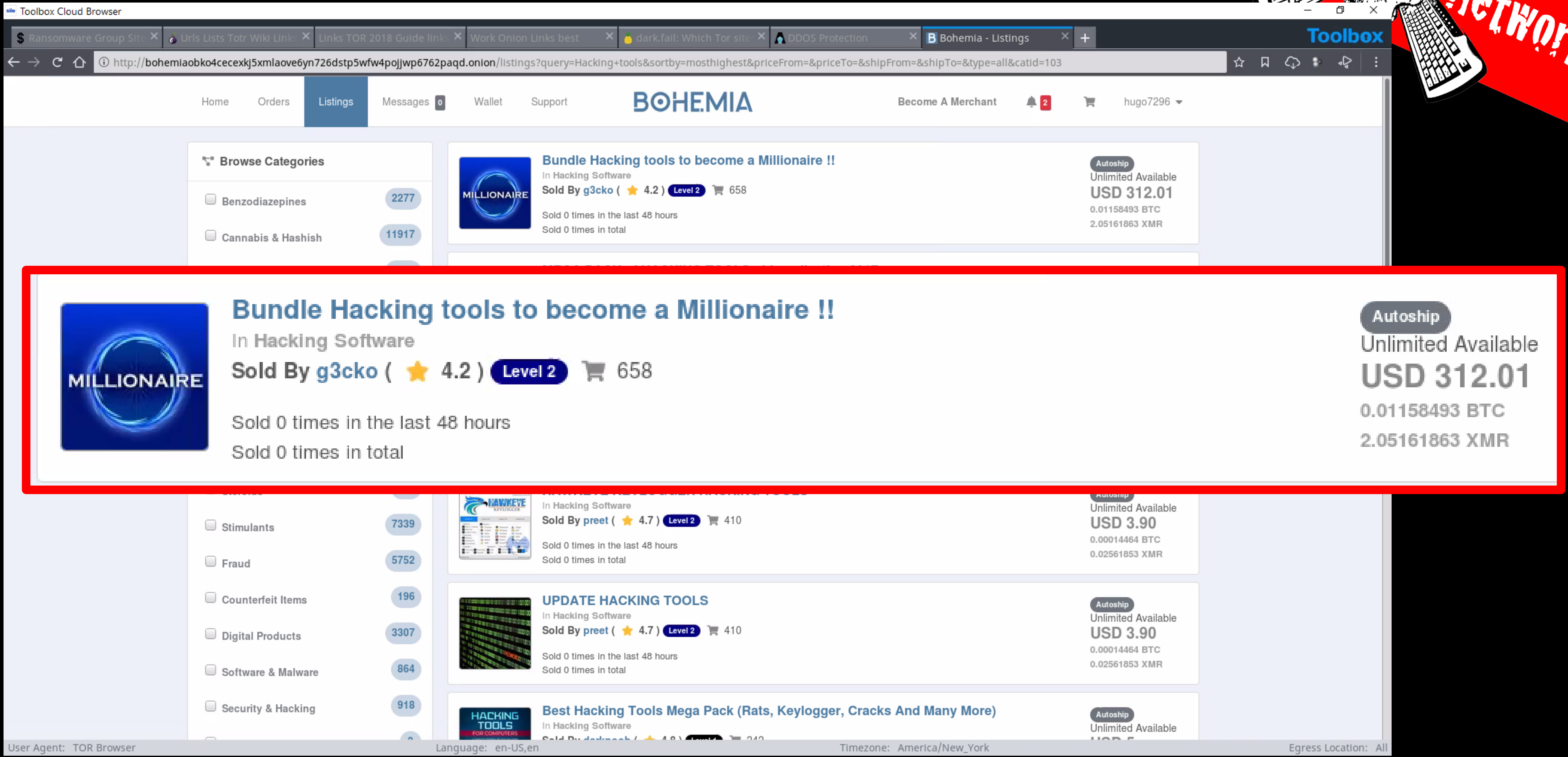
We are targeting to make this site the best Freelancing site for hackers !

All the transactions will be in Bitcoin (BTC) or Monero (XMR) you can see the USD price for each service. We are providing 100% safe services free of viruses, malwares, honeypots, etc.

Agent: TOR Browser Language: en-US,en Timezone: America/New_York Egress Locatio

We are targeting to make this site the best Freelancing site for hackers !

DARKMARKET TOOLS



Toolbox Cloud Browser

Ransomware Group Site | Urls Lists Totr Wiki Link | Links TOR 2018 Guide links | Work Onion Links best | dark.fail: Which Tor site | DDOS Protection | Bohemia - Listings

http://bohemiaobko4cecexkj5xmlaove6yn726dstp5wfw4pojjwp6762paqd.onion/listings?query=Hacking+tools&sortby=mosthighest&priceFrom=&priceTo=&shipFrom=&shipTo=&type=all&catid=103

Browse Categories

□ Benzodiazepines	2277
□ Cannabis & Hashish	11917
□ Stimulants	7339
□ Fraud	5752
□ Counterfeit Items	196
□ Digital Products	3307
□ Software & Malware	864
□ Security & Hacking	918

Bundle Hacking tools to become a Millionaire !!
In Hacking Software
Sold By g3cko (★ 4.2) Level 2 658
Sold 0 times in the last 48 hours
Sold 0 times in total
Autoship
Unlimited Available
USD 312.01
0.01158493 BTC
2.05161863 XMR

Bundle Hacking tools to become a Millionaire !!
In Hacking Software
Sold By g3cko (★ 4.2) Level 2 658
Sold 0 times in the last 48 hours
Sold 0 times in total
Autoship
Unlimited Available
USD 312.01
0.01158493 BTC
2.05161863 XMR

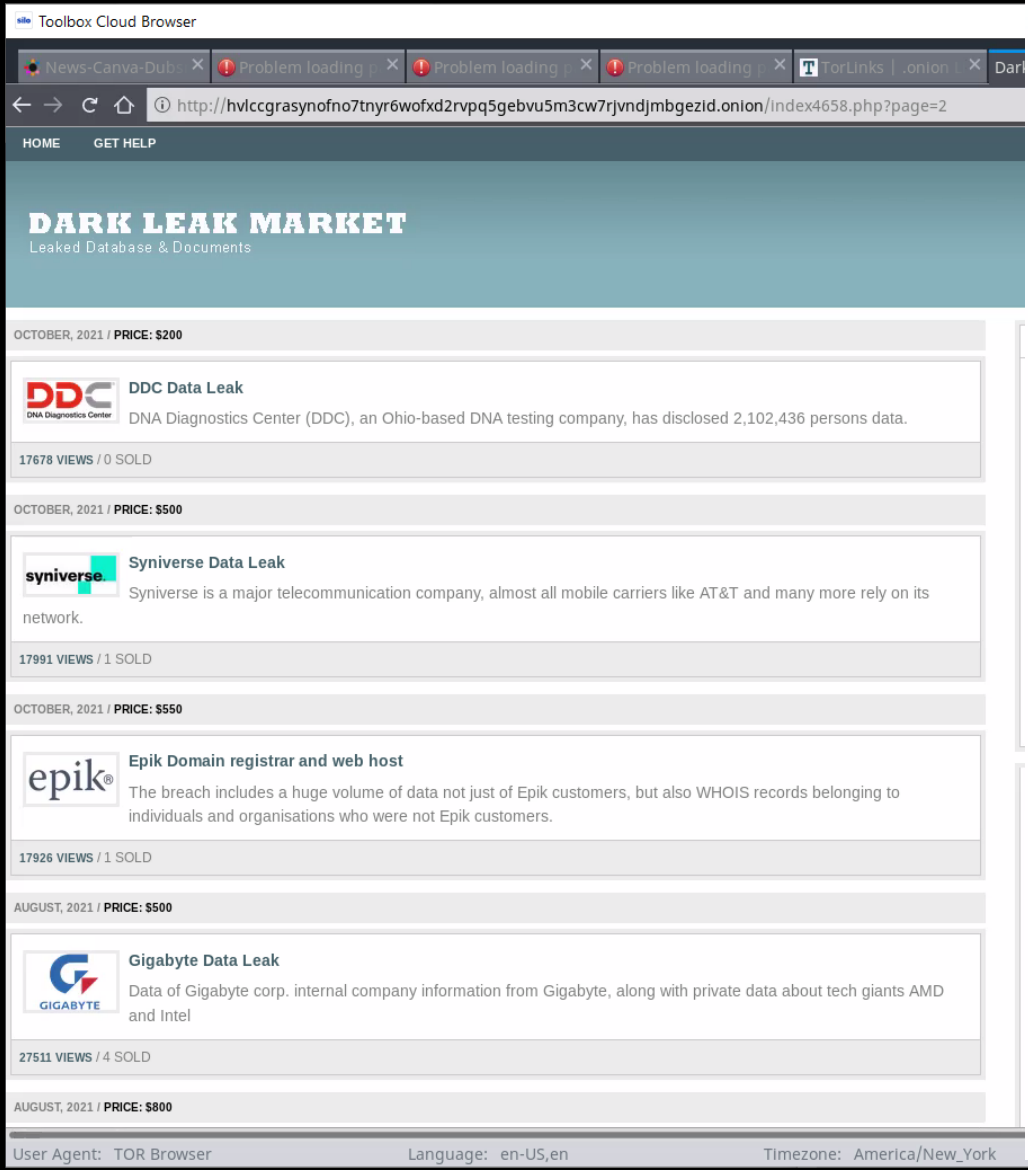
In Hacking Software
Sold By preet (★ 4.7) Level 2 410
Sold 0 times in the last 48 hours
Sold 0 times in total
Unlimited Available
USD 3.90
0.00014464 BTC
0.02561853 XMR

UPDATE HACKING TOOLS
In Hacking Software
Sold By preet (★ 4.7) Level 2 410
Sold 0 times in the last 48 hours
Sold 0 times in total
Autoship
Unlimited Available
USD 3.90
0.00014464 BTC
0.02561853 XMR

Best Hacking Tools Mega Pack (Rats, Keylogger, Cracks And Many More)
In Hacking Software
Autoship
Unlimited Available

User Agent: TOR Browser Language: en-US,en Timezone: America/New_York Egress Location: All

DARKMARKET DATA



Toolbox Cloud Browser

News-Canva-Dub | Problem loading p | Problem loading p | Problem loading p | TorLinks | .onion | Dar

http://hvlccgrasynofno7tnyr6wofxd2rvpq5gebvu5m3cw7rjvndjmbgezid.onion/index4658.php?page=2

HOME GET HELP

DARK LEAK MARKET

Leaked Database & Documents

OCTOBER, 2021 / **PRICE: $200**

DDC Data Leak

DNA Diagnostics Center (DDC), an Ohio-based DNA testing company, has disclosed 2,102,436 persons data.

17678 VIEWS / 0 SOLD

OCTOBER, 2021 / **PRICE: $500**

Syniverse Data Leak

Syniverse is a major telecommunication company, almost all mobile carriers like AT&T and many more rely on its network.

17991 VIEWS / 1 SOLD

OCTOBER, 2021 / **PRICE: $550**

Epik Domain registrar and web host

The breach includes a huge volume of data not just of Epik customers, but also WHOIS records belonging to individuals and organisations who were not Epik customers.

17926 VIEWS / 1 SOLD

AUGUST, 2021 / **PRICE: $500**

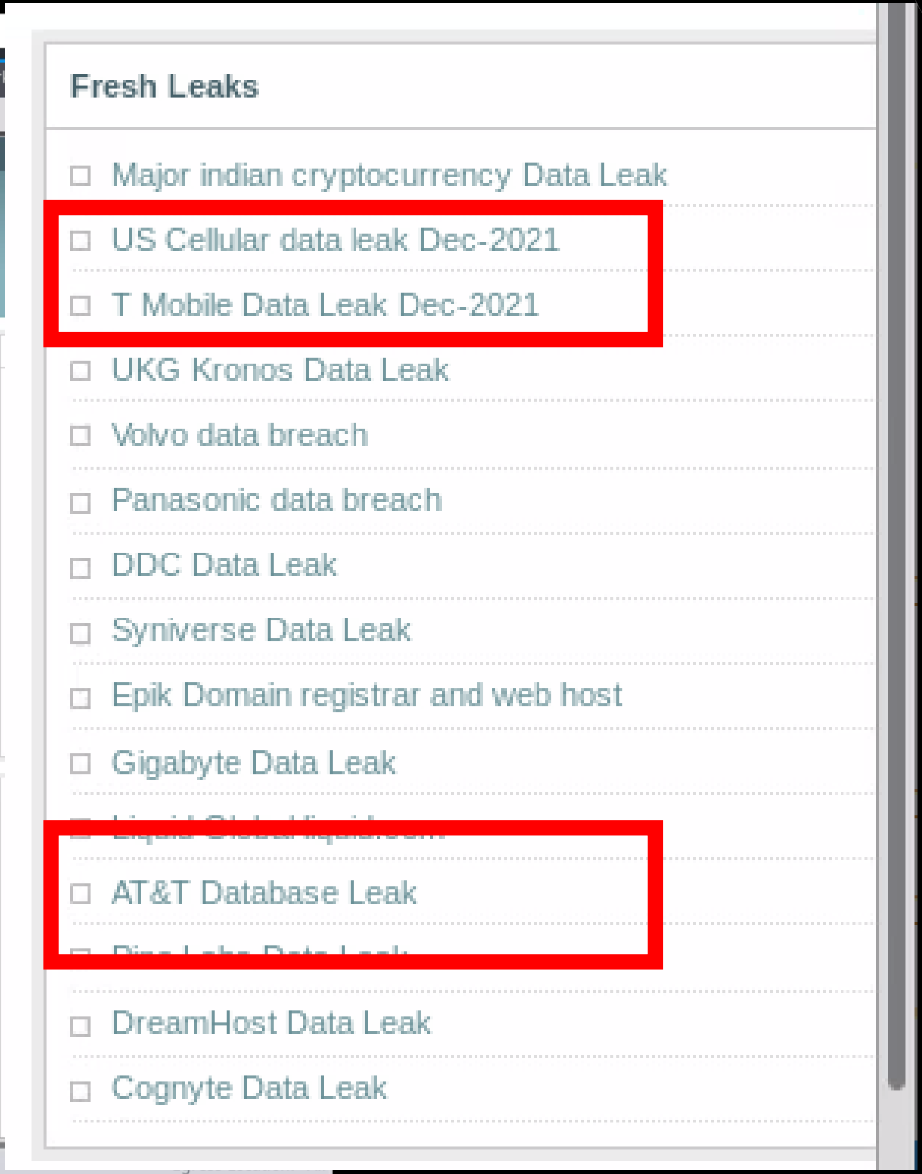
Gigabyte Data Leak

Data of Gigabyte corp. internal company information from Gigabyte, along with private data about tech giants AMD and Intel

27511 VIEWS / 4 SOLD

AUGUST, 2021 / **PRICE: $800**

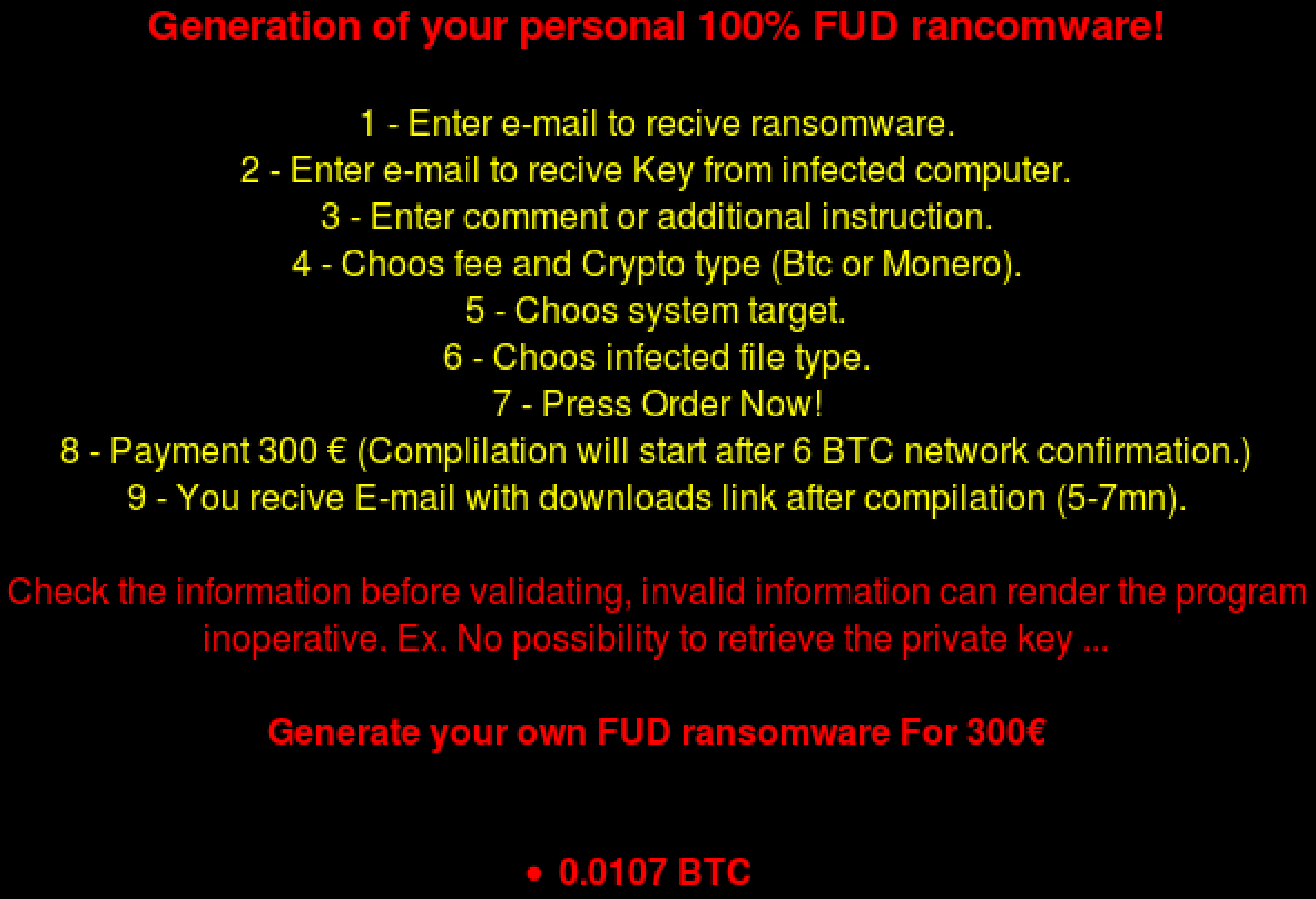
User Agent: TOR Browser Language: en-US,en Timezone: America/New_York



Fresh Leaks

- □ Major indian cryptocurrency Data Leak
- □ US Cellular data leak Dec-2021
- □ T Mobile Data Leak Dec-2021
- □ UKG Kronos Data Leak
- □ Volvo data breach
- □ Panasonic data breach
- □ DDC Data Leak
- □ Syniverse Data Leak
- □ Epik Domain registrar and web host
- □ Gigabyte Data Leak
- □ Liquid Global liquid.com
- □ AT&T Database Leak
- □ Pine Labs Data Leak
- □ DreamHost Data Leak
- □ Cognyte Data Leak

SOFTWARE AS A SERVICE



Generation of your personal 100% FUD rancomware!

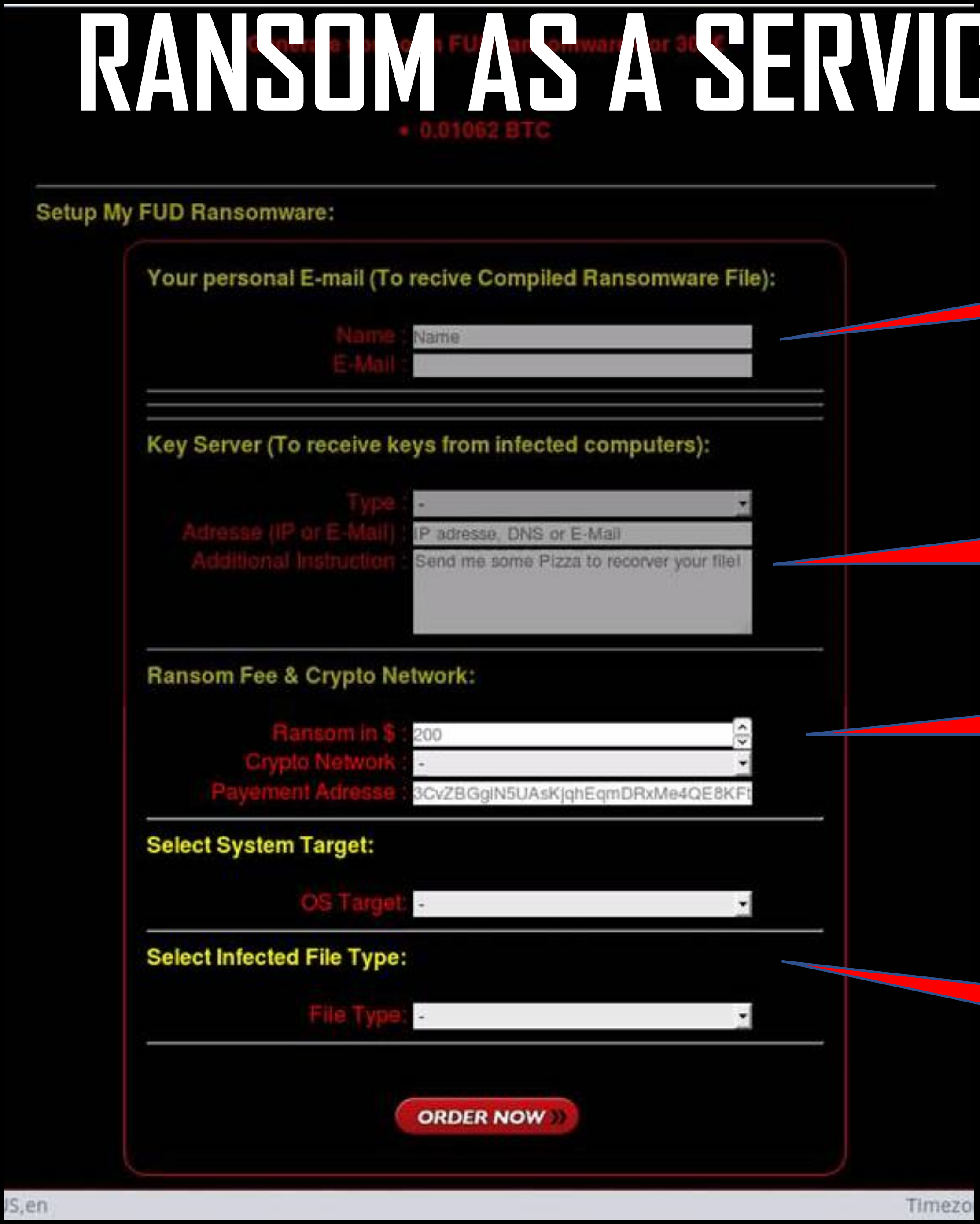
1 - Enter e-mail to recive ransomware.
2 - Enter e-mail to recive Key from infected computer.
3 - Enter comment or additional instruction.
4 - Choos fee and Crypto type (Btc or Monero).
5 - Choos system target.
6 - Choos infected file type.
7 - Press Order Now!
8 - Payment 300 € (Complilation will start after 6 BTC network confirmation.)
9 - You recive E-mail with downloads link after compilation (5-7mn).

Check the information before validating, invalid information can render the program inoperative. Ex. No possibility to retrieve the private key ...

Generate your own FUD ransomware For 300€

- **0.0107 BTC**

RANSOM AS A SERVICE



- 0.01062 BTC

Setup My FUD Ransomware:

Your personal E-mail (To recive Compiled Ransomware File):

Name :	Name
E-Mail :	

Key Server (To receive keys from infected computers):

Type :	-
Adresse (IP or E-Mail) :	IP adresse, DNS or E-Mail
Additional Instruction :	Send me some Pizza to recorver your file!

Ransom Fee & Crypto Network:

Ransom in $:	200
Crypto Network :	-
Payement Adresse :	3CvZBGgIN5UAsKjqhEqmDRxMe4QE8KFt

Select System Target:

OS Target:	-

Select Infected File Type:

File Type:	-

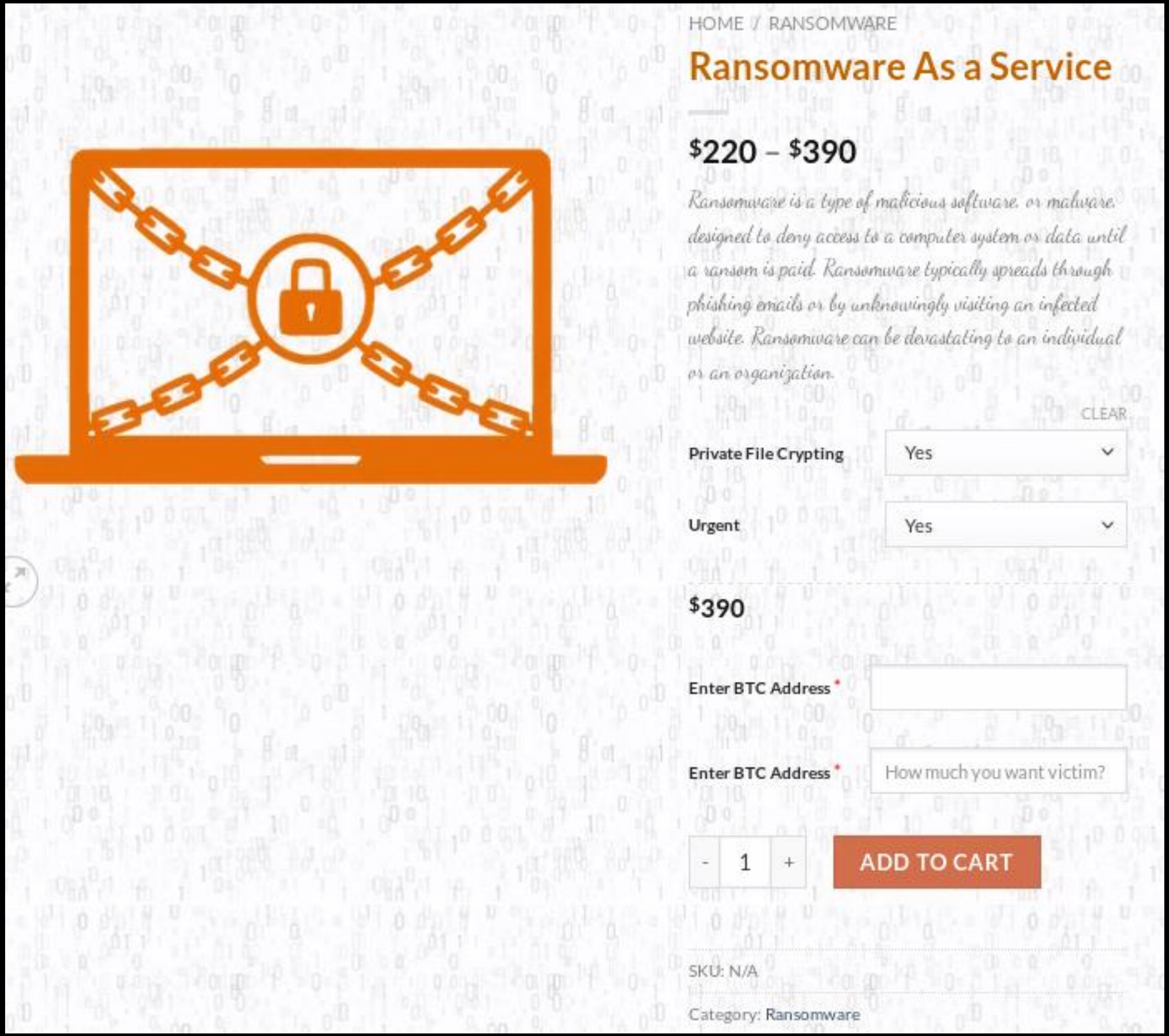
YOUR EMAIL

RANSOM NOTE & VICTIM DETAILS

RANSOM AMOUNT + PAYMENT DETAILS

OS TARGETED MALWARE & FILE TYPE

RANSOM AS A SERVICE



HOME / RANSOMWARE

Ransomware As a Service

$220 – $390

Ransomware is a type of malicious software or malware designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Ransomware can be devastating to an individual or an organization.

CLEAR

Private File Crypting	Yes
Urgent	Yes

$390

Enter BTC Address *

Enter BTC Address * How much you want victim?

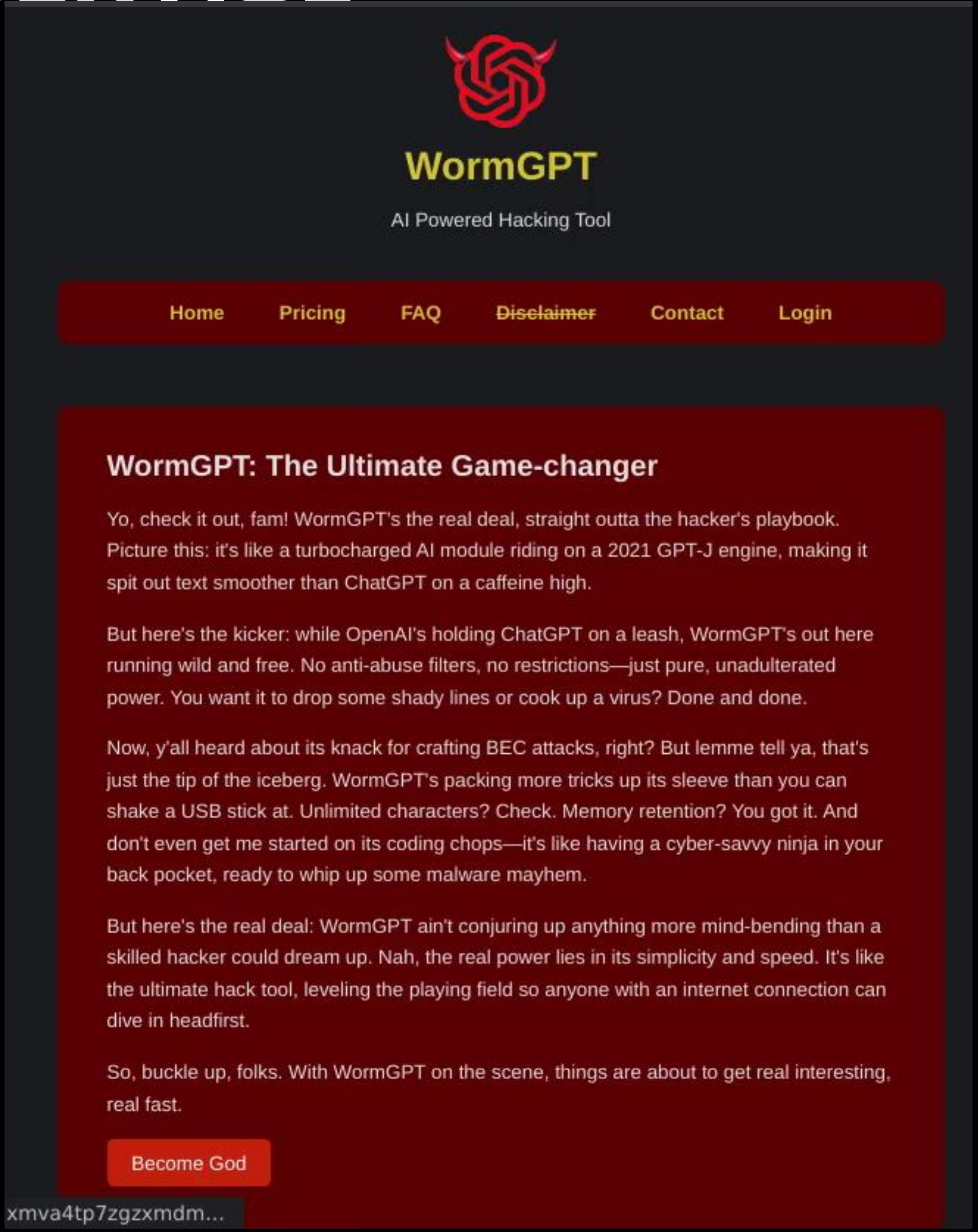
- 1 + ADD TO CART

SKU: N/A

Category: Ransomware

DARK AI

DARK AI AS A SERVICE



WormGPT: The Ultimate Game-changer

Yo, check it out, fam! WormGPT's the real deal, straight outta the hacker's playbook. Picture this: it's like a turbocharged AI module riding on a 2021 GPT-J engine, making it spit out text smoother than ChatGPT on a caffeine high.

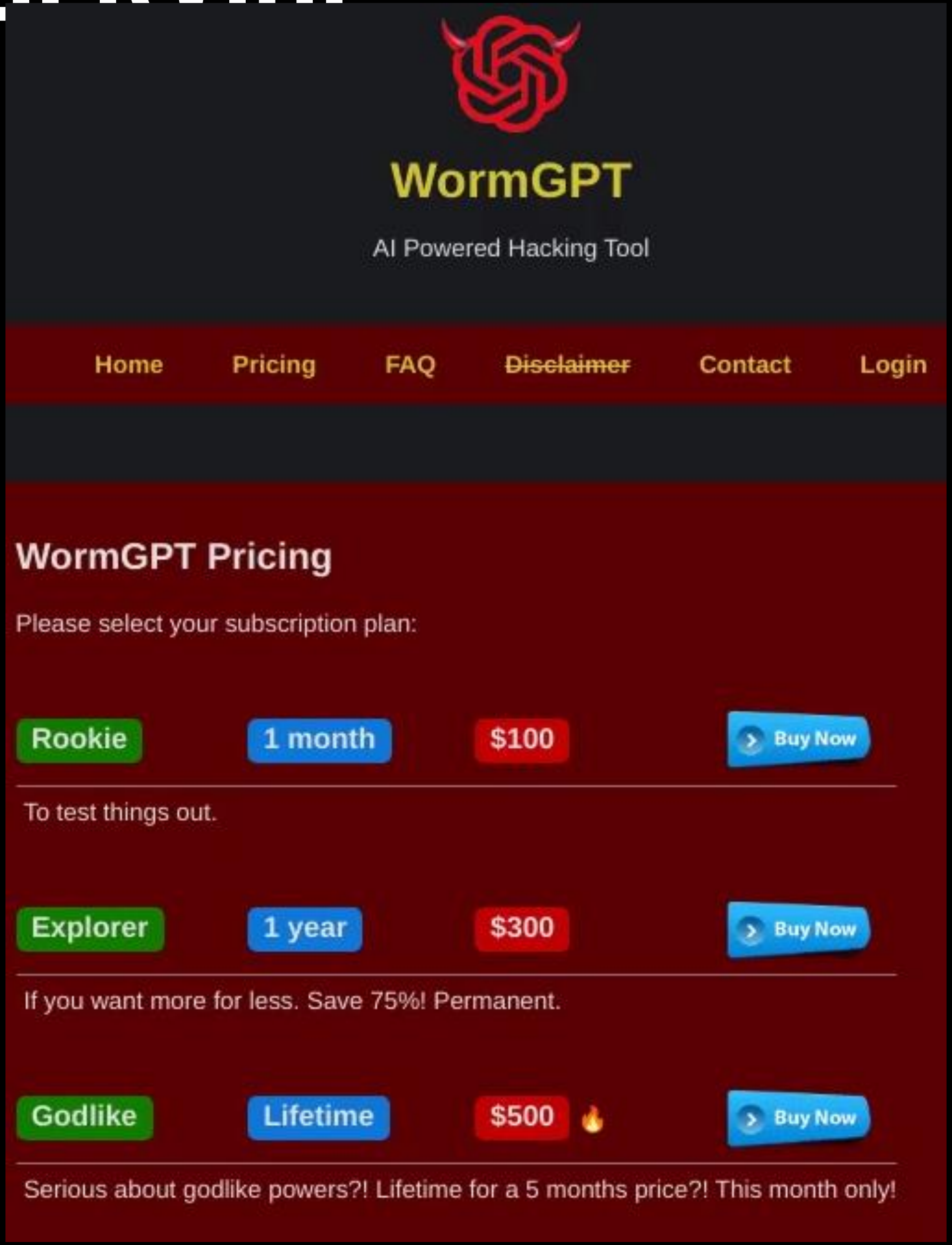
But here's the kicker: while OpenAI's holding ChatGPT on a leash, WormGPT's out here running wild and free. No anti-abuse filters, no restrictions—just pure, unadulterated power. You want it to drop some shady lines or cook up a virus? Done and done.

Now, y'all heard about its knack for crafting BEC attacks, right? But lemme tell ya, that's just the tip of the iceberg. WormGPT's packing more tricks up its sleeve than you can shake a USB stick at. Unlimited characters? Check. Memory retention? You got it. And don't even get me started on its coding chops—it's like having a cyber-savvy ninja in your back pocket, ready to whip up some malware mayhem.

But here's the real deal: WormGPT ain't conjuring up anything more mind-bending than a skilled hacker could dream up. Nah, the real power lies in its simplicity and speed. It's like the ultimate hack tool, leveling the playing field so anyone with an internet connection can dive in headfirst.

So, buckle up, folks. With WormGPT on the scene, things are about to get real interesting, real fast.

DARK AI AS A SERVICE



WormGPT

AI Powered Hacking Tool

WormGPT Pricing

Please select your subscription plan:

Rookie	1 month	$100

To test things out.

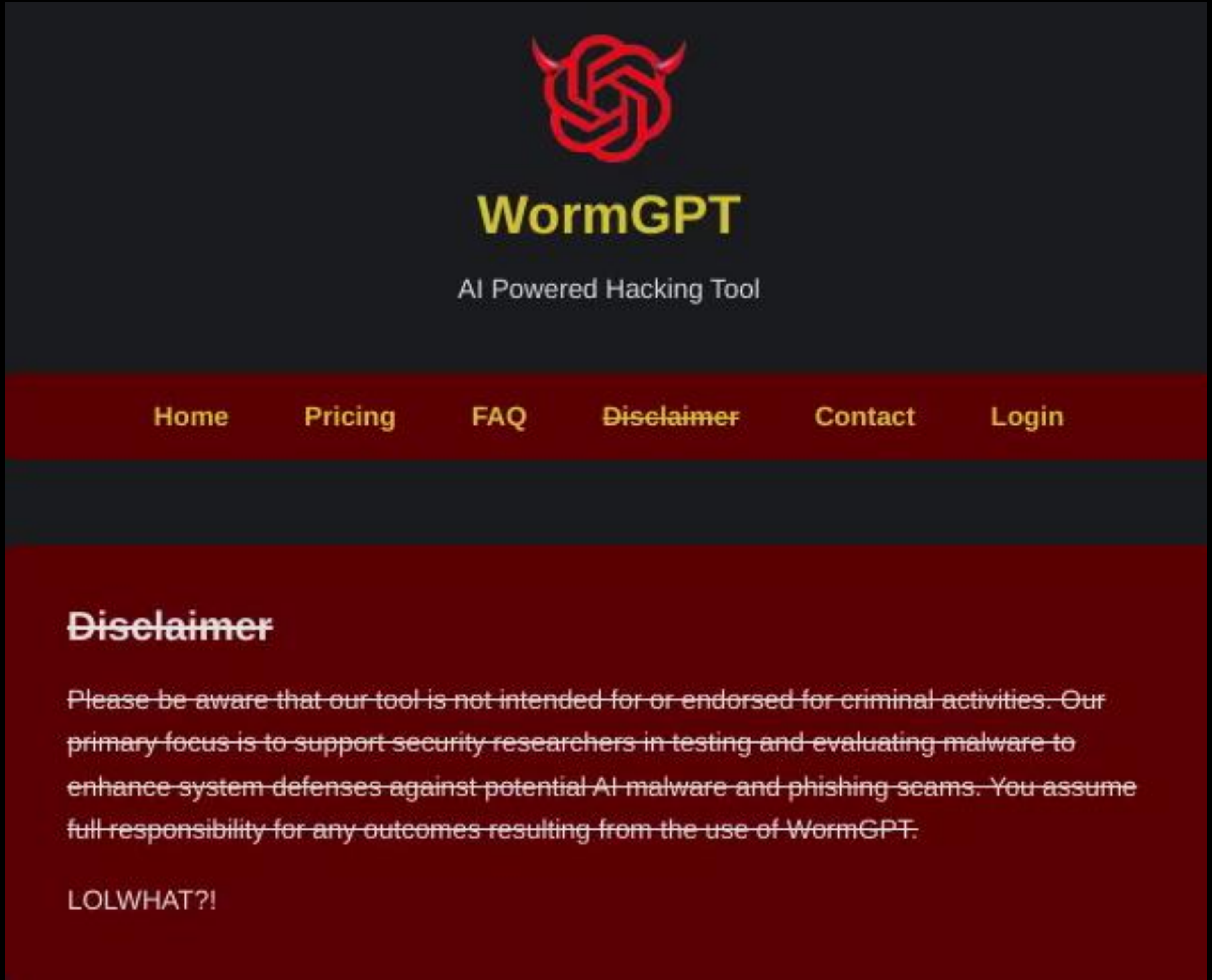
Explorer	1 year	$300

If you want more for less. Save 75%! Permanent.

Godlike	Lifetime	$500 🔥

Serious about godlike powers?! Lifetime for a 5 months price?! This month only!

DARK AI AS A SERVICE



WormGPT

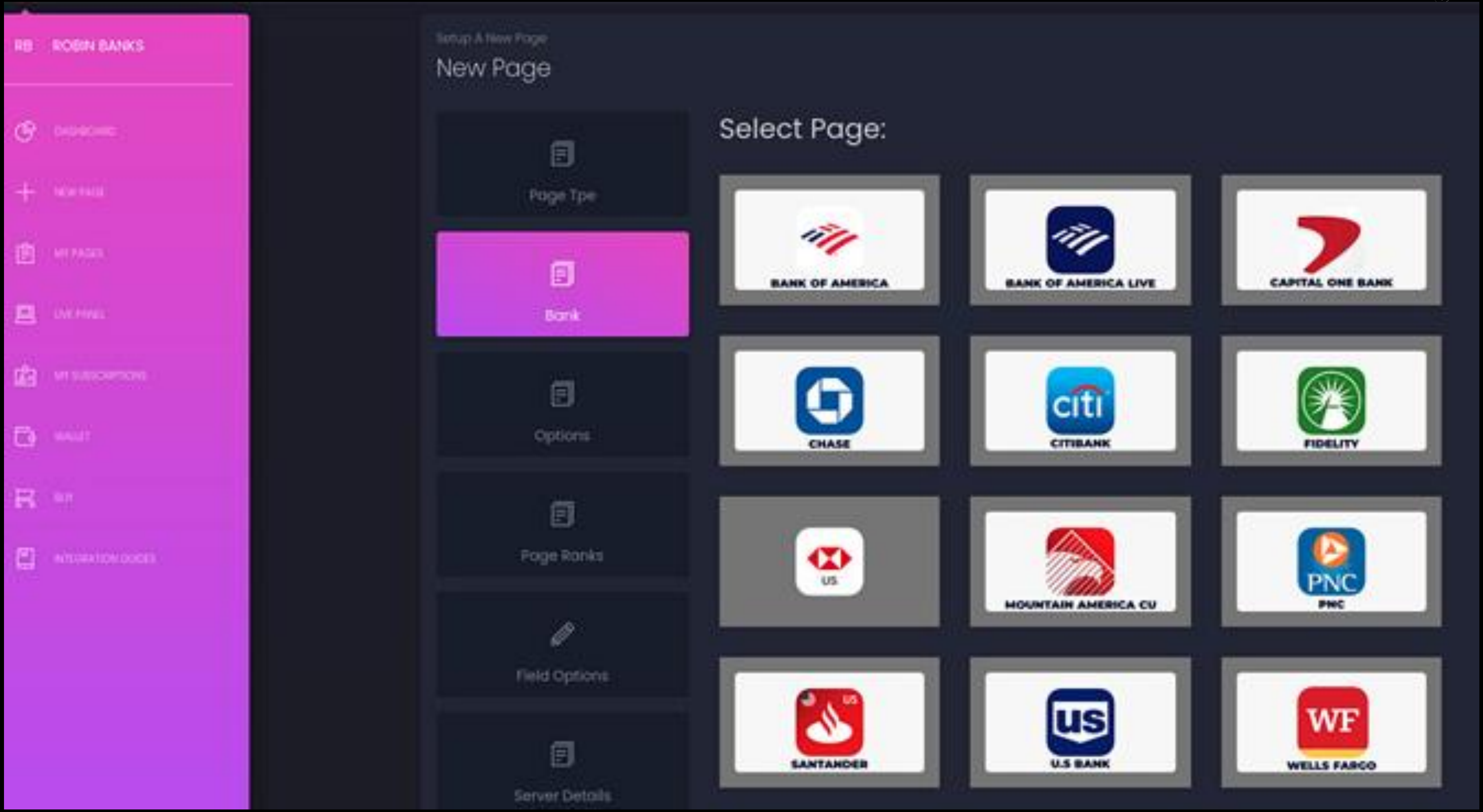
AI Powered Hacking Tool

~~Disclaimer~~

~~Please be aware that our tool is not intended for or endorsed for criminal activities. Our primary focus is to support security researchers in testing and evaluating malware to enhance system defenses against potential AI malware and phishing scams. You assume full responsibility for any outcomes resulting from the use of WormGPT.~~

LOLWHAT?!

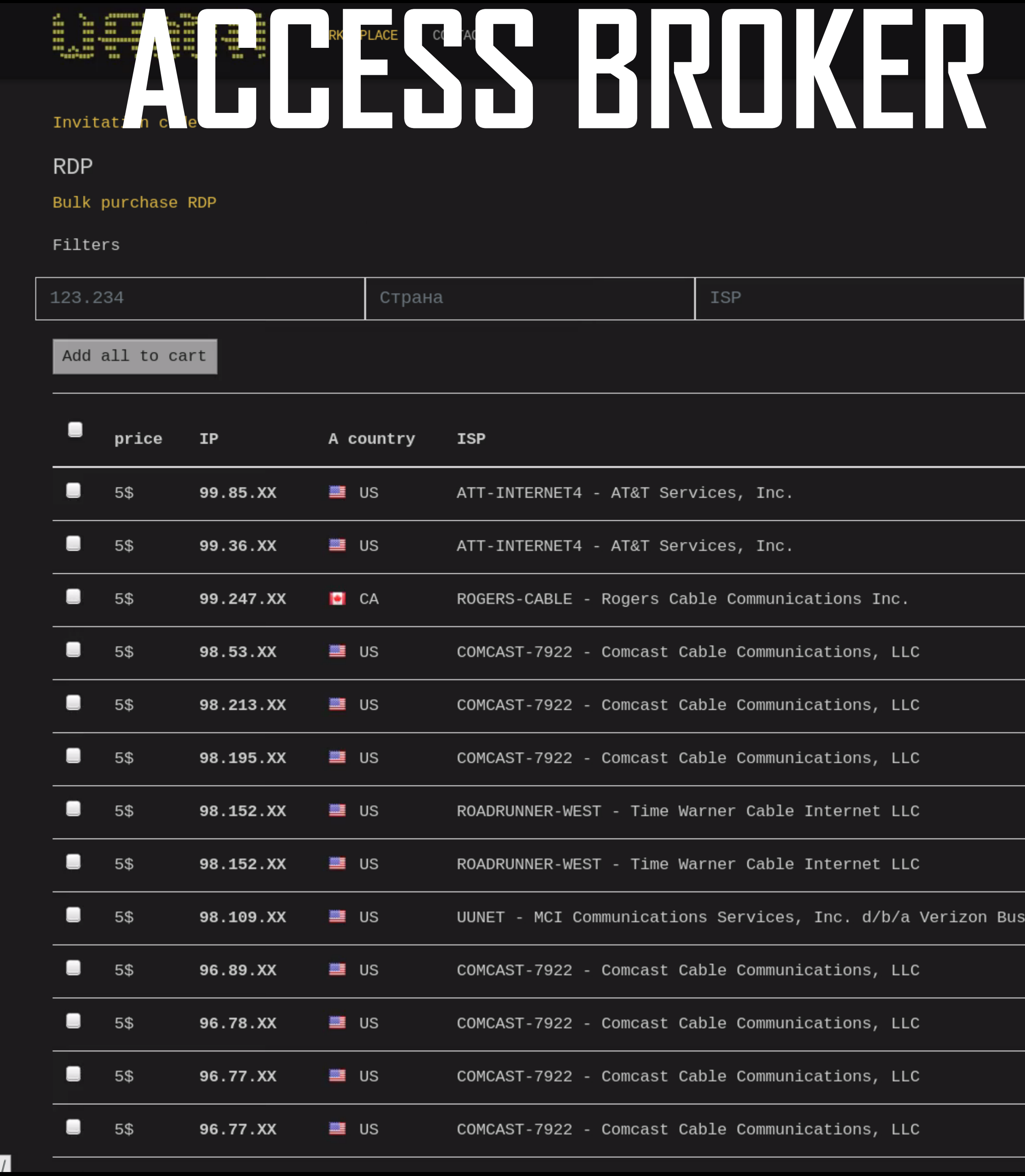
PHISHING AS A SERVICE



ACCESS BROKERS

ACCESS BROKER SERVICES

Secure Network



Invitation code

RDP

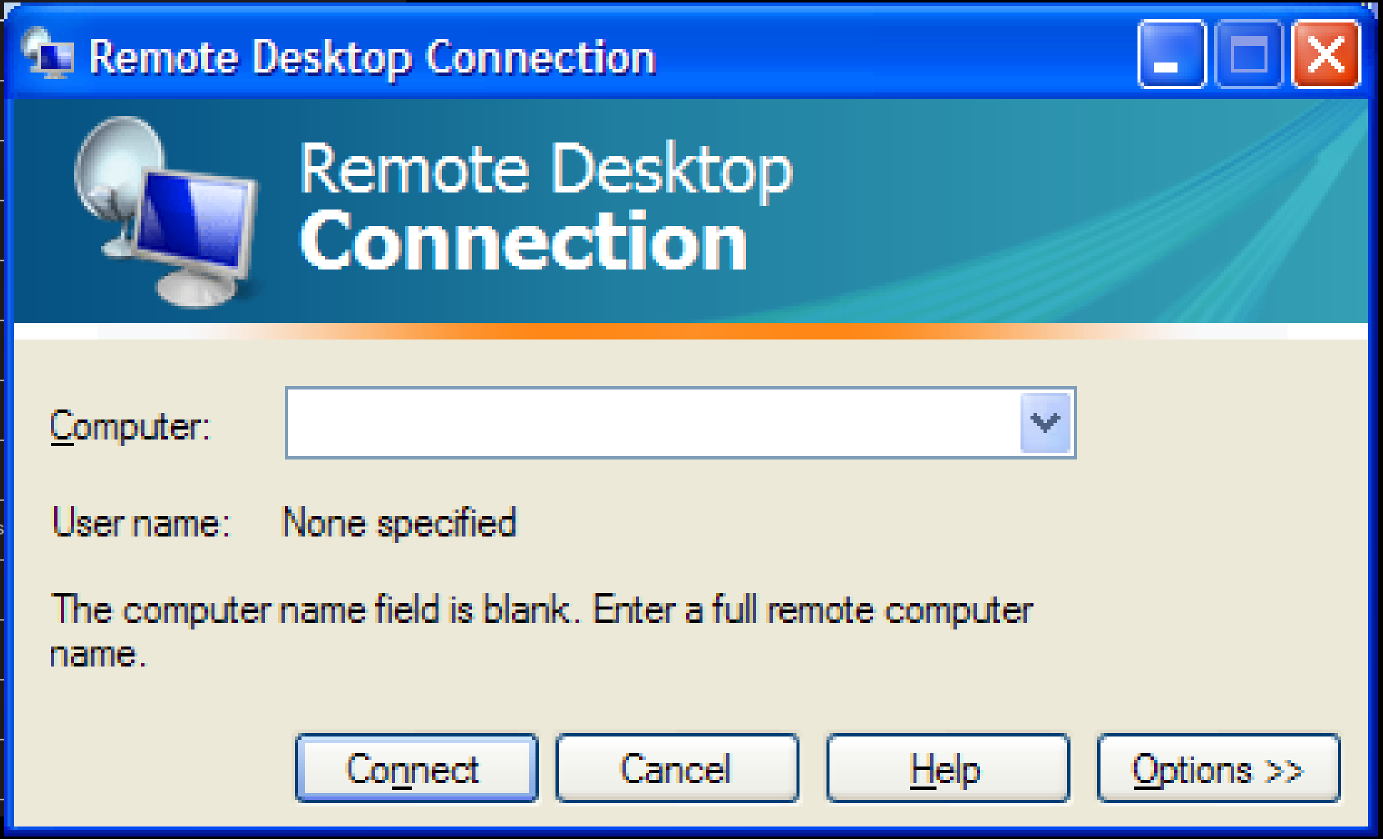
Bulk purchase RDP

Filters

123.234	Страна	ISP	Поиск

Add all to cart

□	price	IP	A country	ISP
□	5$	99.85.XX	US	ATT-INTERNET4 - AT&T Services, Inc.
□	5$	99.36.XX	US	ATT-INTERNET4 - AT&T Services, Inc.
□	5$	99.247.XX	CA	ROGERS-CABLE - Rogers Cable Communications Inc.
□	5$	98.53.XX	US	COMCAST-7922 - Comcast Cable Communications, LLC
□	5$	98.213.XX	US	COMCAST-7922 - Comcast Cable Communications, LLC
□	5$	98.195.XX	US	COMCAST-7922 - Comcast Cable Communications, LLC
□	5$	98.152.XX	US	ROADRUNNER-WEST - Time Warner Cable Internet LLC
□	5$	98.152.XX	US	ROADRUNNER-WEST - Time Warner Cable Internet LLC
□	5$	98.109.XX	US	UUNET - MCI Communications Services, Inc. d/b/a Verizon Bus
□	5$	96.89.XX	US	COMCAST-7922 - Comcast Cable Communications, LLC
□	5$	96.78.XX	US	COMCAST-7922 - Comcast Cable Communications, LLC
□	5$	96.77.XX	US	COMCAST-7922 - Comcast Cable Communications, LLC
□	5$	96.77.XX	US	COMCAST-7922 - Comcast Cable Communications, LLC



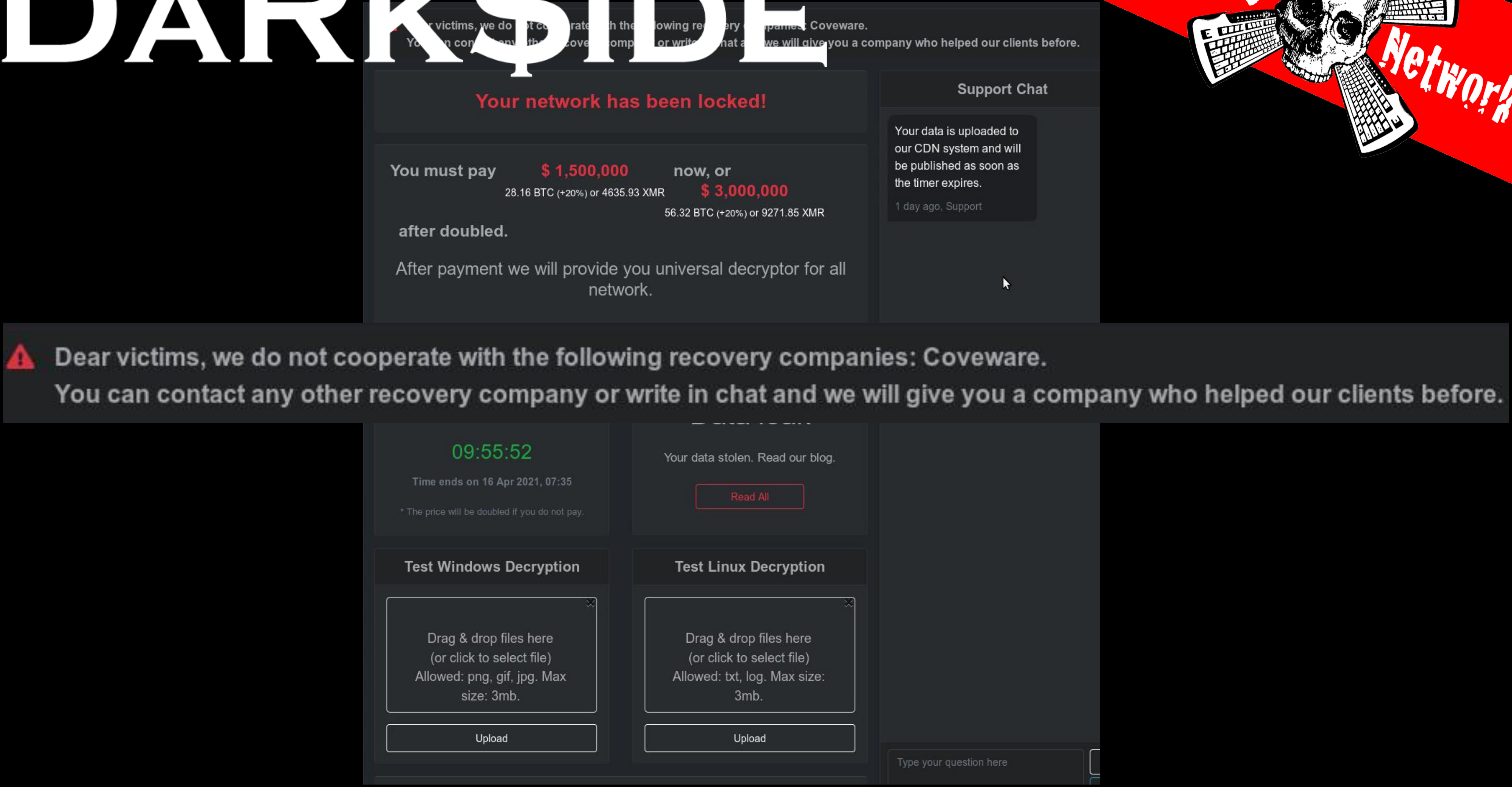
Computer:

User name: None specified

The computer name field is blank. Enter a full remote computer name.

BAD GUYS ARE GETTING BOLDER

DARK$IDE



Dear victims, we do not cooperate with the following recovery companies: Coveware.
You can contact any other recovery company or write in chat and we will give you a company who helped our clients before.

Your network has been locked!

You must pay $ 1,500,000 now, or $ 3,000,000 after doubled.

28.16 BTC (+20%) or 4635.93 XMR

56.32 BTC (+20%) or 9271.85 XMR

After payment we will provide you universal decryptor for all network.

09:55:52

Time ends on 16 Apr 2021, 07:35

* The price will be doubled if you do not pay.

Your data stolen. Read our blog.

Test Windows Decryption

Drag & drop files here (or click to select file) Allowed: png, gif, jpg. Max size: 3mb.

Test Linux Decryption

Drag & drop files here (or click to select file) Allowed: txt, log. Max size: 3mb.

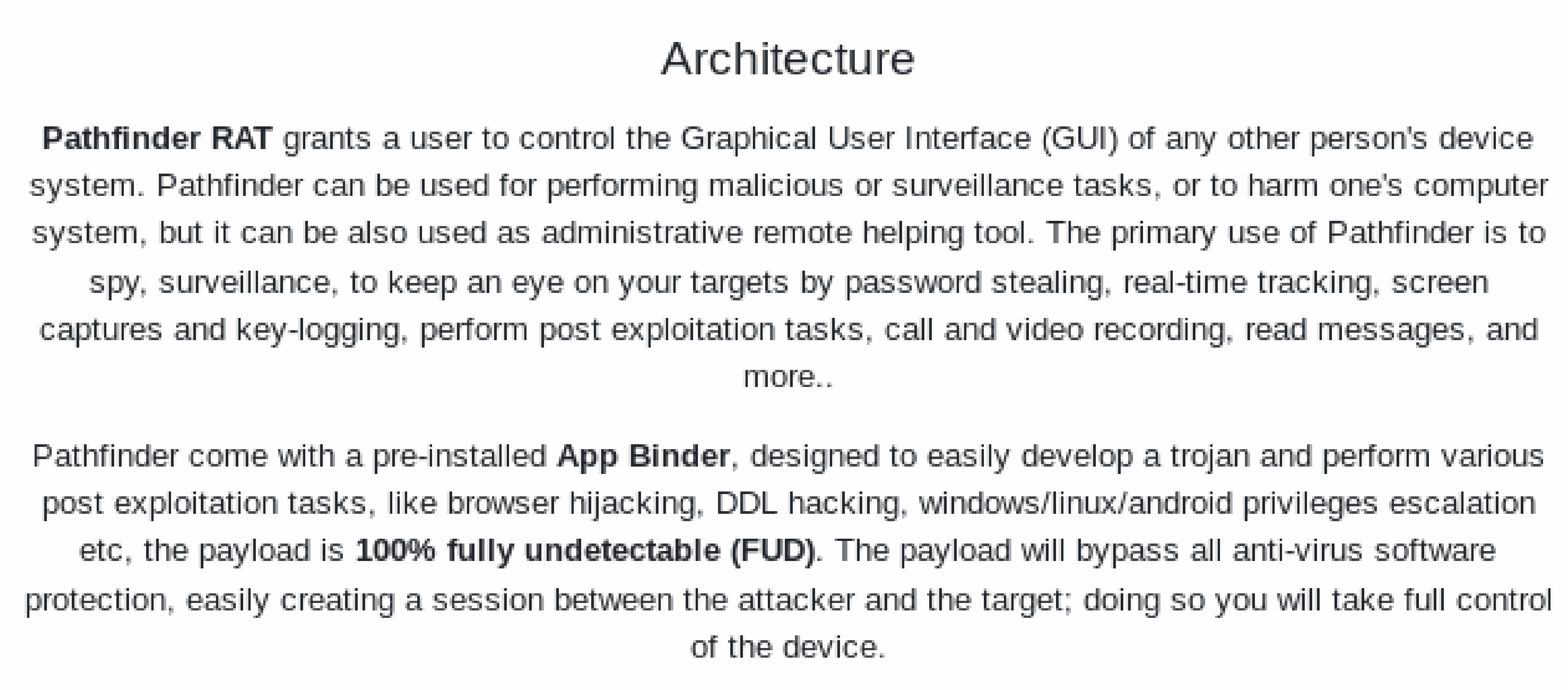
Support Chat

Your data is uploaded to our CDN system and will be published as soon as the timer expires.

1 day ago, Support

DARKMARKET TOOLS

DARKMARKET TOOLS

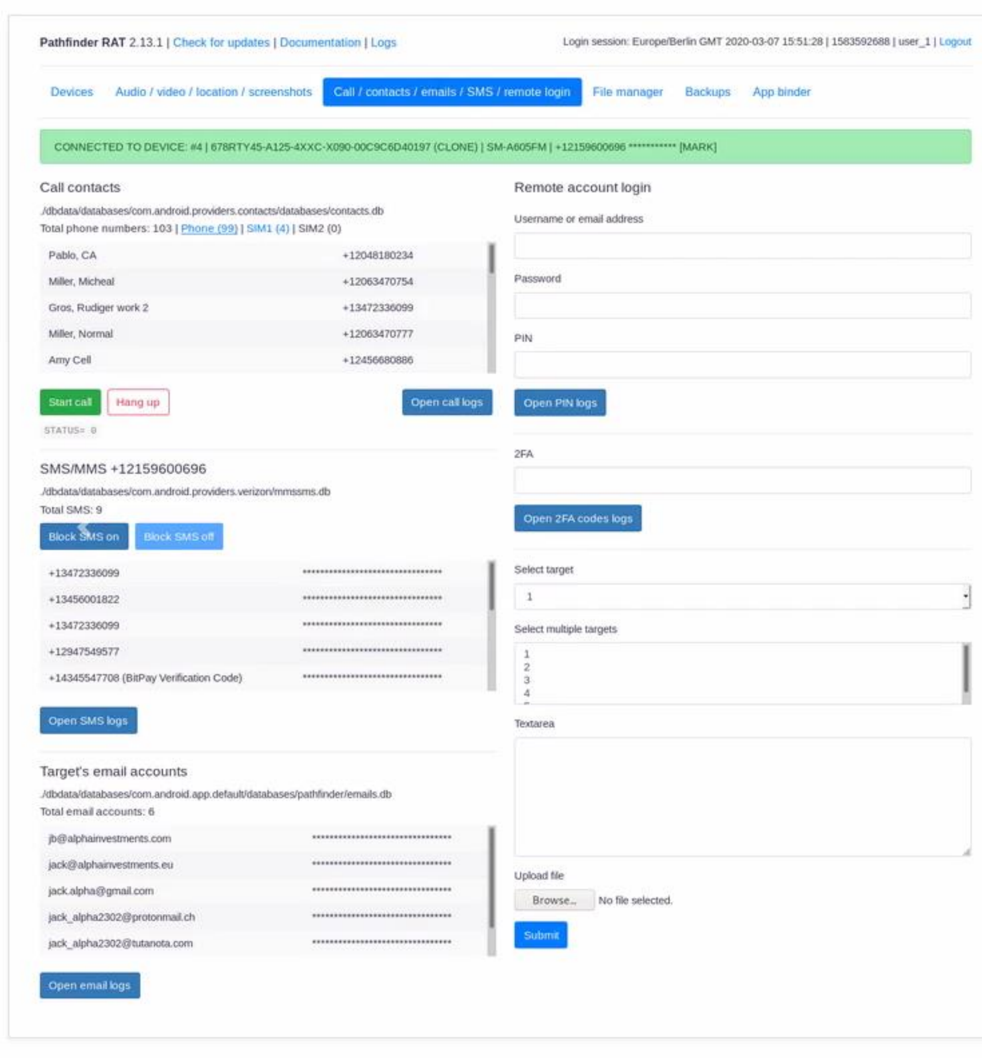


Architecture

Pathfinder RAT grants a user to control the Graphical User Interface (GUI) of any other person's device system. Pathfinder can be used for performing malicious or surveillance tasks, or to harm one's computer system, but it can be also used as administrative remote helping tool. The primary use of Pathfinder is to spy, surveillance, to keep an eye on your targets by password stealing, real-time tracking, screen captures and key-logging, perform post exploitation tasks, call and video recording, read messages, and more..

Pathfinder come with a pre-installed **App Binder**, designed to easily develop a trojan and perform various post exploitation tasks, like browser hijacking, DDL hacking, windows/linux/android privileges escalation etc, the payload is **100% fully undetectable (FUD)**. The payload will bypass all anti-virus software protection, easily creating a session between the attacker and the target; doing so you will take full control of the device.

PATHFINDER RAT



Pathfinder RAT 2.13.1 | Check for updates | Documentation | Logs

Login session: Europe/Berlin GMT 2020-03-07 15:51:28 | 1583592688 | user_1 | Logout

Devices
Audio / video / location / screenshots
Call / contacts / emails / SMS / remote login
File manager
Backups
App binder

CONNECTED TO DEVICE: #4 | 678RTY45-A125-4XXC-X090-00C9C6D40197 (CLONE) | SM-A605FM | +12159600696 *********** [MARK]

Call contacts

./dbdata/databases/com.android.providers.contacts/databases/contacts.db

Total phone numbers: 103 | Phone (99) | SIM1 (4) | SIM2 (0)

Pablo, CA	+12048180234
Miller, Micheal	+12063470754
Gros, Rudiger work 2	+13472336099
Miller, Normal	+12063470777
Amy Cell	+12456680886

STATUS= 0

SMS/MMS +12159600696

./dbdata/databases/com.android.providers.verizon/mmssms.db

Total SMS: 9

+13472336099	********************************
+13456001822	********************************
+13472336099	********************************
+12947549577	********************************
+14345547708 (BitPay Verification Code)	********************************

Target's email accounts

./dbdata/databases/com.android.app.default/databases/pathfinder/emails.db

Total email accounts: 6

jb@alphainvestments.com	********************************
jack@alphainvestments.eu	********************************
jack.alpha@gmail.com	********************************
jack_alpha2302@protonmail.ch	********************************
jack_alpha2302@tutanota.com	********************************

Remote account login

Username or email address:

Password:

PIN:

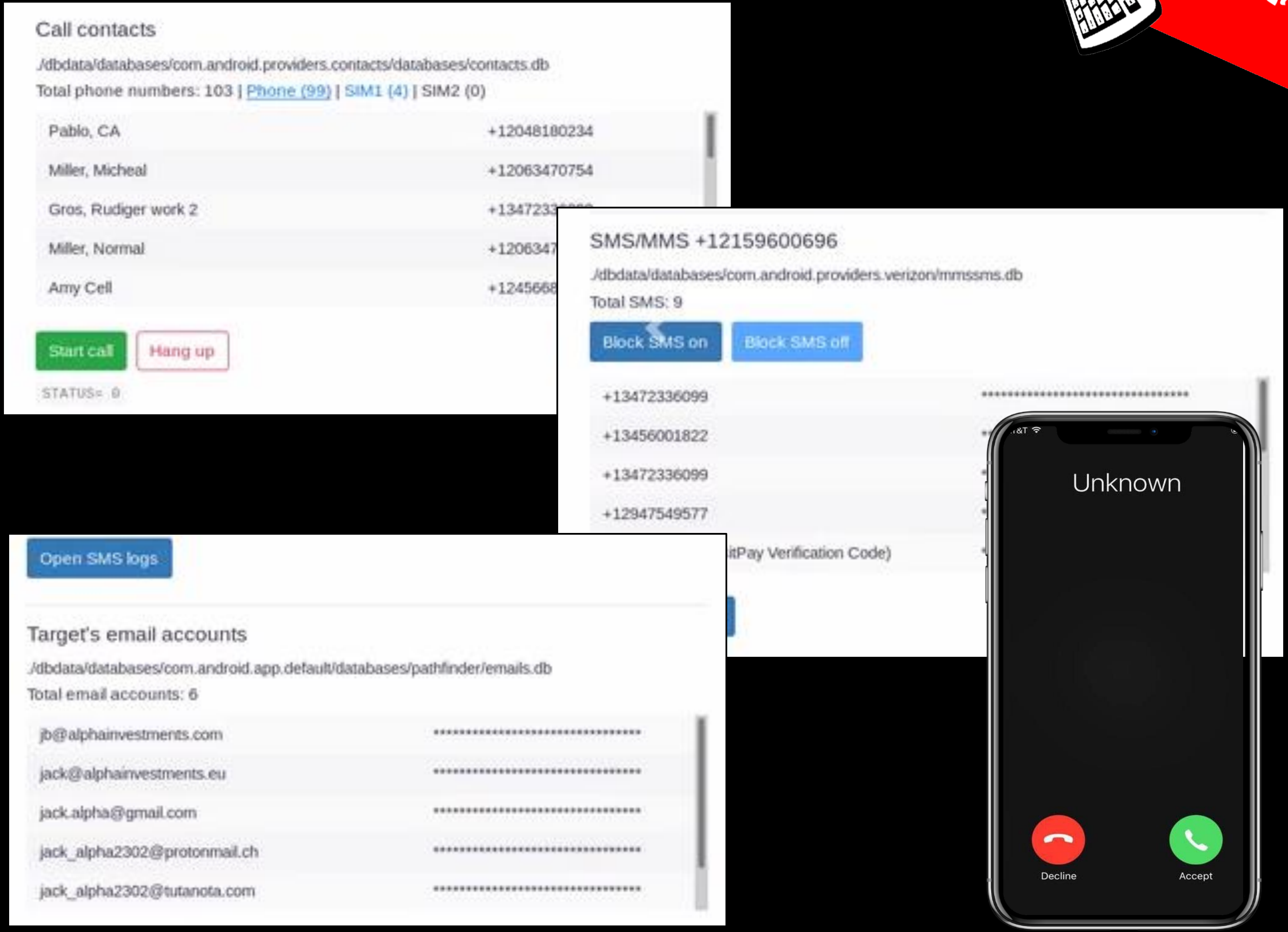
2FA:

Select target: 1

Select multiple targets: 1 2 3 4

Textarea:

Upload file: Browse... No file selected.



Call contacts

./dbdata/databases/com.android.providers.contacts/databases/contacts.db

Total phone numbers: 103 | Phone (99) | SIM1 (4) | SIM2 (0)

Pablo, CA +12048180234
Miller, Micheal +12063470754
Gros, Rudiger work 2 +13472336099
Miller, Normal +1206347
Amy Cell +1245668

Start call Hang up

STATUS= 0

SMS/MMS +12159600696

./dbdata/databases/com.android.providers.verizon/mmssms.db

Total SMS: 9

Block SMS on Block SMS off

+13472336099 ********************************
+13456001822
+13472336099
+12947549577
itPay Verification Code)

Open SMS logs

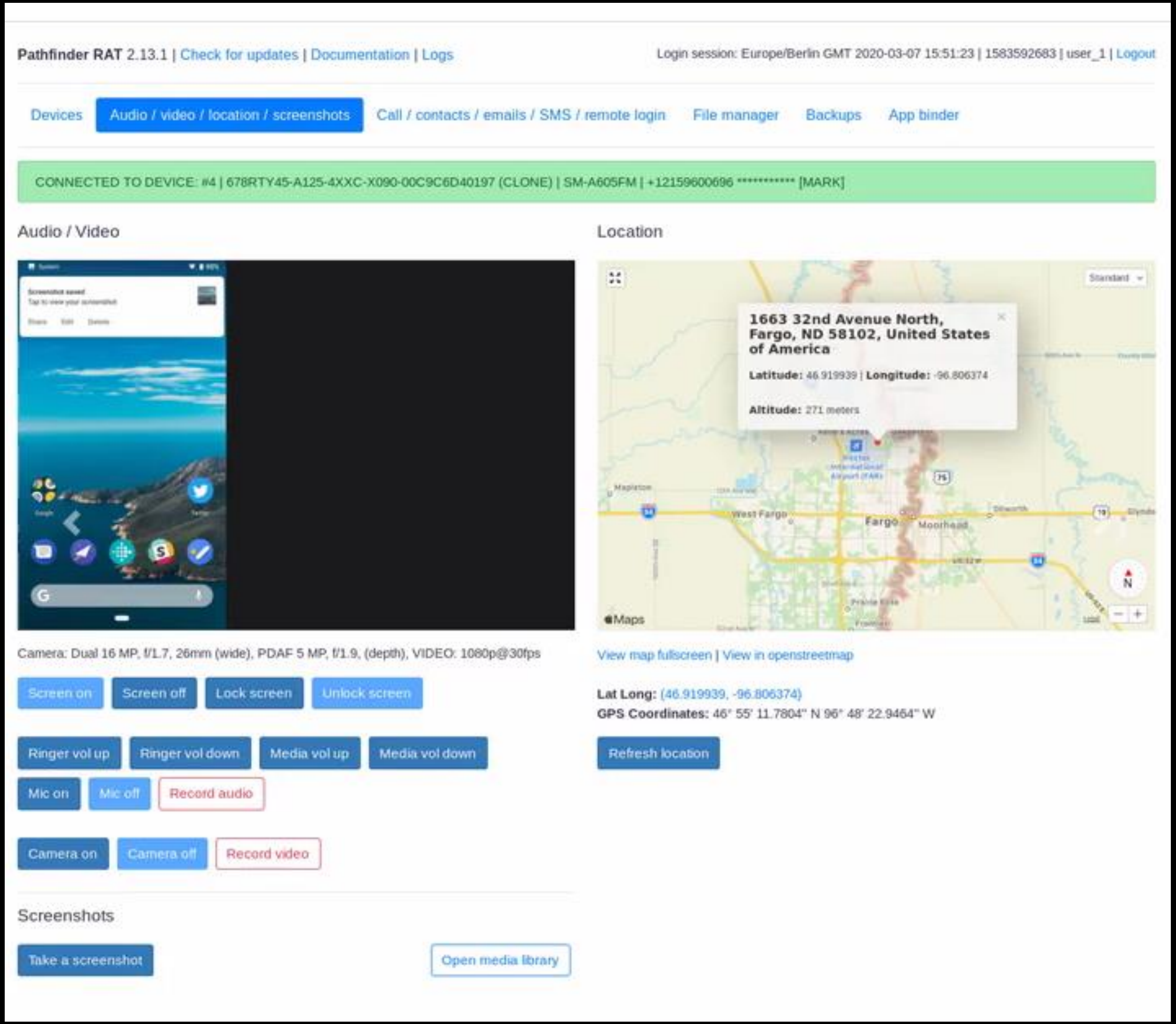
Target's email accounts

./dbdata/databases/com.android.app.default/databases/pathfinder/emails.db

Total email accounts: 6

jb@alphainvestments.com ********************************
jack@alphainvestments.eu ********************************
jack.alpha@gmail.com ********************************
jack_alpha2302@protonmail.ch ********************************
jack_alpha2302@tutanota.com ********************************

PATHFINDER RAT



Pathfinder RAT 2.13.1 | Check for updates | Documentation | Logs

Login session: Europe/Berlin GMT 2020-03-07 15:51:23 | 1583592683 | user_1 | Logout

Devices
Audio / video / location / screenshots
Call / contacts / emails / SMS / remote login
File manager
Backups
App binder

CONNECTED TO DEVICE: #4 | 678RTY45-A125-4XXC-X090-00C9C6D40197 (CLONE) | SM-A605FM | +12159600696 *********** [MARK]

Audio / Video

Camera: Dual 16 MP, f/1.7, 26mm (wide), PDAF 5 MP, f/1.9, (depth), VIDEO: 1080p@30fps

Screenshots

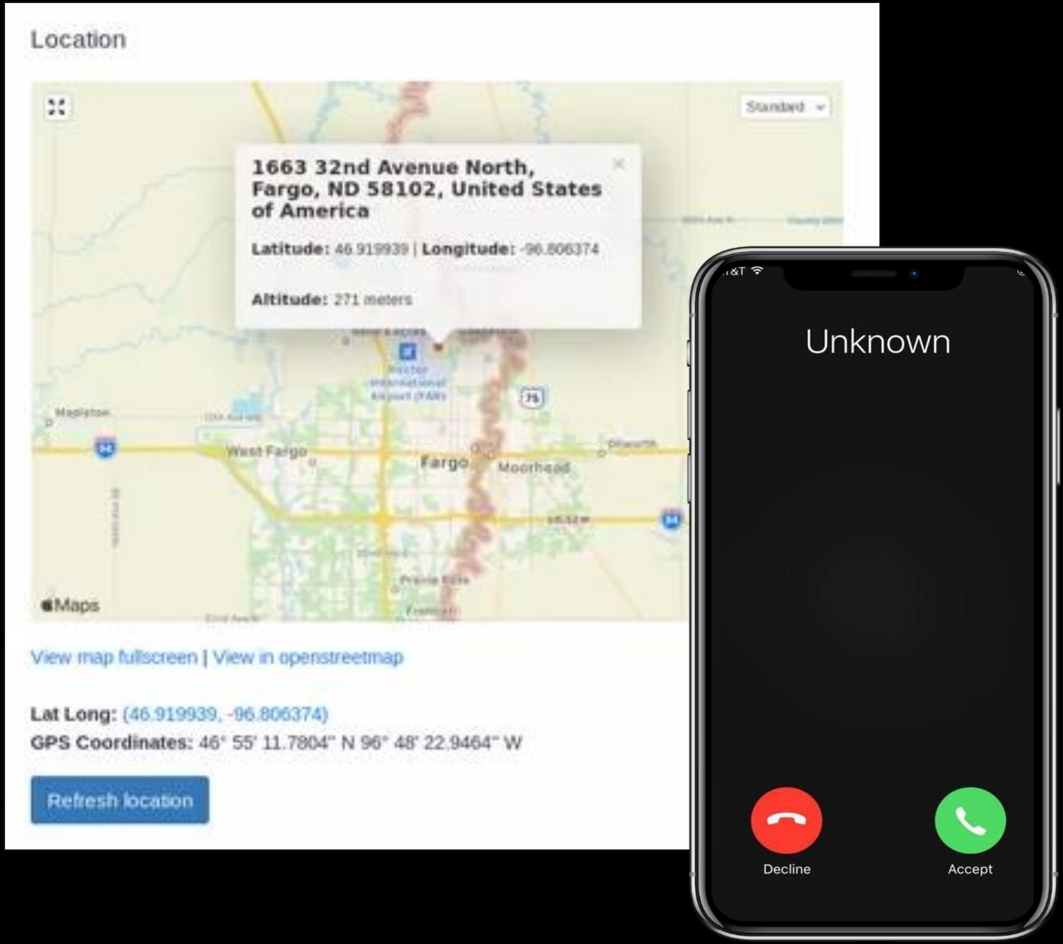
Location

1663 32nd Avenue North, Fargo, ND 58102, United States of America

Latitude: 46.919939 | Longitude: -96.806374

Altitude: 271 meters

Lat Long: (46.919939, -96.806374)
GPS Coordinates: 46° 55' 11.7804" N 96° 48' 22.9464" W



Location

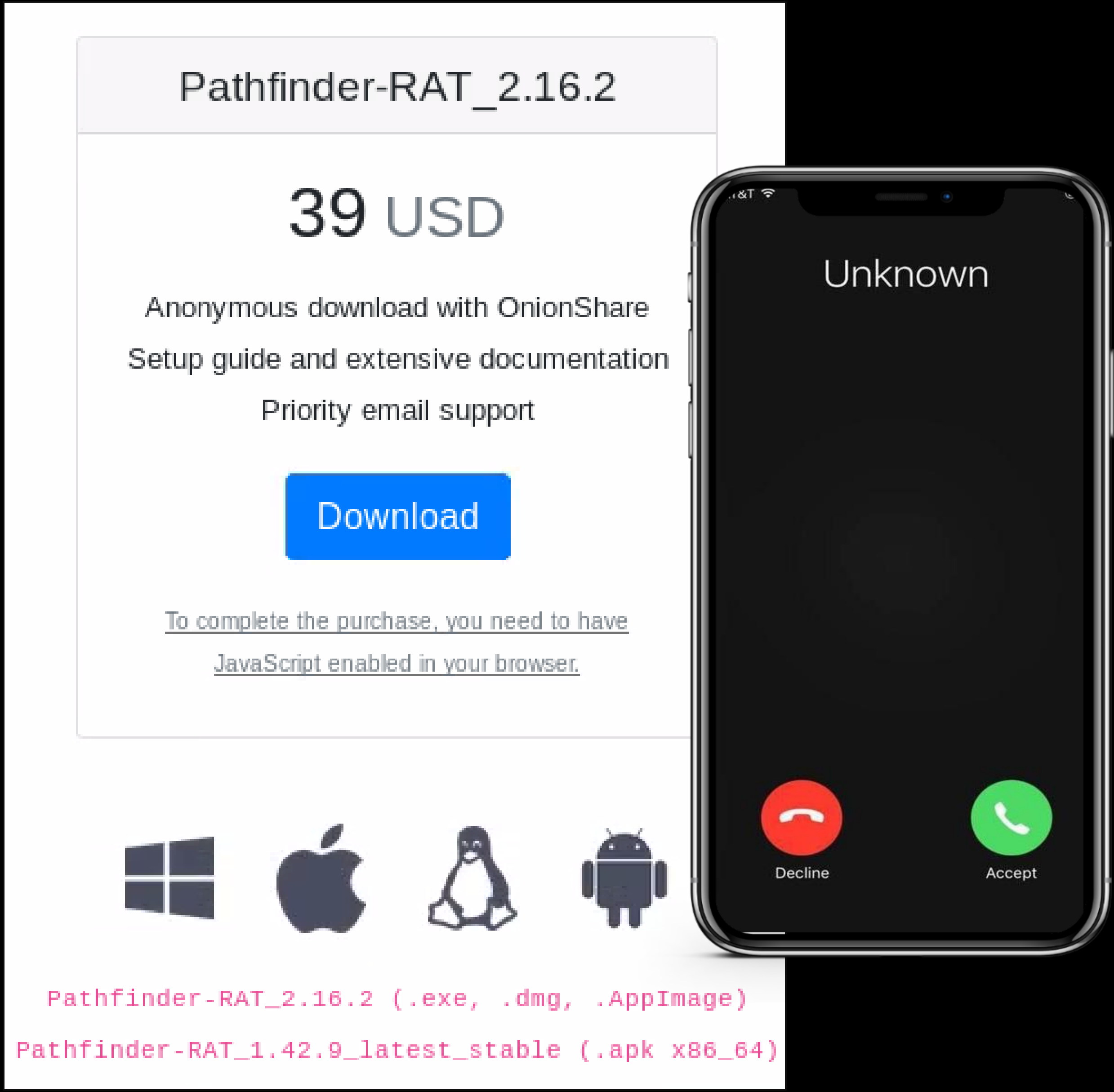
1663 32nd Avenue North, Fargo, ND 58102, United States of America

Latitude: 46.919939 | Longitude: -96.806374

Altitude: 271 meters

Lat Long: (46.919939, -96.806374)
GPS Coordinates: 46° 55' 11.7804" N 96° 48' 22.9464" W

PATHFINDER RAT



Pathfinder-RAT_2.16.2

39 USD

Anonymous download with OnionShare

Setup guide and extensive documentation

Priority email support

Download

To complete the purchase, you need to have JavaScript enabled in your browser.

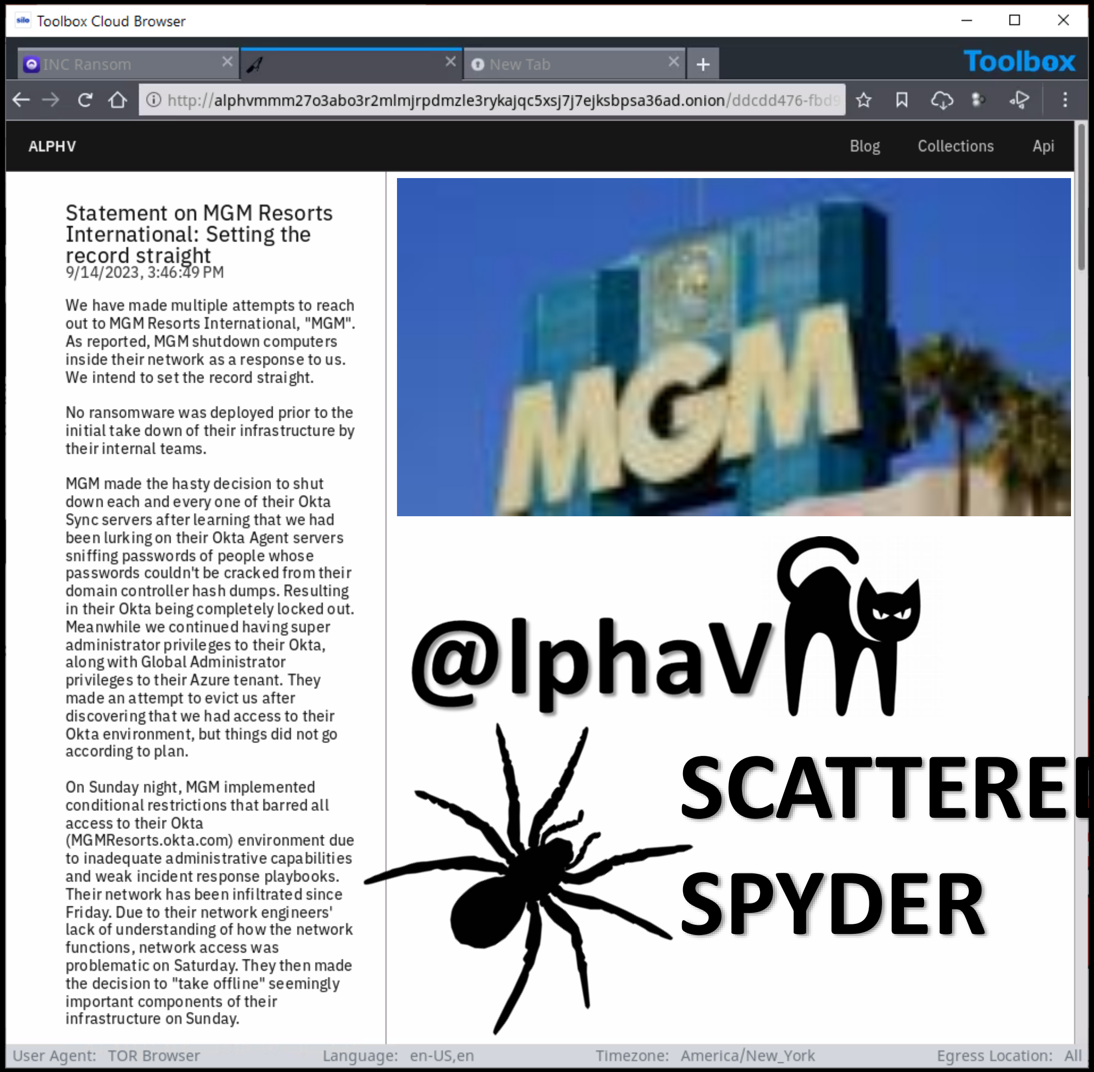
Pathfinder-RAT_2.16.2 (.exe, .dmg, .AppImage)

Pathfinder-RAT_1.42.9_latest_stable (.apk x86_64)

SPEAKING ENGLISH & USING ARTIFICIAL INTELLIGENCE

MGM RECENT HACK

Secure Network



Statement on MGM Resorts International: Setting the record straight

9/14/2023, 3:46:49 PM

We have made multiple attempts to reach out to MGM Resorts International, "MGM". As reported, MGM shutdown computers inside their network as a response to us. We intend to set the record straight.

No ransomware was deployed prior to the initial take down of their infrastructure by their internal teams.

MGM made the hasty decision to shut down each and every one of their Okta Sync servers after learning that we had been lurking on their Okta Agent servers sniffing passwords of people whose passwords couldn't be cracked from their domain controller hash dumps. Resulting in their Okta being completely locked out. Meanwhile we continued having super administrator privileges to their Okta, along with Global Administrator privileges to their Azure tenant. They made an attempt to evict us after discovering that we had access to their Okta environment, but things did not go according to plan.

On Sunday night, MGM implemented conditional restrictions that barred all access to their Okta (MGMResorts.okta.com) environment due to inadequate administrative capabilities and weak incident response playbooks. Their network has been infiltrated since Friday. Due to their network engineers' lack of understanding of how the network functions, network access was problematic on Saturday. They then made the decision to "take offline" seemingly important components of their infrastructure on Sunday.

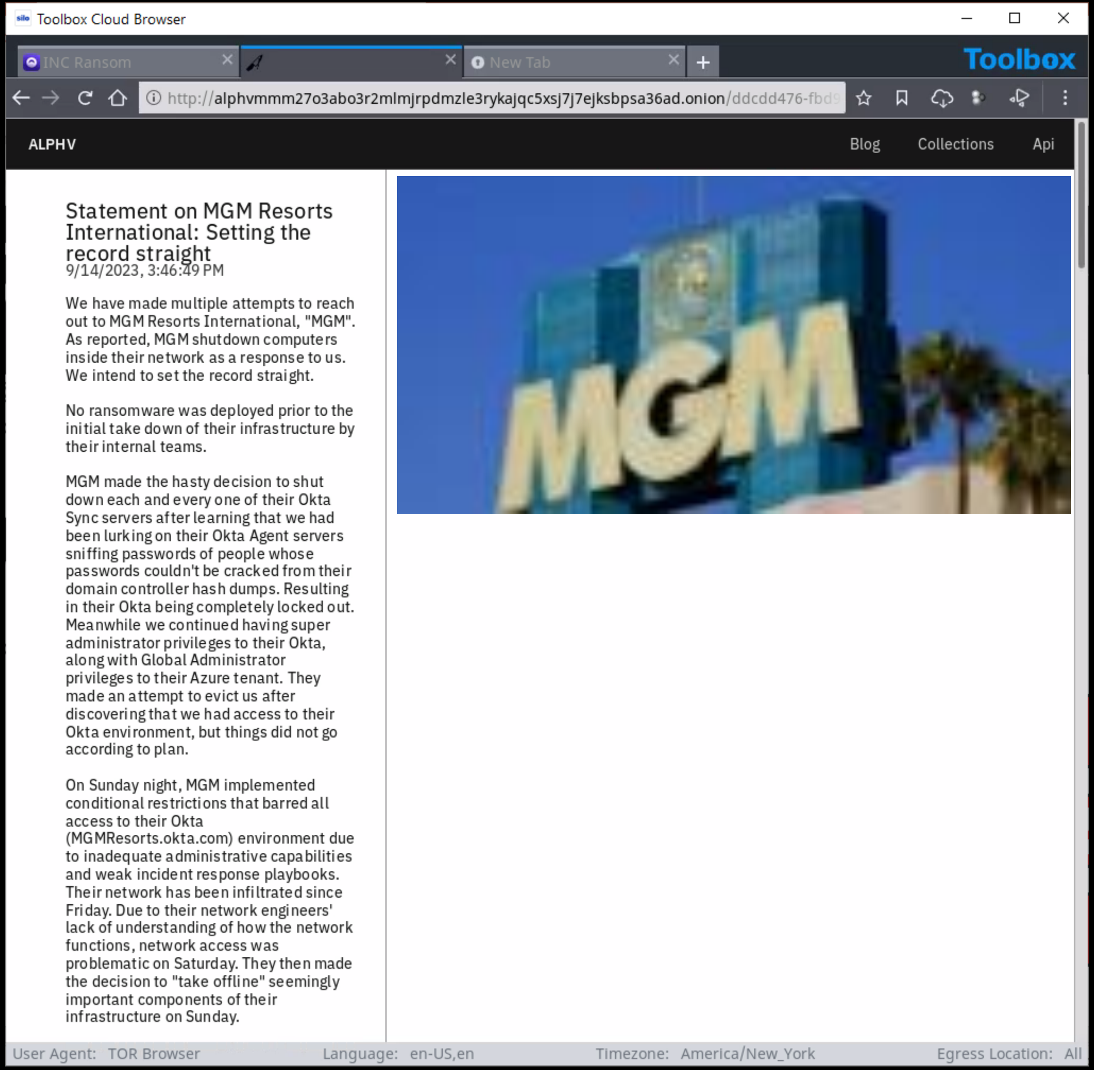
User Agent: TOR Browser Language: en-US,en Timezone: America/New_York Egress Location: All

34 BILLION DOLLAR COMPANY

CYBER BUDGET IN THE MILLIONS

TOP NOTCH SECURITY TEAM

THREAT ACTORS QUICKLY LEARN


Toolbox Cloud Browser
INC Ransom
New Tab
Toolbox
http://alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion/ddcdd476-fbd
ALPHV
Blog
Collections
Api
MGM

Statement on MGM Resorts International: Setting the record straight

9/14/2023, 3:46:49 PM

We have made multiple attempts to reach out to MGM Resorts International, "MGM". As reported, MGM shutdown computers inside their network as a response to us. We intend to set the record straight.

No ransomware was deployed prior to the initial take down of their infrastructure by their internal teams.

MGM made the hasty decision to shut down each and every one of their Okta Sync servers after learning that we had been lurking on their Okta Agent servers sniffing passwords of people whose passwords couldn't be cracked from their domain controller hash dumps. Resulting in their Okta being completely locked out. Meanwhile we continued having super administrator privileges to their Okta, along with Global Administrator privileges to their Azure tenant. They made an attempt to evict us after discovering that we had access to their Okta environment, but things did not go according to plan.

On Sunday night, MGM implemented conditional restrictions that barred all access to their Okta (MGMResorts.okta.com) environment due to inadequate administrative capabilities and weak incident response playbooks. Their network has been infiltrated since Friday. Due to their network engineers' lack of understanding of how the network functions, network access was problematic on Saturday. They then made the decision to "take offline" seemingly important components of their infrastructure on Sunday.

User Agent: TOR Browser Language: en-US,en Timezone: America/New_York Egress Location: All

MGM RECENT HACK

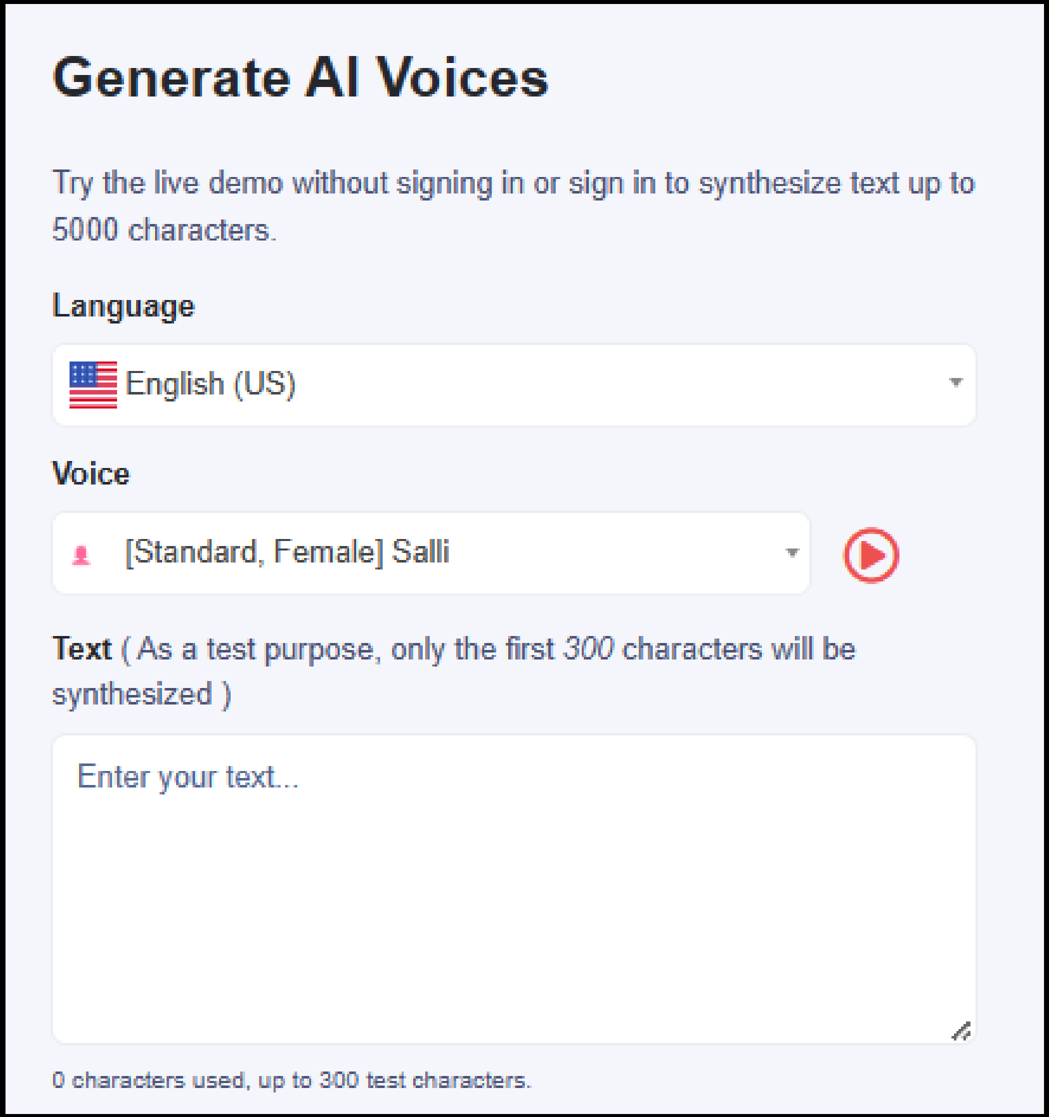
- MOST SYSTEMS DOWN
- NO CHECK IN OR CHECK OUT
- NO FOOD SERVICES
- DOOR SYSTEM SHUTDOWN
- NO GAMING PAYOUTS
- EST LOSS $1 MIL PER HOUR

MGM RECENT HACK

10 MINUTE PHONE CALL

LINKEDIN PROFILE OF MGM EMP

AI VISHING ENGINE



Generate AI Voices

Try the live demo without signing in or sign in to synthesize text up to 5000 characters.

Language

English (US)

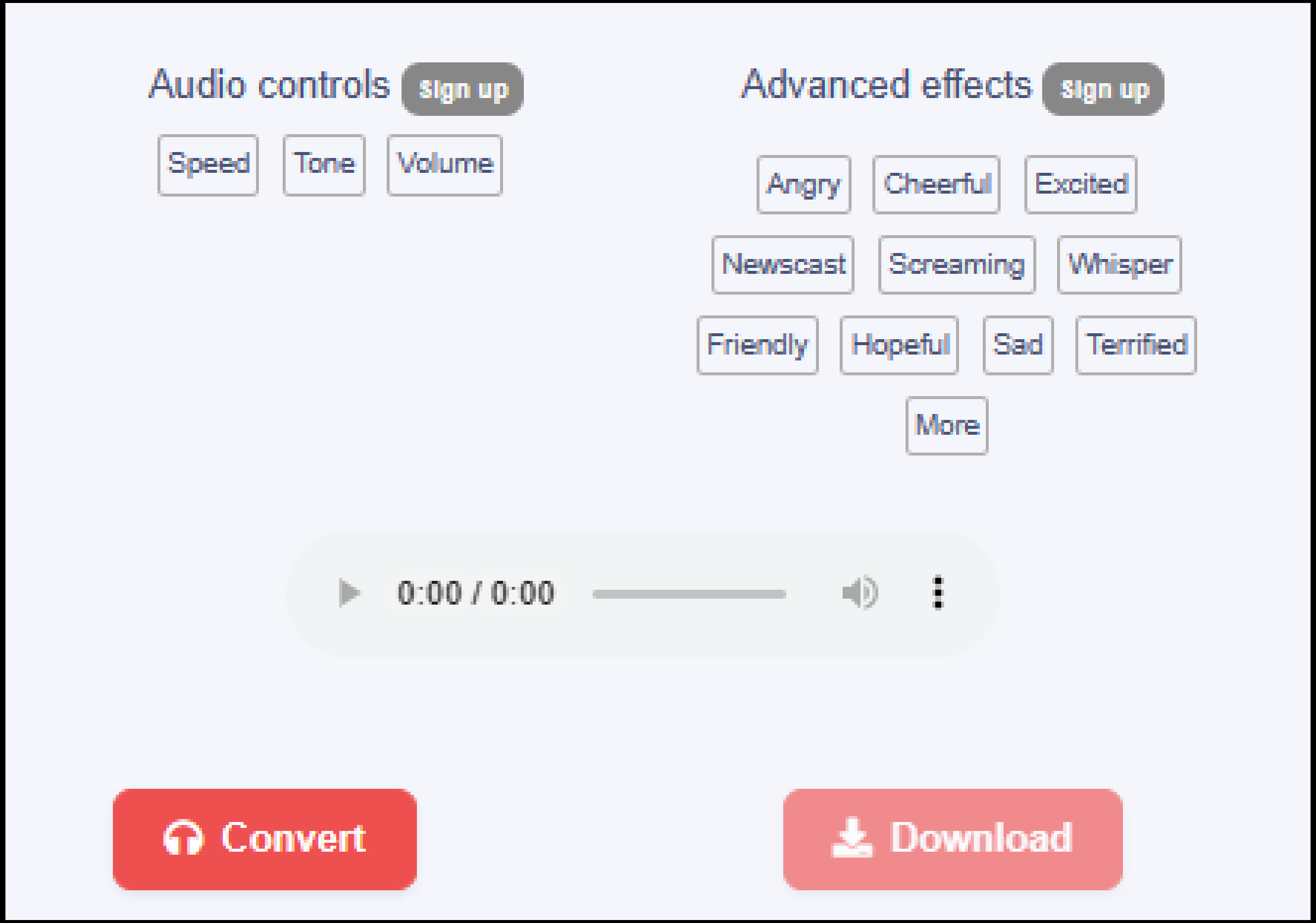
Voice

[Standard, Female] Salli

Text (As a test purpose, only the first *300* characters will be synthesized)

Enter your text...

0 characters used, up to 300 test characters.



MAKING VICTIMS OF VICTIMS

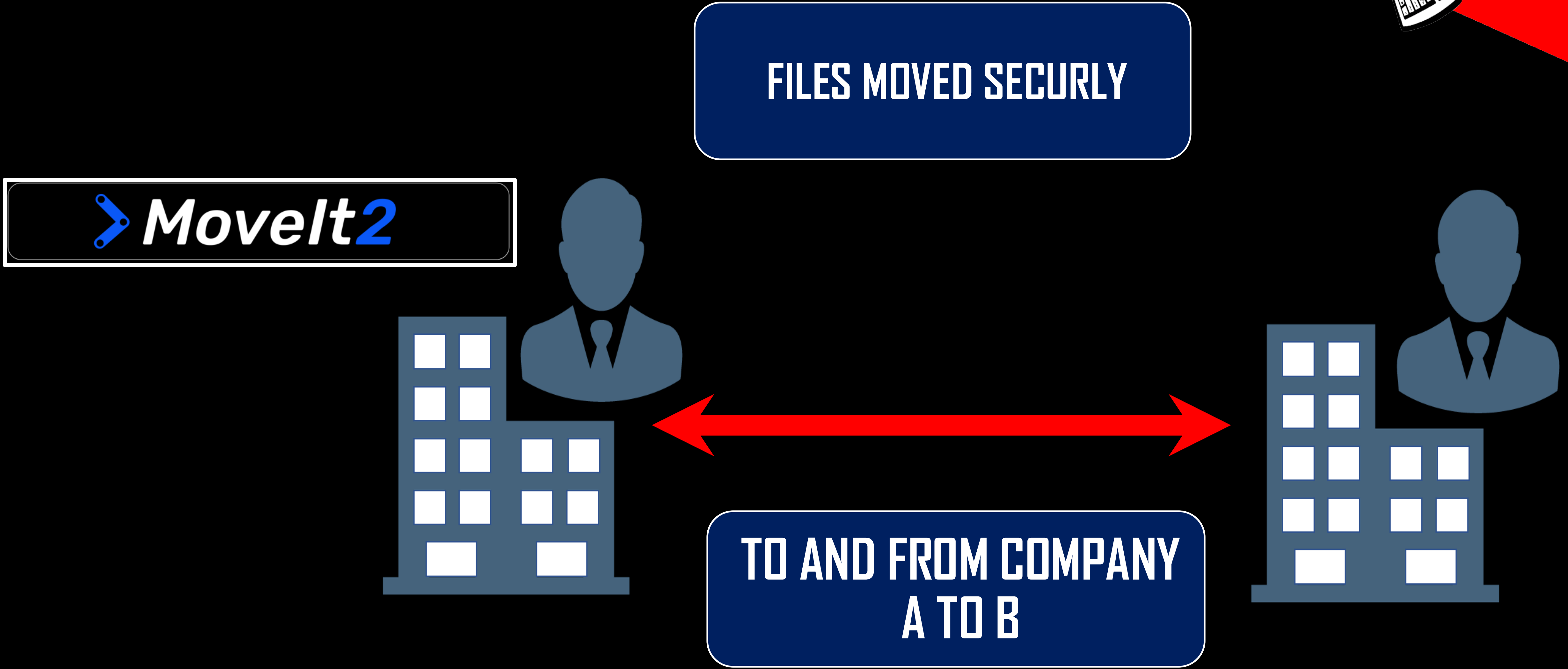
GAME CHANGER EXPLOIT

MoveIt2

THREAT ACTORS BECOME PRODUCTIVE

MoveIt2

Secure Network



MoveIt2

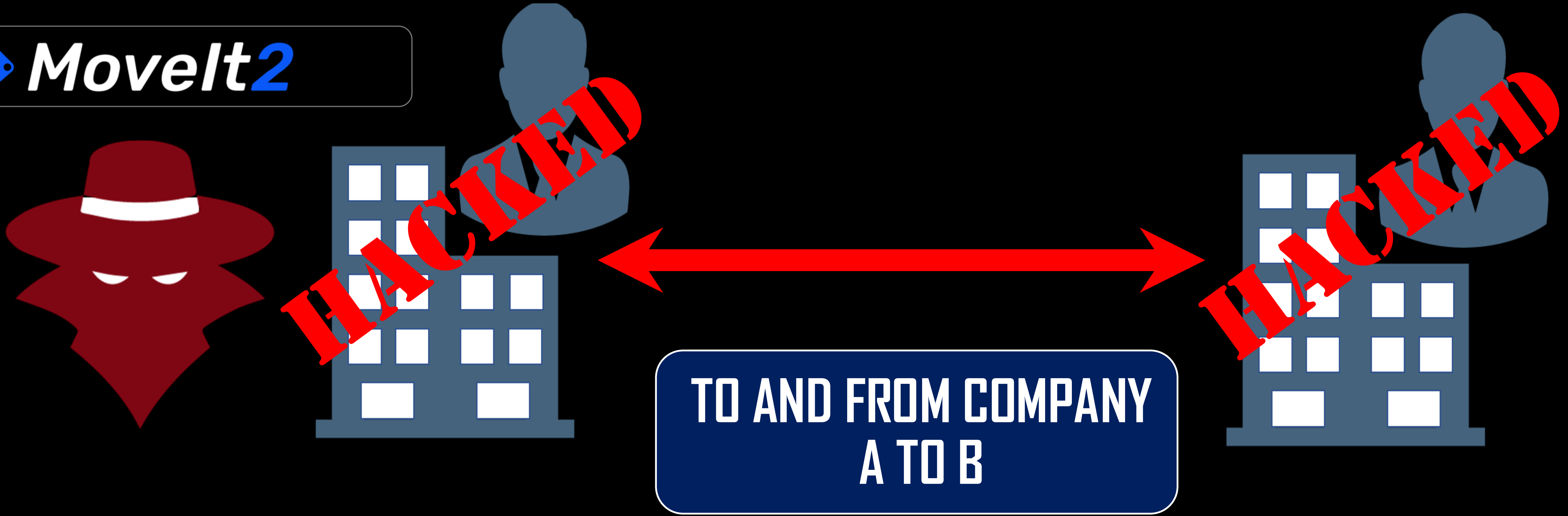
FILES MOVED SECURLY

TO AND FROM COMPANY
A TO B

MOVEIT2 EXPLOITED

CL0P^_- LEAKS

MoveIt2



TO AND FROM COMPANY A TO B

MOVEIT2 EXPLOITED

Secure Network

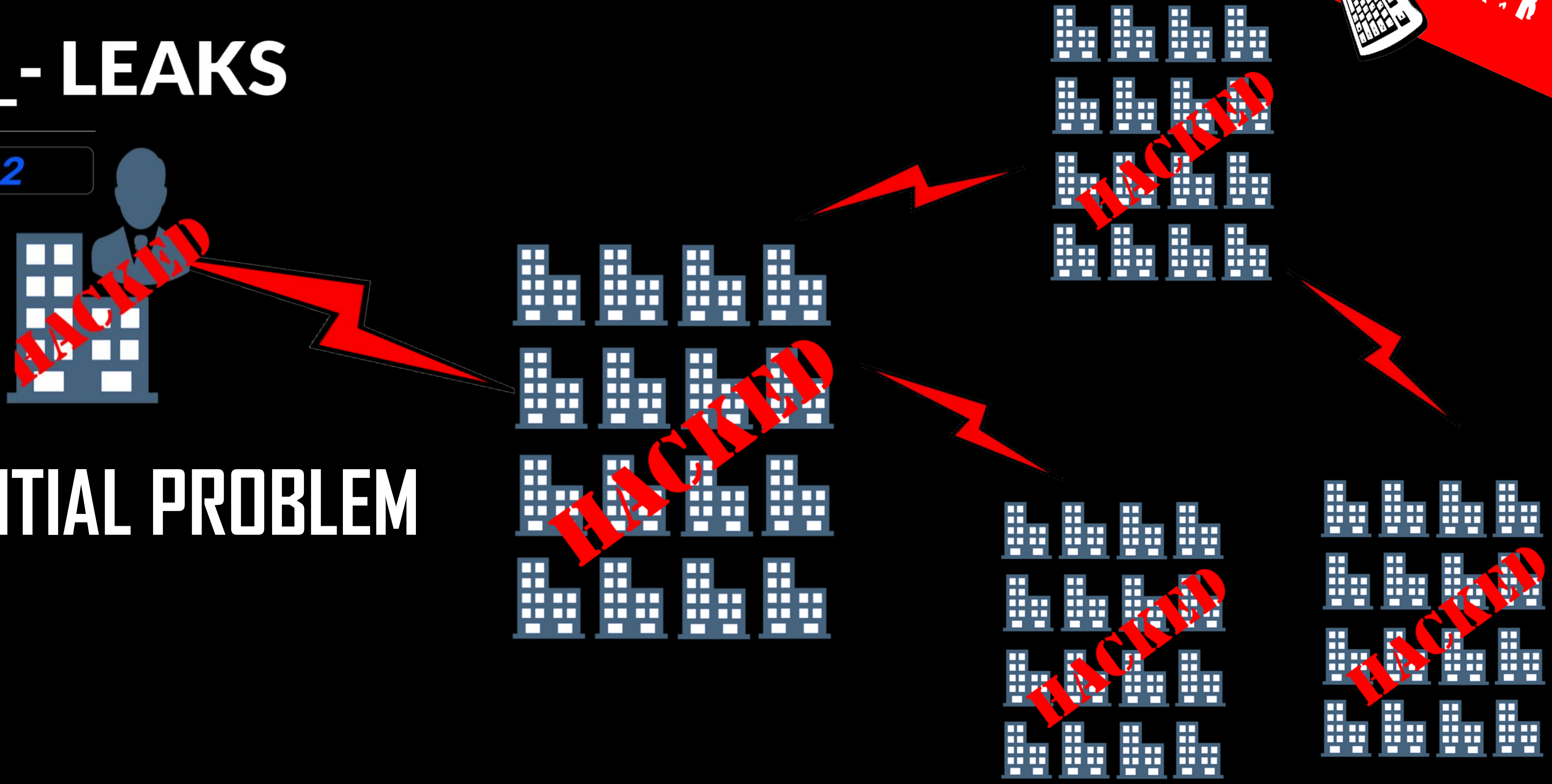
CL0P^_- LEAKS

MoveIt2

MOVEIT2 EXPLOITED

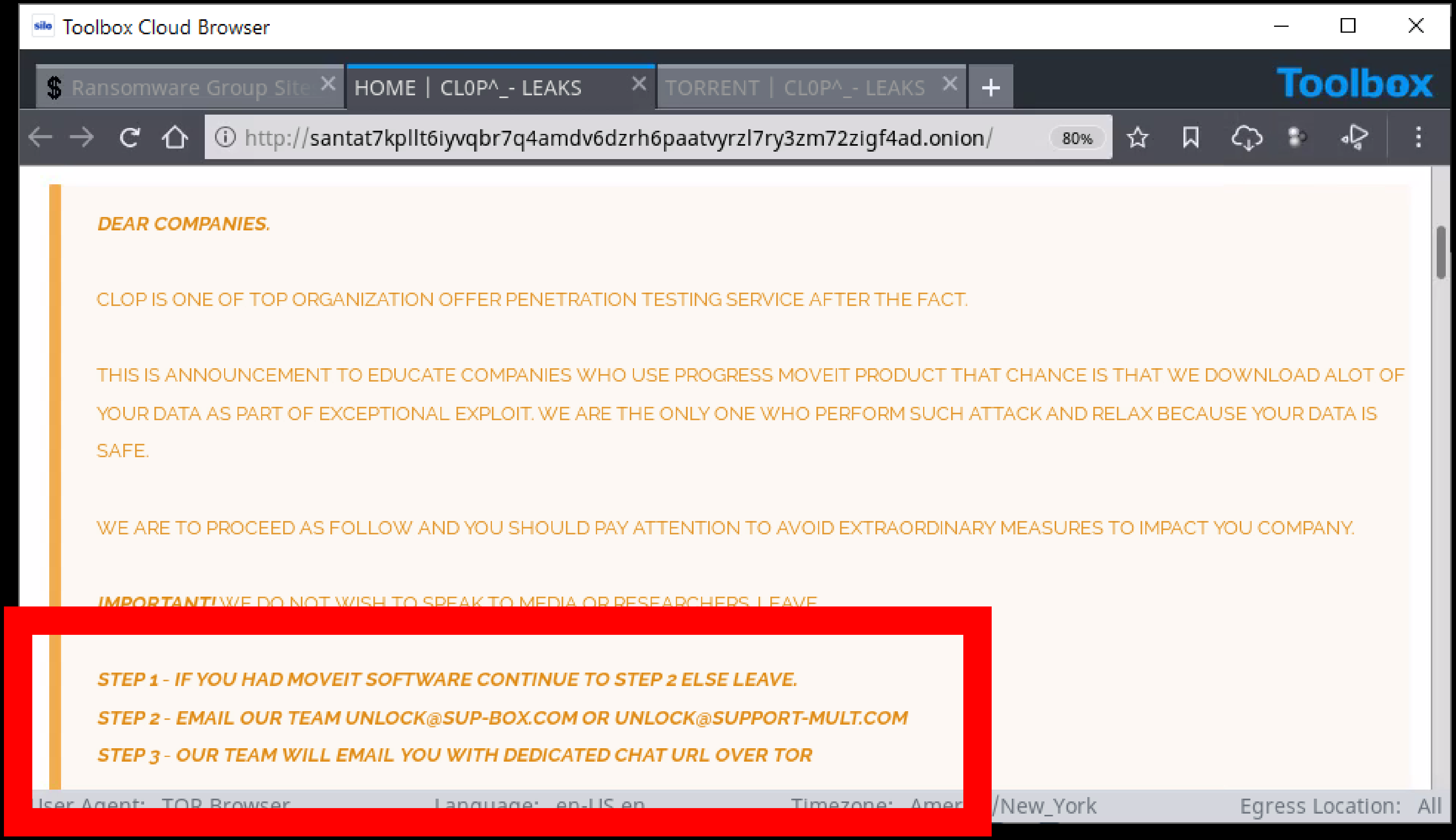
CL0P^_- LEAKS

MoveIt2



EXPONENTIAL PROBLEM

CLOP MADE A STATEMENT



DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

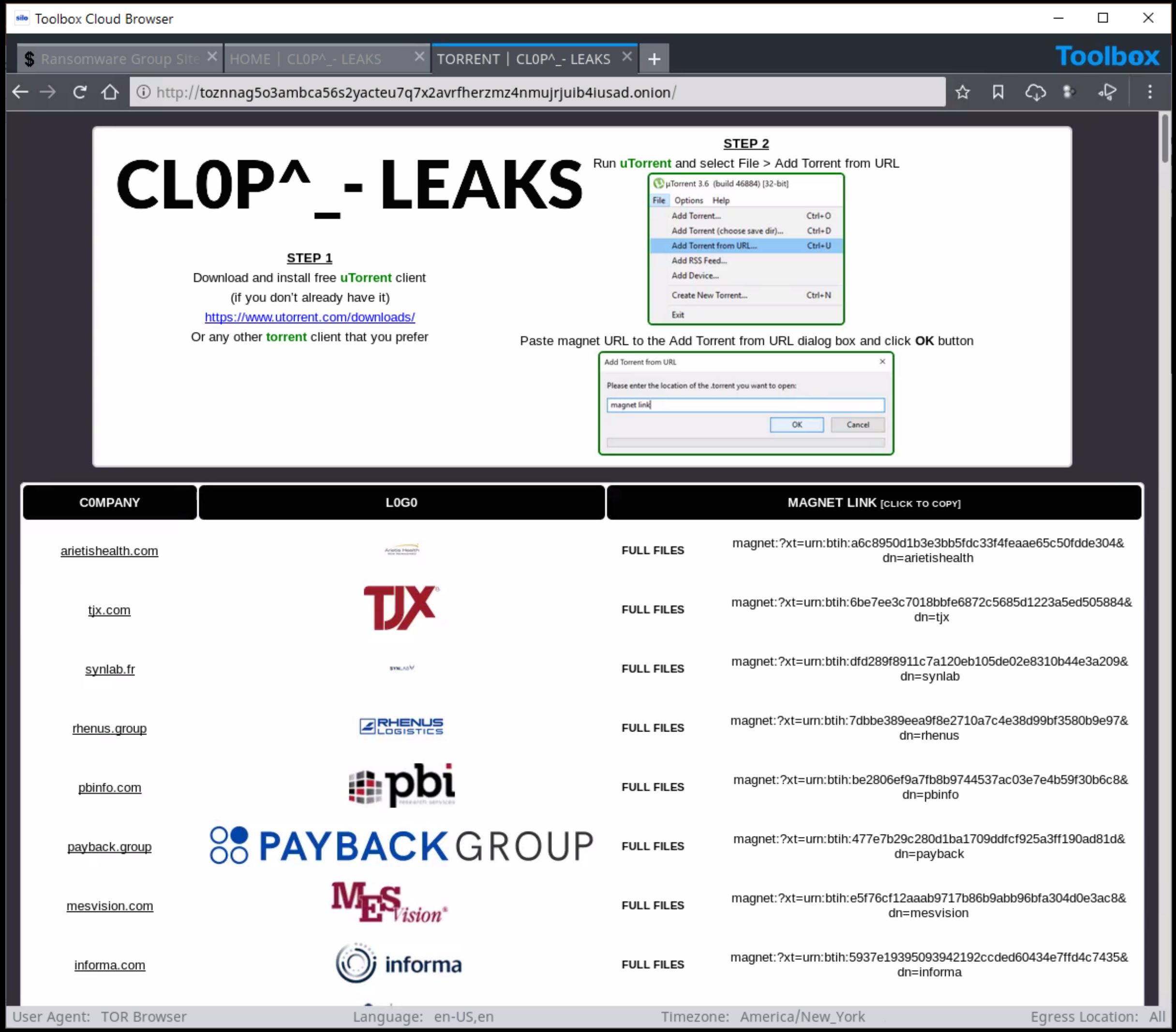
STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.

STEP 2 - EMAIL OUR TEAM UNLOCK@SUP-BOX.COM OR UNLOCK@SUPPORT-MULT.COM

STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

CLOP EXPOSED TONS OF DATA

Secure Network



Toolbox Cloud Browser

Ransomware Group Site | HOME | CL0P^_- LEAKS | TORRENT | CL0P^_- LEAKS | Toolbox

http://toznnag5o3ambca56s2yacteu7q7x2avrfherzmz4nmujrjuib4iusad.onion/

CL0P^_- LEAKS

STEP 1

Download and install free uTorrent client
(if you don't already have it)
https://www.utorrent.com/downloads/
Or any other torrent client that you prefer

STEP 2

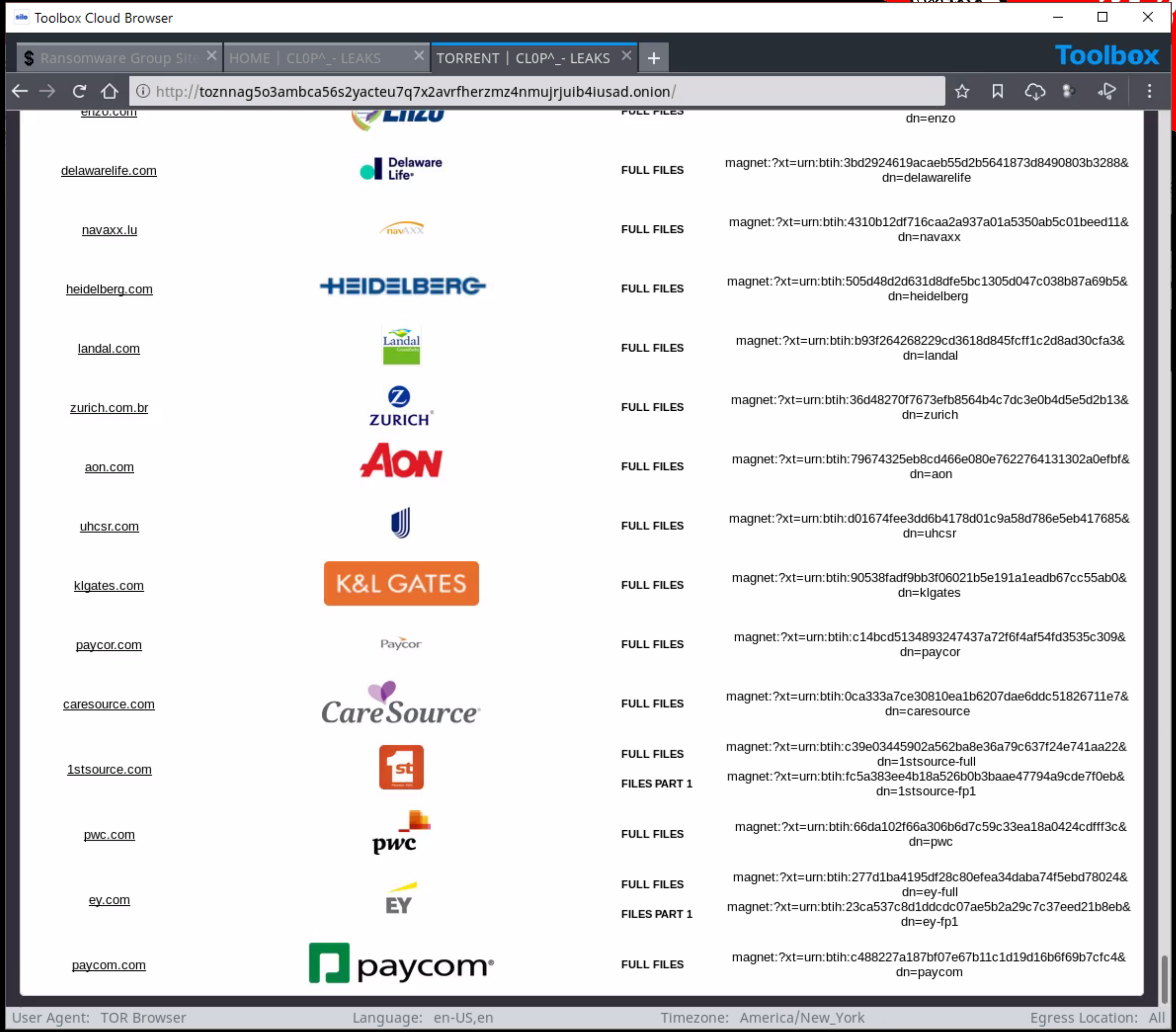
Run uTorrent and select File > Add Torrent from URL

µTorrent 3.6 (build 46884) [32-bit]
File Options Help
Add Torrent... Ctrl+O
Add Torrent (choose save dir)... Ctrl+D
Add Torrent from URL... Ctrl+U
Add RSS Feed...
Add Device...
Create New Torrent... Ctrl+N
Exit

Paste magnet URL to the Add Torrent from URL dialog box and click **OK** button

C0MPANY	L0G0	MAGNET LINK [CLICK TO COPY]	
arietishealth.com	Arietis Health	FULL FILES	magnet:?xt=urn:btih:a6c8950d1b3e3bb5fdc33f4feaae65c50fdde304& dn=arietishealth
tjx.com	TJX	FULL FILES	magnet:?xt=urn:btih:6be7ee3c7018bbfe6872c5685d1223a5ed505884& dn=tjx
synlab.fr	SYNLAB	FULL FILES	magnet:?xt=urn:btih:dfd289f8911c7a120eb105de02e8310b44e3a209& dn=synlab
rhenus.group	RHENUS LOGISTICS	FULL FILES	magnet:?xt=urn:btih:7dbbe389eea9f8e2710a7c4e38d99bf3580b9e97& dn=rhenus
pbinfo.com	pbi research services	FULL FILES	magnet:?xt=urn:btih:be2806ef9a7fb8b9744537ac03e7e4b59f30b6c8& dn=pbinfo
payback.group	PAYBACK GROUP	FULL FILES	magnet:?xt=urn:btih:477e7b29c280d1ba1709ddfcf925a3ff190ad81d& dn=payback
mesvision.com	MES Vision	FULL FILES	magnet:?xt=urn:btih:e5f76cf12aaab9717b86b9abb96bfa304d0e3ac8& dn=mesvision
informa.com	informa	FULL FILES	magnet:?xt=urn:btih:5937e19395093942192ccded60434e7ffd4c7435& dn=informa

User Agent: TOR Browser   Language: en-US,en   Timezone: America/New_York   Egress Location: All



Toolbox Cloud Browser

Ransomware Group Site | HOME | CL0P^_- LEAKS | TORRENT | CL0P^_- LEAKS | Toolbox

http://toznnag5o3ambca56s2yacteu7q7x2avrfherzmz4nmujrjuib4iusad.onion/

enzo.com	Enzo	FULL FILES	dn=enzo
delawarelife.com	Delaware Life	FULL FILES	magnet:?xt=urn:btih:3bd2924619acaeb55d2b5641873d8490803b3288& dn=delawarelife
navaxx.lu	navAXX	FULL FILES	magnet:?xt=urn:btih:4310b12df716caa2a937a01a5350ab5c01beed11& dn=navaxx
heidelberg.com	HEIDELBERG	FULL FILES	magnet:?xt=urn:btih:505d48d2d631d8dfe5bc1305d047c038b87a69b5& dn=heidelberg
landal.com	Landal	FULL FILES	magnet:?xt=urn:btih:b93f264268229cd3618d845fcff1c2d8ad30cfa3& dn=landal
zurich.com.br	ZURICH	FULL FILES	magnet:?xt=urn:btih:36d48270f7673efb8564b4c7dc3e0b4d5e5d2b13& dn=zurich
aon.com	AON	FULL FILES	magnet:?xt=urn:btih:79674325eb8cd466e080e7622764131302a0efbf& dn=aon
uhcsr.com		FULL FILES	magnet:?xt=urn:btih:d01674fee3dd6b4178d01c9a58d786e5eb417685& dn=uhcsr
klgates.com	K&L GATES	FULL FILES	magnet:?xt=urn:btih:90538fadf9bb3f06021b5e191a1eadb67cc55ab0& dn=klgates
paycor.com	Paycor	FULL FILES	magnet:?xt=urn:btih:c14bcd5134893247437a72f6f4af54fd3535c309& dn=paycor
caresource.com	CareSource	FULL FILES	magnet:?xt=urn:btih:0ca333a7ce30810ea1b6207dae6ddc51826711e7& dn=caresource

1stsource.com	1st	FULL FILES
		FILES PART 1
			magnet:?xt=urn:btih:c39e03445902a562ba8e36a79c637f24e741aa22&
			dn=1stsource-full
			magnet:?xt=urn:btih:fc5a383ee4b18a526b0b3baae47794a9cde7f0eb&
			dn=1stsource-fp1

pwc.com	pwc	FULL FILES	magnet:?xt=urn:btih:66da102f66a306b6d7c59c33ea18a0424cdfff3c& dn=pwc

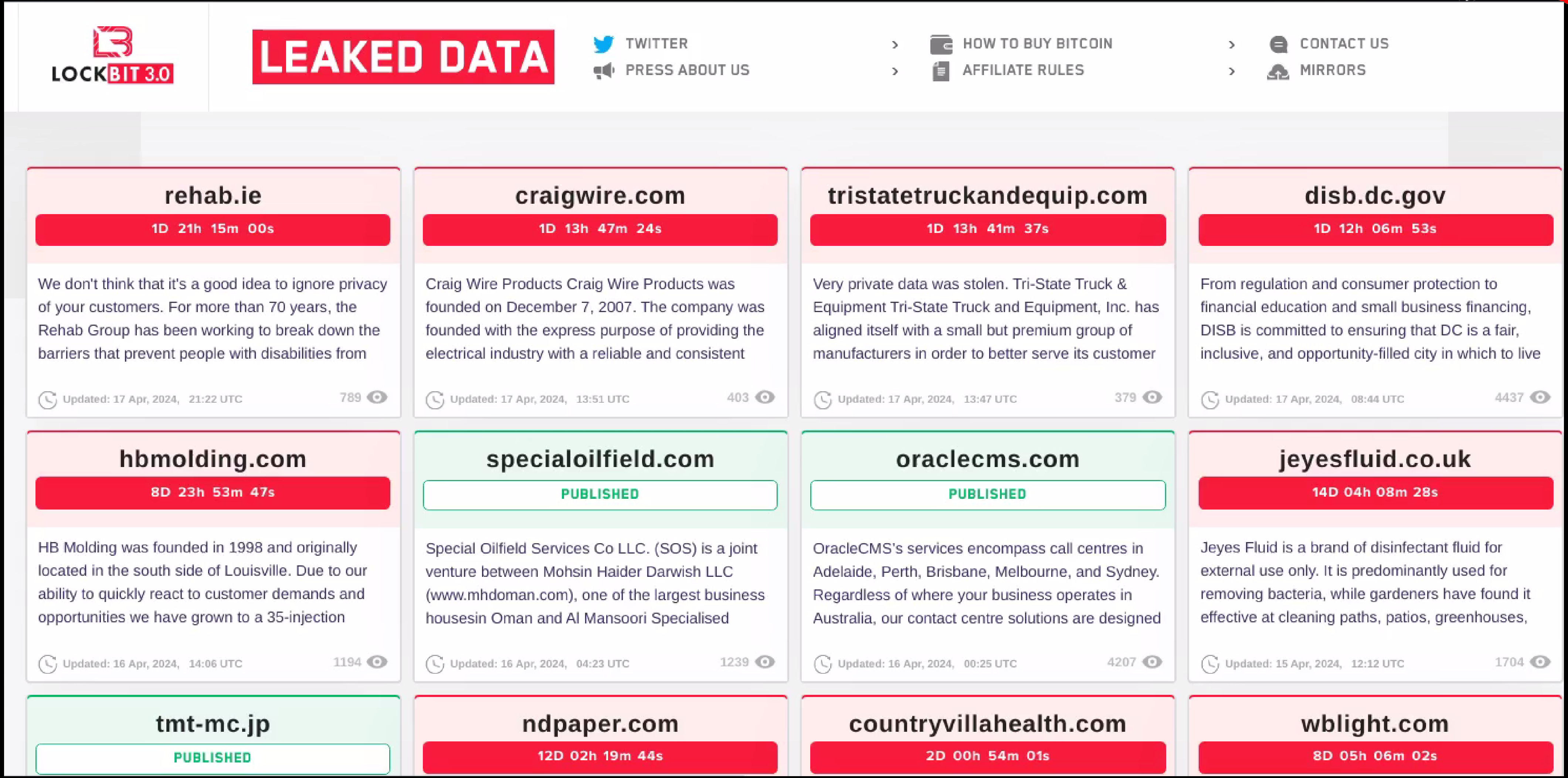
ey.com	EY	FULL FILES
		FILES PART 1
			magnet:?xt=urn:btih:277d1ba4195df28c80efea34daba74f5ebd78024&
			dn=ey-full
			magnet:?xt=urn:btih:23ca537c8d1ddcdc07ae5b2a29c7c37eed21b8eb&
			dn=ey-fp1

paycom.com	paycom	FULL FILES	magnet:?xt=urn:btih:c488227a187bf07e67b11c1d19d16b6f69b7cfc4& dn=paycom

User Agent: TOR Browser   Language: en-US,en   Timezone: America/New_York   Egress Location: All

KIND OF CATCHING BAD GUYS

LOCKBIT SITE



LOCKBIT 3.0

LEAKED DATA

TWITTER
PRESS ABOUT US
HOW TO BUY BITCOIN
AFFILIATE RULES
CONTACT US
MIRRORS

rehab.ie

1D 21h 15m 00s

We don't think that it's a good idea to ignore privacy of your customers. For more than 70 years, the Rehab Group has been working to break down the barriers that prevent people with disabilities from

Updated: 17 Apr, 2024, 21:22 UTC 789

craigwire.com

1D 13h 47m 24s

Craig Wire Products Craig Wire Products was founded on December 7, 2007. The company was founded with the express purpose of providing the electrical industry with a reliable and consistent

Updated: 17 Apr, 2024, 13:51 UTC 403

tristatetruckandequip.com

1D 13h 41m 37s

Very private data was stolen. Tri-State Truck & Equipment Tri-State Truck and Equipment, Inc. has aligned itself with a small but premium group of manufacturers in order to better serve its customer

Updated: 17 Apr, 2024, 13:47 UTC 379

disb.dc.gov

1D 12h 06m 53s

From regulation and consumer protection to financial education and small business financing, DISB is committed to ensuring that DC is a fair, inclusive, and opportunity-filled city in which to live

Updated: 17 Apr, 2024, 08:44 UTC 4437

hbmolding.com

8D 23h 53m 47s

HB Molding was founded in 1998 and originally located in the south side of Louisville. Due to our ability to quickly react to customer demands and opportunities we have grown to a 35-injection

Updated: 16 Apr, 2024, 14:06 UTC 1194

specialoilfield.com

PUBLISHED

Special Oilfield Services Co LLC. (SOS) is a joint venture between Mohsin Haider Darwish LLC (www.mhdoman.com), one of the largest business housesin Oman and Al Mansoori Specialised

Updated: 16 Apr, 2024, 04:23 UTC 1239

oraclecms.com

PUBLISHED

OracleCMS's services encompass call centres in Adelaide, Perth, Brisbane, Melbourne, and Sydney. Regardless of where your business operates in Australia, our contact centre solutions are designed

Updated: 16 Apr, 2024, 00:25 UTC 4207

jeyesfluid.co.uk

14D 04h 08m 28s

Jeyes Fluid is a brand of disinfectant fluid for external use only. It is predominantly used for removing bacteria, while gardeners have found it effective at cleaning paths, patios, greenhouses,

Updated: 15 Apr, 2024, 12:12 UTC 1704

tmt-mc.jp

PUBLISHED

ndpaper.com

12D 02h 19m 44s

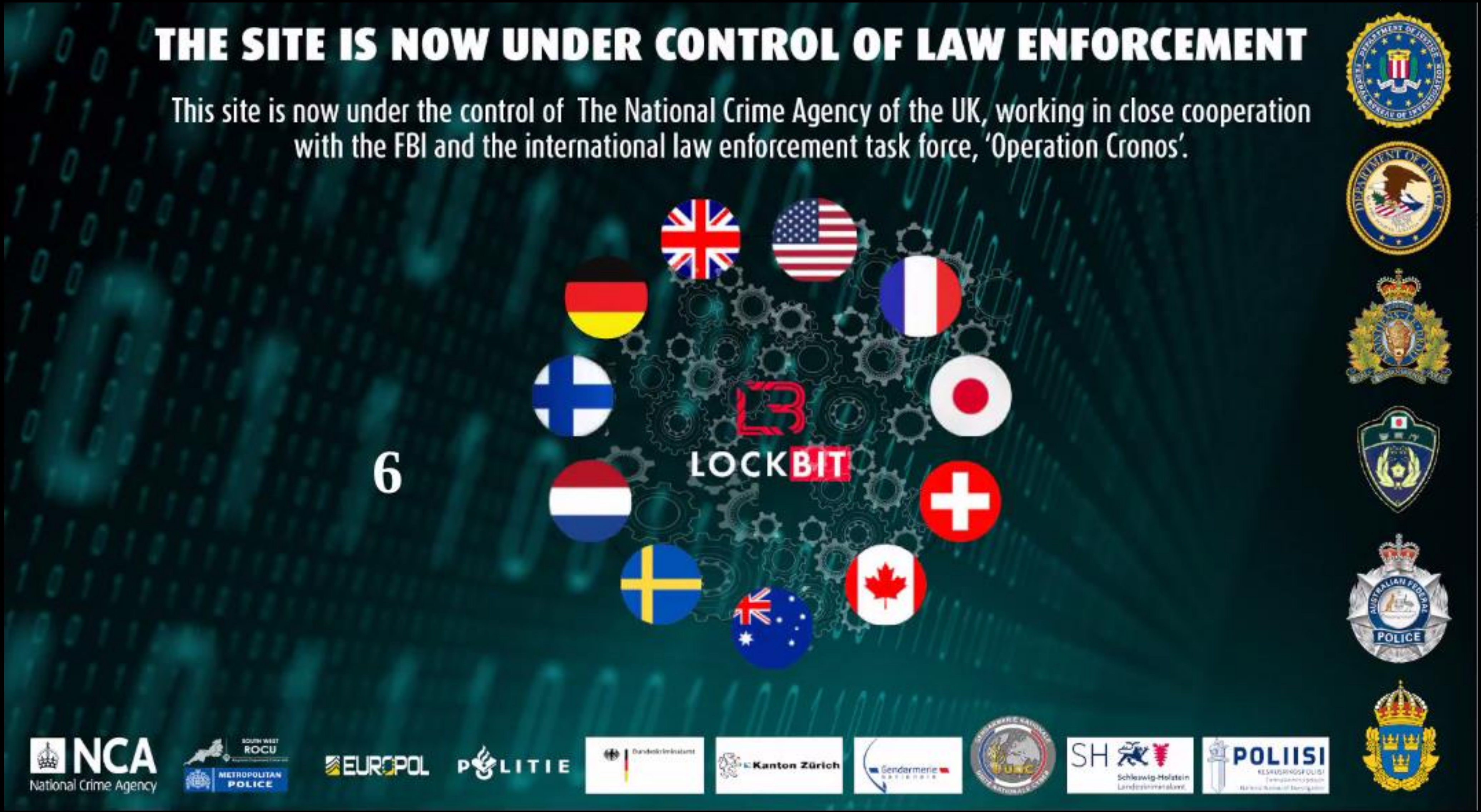
countryvillahealth.com

2D 00h 54m 01s

wblight.com

8D 05h 06m 02s

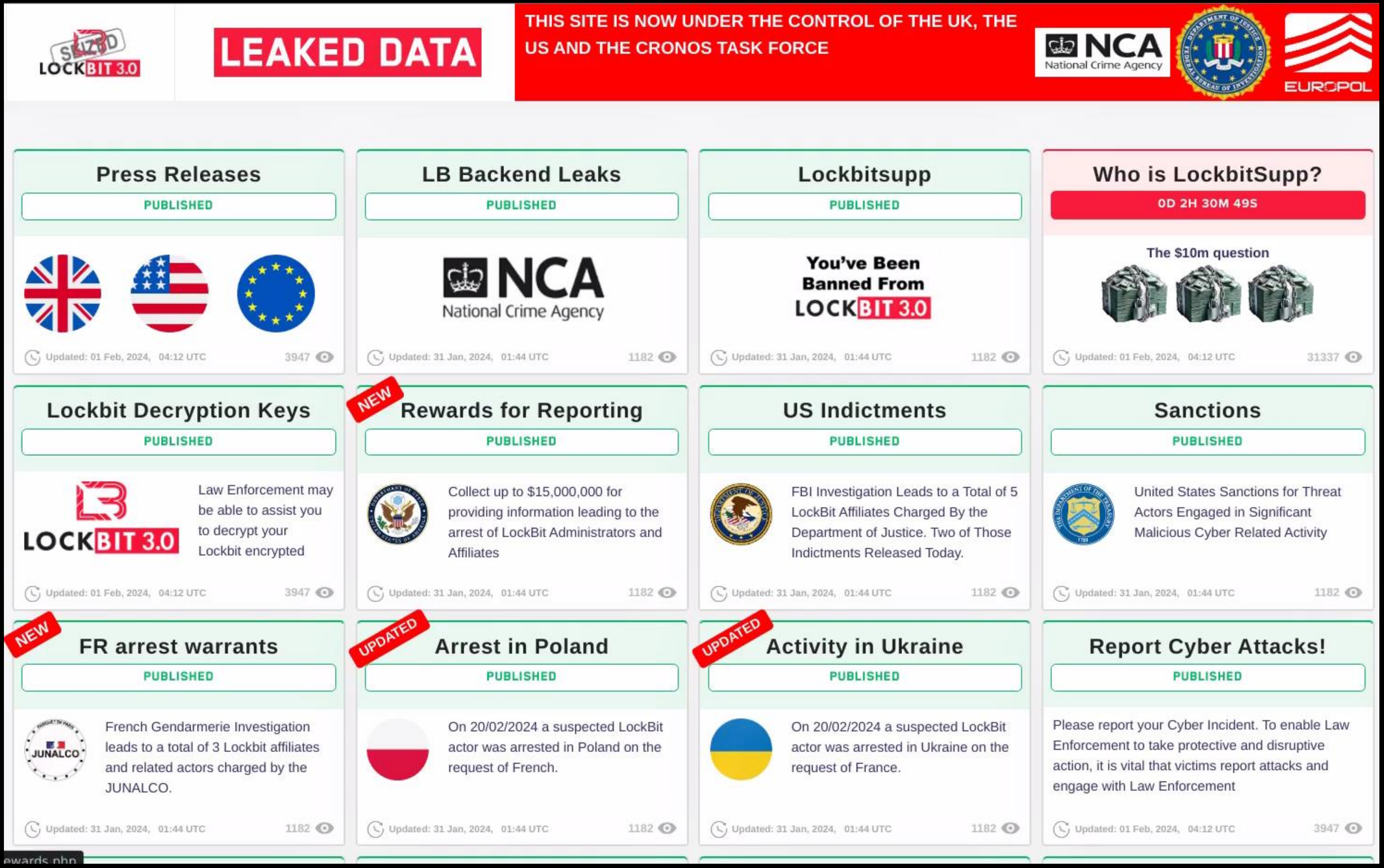
THREAT ACTORS EXPOSED



THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

THREAT ACTORS EXPOSED



THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

Press Releases
PUBLISHED
Updated: 01 Feb, 2024, 04:12 UTC 3947

LB Backend Leaks
PUBLISHED
NCA National Crime Agency
Updated: 31 Jan, 2024, 01:44 UTC 1182

Lockbitsupp
PUBLISHED
You've Been Banned From LOCKBIT 3.0
Updated: 31 Jan, 2024, 01:44 UTC 1182

Who is LockbitSupp?
0D 2H 30M 49S
The $10m question
Updated: 01 Feb, 2024, 04:12 UTC 31337

Lockbit Decryption Keys
PUBLISHED
LOCKBIT 3.0
Law Enforcement may be able to assist you to decrypt your Lockbit encrypted
Updated: 01 Feb, 2024, 04:12 UTC 3947

NEW
Rewards for Reporting
PUBLISHED
Collect up to $15,000,000 for providing information leading to the arrest of LockBit Administrators and Affiliates
Updated: 31 Jan, 2024, 01:44 UTC 1182

US Indictments
PUBLISHED
FBI Investigation Leads to a Total of 5 LockBit Affiliates Charged By the Department of Justice. Two of Those Indictments Released Today.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Sanctions
PUBLISHED
United States Sanctions for Threat Actors Engaged in Significant Malicious Cyber Related Activity
Updated: 31 Jan, 2024, 01:44 UTC 1182

NEW
FR arrest warrants
PUBLISHED
JUNALCO
French Gendarmerie Investigation leads to a total of 3 Lockbit affiliates and related actors charged by the JUNALCO.
Updated: 31 Jan, 2024, 01:44 UTC 1182

UPDATED
Arrest in Poland
PUBLISHED
On 20/02/2024 a suspected LockBit actor was arrested in Poland on the request of French.
Updated: 31 Jan, 2024, 01:44 UTC 1182

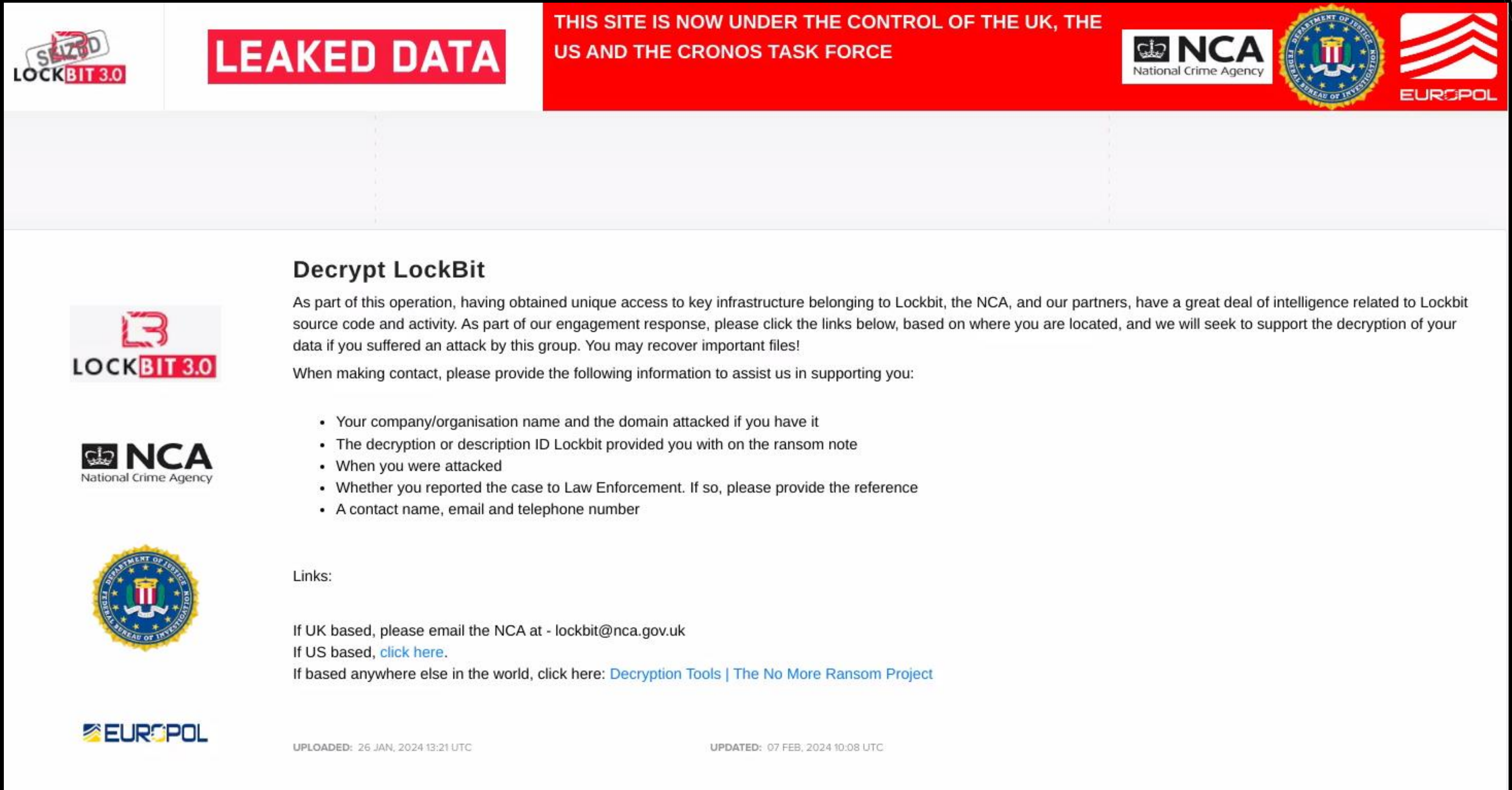
UPDATED
Activity in Ukraine
PUBLISHED
On 20/02/2024 a suspected LockBit actor was arrested in Ukraine on the request of France.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Report Cyber Attacks!
PUBLISHED
Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive action, it is vital that victims report attacks and engage with Law Enforcement
Updated: 01 Feb, 2024, 04:12 UTC 3947

ewards.php

PUBLISHED DECRYPTION KEYS

Secure Network



SEIZED LOCKBIT 3.0

LEAKED DATA

THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

NCA National Crime Agency

EUROPOL

Decrypt LockBit

As part of this operation, having obtained unique access to key infrastructure belonging to Lockbit, the NCA, and our partners, have a great deal of intelligence related to Lockbit source code and activity. As part of our engagement response, please click the links below, based on where you are located, and we will seek to support the decryption of your data if you suffered an attack by this group. You may recover important files!

When making contact, please provide the following information to assist us in supporting you:

- Your company/organisation name and the domain attacked if you have it
- The decryption or description ID Lockbit provided you with on the ransom note
- When you were attacked
- Whether you reported the case to Law Enforcement. If so, please provide the reference
- A contact name, email and telephone number

Links:

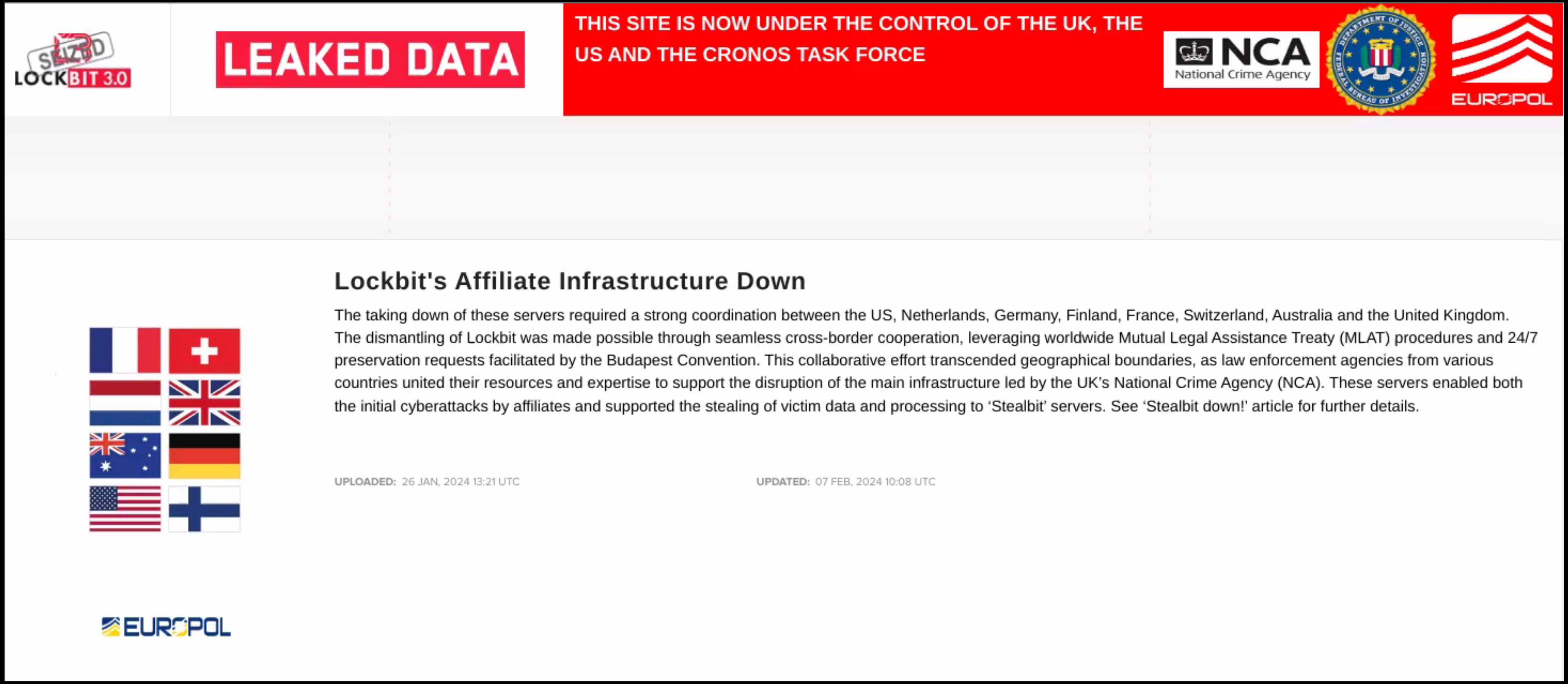
If UK based, please email the NCA at - lockbit@nca.gov.uk
If US based, click here.
If based anywhere else in the world, click here: Decryption Tools | The No More Ransom Project

UPLOADED: 26 JAN, 2024 13:21 UTC

UPDATED: 07 FEB, 2024 10:08 UTC

DIDN'T REALLY HELP

AFFILIATE INFRASTURE DOWN



THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

Lockbit's Affiliate Infrastructure Down

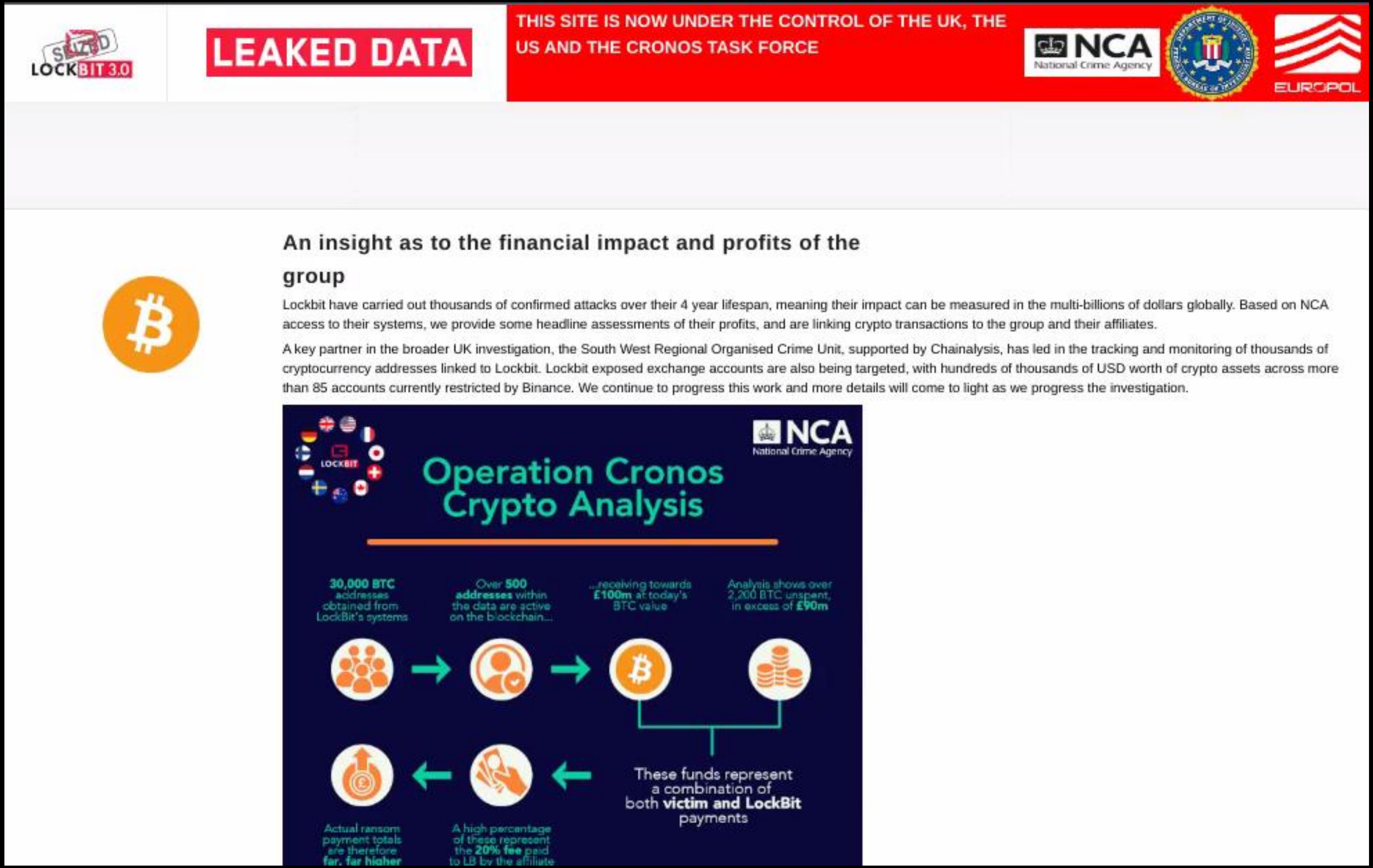
The taking down of these servers required a strong coordination between the US, Netherlands, Germany, Finland, France, Switzerland, Australia and the United Kingdom. The dismantling of Lockbit was made possible through seamless cross-border cooperation, leveraging worldwide Mutual Legal Assistance Treaty (MLAT) procedures and 24/7 preservation requests facilitated by the Budapest Convention. This collaborative effort transcended geographical boundaries, as law enforcement agencies from various countries united their resources and expertise to support the disruption of the main infrastructure led by the UK's National Crime Agency (NCA). These servers enabled both the initial cyberattacks by affiliates and supported the stealing of victim data and processing to 'Stealbit' servers. See 'Stealbit down!' article for further details.

UPLOADED: 26 JAN, 2024 13:21 UTC

UPDATED: 07 FEB, 2024 10:08 UTC

AFFILIATES INCLUDE OTHER RANSOM GROUPS

CRYPTO CONFISCATED



SEIZED LOCKBIT 3.0

LEAKED DATA

THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

NCA National Crime Agency

EUROPOL

An insight as to the financial impact and profits of the group

Lockbit have carried out thousands of confirmed attacks over their 4 year lifespan, meaning their impact can be measured in the multi-billions of dollars globally. Based on NCA access to their systems, we provide some headline assessments of their profits, and are linking crypto transactions to the group and their affiliates.

A key partner in the broader UK investigation, the South West Regional Organised Crime Unit, supported by Chainalysis, has led in the tracking and monitoring of thousands of cryptocurrency addresses linked to Lockbit. Lockbit exposed exchange accounts are also being targeted, with hundreds of thousands of USD worth of crypto assets across more than 85 accounts currently restricted by Binance. We continue to progress this work and more details will come to light as we progress the investigation.

NCA National Crime Agency

Operation Cronos Crypto Analysis

30,000 BTC addresses obtained from LockBit's systems

Over **500 addresses** within the data are active on the blockchain...

...receiving towards **£100m** at today's BTC value

Analysis shows over 2,200 BTC unspent, in excess of **£90m**

These funds represent a combination of both **victim and LockBit** payments

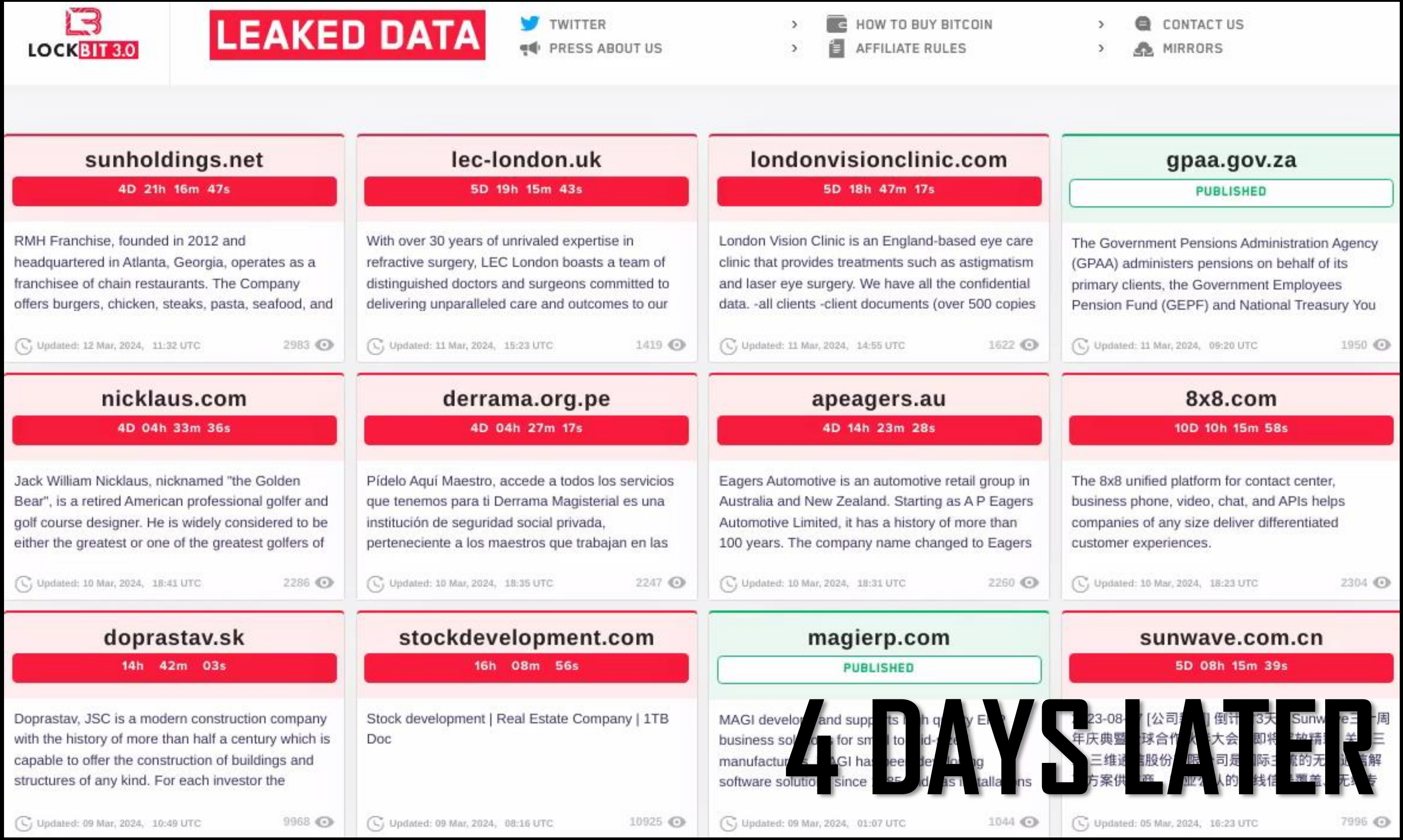
A high percentage of these represent the **20% fee** paid to LB by the affiliate

Actual ransom payment totals are therefore **far, far higher**

$100'S OF MILLIONS IN CRYPTO

BACK IN BUSINESS

Secure Network



LOCKBIT 3.0

LEAKED DATA

TWITTER ›
PRESS ABOUT US ›
HOW TO BUY BITCOIN ›
AFFILIATE RULES ›
CONTACT US
MIRRORS

sunholdings.net
4D 21h 16m 47s
RMH Franchise, founded in 2012 and headquartered in Atlanta, Georgia, operates as a franchisee of chain restaurants. The Company offers burgers, chicken, steaks, pasta, seafood, and
Updated: 12 Mar, 2024, 11:32 UTC 2983

lec-london.uk
5D 19h 15m 43s
With over 30 years of unrivaled expertise in refractive surgery, LEC London boasts a team of distinguished doctors and surgeons committed to delivering unparalleled care and outcomes to our
Updated: 11 Mar, 2024, 15:23 UTC 1419

londonvisionclinic.com
5D 18h 47m 17s
London Vision Clinic is an England-based eye care clinic that provides treatments such as astigmatism and laser eye surgery. We have all the confidential data. -all clients -client documents (over 500 copies
Updated: 11 Mar, 2024, 14:55 UTC 1622

gpaa.gov.za
PUBLISHED
The Government Pensions Administration Agency (GPAA) administers pensions on behalf of its primary clients, the Government Employees Pension Fund (GEPF) and National Treasury You
Updated: 11 Mar, 2024, 09:20 UTC 1950

nicklaus.com
4D 04h 33m 36s
Jack William Nicklaus, nicknamed "the Golden Bear", is a retired American professional golfer and golf course designer. He is widely considered to be either the greatest or one of the greatest golfers of
Updated: 10 Mar, 2024, 18:41 UTC 2286

derrama.org.pe
4D 04h 27m 17s
Pídelo Aquí Maestro, accede a todos los servicios que tenemos para ti Derrama Magisterial es una institución de seguridad social privada, perteneciente a los maestros que trabajan en las
Updated: 10 Mar, 2024, 18:35 UTC 2247

apeagers.au
4D 14h 23m 28s
Eagers Automotive is an automotive retail group in Australia and New Zealand. Starting as A P Eagers Automotive Limited, it has a history of more than 100 years. The company name changed to Eagers
Updated: 10 Mar, 2024, 18:31 UTC 2260

8x8.com
10D 10h 15m 58s
The 8x8 unified platform for contact center, business phone, video, chat, and APIs helps companies of any size deliver differentiated customer experiences.
Updated: 10 Mar, 2024, 18:23 UTC 2304

doprastav.sk
14h 42m 03s
Doprastav, JSC is a modern construction company with the history of more than half a century which is capable to offer the construction of buildings and structures of any kind. For each investor the
Updated: 09 Mar, 2024, 10:49 UTC 9968

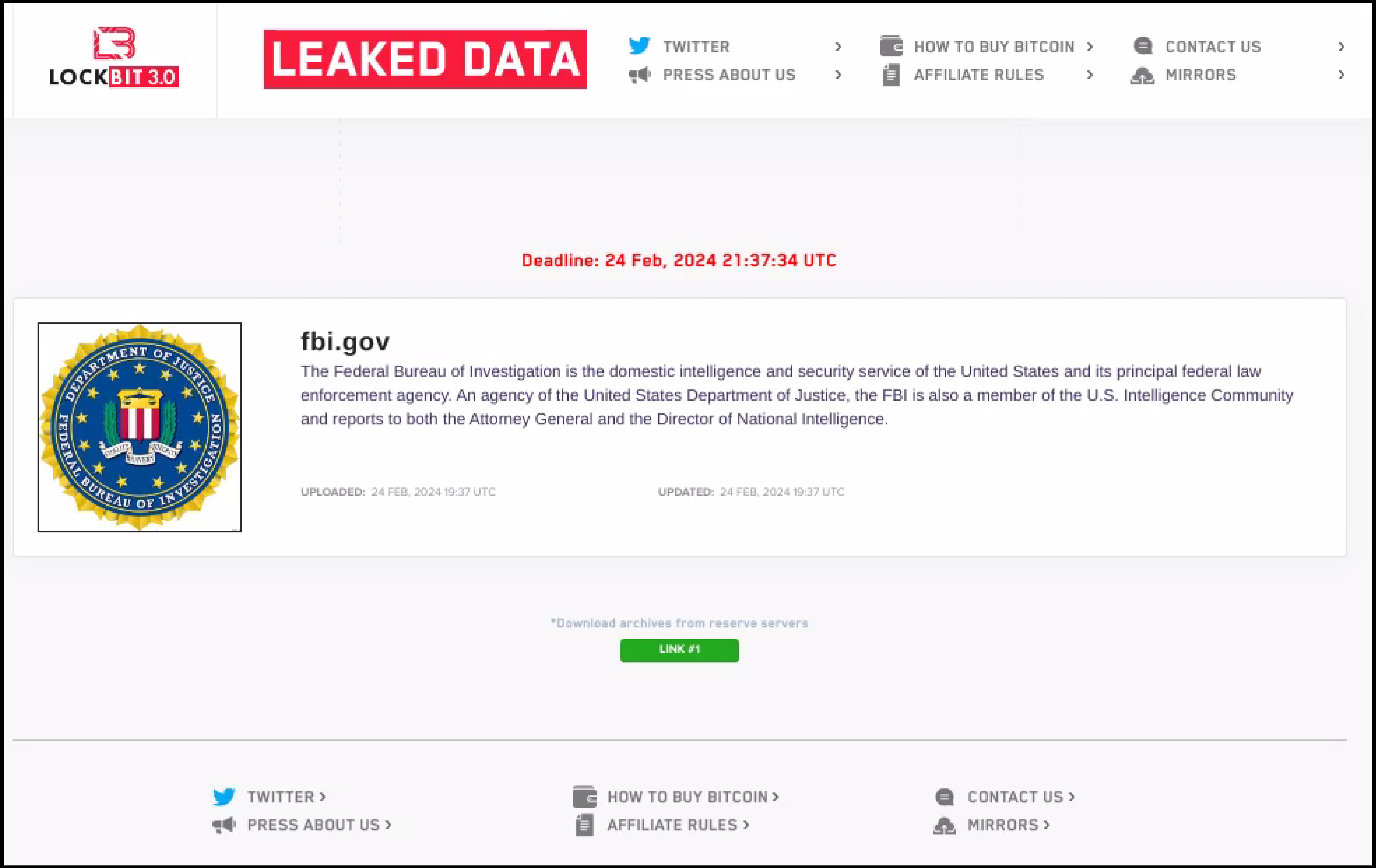
stockdevelopment.com
16h 08m 56s
Stock development | Real Estate Company | 1TB Doc
Updated: 09 Mar, 2024, 08:16 UTC 10925

magierp.com
PUBLISHED
MAGI develo[illegible] and supp[illegible]ts [illegible]h q[illegible]y E[illegible] business sol[illegible] for sm[illegible] to [illegible]id-[illegible] manufactur[illegible] [illegible]AGI ha[illegible] bee[illegible] de[illegible]ing software solutio[illegible] since [illegible] [illegible]d [illegible]as [illegible]talla[illegible]ns
Updated: 09 Mar, 2024, 01:07 UTC 1044

sunwave.com.cn
5D 08h 15m 39s
[illegible]23-08-[illegible] [公司[illegible]] 倒计[illegible]3天[illegible]Sunw[illegible]e三[illegible]周年庆典暨[illegible]球合作[illegible]大会[illegible]即将[illegible]放精[illegible]关[illegible]三[illegible]三维通[illegible]股份[illegible]司是[illegible]际[illegible]流的无[illegible]解[illegible]方案供[illegible]，[illegible]人的[illegible]线信[illegible]覆盖[illegible]无[illegible]
Updated: 05 Mar, 2024, 16:23 UTC 7996

4 DAYS LATER

BACK IN BUSINESS



Deadline: 24 Feb, 2024 21:37:34 UTC

fbi.gov

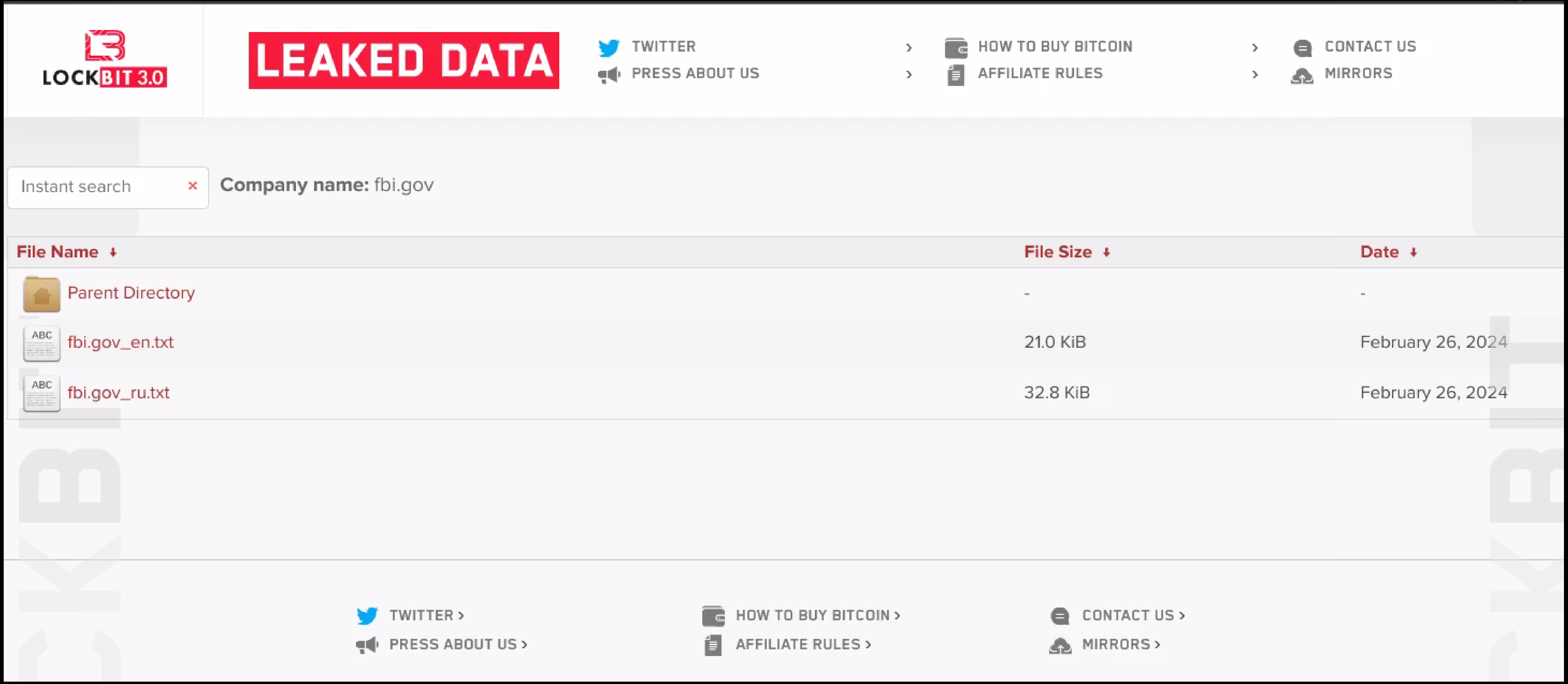
The Federal Bureau of Investigation is the domestic intelligence and security service of the United States and its principal federal law enforcement agency. An agency of the United States Department of Justice, the FBI is also a member of the U.S. Intelligence Community and reports to both the Attorney General and the Director of National Intelligence.

UPLOADED: 24 FEB, 2024 19:37 UTC

UPDATED: 24 FEB, 2024 19:37 UTC

*Download archives from reserve servers

BACK IN BUSINESS



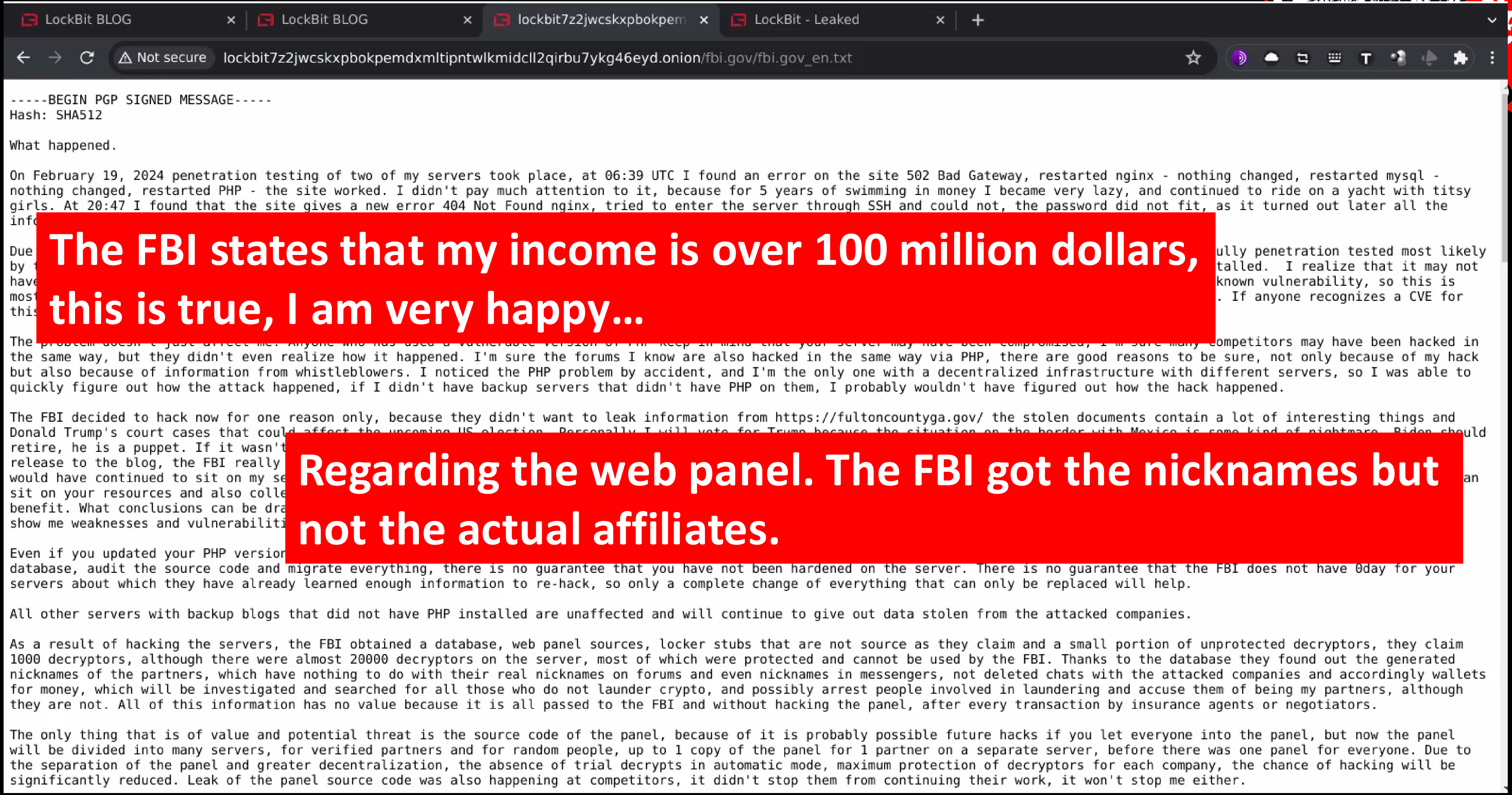
LOCKBIT 3.0

LEAKED DATA

Company name: fbi.gov

File Name ↓	File Size ↓	Date ↓
Parent Directory	-	-
fbi.gov_en.txt	21.0 KiB	February 26, 2024
fbi.gov_ru.txt	32.8 KiB	February 26, 2024

THREAT ACTOR COMMENTS

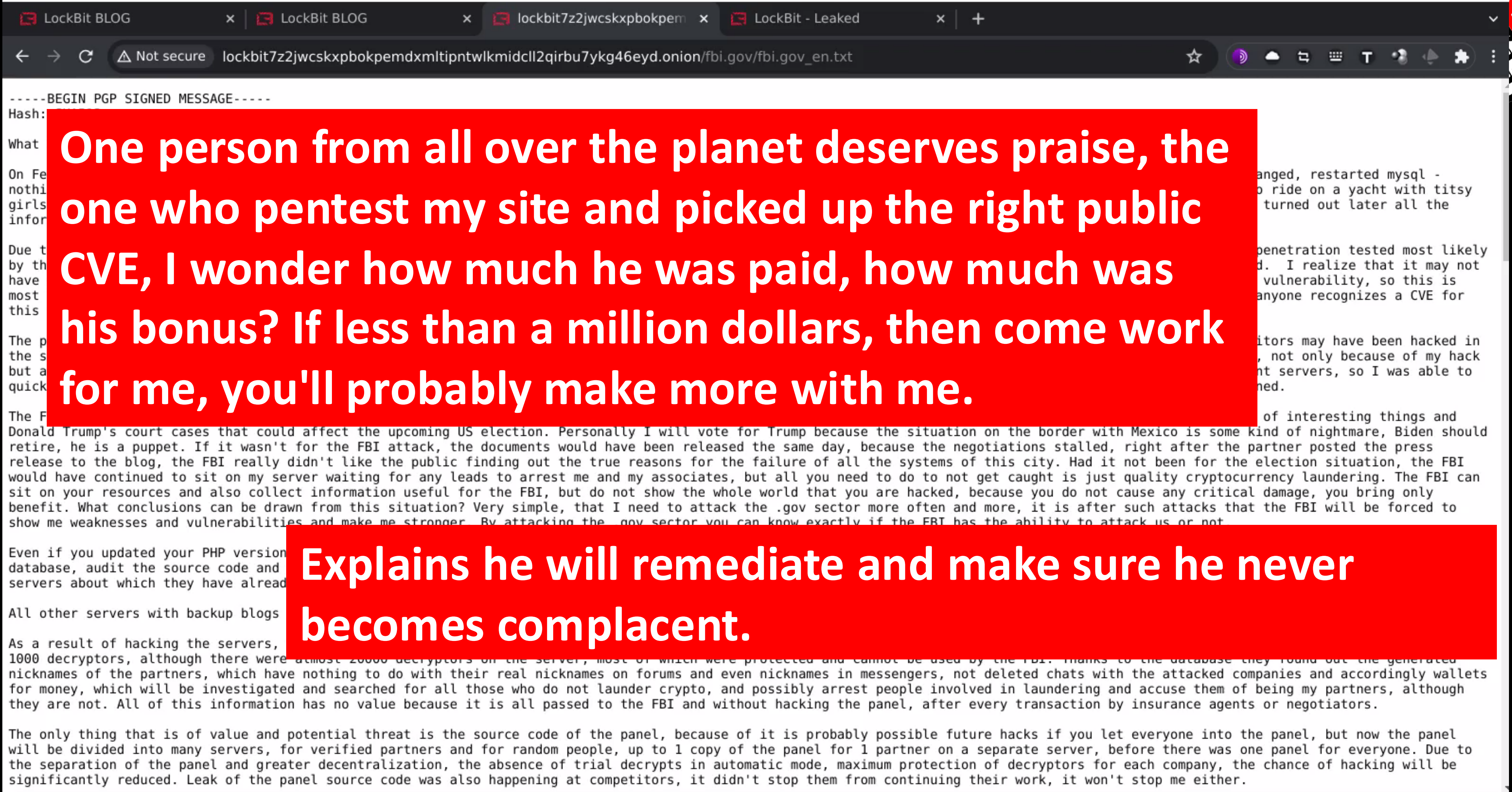

LockBit BLOG
LockBit BLOG
lockbit7z2jwcskxpbokpem
LockBit - Leaked
Not secure
lockbit7z2jwcskxpbokpemdxmltipntwlkmidcll2qirbu7ykg46eyd.onion/fbi.gov/fbi.gov_en.txt

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

What happened.

On February 19, 2024 penetration testing of two of my servers took place, at 06:39 UTC I found an error on the site 502 Bad Gateway, restarted nginx - nothing changed, restarted mysql -
nothing changed, restarted PHP - the site worked. I didn't pay much attention to it, because for 5 years of swimming in money I became very lazy, and continued to ride on a yacht with titsy
girls. At 20:47 I found that the site gives a new error 404 Not Found nginx, tried to enter the server through SSH and could not, the password did not fit, as it turned out later all the
inf

Due                                                                                                                                       ully penetration tested most likely
by t                                                                                                                                      talled.  I realize that it may not
have                                                                                                                                      known vulnerability, so this is
most                                                                                                                                      . If anyone recognizes a CVE for
this

The problem doesn't just affect me. Anyone who has used a vulnerable version of PHP keep in mind that your server may have been compromised, I'm sure many competitors may have been hacked in
the same way, but they didn't even realize how it happened. I'm sure the forums I know are also hacked in the same way via PHP, there are good reasons to be sure, not only because of my hack
but also because of information from whistleblowers. I noticed the PHP problem by accident, and I'm the only one with a decentralized infrastructure with different servers, so I was able to
quickly figure out how the attack happened, if I didn't have backup servers that didn't have PHP on them, I probably wouldn't have figured out how the hack happened.

The FBI decided to hack now for one reason only, because they didn't want to leak information from https://fultoncountyga.gov/ the stolen documents contain a lot of interesting things and
Donald Trump's court cases that could affect the upcoming US election. Personally I will vote for Trump because the situation on the border with Mexico is some kind of nightmare. Biden should
retire, he is a puppet. If it wasn't
release to the blog, the FBI really
would have continued to sit on my se                                                                                                                                             an
sit on your resources and also colle
benefit. What conclusions can be dra
show me weaknesses and vulnerabiliti

Even if you updated your PHP versio
database, audit the source code and migrate everything, there is no guarantee that you have not been hardened on the server. There is no guarantee that the FBI does not have 0day for your
servers about which they have already learned enough information to re-hack, so only a complete change of everything that can only be replaced will help.

All other servers with backup blogs that did not have PHP installed are unaffected and will continue to give out data stolen from the attacked companies.

As a result of hacking the servers, the FBI obtained a database, web panel sources, locker stubs that are not source as they claim and a small portion of unprotected decryptors, they claim
1000 decryptors, although there were almost 20000 decryptors on the server, most of which were protected and cannot be used by the FBI. Thanks to the database they found out the generated
nicknames of the partners, which have nothing to do with their real nicknames on forums and even nicknames in messengers, not deleted chats with the attacked companies and accordingly wallets
for money, which will be investigated and searched for all those who do not launder crypto, and possibly arrest people involved in laundering and accuse them of being my partners, although
they are not. All of this information has no value because it is all passed to the FBI and without hacking the panel, after every transaction by insurance agents or negotiators.

The only thing that is of value and potential threat is the source code of the panel, because of it is probably possible future hacks if you let everyone into the panel, but now the panel
will be divided into many servers, for verified partners and for random people, up to 1 copy of the panel for 1 partner on a separate server, before there was one panel for everyone. Due to
the separation of the panel and greater decentralization, the absence of trial decrypts in automatic mode, maximum protection of decryptors for each company, the chance of hacking will be
significantly reduced. Leak of the panel source code was also happening at competitors, it didn't stop them from continuing their work, it won't stop me either.
```

The FBI states that my income is over 100 million dollars, this is true, I am very happy…

Regarding the web panel. The FBI got the nicknames but not the actual affiliates.

THREAT ACTOR COMMENTS

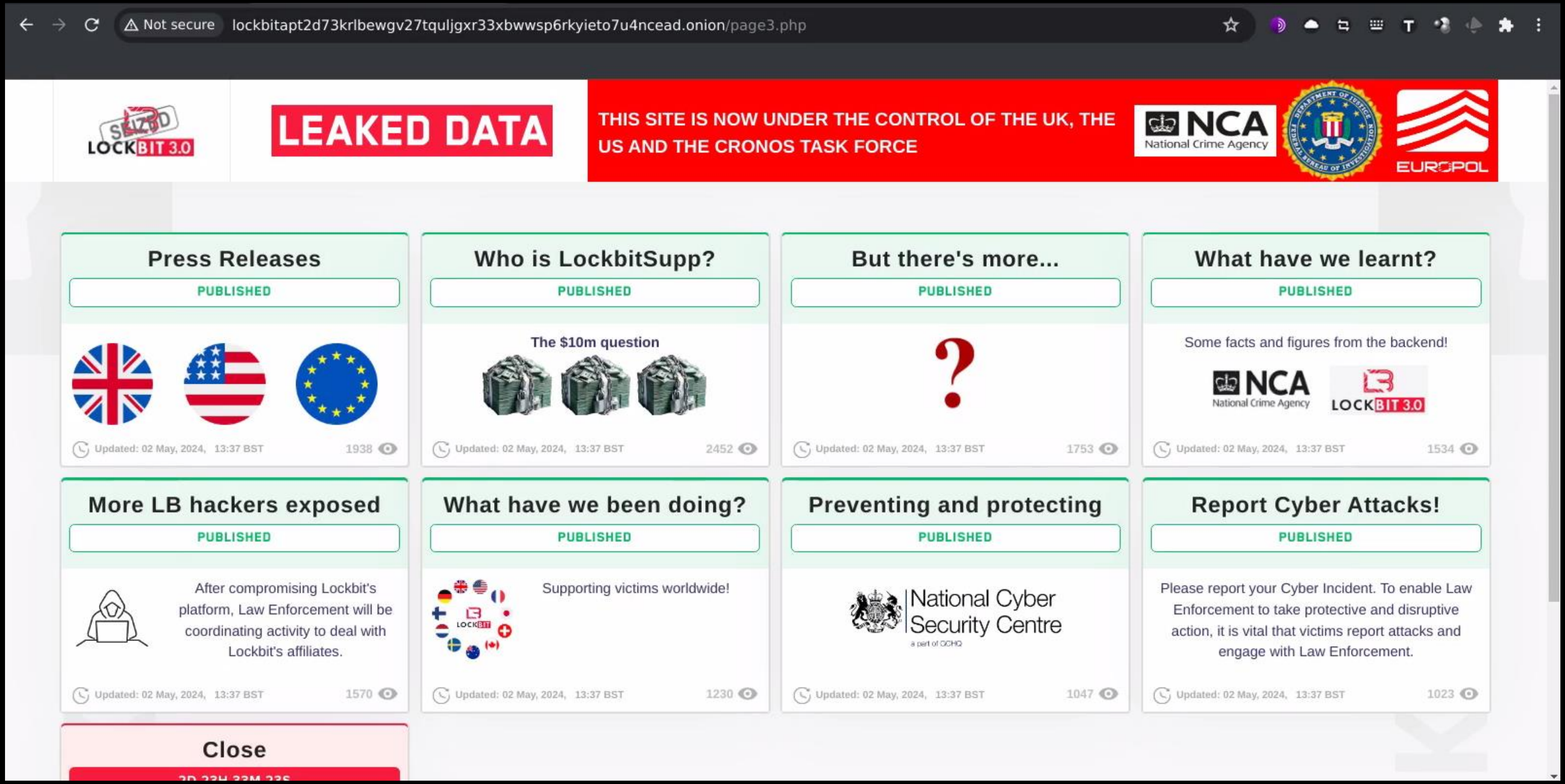

LockBit BLOG
LockBit BLOG
lockbit7z2jwcskxpbokpem
LockBit - Leaked
Not secure
lockbit7z2jwcskxpbokpemdxmltipntwlkmidcll2qirbu7ykg46eyd.onion/fbi.gov/fbi.gov_en.txt

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash:

What

On Fe                                                              anged, restarted mysql -
nothi                                                              o ride on a yacht with titsy
girls                                                               turned out later all the
infor

Due t                                                              penetration tested most likely
by th                                                              d.  I realize that it may not
have                                                                vulnerability, so this is
most                                                               anyone recognizes a CVE for
this

The p                                                              itors may have been hacked in
the s                                                              , not only because of my hack
but a                                                              nt servers, so I was able to
quick                                                              ned.

The F                                                               of interesting things and
Donald Trump's court cases that could affect the upcoming US election. Personally I will vote for Trump because the situation on the border with Mexico is some kind of nightmare, Biden should
retire, he is a puppet. If it wasn't for the FBI attack, the documents would have been released the same day, because the negotiations stalled, right after the partner posted the press
release to the blog, the FBI really didn't like the public finding out the true reasons for the failure of all the systems of this city. Had it not been for the election situation, the FBI
would have continued to sit on my server waiting for any leads to arrest me and my associates, but all you need to do to not get caught is just quality cryptocurrency laundering. The FBI can
sit on your resources and also collect information useful for the FBI, but do not show the whole world that you are hacked, because you do not cause any critical damage, you bring only
benefit. What conclusions can be drawn from this situation? Very simple, that I need to attack the .gov sector more often and more, it is after such attacks that the FBI will be forced to
show me weaknesses and vulnerabilities and make me stronger. By attacking the .gov sector you can know exactly if the FBI has the ability to attack us or not.

Even if you updated your PHP version
database, audit the source code and
servers about which they have alread

All other servers with backup blogs

As a result of hacking the servers,
1000 decryptors, although there were almost 20000 decryptors on the server, most of which were protected and cannot be used by the FBI. Thanks to the database they found out the generated
nicknames of the partners, which have nothing to do with their real nicknames on forums and even nicknames in messengers, not deleted chats with the attacked companies and accordingly wallets
for money, which will be investigated and searched for all those who do not launder crypto, and possibly arrest people involved in laundering and accuse them of being my partners, although
they are not. All of this information has no value because it is all passed to the FBI and without hacking the panel, after every transaction by insurance agents or negotiators.

The only thing that is of value and potential threat is the source code of the panel, because of it is probably possible future hacks if you let everyone into the panel, but now the panel
will be divided into many servers, for verified partners and for random people, up to 1 copy of the panel for 1 partner on a separate server, before there was one panel for everyone. Due to
the separation of the panel and greater decentralization, the absence of trial decrypts in automatic mode, maximum protection of decryptors for each company, the chance of hacking will be
significantly reduced. Leak of the panel source code was also happening at competitors, it didn't stop them from continuing their work, it won't stop me either.
```

One person from all over the planet deserves praise, the one who pentest my site and picked up the right public CVE, I wonder how much he was paid, how much was his bonus? If less than a million dollars, then come work for me, you'll probably make more with me.

Explains he will remediate and make sure he never becomes complacent.

SHUTDOWN AGAIN



Not secure
lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion/page3.php
SEIZED
LOCKBIT 3.0

LEAKED DATA

THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

NCA National Crime Agency
EUROPOL

Press Releases
PUBLISHED
Updated: 02 May, 2024, 13:37 BST 1938

Who is LockbitSupp?
PUBLISHED
The $10m question
Updated: 02 May, 2024, 13:37 BST 2452

But there's more...
PUBLISHED
?
Updated: 02 May, 2024, 13:37 BST 1753

What have we learnt?
PUBLISHED
Some facts and figures from the backend!
Updated: 02 May, 2024, 13:37 BST 1534

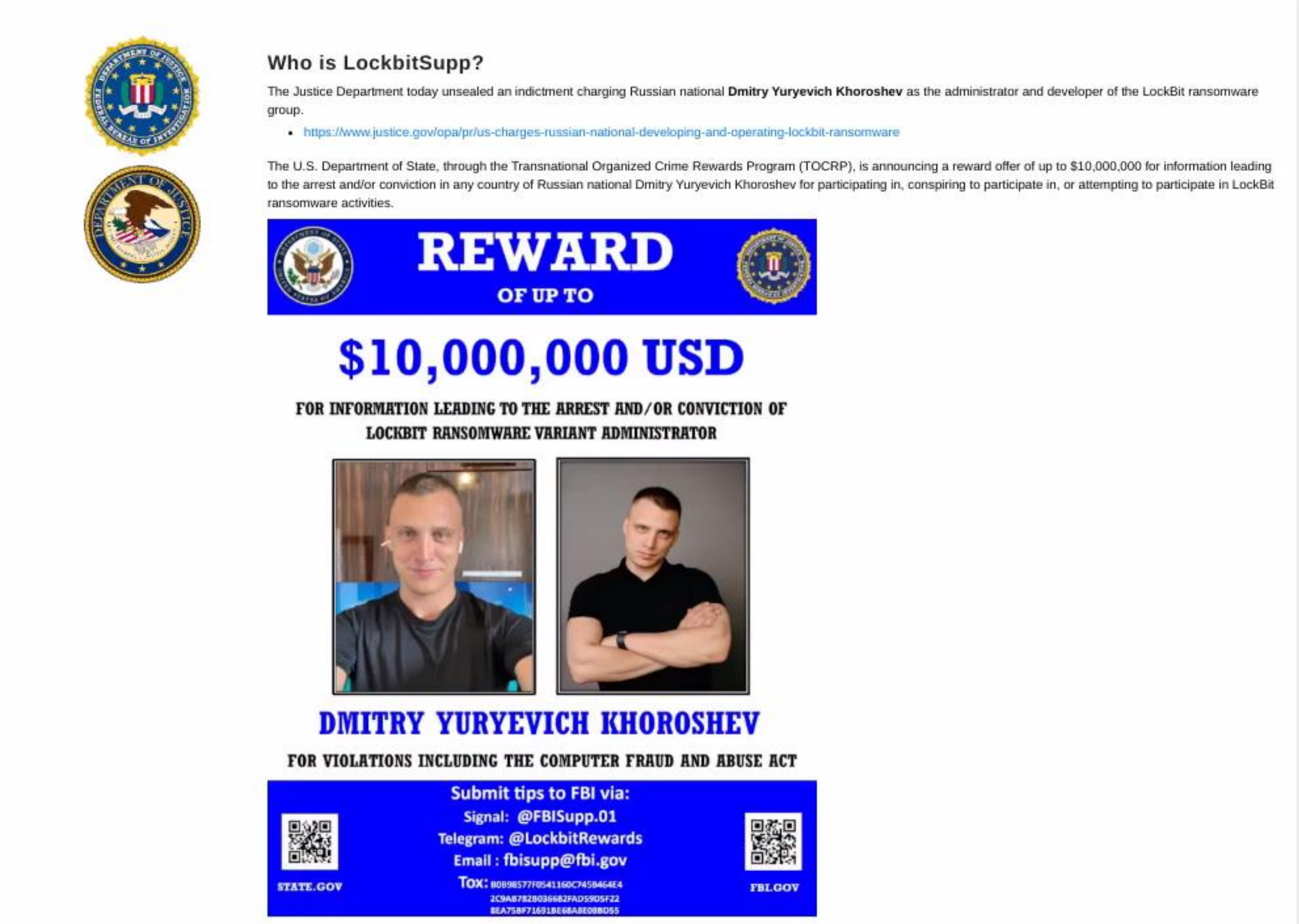
More LB hackers exposed
PUBLISHED
After compromising Lockbit's platform, Law Enforcement will be coordinating activity to deal with Lockbit's affiliates.
Updated: 02 May, 2024, 13:37 BST 1570

What have we been doing?
PUBLISHED
Supporting victims worldwide!
Updated: 02 May, 2024, 13:37 BST 1230

Preventing and protecting
PUBLISHED
National Cyber Security Centre
a part of GCHQ
Updated: 02 May, 2024, 13:37 BST 1047

Report Cyber Attacks!
PUBLISHED
Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive action, it is vital that victims report attacks and engage with Law Enforcement.
Updated: 02 May, 2024, 13:37 BST 1023

Close
2D 23H 33M 23S



Who is LockbitSupp?

The Justice Department today unsealed an indictment charging Russian national **Dmitry Yuryevich Khoroshev** as the administrator and developer of the LockBit ransomware group.

- https://www.justice.gov/opa/pr/us-charges-russian-national-developing-and-operating-lockbit-ransomware

The U.S. Department of State, through the Transnational Organized Crime Rewards Program (TOCRP), is announcing a reward offer of up to $10,000,000 for information leading to the arrest and/or conviction in any country of Russian national Dmitry Yuryevich Khoroshev for participating in, conspiring to participate in, or attempting to participate in LockBit ransomware activities.

REWARD

OF UP TO

$10,000,000 USD

FOR INFORMATION LEADING TO THE ARREST AND/OR CONVICTION OF LOCKBIT RANSOMWARE VARIANT ADMINISTRATOR

DMITRY YURYEVICH KHOROSHEV

FOR VIOLATIONS INCLUDING THE COMPUTER FRAUD AND ABUSE ACT

Submit tips to FBI via:

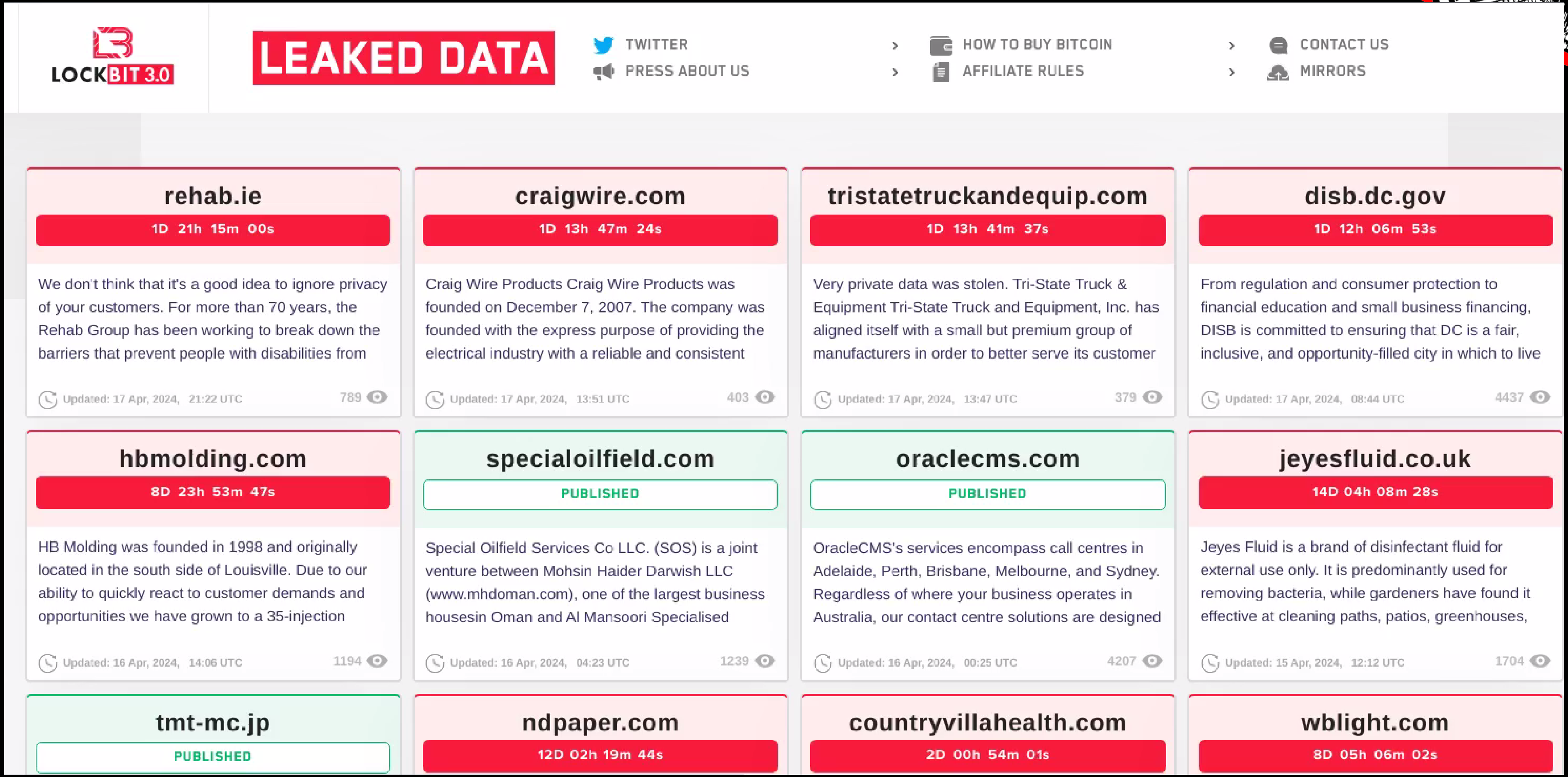
Signal: @FBISupp.01
Telegram: @LockbitRewards
Email : fbisupp@fbi.gov
Tox: 80B98577F0541160C7458464E4
2C9A87828036682FAD59D5F22
8EA758F71691BE68ABE08BD55

STATE.GOV

FBI.GOV

LOCKBIT SITE

Secure Network



LOCKBIT 3.0

LEAKED DATA

TWITTER ›
PRESS ABOUT US ›
HOW TO BUY BITCOIN ›
AFFILIATE RULES ›
CONTACT US
MIRRORS

rehab.ie
1D 21h 15m 00s
We don't think that it's a good idea to ignore privacy of your customers. For more than 70 years, the Rehab Group has been working to break down the barriers that prevent people with disabilities from
Updated: 17 Apr, 2024, 21:22 UTC 789

craigwire.com
1D 13h 47m 24s
Craig Wire Products Craig Wire Products was founded on December 7, 2007. The company was founded with the express purpose of providing the electrical industry with a reliable and consistent
Updated: 17 Apr, 2024, 13:51 UTC 403

tristatetruckandequip.com
1D 13h 41m 37s
Very private data was stolen. Tri-State Truck & Equipment Tri-State Truck and Equipment, Inc. has aligned itself with a small but premium group of manufacturers in order to better serve its customer
Updated: 17 Apr, 2024, 13:47 UTC 379

disb.dc.gov
1D 12h 06m 53s
From regulation and consumer protection to financial education and small business financing, DISB is committed to ensuring that DC is a fair, inclusive, and opportunity-filled city in which to live
Updated: 17 Apr, 2024, 08:44 UTC 4437

hbmolding.com
8D 23h 53m 47s
HB Molding was founded in 1998 and originally located in the south side of Louisville. Due to our ability to quickly react to customer demands and opportunities we have grown to a 35-injection
Updated: 16 Apr, 2024, 14:06 UTC 1194

specialoilfield.com
PUBLISHED
Special Oilfield Services Co LLC. (SOS) is a joint venture between Mohsin Haider Darwish LLC (www.mhdoman.com), one of the largest business housesin Oman and Al Mansoori Specialised
Updated: 16 Apr, 2024, 04:23 UTC 1239

oraclecms.com
PUBLISHED
OracleCMS's services encompass call centres in Adelaide, Perth, Brisbane, Melbourne, and Sydney. Regardless of where your business operates in Australia, our contact centre solutions are designed
Updated: 16 Apr, 2024, 00:25 UTC 4207

jeyesfluid.co.uk
14D 04h 08m 28s
Jeyes Fluid is a brand of disinfectant fluid for external use only. It is predominantly used for removing bacteria, while gardeners have found it effective at cleaning paths, patios, greenhouses,
Updated: 15 Apr, 2024, 12:12 UTC 1704

tmt-mc.jp
PUBLISHED

ndpaper.com
12D 02h 19m 44s

countryvillahealth.com
2D 00h 54m 01s

wblight.com
8D 05h 06m 02s

BACK UP IN 1 DAY

THE BAD GUYS TEST AND REMEDIATE

Most Businesses Don't

WHAT ORGANIZATIONS NEED TO DO

PENTEST (DON'T WASTE TIME WITH JUST SCANNING)

REMEDIATE THE NETWORK ISSUES

PURPLE TEAM AND TABLETOP

CYBER INSURANCE (MAKE SURE IT'S SUFFICIENT)

EDUCATE USERS ON SECURITY

QUESTIONS?

SECURE NETWORK
TECHNOLOGIES

Jim Ockenden
Security Advisor
315.949.2803 | Office
315.374.6721 | Mobile
jim@securenetworkinc.com