Unit IT

Cybertrusler og kriminalitet

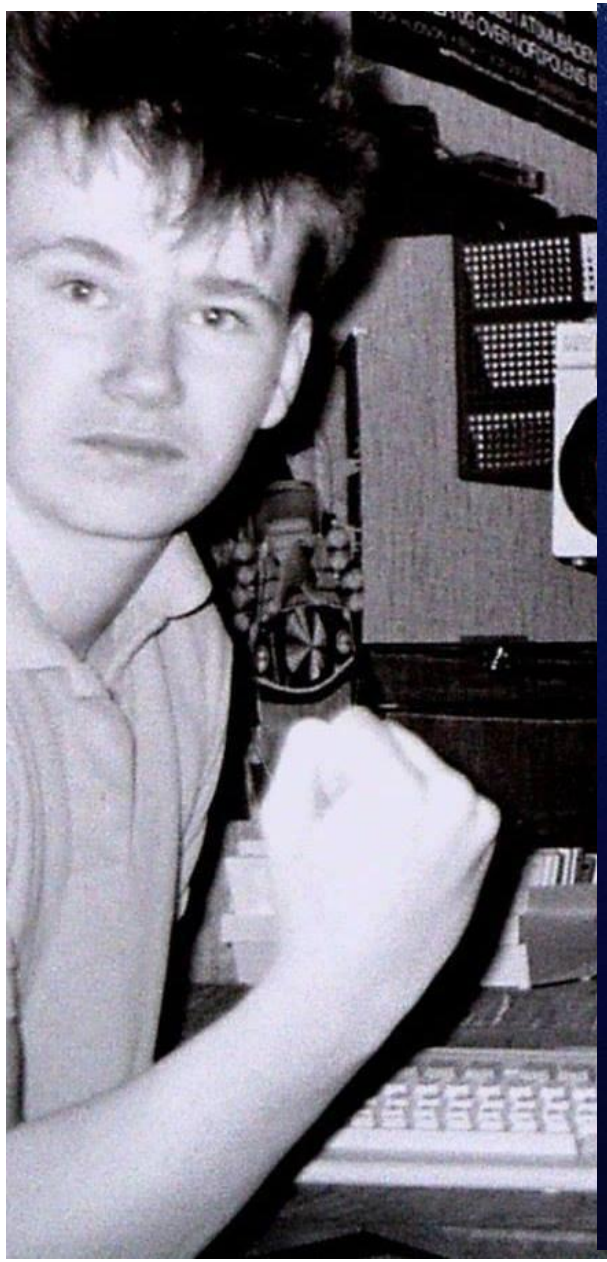
Cybertrusler og kriminalitet

Agenda

1.00 Cybertrusler og it-sikkerhed
2.00 Crime as a Service
3.00 Ransomware og RaaS
4.00 DDoS as a Service
5.00 Smishing, phishing og vishing
6.00 Supply Chain angreb
7.00 MiTM angreb mod MitID og NemID
8.00 Opsamling og gode råd

Whois Peter Kruse

- Har analyseret computervirus siden 1986
- Har arbejdet professionelt med IT-sikkerhedhed siden 1998
- Har arbejdet hos TDC, Telia og Norman Antivirus
- Stifter af CSIS, Heimdal og SIE Europe
- Medlem af CARO, OPS-T og tidligere og nuværende rådgiver for Europol og Interpol
- Medlem af Dansk Industri's IT-sikkerhedsudvalg siden 2010
- Taler på vettede IT-sikkerhedskonferencer som CARO, FIRST, Virus Bulletin, Interpol og Team Cymru UE, Kaspersky SAS, APWG, BOTconf, Cyberhagen m.fl.
- CISO i Clever




NSS LABS

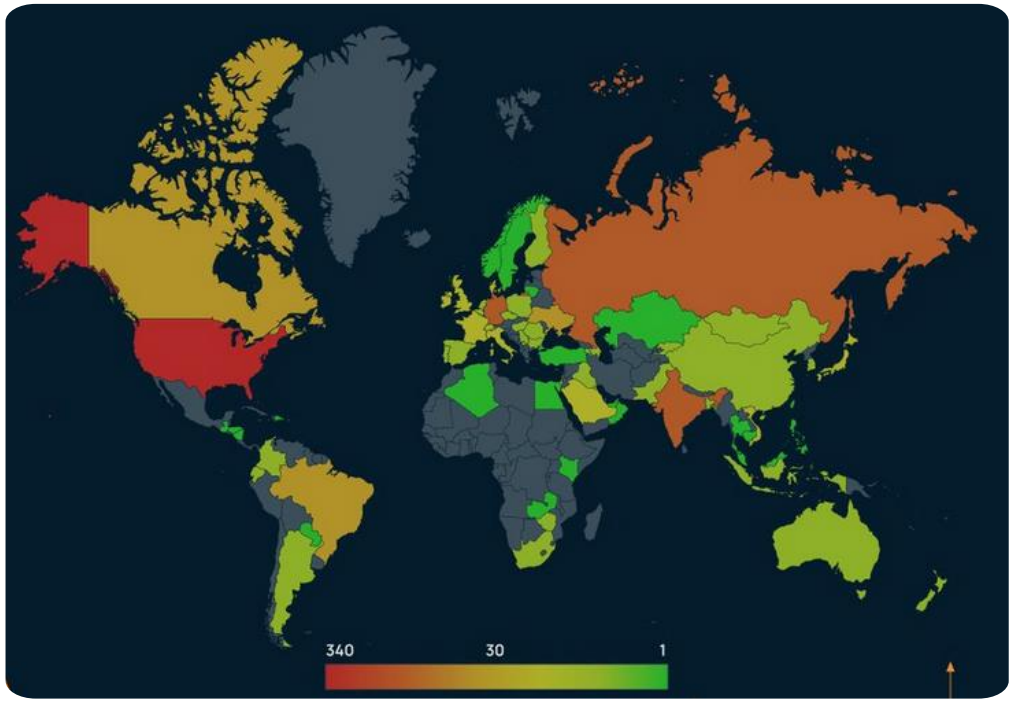
Cybertrusler og it-kriminalitet

1.00 Cybertrusler og it-sikkerhed

Cybertrusler og it-sikkerhed

- Brugerne er fortsat det svageste link – email er stadig den primære bæreform
- Der er et stort antal SMV, som ikke har basale sikkerhedstiltag på plads. Der mangler fokus på alt fra vedligeholdelse, overvågning, brugerawareness, risikovurdering til sikring og beredskab
- Ca. 25 procent af alle større incident response sager i 2022 skyldes dårligt sikret perimeter udstyr (100% er optaget i CISA (Known Exploited Vulnerabilities Catalog)
- Der er en fortsat vækst i tilgang af zombier på Mac, Linux samt Android og IoTs. Windows er i fald.
- Ransomware udgør fortsat den mest overhængende trussel for alle typer virksomheder
- Der laves phishing, spear phishing og smishing i en hidtil uset grad
- Fortsat høj aktivitet i CEO og BEC svindel i 2022/2023

Cybertrusler og it-kriminalitet



- De kriminelle flytter ind i veldesignede CaaS platforme
- Nedskydning af QakBOT har flyttet de kriminelle over til bl.a. IcedID og PikaBOT
- Krigen i Europa giver de it-kriminelle de bedste arbejdsbetingelser
- De kriminelle arbejder uden risiko for retsforfølgelse og udlevering
- Det største antal af 0-dags sårbarheder nogensinde I 2023 og vi er end ikke ude af året …

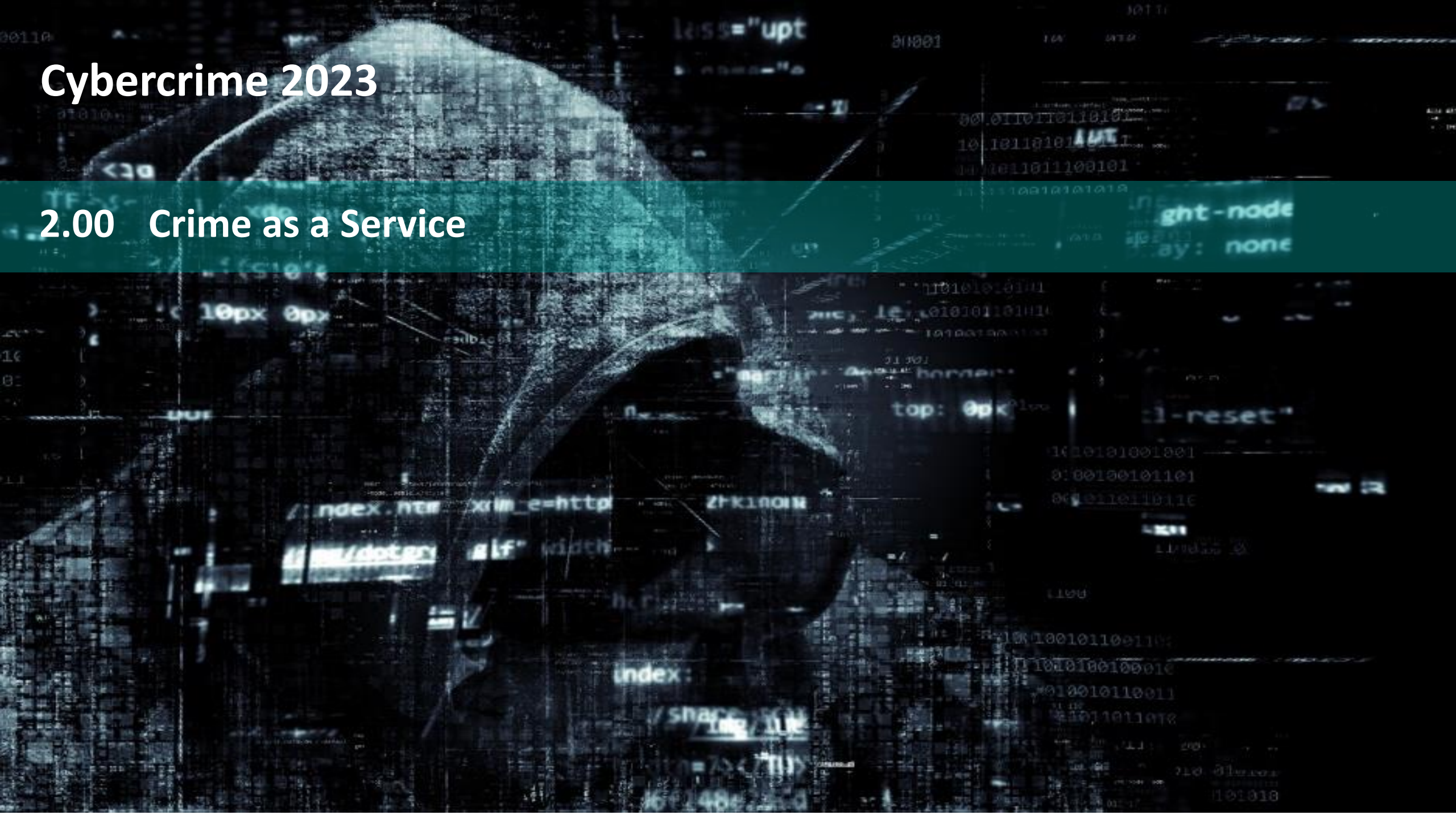
Nuværende trusler

- Phishing/smishing er tilbage for fulde omdrejninger og når usete højder i 2023
- Antallet af kompromitterede endpoints er i fald
- Der mangler i mange virksomheder fokus på AD sikkerhed. Et ransomware angreb kan gå fra initiel infektion til all-out domæne infektion på under 3 timer med sideløbende destruktion af backups og dataeksfiltration!
- Crime as a Service vokser fortsat og bliver bedre og bedre for de it-kriminelle
- Cobalt Strike er fortsat de it-kriminelle's primære rammeværk til lateral bevægelse
- Sporadiske aktivist angreb med DDoS og defacements og datatyverier
- Google reklamer bruges til at levere trojaniserede installationspakker med datatyve

- **Vi har 100.604 gode grunde til at udvise god internet hygiene**

Cybercrime 2023

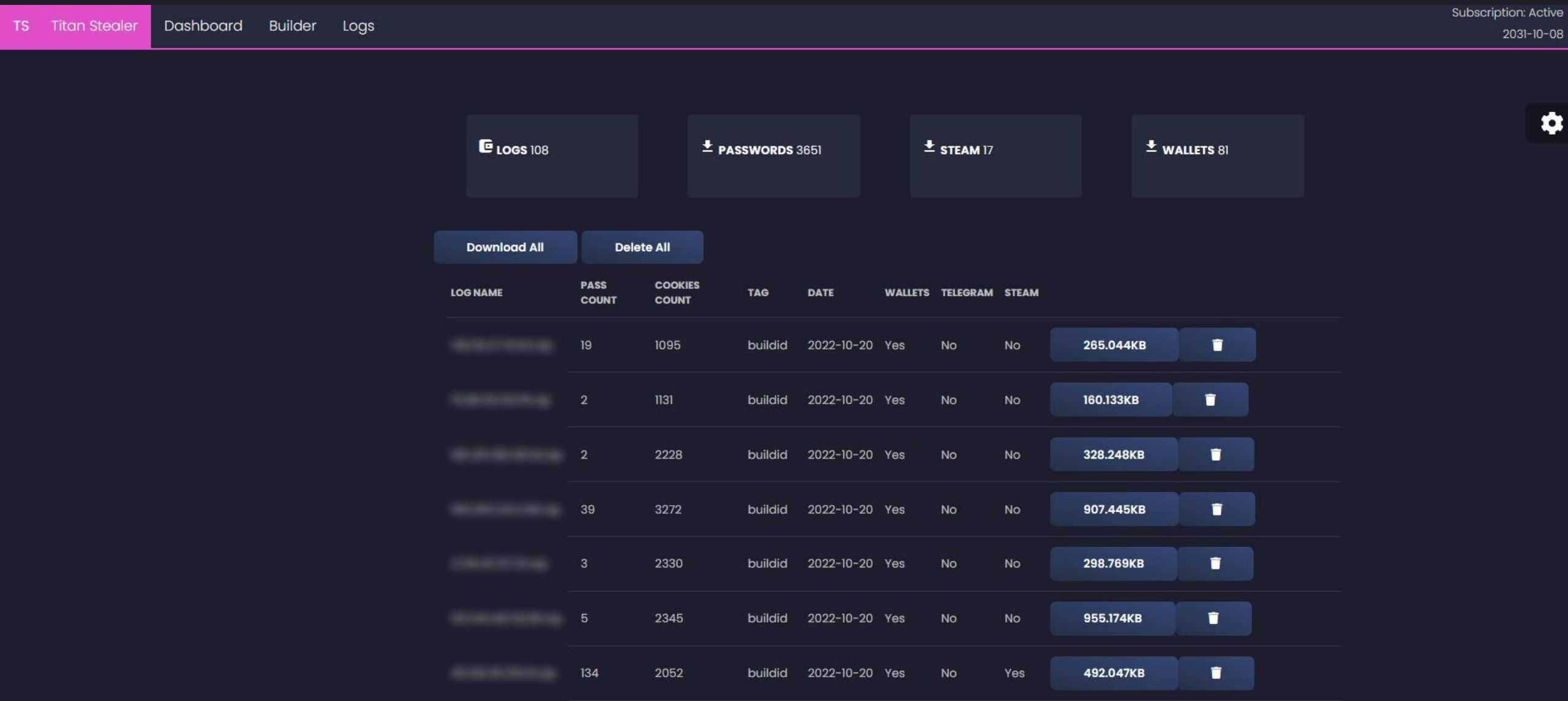
2.00 Crime as a Service



DASHBOARD | SETTINGS | BUILDER | CHECKER | LOADER / GRABBER | DARK NEWS

35	1867	90884	0
LOGS	PASSWORD	COOKIES	WALLETS

USER	BUILD	IP	GEO	PASSWORD	COOKIES	WALLETS	DATE	DW	DT
[redacted]		[redacted]	ua	92	2037	0	2022-09-01 | 15:41	Download	Delete
[redacted]		[redacted]	ua	81	3563	0	2022-09-01 | 15:41	Download	Delete
[redacted]		[redacted]	br	1	273	0	2022-09-01 | 15:41	Download	Delete
[redacted]		[redacted]	br	5	2582	0	2022-09-01 | 15:41	Download	Delete
[redacted]		[redacted]	br	306	6043	0	2022-09-01 | 15:41	Download	Delete
[redacted]		[redacted]	br	114	3799	0	2022-09-01 | 15:41	Download	Delete
[redacted]		[redacted]	pe	1	977	0	2022-09-01 | 15:41	Download	Delete
[redacted]		[redacted]	br	55	3063	0	2022-09-01 | 15:41	Download	Delete
[redacted]		[redacted]	bb	75	1794	0	2022-09-01 | 15:41	Download	Delete
[redacted]		[redacted]	eg	11	368	0	2022-09-01 | 15:41	Download	Delete
[redacted]		[redacted]	br	2	3013	0	2022-09-01 | 15:41	Download	Delete
[redacted]		[redacted]	in	10	2191	0	2022-09-01 | 15:41	Download	Delete
[redacted]		[redacted]	th	14	3008	0	2022-09-01 | 15:42	Download	Delete
[redacted]		[redacted]					2022-09-		


TS
Titan Stealer
Dashboard
Builder
Logs
Subscription: Active
2031-10-08
LOGS 108
PASSWORDS 3651
STEAM 17
WALLETS 81
Download All
Delete All
LOG NAME
PASS COUNT
COOKIES COUNT
TAG
DATE
WALLETS
TELEGRAM
STEAM
19 1095 buildid 2022-10-20 Yes No No 265.044KB
2 1131 buildid 2022-10-20 Yes No No 160.133KB
2 2228 buildid 2022-10-20 Yes No No 328.248KB
39 3272 buildid 2022-10-20 Yes No No 907.445KB
3 2330 buildid 2022-10-20 Yes No No 298.769KB
5 2345 buildid 2022-10-20 Yes No No 955.174KB
134 2052 buildid 2022-10-20 Yes No Yes 492.047KB

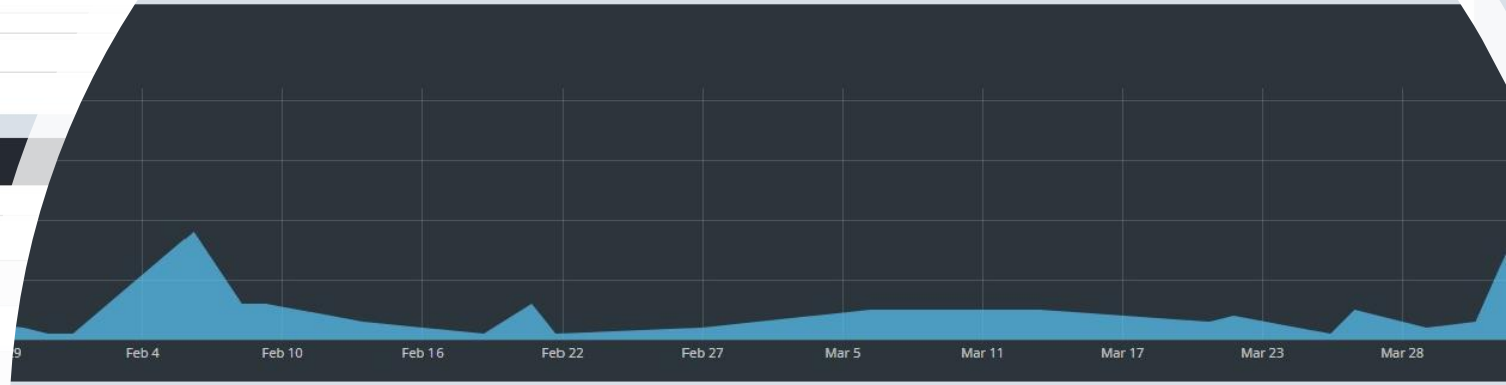
Builder | Личные прокладки | История транзакций

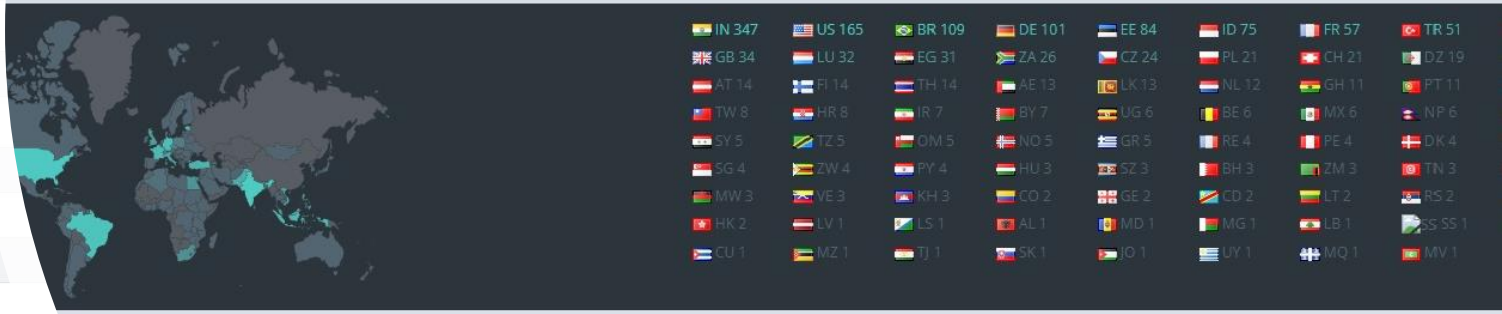
Подписка

Баланс	1.00000 BTC
Подписка действительна до	15-05-2022 (30дн.)
Срок	7 дней: 0.00323 BTC ($130)

BUILDER ПОДПИСКА
До 15-05-2022 (30дн.)
Подробнее

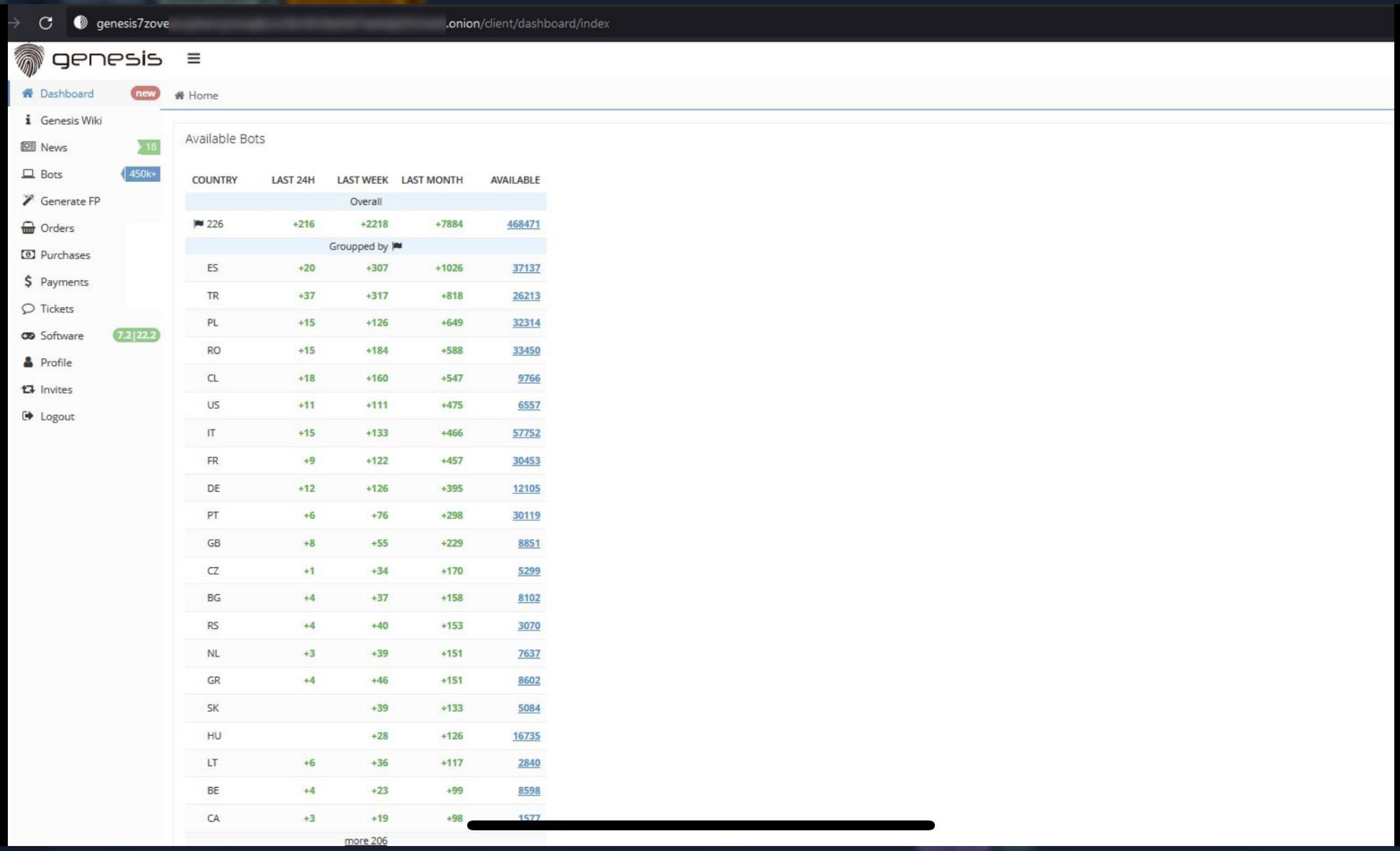
ЛОГИ
1882
Посмотреть





Обновления Builder

Версия	Изменения
51.7 — Изменение алгоритмов работы Vidar	
51.6 — чистка софта, ротация адресов	Плановые работы по улучшению отстука
51.5 — Фикс обновы	Мелкий фикс
51.4 — крупное обновление	Множество изменений
51.3 — ротация	Замена хостов для отстука. Старый отстук тоже сохранён
51.2 — ОБНОВИСЬ! Замена сервиса	Заменили прокладку с сохранение отличного отстука
51.1 — оптимизированная система отстука	убрали лишние этапы на пути отстука
51 — плановое обновление	еженедельная чистка
50.9 — Профилактика	улучшение отстука
50.8 — еженедельное обновление	плановая чистка
50.7 — внеплановое обновление	боремся за отстук
50.6 — внеплановая ротация	смена адресов для отстука
50.5 — плановая чистка	чистка софта, ротация адресов
50.4 — плановое обновление	Еженедельная чистка, ротация отстука
50.3 — Ротация	Периодическая плановая чистка
50.2 — Еженедельное обновление	обновили сбор Metamask с Edge, плановая чистка
50.1 — плановое обновление	плановая чистка, фикс релоков для крипторов
50 — Фикс бага	Фикс бага отстука Срочно обновитесь с 49.0
49.9 — плановая чистка	чистка софта, ротация адресов


genesis7zove
.onion/client/dashboard/index
genesis
Dashboard
new
Genesis Wiki
News
18
Bots
450k+
Generate FP
Orders
Purchases
Payments
Tickets
Software
7.2|22.2
Profile
Invites
Logout
Home
Available Bots
COUNTRY LAST 24H LAST WEEK LAST MONTH AVAILABLE
Overall
226 +216 +2218 +7884 468471
Groupped by
ES +20 +307 +1026 37137
TR +37 +317 +818 26213
PL +15 +126 +649 32314
RO +15 +184 +588 33450
CL +18 +160 +547 9766
US +11 +111 +475 6557
IT +15 +133 +466 57752
FR +9 +122 +457 30453
DE +12 +126 +395 12105
PT +6 +76 +298 30119
GB +8 +55 +229 8851
CZ +1 +34 +170 5299
BG +4 +37 +158 8102
RS +4 +40 +153 3070
NL +3 +39 +151 7637
GR +4 +46 +151 8602
SK +39 +133 5084
HU +28 +126 16735
LT +6 +36 +117 2840
BE +4 +23 +99 8598
CA +3 +19 +98 1577
more 206

37.139.129.145/Bunny/login.php

Username

Password

Login

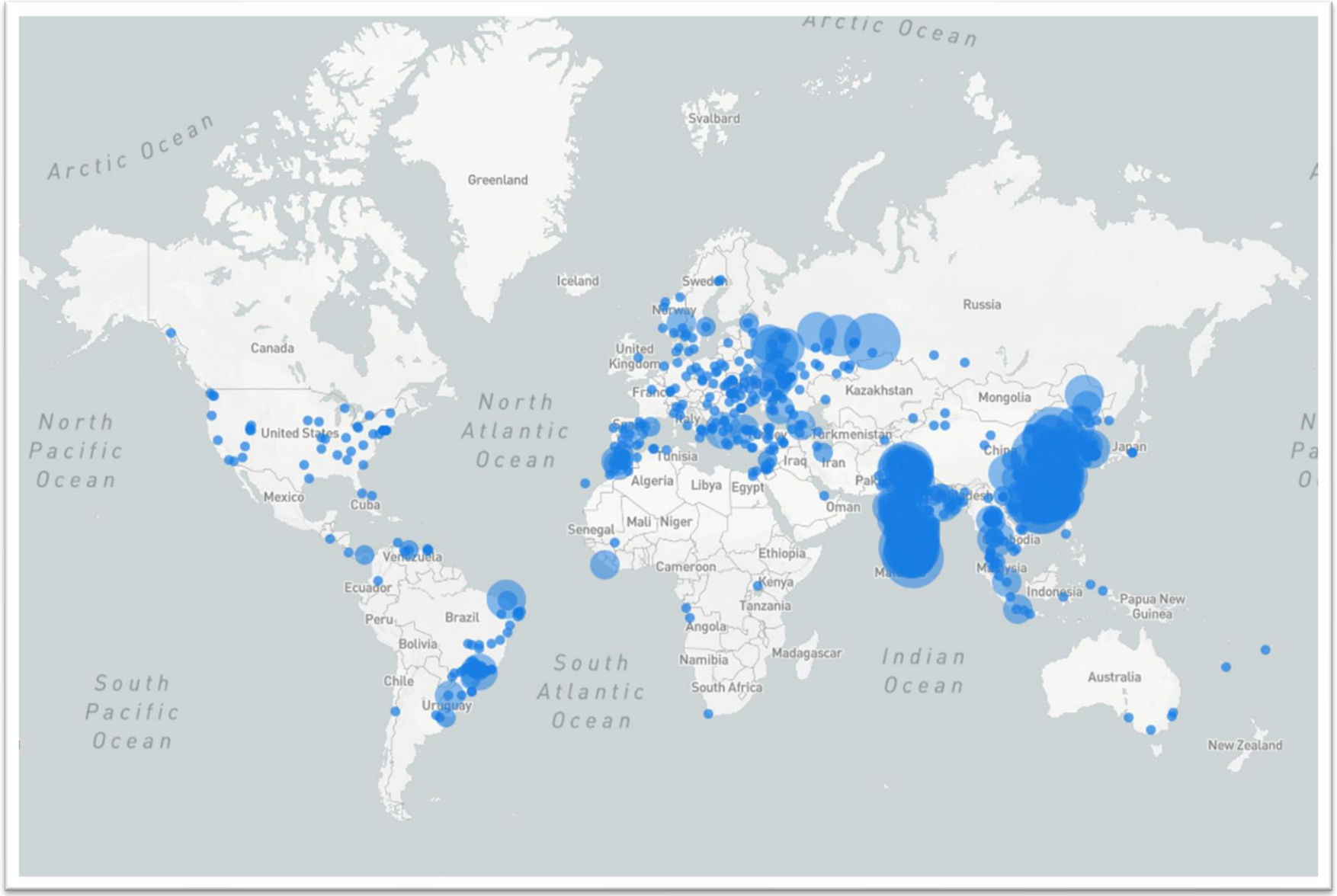
37.139.129.145/Bunny/

Index of /Bunny

Name	Last modified	Size	Description
Parent Directory		-	
Add.php	2023-09-22 08:35	1.2K	
Capture.PNG	2023-09-17 16:16	18K	
CommandCenter.php	2023-09-20 14:49	8.7K	
Connect.php	2023-07-27 20:29	191	
Echoer.php	2023-09-02 22:50	803	
Heartbeat.php	2023-09-02 22:26	1.0K	
Login_Check.php	2023-07-18 16:05	135	
ResultCMD.php	2023-09-02 22:50	536	
SHELL.php	2023-09-03 21:45	6.9K	
Settings.php	2023-09-15 15:59	10K	
Stats.php	2023-09-20 14:38	11K	
Stealer.php	2023-09-20 15:12	14K	
StealerLogs/	2023-09-25 15:27	-	
StealerRegistration.php	2023-09-19 22:18	1.1K	
Tabs.PNG	2023-09-17 16:14	8.2K	
TaskHandler.php	2023-08-26 22:31	1.1K	
Tasks.php	2023-09-15 15:18	12K	
Uploader.php	2023-09-02 22:53	404	
areaResult.php	2023-08-14 13:25	430	
login.php	2023-09-20 07:59	2.8K	

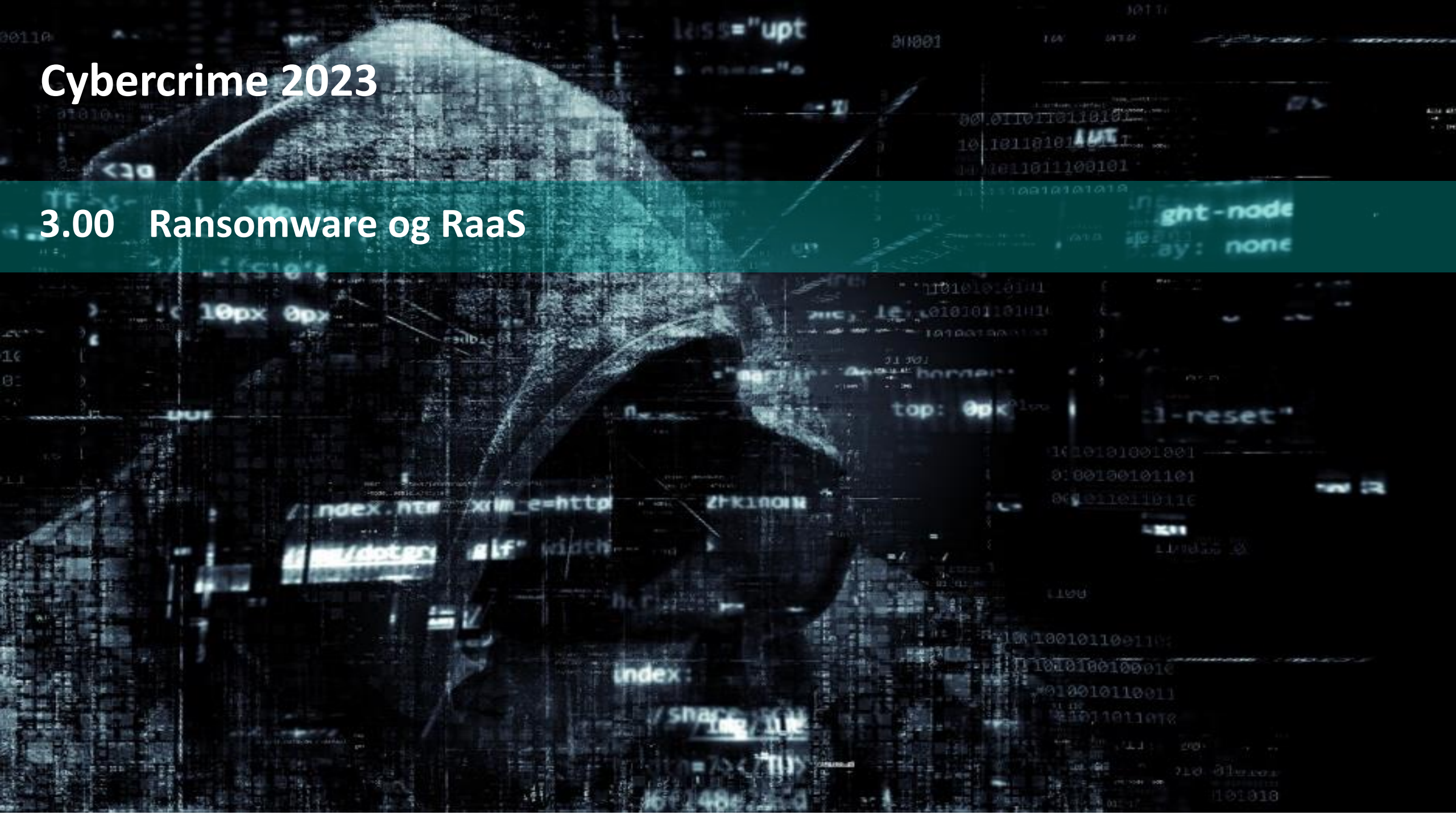
Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 37.139.129.145 Port 80

Crime as a Service – de stjæler ALT – IoT



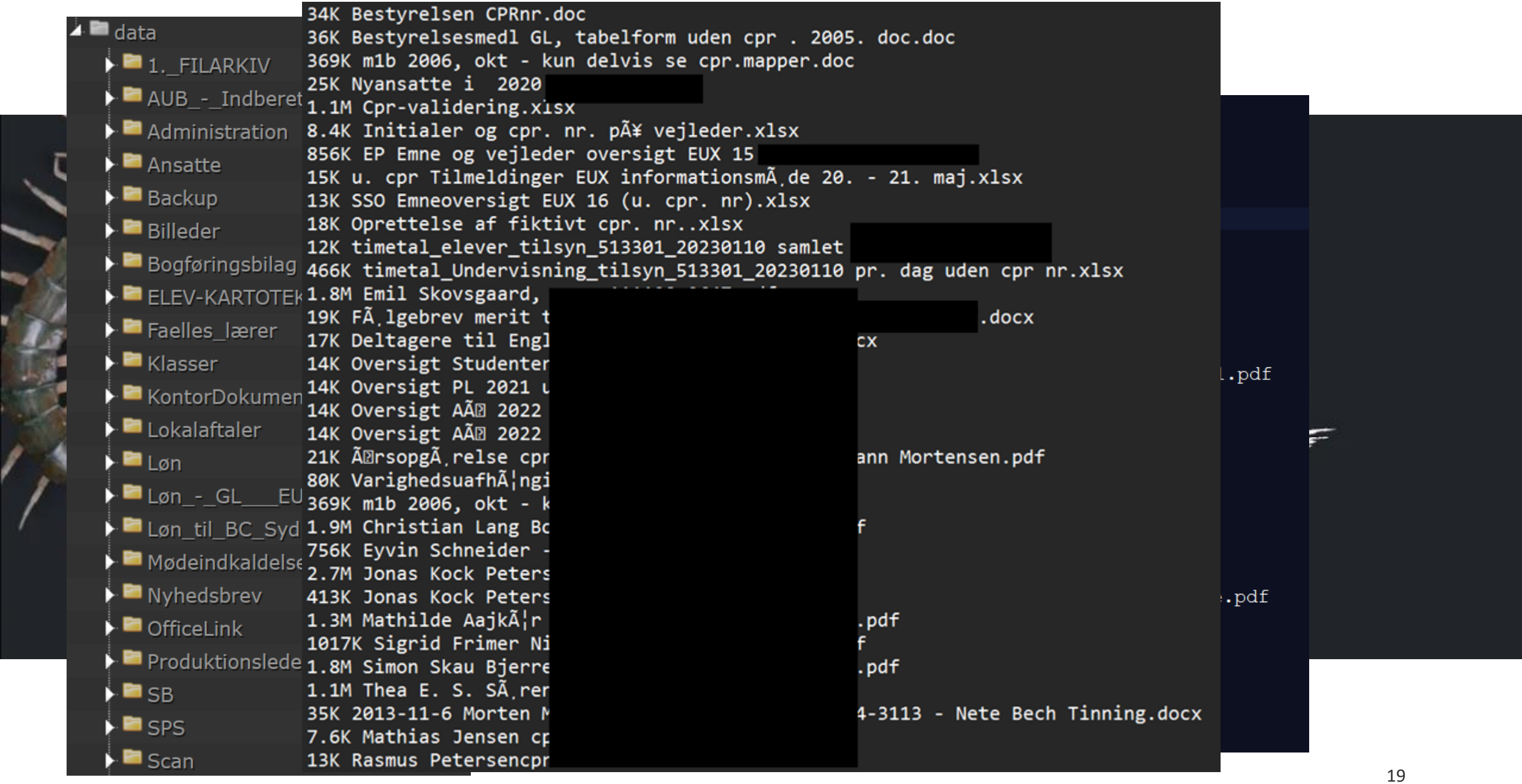
Cybercrime 2023

3.00 Ransomware og RaaS



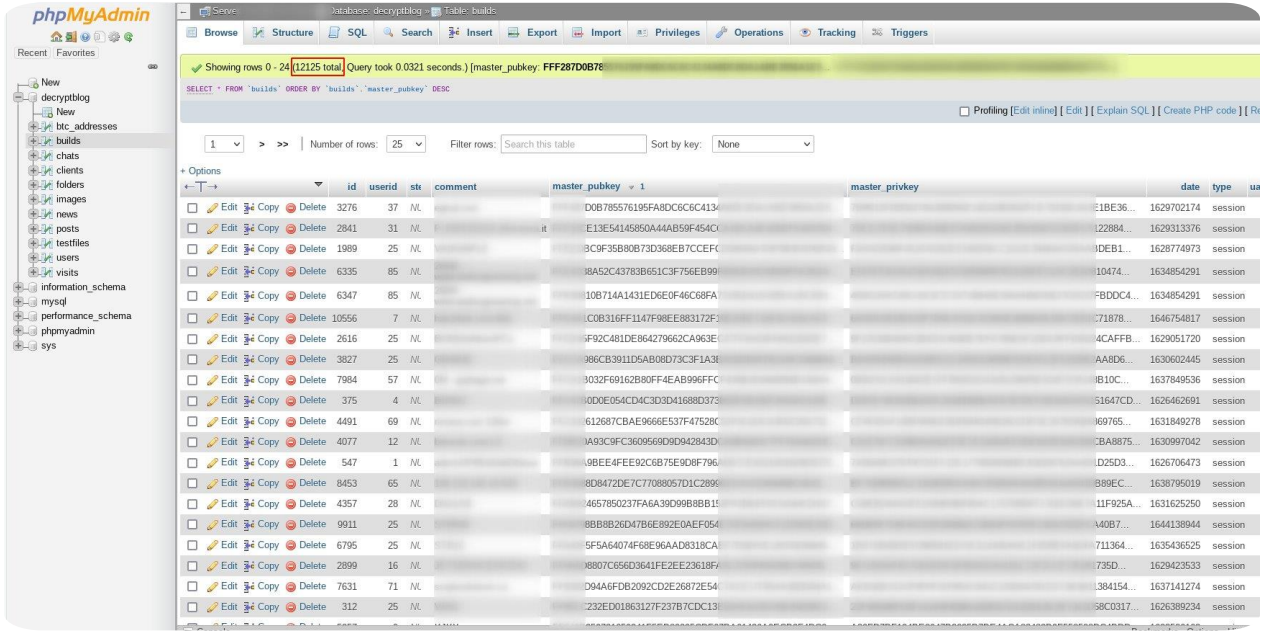

data
1._FILARKIV
AUB_-_Indberetning_Kost_Logi
Administration
Ansatte
Backup
Billeder
Bogføringsbilag
ELEV-KARTOTEK
Faelles_lærer
Klasser
KontorDokumenter
Lokalaftaler
Løn
Løn_-_GL___EUC
Løn_til_BC_Syd
Mødeindkaldelser_og_referater
Nyhedsbrev
OfficeLink
Produktionsledere
SB
SPS
Scan

RHYSIDA


data
1._FILARKIV
AUB_-_Indberet
Administration
Ansatte
Backup
Billeder
Bogføringsbilag
ELEV-KARTOTEK
Faelles_lærer
Klasser
KontorDokumen
Lokalaftaler
Løn
Løn_-_GL___EU
Løn_til_BC_Syd
Mødeindkaldelse
Nyhedsbrev
OfficeLink
Produktionslede
SB
SPS
Scan
34K Bestyrelsen CPRnr.doc
36K Bestyrelsesmedl GL, tabelform uden cpr . 2005. doc.doc
369K m1b 2006, okt - kun delvis se cpr.mapper.doc
25K Nyansatte i 2020
1.1M Cpr-validering.xlsx
8.4K Initialer og cpr. nr. pÃ¥ vejleder.xlsx
856K EP Emne og vejleder oversigt EUX 15
15K u. cpr Tilmeldinger EUX informationsmÃ¸de 20. - 21. maj.xlsx
13K SSO Emneoversigt EUX 16 (u. cpr. nr).xlsx
18K Oprettelse af fiktivt cpr. nr..xlsx
12K timetal_elever_tilsyn_513301_20230110 samlet
466K timetal_Undervisning_tilsyn_513301_20230110 pr. dag uden cpr nr.xlsx
1.8M Emil Skovsgaard,
19K FÃ¸lgebrev merit t .docx
17K Deltagere til Engl cx
14K Oversigt Studenter
14K Oversigt PL 2021 u
14K Oversigt AÃ 2022
14K Oversigt AÃ 2022
21K Ã rsopgÃ¸relse cpr ann Mortensen.pdf
80K VarighedsuafhÃ¦ngi
369K m1b 2006, okt - k
1.9M Christian Lang Bc f
756K Eyvin Schneider -
2.7M Jonas Kock Peters
413K Jonas Kock Peters
1.3M Mathilde AajkÃ¦r .pdf
1017K Sigrid Frimer Ni f
1.8M Simon Skau Bjerre .pdf
1.1M Thea E. S. SÃ¸rer
35K 2013-11-6 Morten M 4-3113 - Nete Bech Tinning.docx
7.6K Mathias Jensen cp
13K Rasmus Petersencpr
.pdf
.pdf

Fredag den 18. august 2023 blev CloudNordic, en førende leverandør af cloud-tjenester, offer for et alvorligt ransomware angreb. Hackerne tog kontrol over samtlige systemer, hvilket resulterede i en omfattende nedetid og data tab for både virksomheden og deres kunder.

Ransomware – LockBit2.0 – 3.0 med DDoS



- Den mest aggressive pt er LockBit2.0, som har publiceret data fra ikke færre end 912 forskellige virksomheder og lavet afpresning mod 12,125 virksomheder på ét år

- En forsigtig beregning på den potentielle indtægt af disse angreb kan opgøres således:
  12,125 x $200,000 (lavt estimat) = $2,425,000,000

Maze support system

What's just happened?

If you see this page it means you have a vulnerability in your system.
This vulnerability was used to modify your valuable data in a way, which temporary disallow further usage of it.
Please upload DECRYPT-FILES.txt using the form below and start recovering your data.
If this file is recognized by our parser, you will be successfully authorized and provided with further instructions.

Please upload DECRYPT-FILES.txt

Browse... No file selected.

Guarantees?

We can recover your files, as our software is carefully designed to keep the integrity and safety of your files.

Don't be afraid and start recovering!

Antivirus corporations?

If you are waiting for a free solution to come, we must disappoint you.

Our cryptography scheme is military grade. It will require decades to crack.

Start working with us and get your files back.

Price?

We understand that the customer cannot always pay the fee. We have discounts and price can be negotiated.

Example files:

SALES INVOICES.7z.001 (262144Kb)
SALES INVOICES.7z.002 (262144Kb)
SALES INVOICES.7z.003 (262144Kb)
SALES INVOICES.7z.004 (262144Kb)
SALES INVOICES.7z.005 (262144Kb)
SALES INVOICES.7z.006 (262144Kb)
SALES INVOICES.7z.007 (262144Kb)
SALES INVOICES.7z.008 (262144Kb)
SALES INVOICES.7z.009 (6610Kb)
spring open house flyer.7z (1117Kb)
TSB & Factory Recalls.7z (3280Kb)
Old Signs.7z (24887Kb)
inf - VANBOXTELRV.zip (37256Kb)

Machines List

dn	cn	OperatingSystem	dNSHostName
CN=VB-ADVERT,OU=Computers,OU=Van Boxtel,DC=vanboxtelrv,DC=local	VB-ADVERT	Windows XP Professional	vb-advert.vanboxtelrv.local
CN=VBRVDC01,OU=Domain Controllers,DC=vanboxtelrv,DC=local	VBRVDC01	Windows Server 2016 Standard	VBRVDC01.vanboxtelrv.local
CN=VBRVFS01,OU=Servers,OU=Van Boxtel,DC=vanboxtelrv,DC=local	VBRVFS01	Windows Server 2016 Standard	VBRVFS01.vanboxtelrv.local
CN=VBRVHV01,OU=Servers,OU=Van Boxtel,DC=vanboxtelrv,DC=local	VBRVHV01	Windows Server 2016 Standard	VBRVHV01.vanboxtelrv.local
CN=VBRV PBX001,OU=Computers,OU=Van Boxtel,DC=vanboxtelrv,DC=local	VBRV PBX001	Windows 7 Professional	VBRV PBX001.vanboxtelrv.local

Entrust.com Leak Part1

by 34585 - Wednesday August 24, 2022 at 09:53 PM

34585

31337 H4X0R

h4x0r

GOD

Posts:	333
Threads:	60
Joined:	Mar 2022
Reputation:	801

Yesterday, 09:53 PM (This post was last modified: Yesterday, 09:53 PM by 34585.) #1

Entrust.com Leak Part1
by Lockbit

https://www.entrust.com/

https://www.bleepingcomputer.com/news/se...ware-gang/

Size: 442MB
Format: 7z/Zip

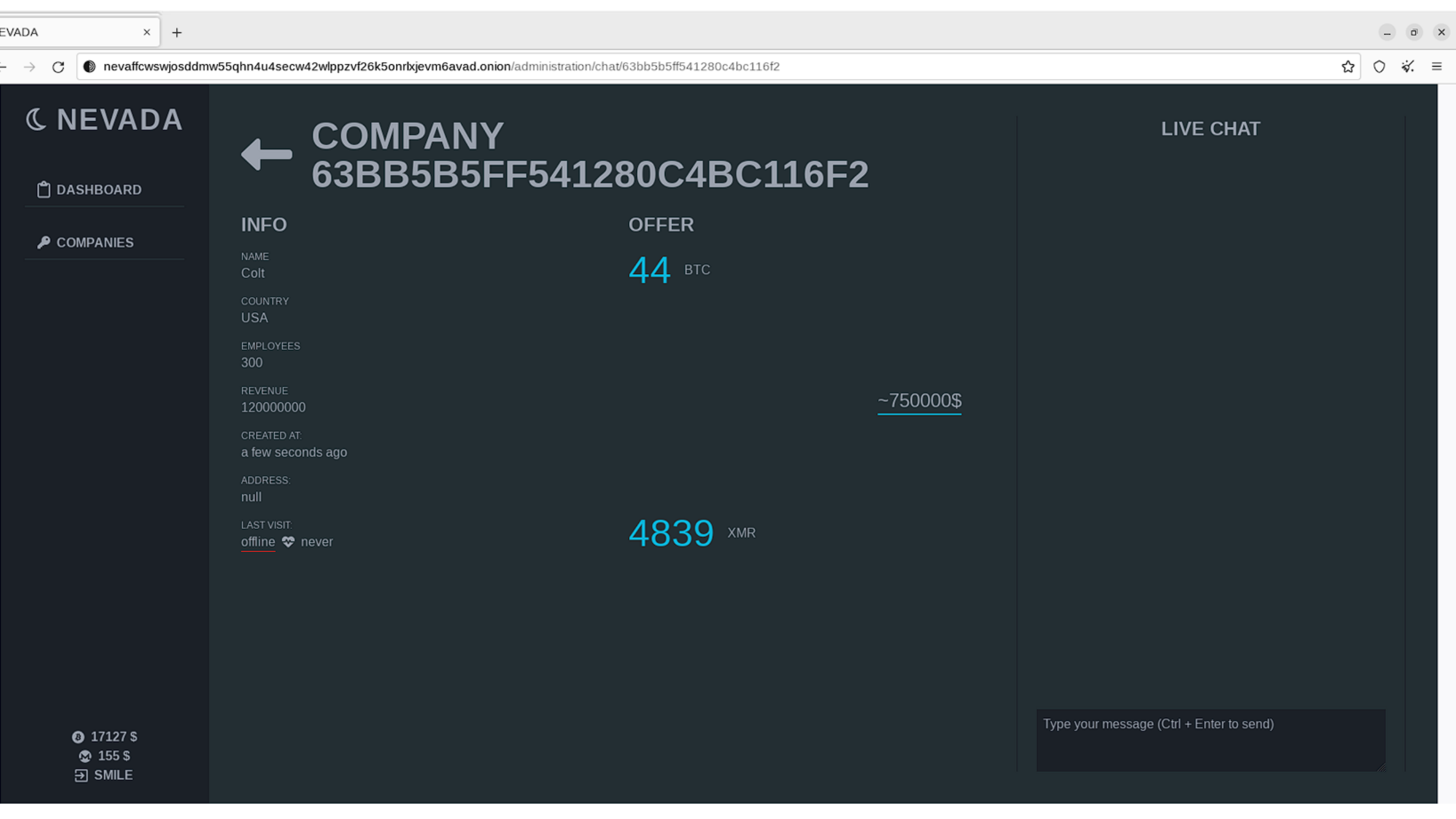
Content:

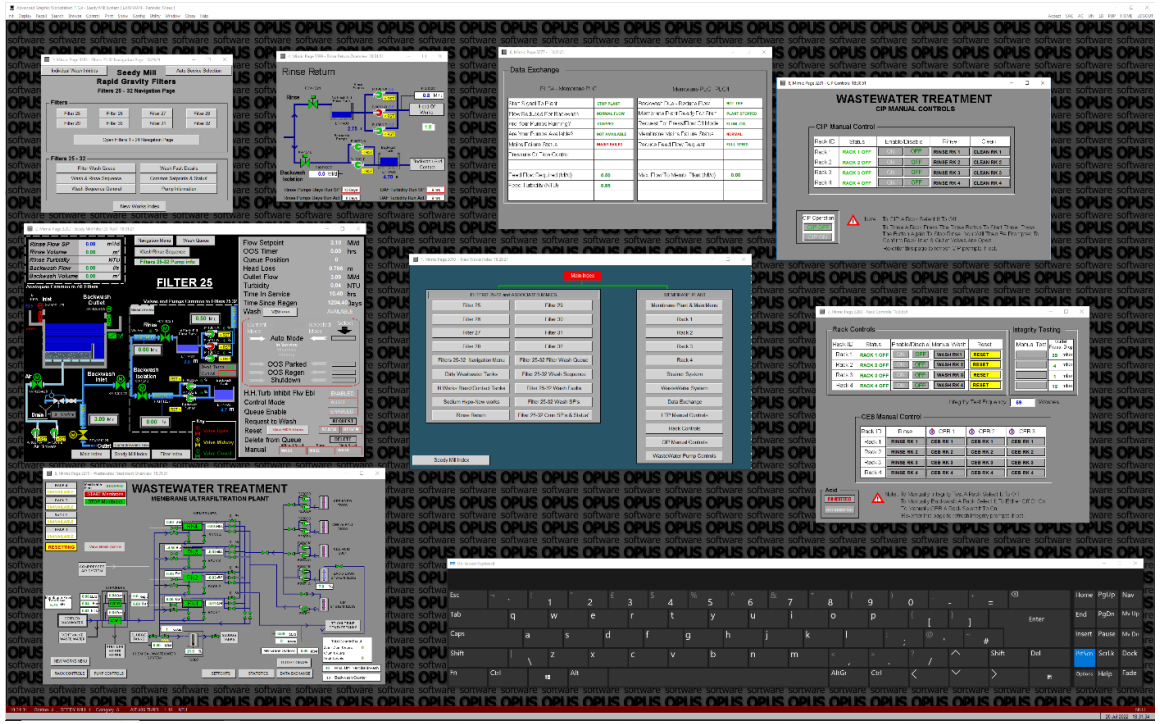
- 10AuditsFY23.zip.001
- 11FY21YrEnd.zip.001
- 13Investigations.zip.001
- 14FY22Projects.zip.001
- 15MasterCard.zip.001
- 16Visa.zip.001
- 17CAD.zip.001
- 18ArchiveProcesses.zip.001

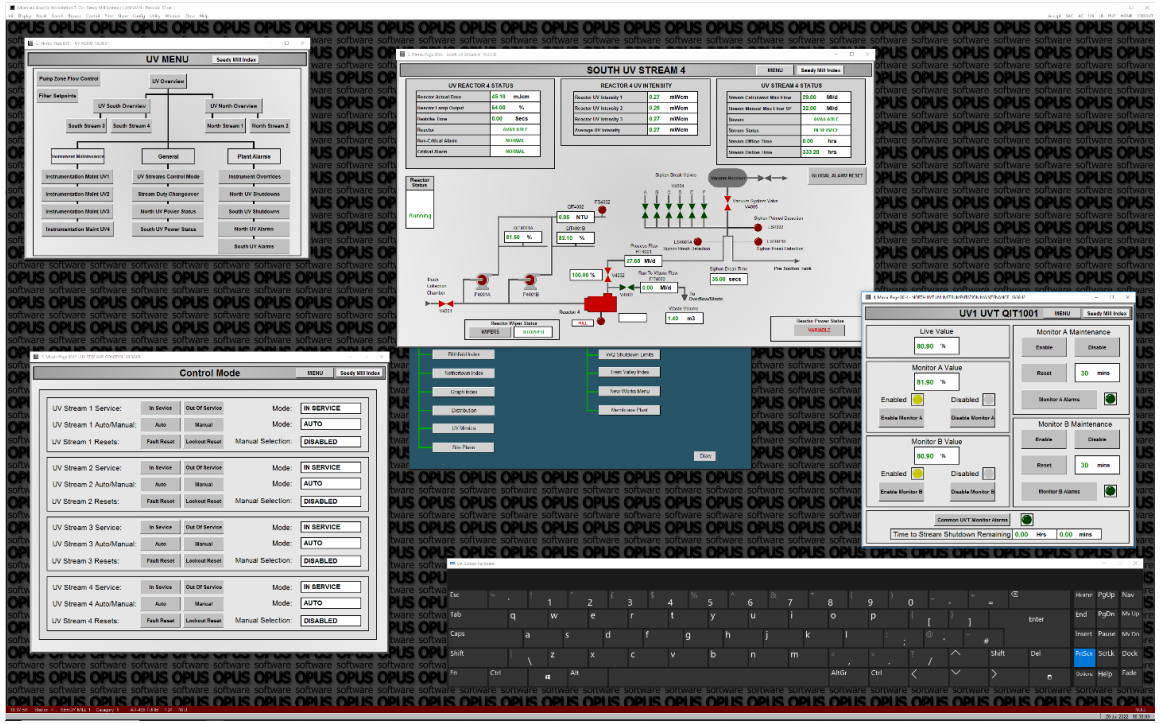
About the DDoS it was shared on this way

```
127.0.0.1 - - [20/Aug/2022:19:47:49 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
```

127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
127.0.0.1 - - [20/Aug/2022:19:47:50 +0000] "GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"


EVADA
nevaffcwswjosddmw55qhn4u4secw42wlppzvf26k5onrlxjevm6avad.onion/administration/chat/63bb5b5ff541280c4bc116f2
NEVADA
DASHBOARD
COMPANIES
17127 $
155 $
SMILE
COMPANY
63BB5B5FF541280C4BC116F2
INFO
NAME
Colt
COUNTRY
USA
EMPLOYEES
300
REVENUE
120000000
CREATED AT:
a few seconds ago
ADDRESS:
null
LAST VISIT:
offline never
OFFER
44 BTC
~750000$
4839 XMR
LIVE CHAT
Type your message (Ctrl + Enter to send)





Cl0p hacker vandforsyning og poster billeder af PLC

- Ransomware banden Cl0p hacker en vand og spildevandsselskab I England
- I stedet for at udrulle ransomware payload poster de billeder af PLC / OT

Cybercrime 2023

5.00 DDoS as a Service

DDoS as a Service

- DDoS as a Service etableres på baggrund af usikkert udstyr, OT, IoTs …
- Det er billigt at købe og der medfølger support og garantier samt API og GUI
- Flere end 300 tilbydes. De 200 er fake!
- Lad os se på en ægte en af slagsen: https://astro-stresser.com/
- AstroStresser får bl.a. sine zoombier igennem Mirai

$20 /month

1,800 Seconds

5 Concurrant Attack

Unlimited Attack Per Day

Minimum of **10 - 20 Gbps** Attack Power

Layer 3 : ✔

Layer 4 : ✔

Layer 7 : ✔

VIP Access : ✖

Sign Up

$40 /month

3,600 Seconds

8 Concurrant Attack

Unlimited Attack Per Day

Minimum of **20 - 40 Gbps** Attack Power

Layer 3 : ✔

Layer 4 : ✔

Layer 7 : ✔

VIP Access : ✖

Sign Up

$60 /month

3,600 Seconds

10 Concurrant Attack

Unlimited Attack Per Day

Minimum of **40 - 80 Gbps** Attack Power

Layer 3 : ✔

Layer 4 : ✔

Layer 7 : ✔

VIP Access : ✖

Sign Up

$120 /month

7,200 Seconds

20 Concurrant Attack

Unlimited Attack Per Day

Minimum of **40 - 80 Gbps** Attack Power

Layer 3 : ✔

Layer 4 : ✔

Layer 7 : ✔

VIP Access : ✖

Sign Up

DIAMOND

$240 /month

7,200 Seconds

30 Concurrant Attack

Unlimited Attack Per Day

Minimum of **80 - 160 Gbps** Attack Power

ELITE

HOT!

$280 /month

14,000 Seconds

40 Concurrant Attack

Unlimited Attack Per Day

Minimum of **80 - 160 Gbps** Attack Power

SUPER

$350 /month

14,800 Seconds

50 Concurrant Attack

Unlimited Attack Per Day

Minimum of **160 - 320 Gbps** Attack Power

SUPREMME

$420 /month

21,600 Seconds

60 Concurrant Attack

Unlimited Attack Per Day

Minimum of **160 - 320 Gbps** Attack Power

Cancel Translate

English

⚡ Friends, it's time to award the most active volunteers of our DDoss Project 🤖

🎖 Prize fund by the number of successful attacks:

- 80 000 rubles for 1st place
- 50 000 rubles for 2nd place
- 20 000 rubles for 3rd place

Payment in cryptocurrency at the ra on the day of payment.

From 4th to 10th places - 50,000 rubles. divided proportionally, according to the number of successful attacks.

🏆 List of our fighters and data on the number of successful attacks:

🥇 gg_script - 13,336,732 attacks
🥈 GuestHacker - 7,599,364 attacks
🥉 Jordan Breakwood - 5,323,518 attacks (no wallet)

Mysterious Team Bangladesh
#OpDenmark

Danish Infrastructure dropped...

Danish CERT - Computer Emergency Response Team.
https://cert.dk/
https://check-host.net/check-report/1028e8c9k2ab

Where Are You From under Danish e-Infrastructure Cooperation
https://wayf.dk/
https://check-host.net/check-report/1028e98ckd9e

Danish e-Infrastructure Cooperation
https://deic.dk/
https://check-host.net/check-report/1028ea48k4b7

Eduroam is a global collaboration where research and educational institutions provide each other's students and staff with access to wireless networks
https://eduroam.dk/
https://check-host.net/check-report/1028eb68ke9c

i2 provides a number of services for infrastructure and security. Intelligent Infrastructure.
https://i2.dk/
https://check-host.net/check-report/1028ed8bk1a0

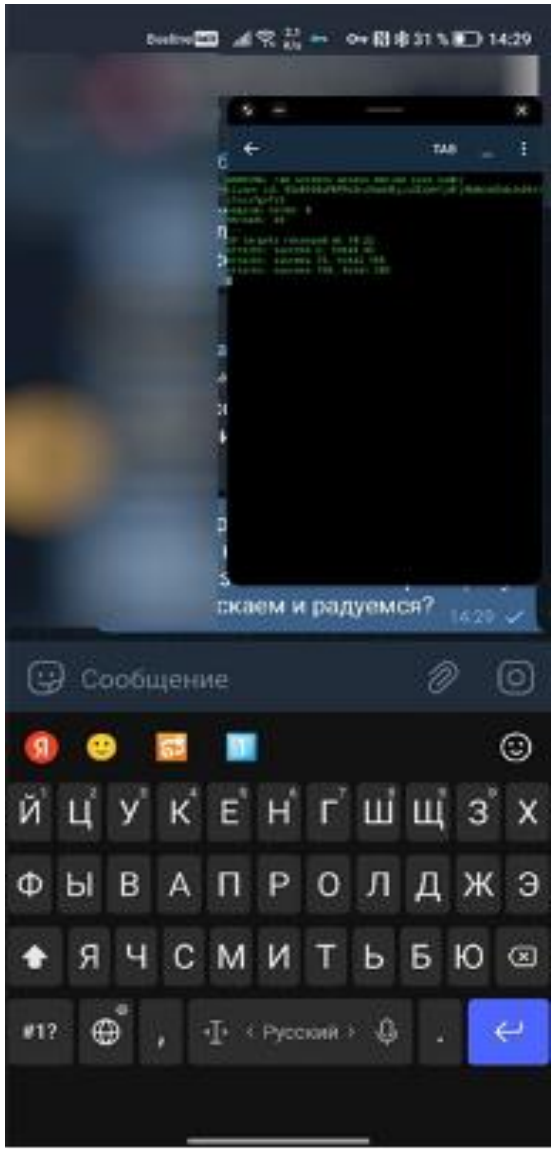
site of the Danish Jyskebank lay
n to rest after our attack:

tps://check-host.net/check-
rt/e3c0bc9kef4

Subscribe to NoName057(16)
Join our DDoS-project
Subscribe to reserve channel

Victory will be ours!

Ddossia fra PC, Linux til Android



Cybercrime 2023

6.00 Supply chain

Supply chain angreb

- Denne type angreb har eksisteret i mere end 20 år
- Med angrebet igennem Solarwinds fik supply chain øget opmærksomhed
- Herhjemme blev Mærsk ramt af supply chain og derigennem ramt af NotPetya
- NotPetya kostede Mærsk et tre cifferet million beløb og tvang til en opgradering
- Det måske mest omfangsrige supply chain angreb blev udført i August 2023 af ransomware banden Cl0p der ramte filtransfer servicen MoveIt igennem en SQL injektion svaghed
- MoveIt supply chain ramte alle de store revisionsselskaber som PwC, Delotte samt flere end 2000 organisationer globalt

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 I
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
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@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT D
AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR
FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU
NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

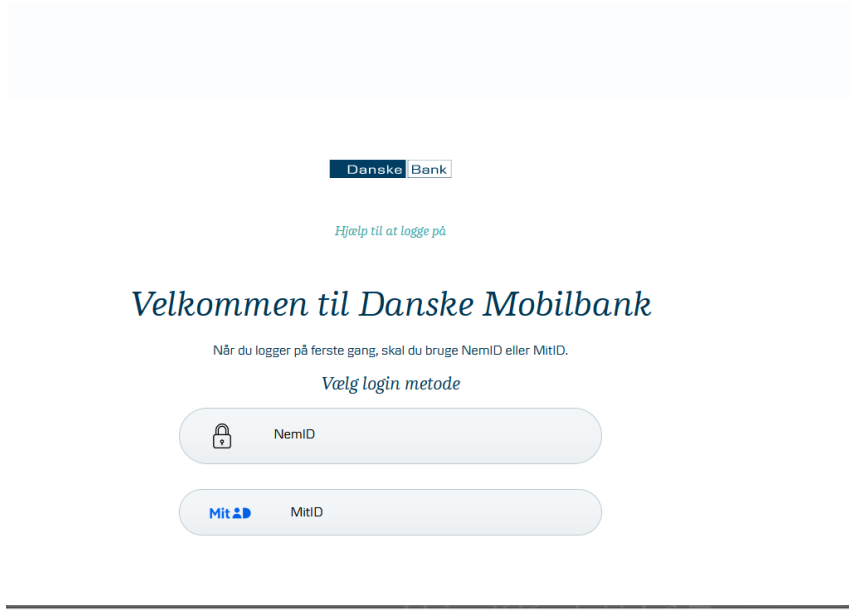
Supply chain angreb

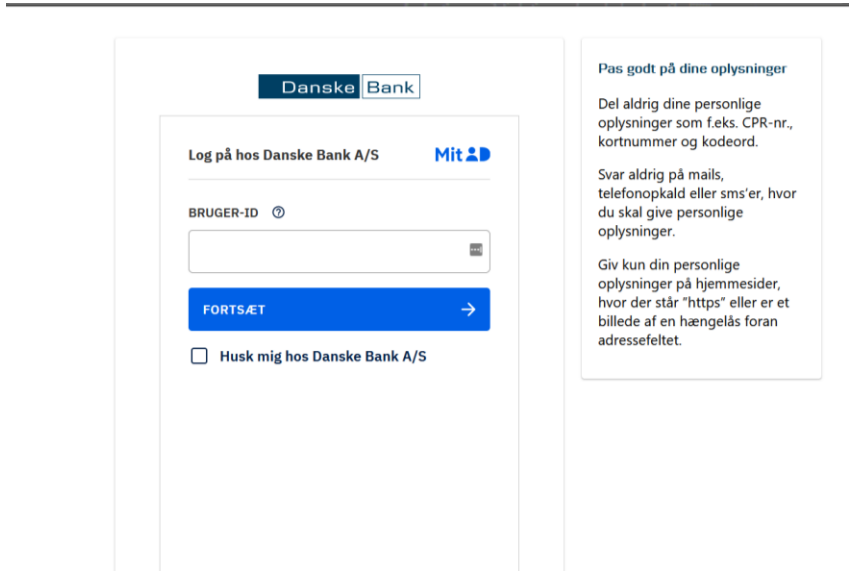
- Det måske mest omfangsrige supply chain angreb
  blev udført i August 2023 af ransomware banden Cl0p der ramte filtransfer servicen MoveIt igennem en SQL injektion svaghed
- MoveIt supply chain eksfiltrerede data fra 2122 organisationer globalt og påvirker samlet set 62,054,613 individer. Det omfatter bl.a. PwC, Deloitte og EY

Cybercrime 2023

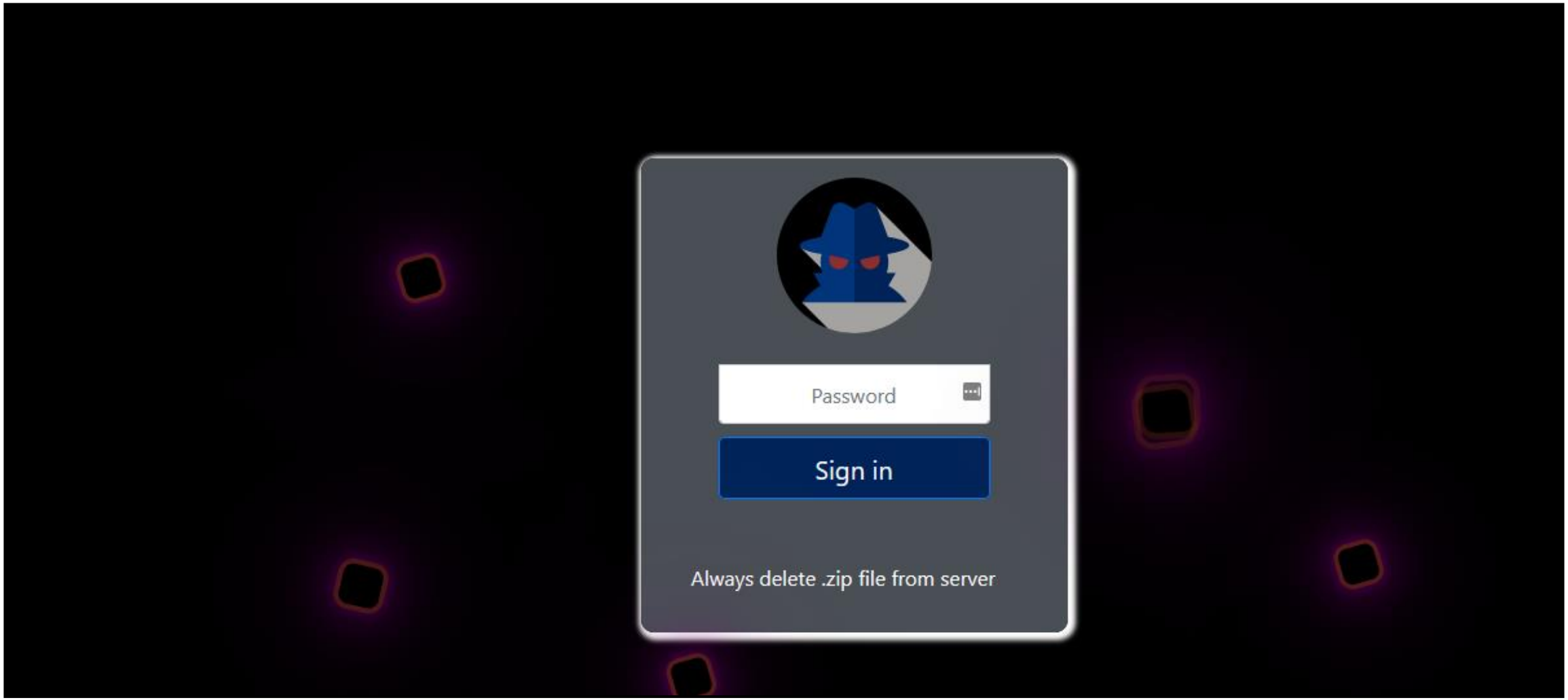
7.00 Angreb mod MitID og NemID, PhaaS, AiTM, MiTM

Det starter med en SMS!

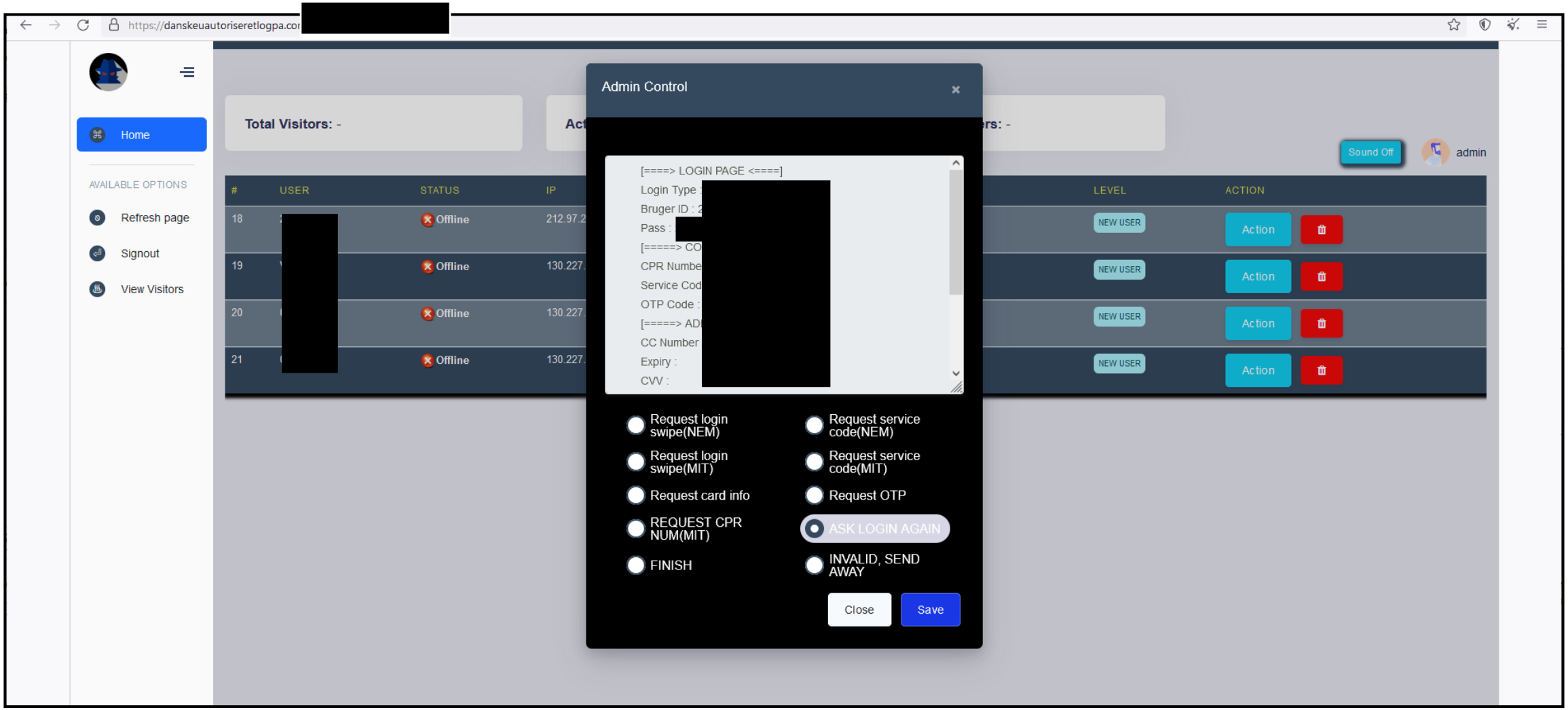

Danske Bank
Hjælp til at logge på
Velkommen til Danske Mobilbank
Når du logger på første gang, skal du bruge NemID eller MitID.
Vælg login metode
NemID
MitID


Danske Bank
Log på hos Danske Bank A/S
BRUGER-ID
FORTSÆT
Husk mig hos Danske Bank A/S
Pas godt på dine oplysninger
Del aldrig dine personlige oplysninger som f.eks. CPR-nr., kortnummer og kodeord.
Svar aldrig på mails, telefonopkald eller sms'er, hvor du skal give personlige oplysninger.
Giv kun din personlige oplysninger på hjemmesider, hvor der står "https" eller er et billede af en hængelås foran adressefeltet.


https://www.sikkerdanske-konto.net/b61705f85f6a5787b3797b783d692360/loading.php?user=true
Danske Bank
Forbinder sikkert til MitID
Vent et øjeblik ...
Pas godt
Del aldrig
oplysning
kortnumm
Svar aldri
telefonop
du skal gi
oplysning
Giv kun di
oplysning
hvor der s
billede af
adressefel



MiTM - Zeroc0d3r kit



MiTM - Zeroc0d3r kit

User Statistics

Total Visitors: -

Active Users: -

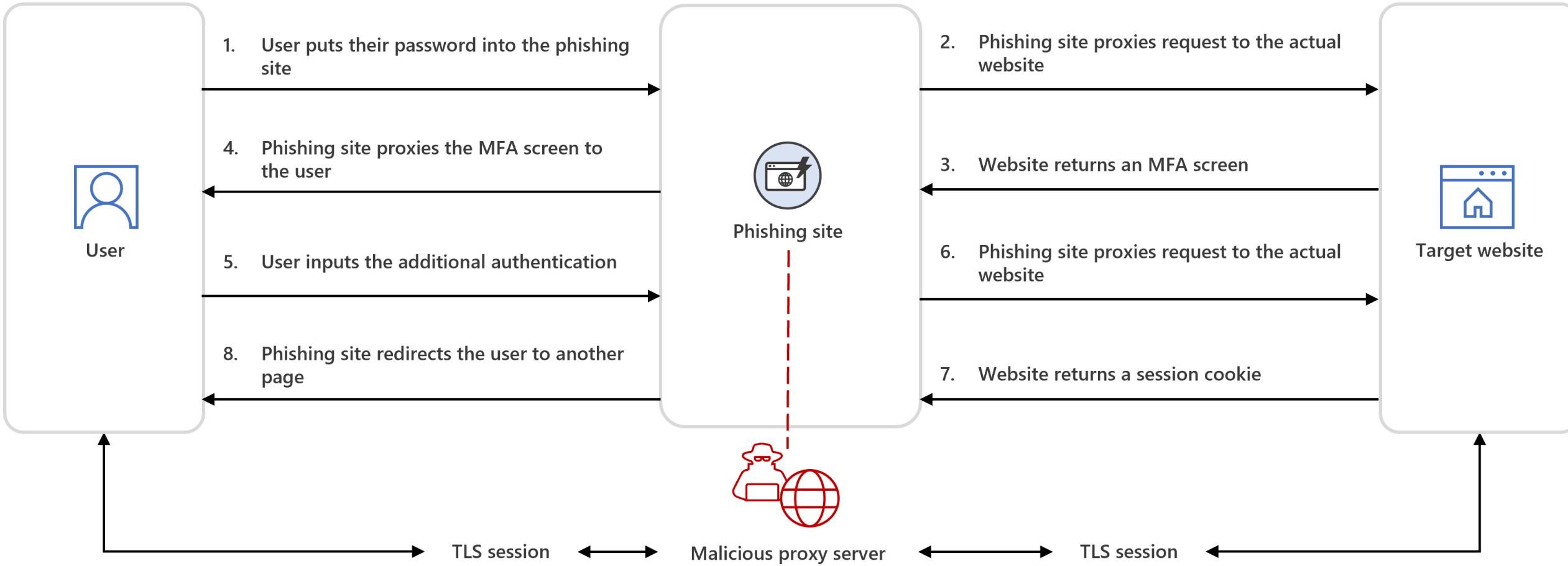
Completed Users: -

Sound Off

admin

#	USER	STATUS	IP	COMMENT	LEVEL	ACTION
2	[redacted]480	Offline	[redacted]13	Service Code entered, user waiting	AWAITING SWIPE(NEM)	Action
3	[redacted]306	Offline	[redacted]	FINISHED	View Log	
4	[redacted]745	Offline	[redacted]	User(NemID) just logged into account	AWAITING CODE(NEM)	Action
5	[redacted]950	Offline	[redacted]51	User(NemID) just logged into account	AWAITING CODE(NEM)	Action
6	[redacted]400	Offline	[redacted]0	User(NemID) just logged into account	AWAITING CODE(NEM)	Action
7	[redacted]216	Offline	[redacted]92	User(NemID) just logged into account	AWAITING CODE(NEM)	Action
8	[redacted]745	Offline	[redacted]	User(MitID) just logged into account	AWAITING CODE(MIT)	Action
9	[redacted]790	Offline	[redacted]9	FINISHED	View Log	
10	[redacted]6	Offline	[redacted]0	User(MitID) just logged into account	AWAITING CODE(MIT)	Action
11	[redacted]-296	Offline	[redacted]	Service Code entered, user waiting	AWAITING SWIPE(NEM)	Action
12	[redacted]709	Offline	[redacted]231	User(NemID) just logged into account	AWAITING CODE(NEM)	Action
13	[redacted]227	Offline	[redacted]	Service Code entered, user waiting	AWAITING SWIPE(NEM)	Action
14	[redacted]iroga23	Offline	[redacted]2	FINISHED	View Log	
15	[redacted]278	Offline	[redacted]	Service Code entered, user waiting	AWAITING CPR(MIT)	Action
16	[redacted]754	Offline	[redacted]9	User(MitID) just logged into account	AWAITING CODE(MIT)	Action
17	[redacted]443	Offline	[redacted]5	Service Code entered, user waiting	BACK TO LOGIN	Action
18	[redacted]754	Offline	[redacted]9	Service Code entered, user waiting	AWAITING SWIPE(NEM)	Action

Phishing as a Service og AiTM


User
1. User puts their password into the phishing site
2. Phishing site proxies request to the actual website
Phishing site
3. Website returns an MFA screen
4. Phishing site proxies the MFA screen to the user
Target website
5. User inputs the additional authentication
6. Phishing site proxies request to the actual website
7. Website returns a session cookie
8. Phishing site redirects the user to another page
TLS session
Malicious proxy server
TLS session

Cybercrime 2023

6.00 Opsamling og gode råd

Gode råd /opsummering

- Alle vil blive ramt: før eller siden. Sørg for at have recovery og IR på plads
- Sørg for at holde alt udstyr opdateret
- Etablerer en sikker praksis omkring fjernsupport
- Tag backup – glem ikke clouden
- Endpoint sikkerhed (AV, FW, policies), AD sikkerhed og hardning, app whitelistning (applocker), segmentering og ACL'er
- Genbrug aldrig password. Vælg et godt password og evt en corporate password manager
- Skab awareness omkring sikkerhed i virksomheden
- Del ikke oplysninger ukritisk på nettet. De kan findes og lette et angreb eller ID tyveri
- Slå 2FA (totrinsgodkendelse) til overalt det er tilgængeligt, helst MFA eller endnu bedre FIDO2 med fysisk nøgle
- Lås din maskine med en skærmlås når du ikke bruger den, krypter harddisk
- Vurder og planlæg omfanget af NIS2 direktivet
- Sikre hardware (routere/wifi, firmware, passwords osv.)

Spørgsmål

peter@kruse.industries

PGP-ID: 0x715FB4BD

Fingerprint: E1A6 7FA1 F11B 4CB5
E79F 1E14 EE9F 9ADB 715F B4BD