Erhverv Grenaa

Cybertrusler og IT- sikkerhed

Cybertrusler og IT- sikkerhed

Agenda

1.00 Cybertrusler og it-sikkerhed
2.00 Crime as a Service
3.00 Ransomware og RaaS
4.00 MiTM angreb mod MitID og NemID
5.00 Opsamling og gode råd

Truslen fra ransomware og potentielle datalæk

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

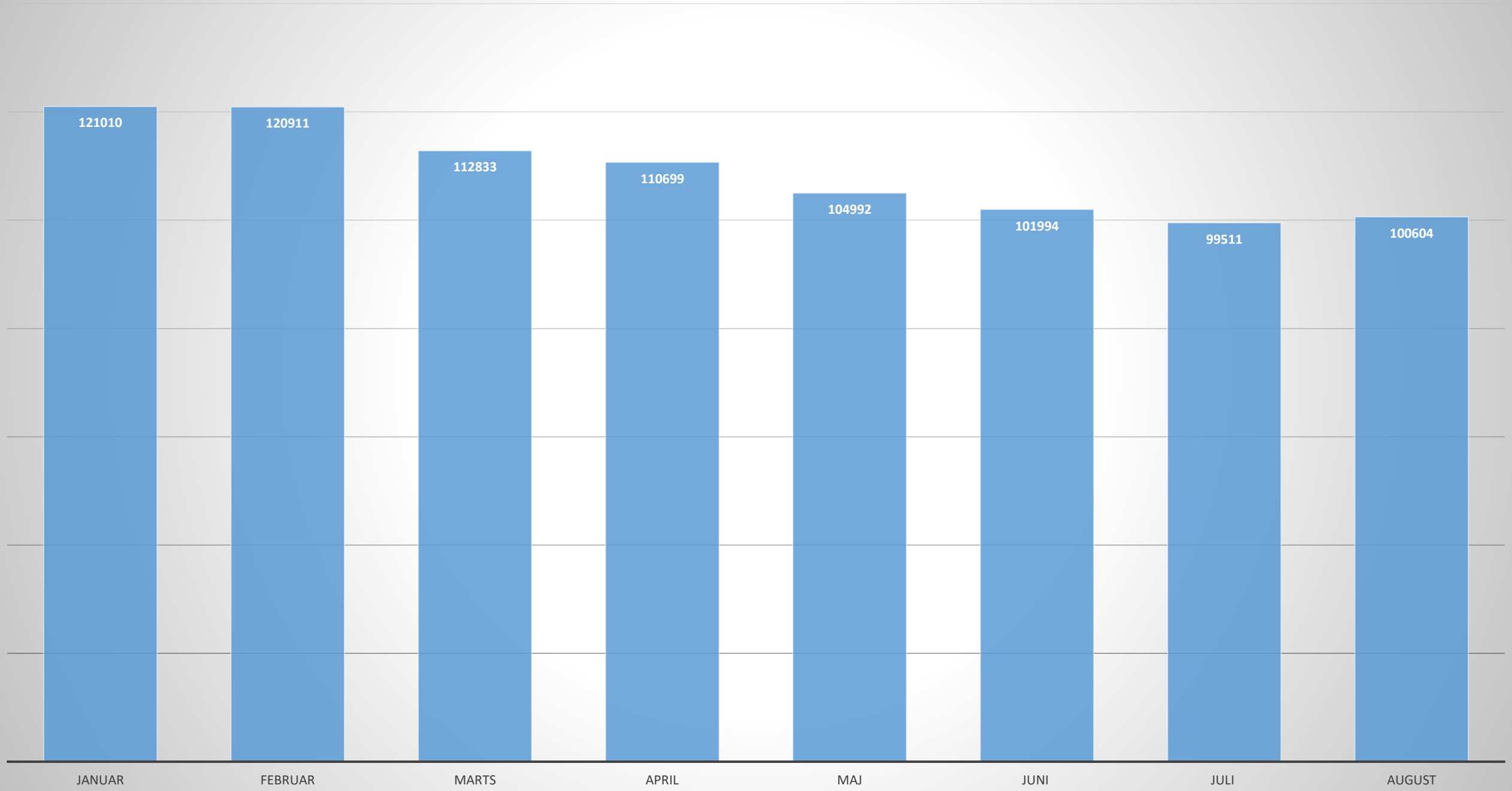
Nuværende trusler

- Phishing/smishing er tilbage for fulde omdrejninger og når usete højder i 2022
- 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
- Emotet spiller fortsat en rolle men Bumblebee, IcedID og QakBOT er i stigning og er mere raffinerede
- Cobalt Strike er fortsat de it-kriminelle's primære rammeværk til lateral bevægelse

Cyberwarfare og hybrid krig

- Angreb mod kritisk infrastruktur er blevet et våben i en ny form for hybrid krigsførsel
- Der laves angreb på supply chain og cloud/hosting udbydere
- APT angreb har fundet vejen til vores BIOS/firmware igennem UEFI
- IoT udstyr misbruges til at etablere adgange og bombe mål
- Konflikten i Ukraine er et godt eksempel på hybrid krigsførsel

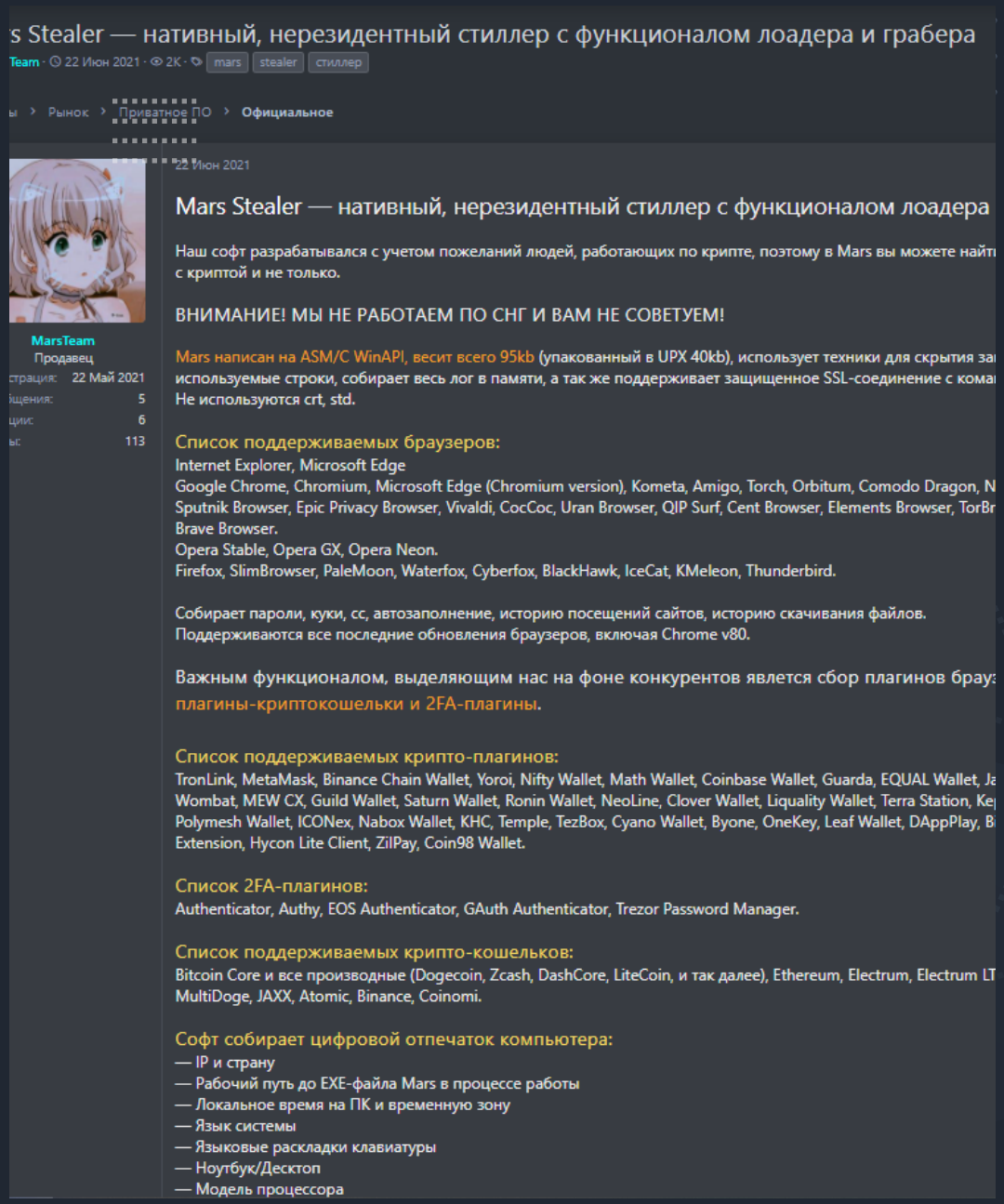
Antal af kompromitterede endpoints 2022



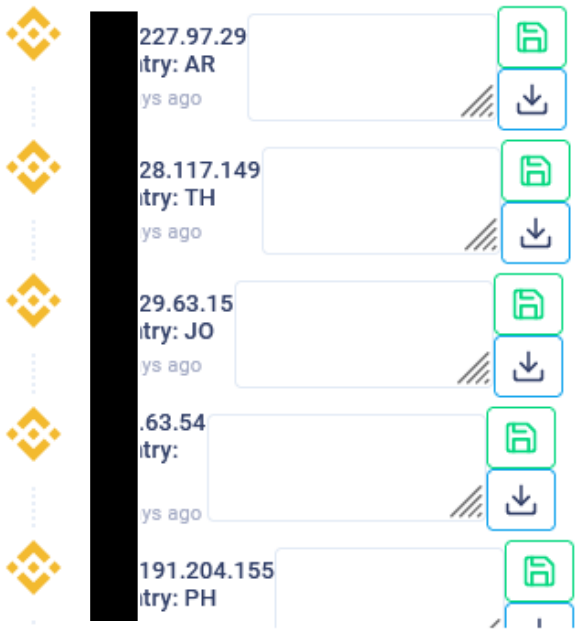
Cybertrusler og IT-sikkerhed

2.00 Crime as a Service

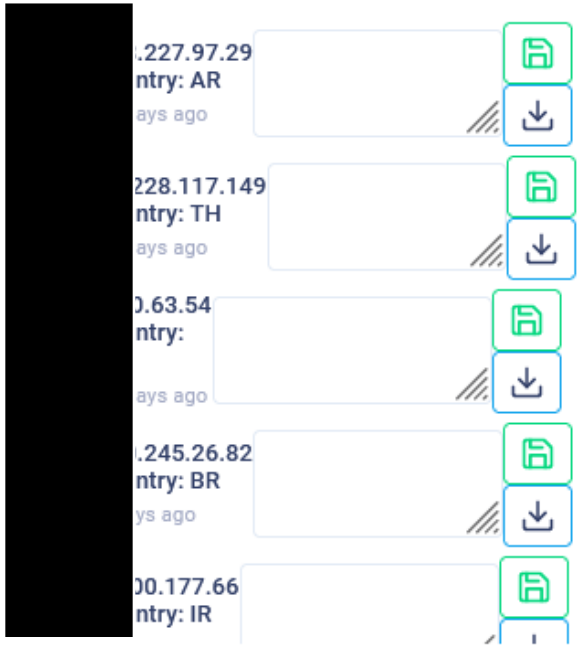
Crime as a Service – de stjæler ALT – Mars stealer



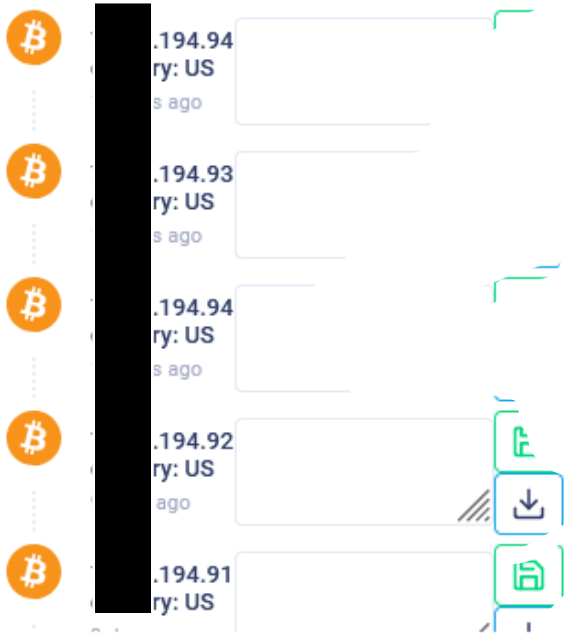
Binance



Blockchain



Crypto



Website Traffic

Site	Count
accounts.google.com	2153
www.facebook.com	1204
login.live.com	953
localhost	541
www.instagram.com	518

Browser Used

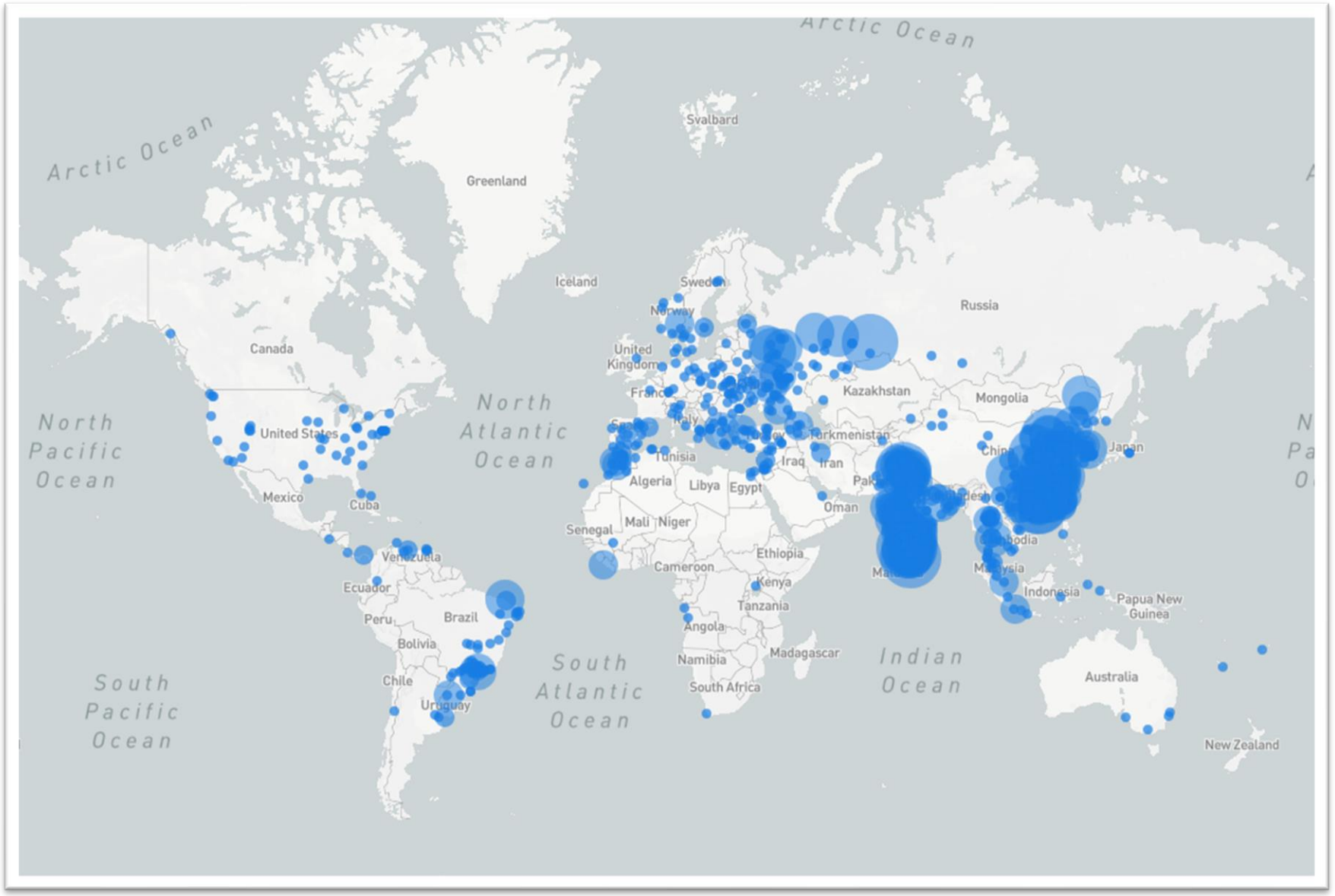
Browser	Count
Chrome	46979
Microsoft Edge	15293
Internet-Explorer	0
Opera	537
Mozilla Firefox	375

Hide empty | With crypto | With plugins | Only unique | Download | Delete | Searched | Search

1 2 3 Last

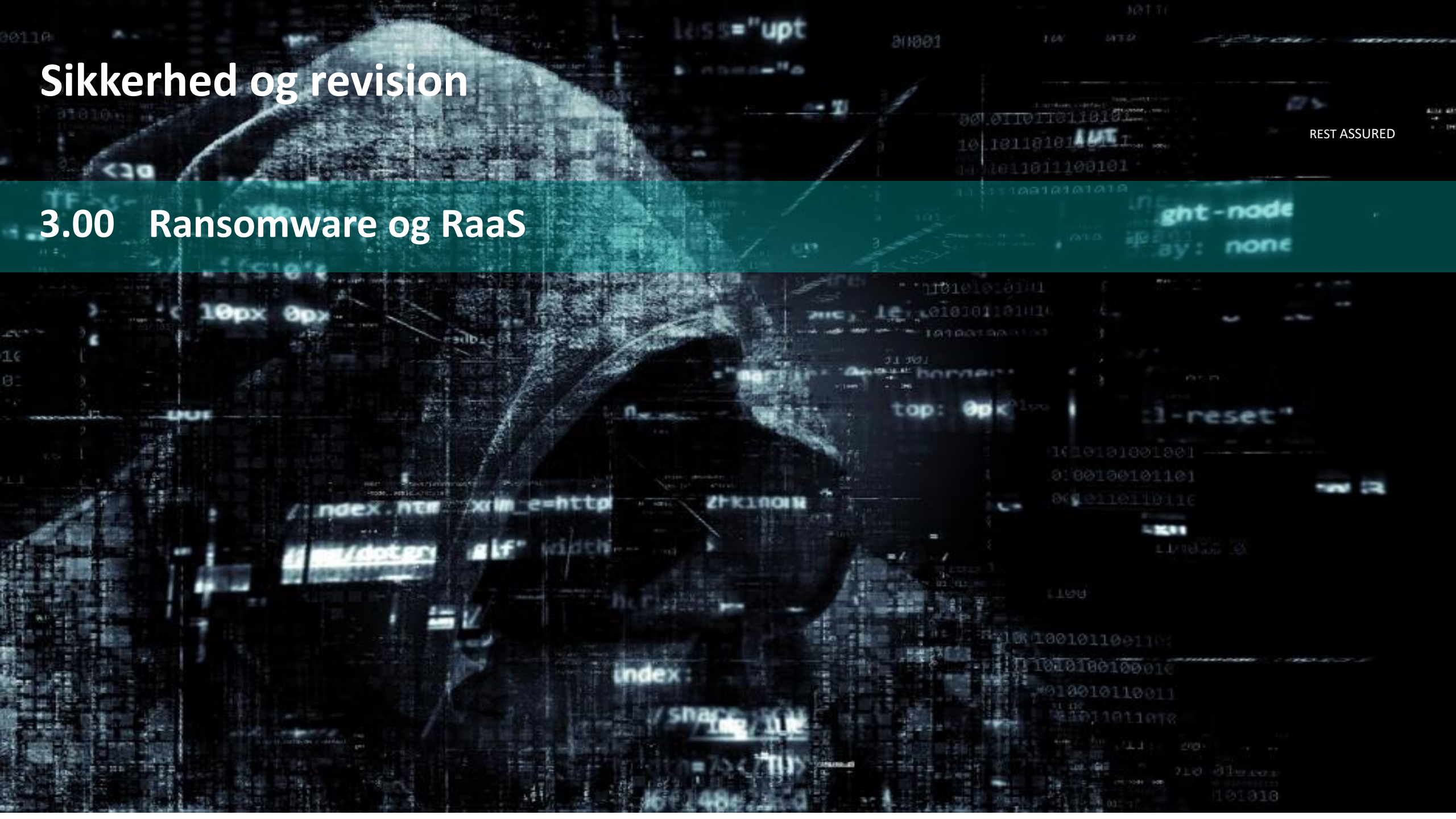
Id	Comment	Data	Marker	IP	Screenshot	Actions	Date
851		B0 0 0		[redacted]0.104.154 DE		download delete	10h 4m 4s ago 2022-02-12 13:13:04
850		B0 0 0		[redacted]6.150.218 US		download delete	11h 6m 35s ago 2022-02-12 12:10:33
849		B0 0 0		[redacted]6.150.218 US		download delete	11h 11m 19s ago 2022-02-12 12:05:49
848		B0 0 0		[redacted]20.100.252 DE		download delete	15h 3m 32s ago 2022-02-12 08:13:36
847		B0 0 0		[redacted]3.143.8 DE		download delete	15h 4m 45s ago 2022-02-12 08:12:23
846		B0 0 0		[redacted]39.165.23 GB		download delete	15h 15m 54s ago 2022-02-12 08:01:14
845		B0 0 4		[redacted]4.41.83 IT		download delete	16h 3m 43s ago 2022-02-12 07:13:25

Crime as a Service – de stjæler ALT – IoT



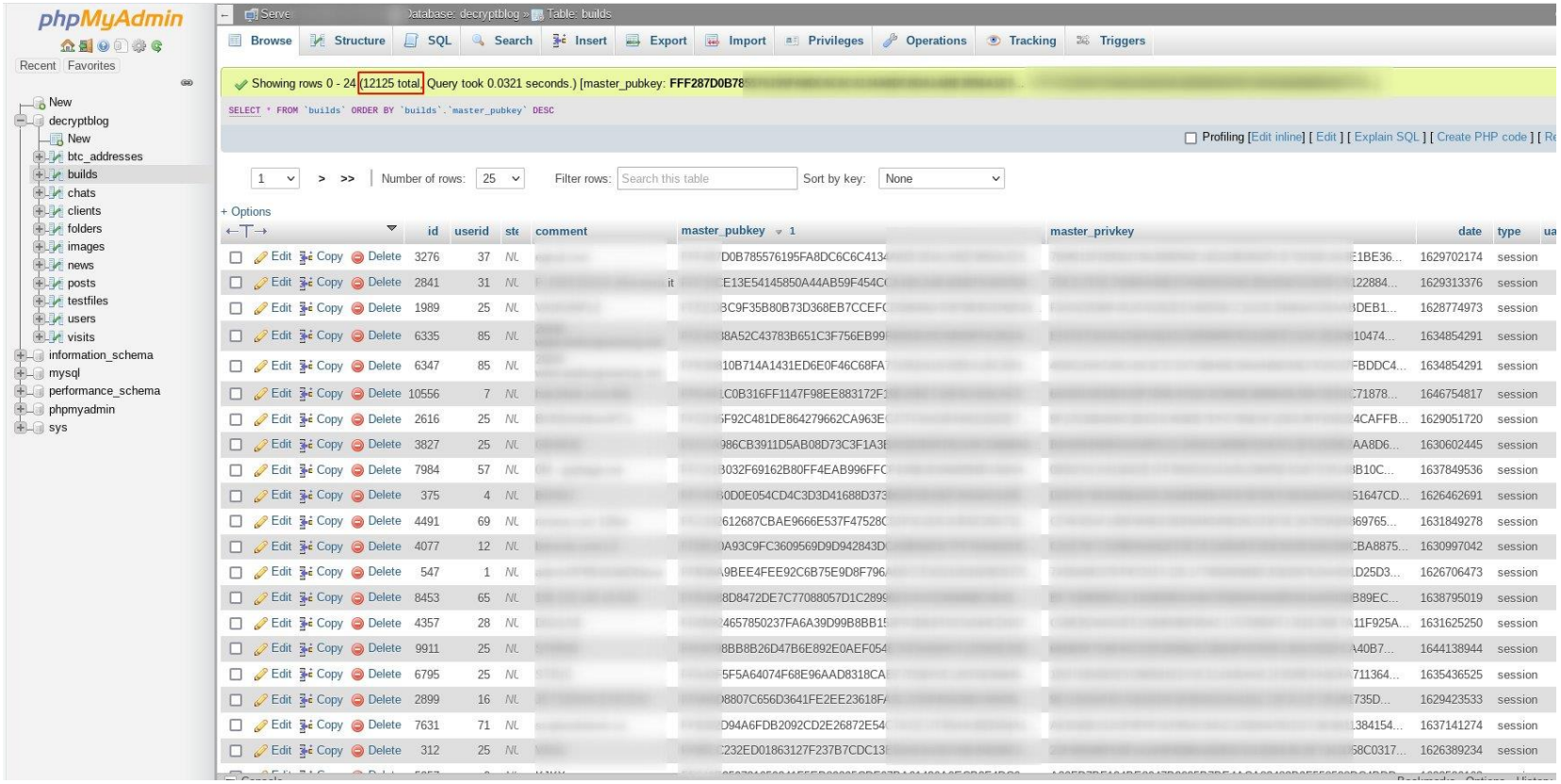
Sikkerhed og revision

3.00 Ransomware og RaaS



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

Weatherford College

OFFLINE 18d 14h 40m

encryp

Weathe
nity col
rd, Texa
in near
and Mir

Websit
wc.edu

Tax Nu
(817) 59

Revenu
$180M

Employ
360

i locked
window
blockin

Update

Read only

16 April

Hello and welcome to Hive.
How may I help you?

Strategy & tactics

April 16

i locked only 1 esxi and some
windows, because edr has

No offer

wh

Type your message

Index of /stratford/

../	
2021 R2T4/	19-Apr-2022 21:23
Accounting Confidential/	19-Apr-2022 21:24
Accounting Requests/	19-Apr-2022 21:45
Budgets/	19-Apr-2022 21:25
Finance/	19-Apr-2022 21:23
PersonINFO/	19-Apr-2022 21:23
PersonINFO2/	19-Apr-2022 21:23
Shurtz Personal/	19-Apr-2022 21:53
ssn/	19-Apr-2022 21:23

Clients Tasks Settings Log Out

ES	
CLIENTS	↓
25	
4	
3	
3	
1	
1	
1	

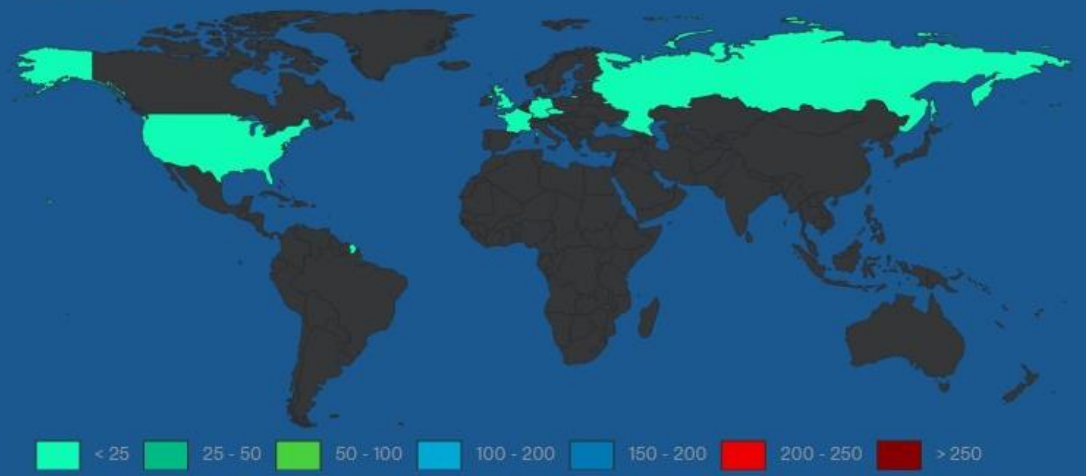
TOP OPERATING SYSTEMS

OS	CLIENTS ↓
Windows 10	30
Windows 7	3
Windows 8.1	2
Windows Server 2016	2
Windows Server 2008	1
Windows 8	0
Windows XP	0
Windows Server 2012	0

TOP ANTIVIRUSES

ANTIVIRUS	CLIENTS ↓
Windows Defender	14
N/A	6
Trend Micro Security Agent	5
Securepoint Antivirus Pro	4
Managed Antivirus-Anti-Malware	1
TeamViewer Endpoint Protection (ITbrain Anti-Malware)	1
Avast Antivirus	1
V3 Lite	1
Avira Antivirus	1
Sophos Home	1
Webroot SecureAnywhere	1
F-Secure SAFE	1
Dr.Web Security Space	1

WORLD MAP



ONLINE	ONLINE TODAY	ONLINE / WEEK	ONLINE / MONTH
32	32	33	38

DEAD	NEW TODAY	NEW / WEEK	NEW / MONTH
6	0	11	38

OS

ANTIVIRUSES

USER RIGHTS

VERSIONS

CLIENT LIST

Show 50 entries

Search:

ID	IP	COUNTRY	OPERATING SYSTEM	ROLE	ANTIVIRUS	RAM	STORAGE	NETWORK	ADDED	STATUS	VERSION
805	87.[redacted]06.63		Microsoft Windows 10 Home	User	Windows Defender	3964 MB	189 / 252 GB	112	20.11.2020, 13:33:50	Online	BR_JOB
819	217.[redacted]7.18		Microsoft Windows 8.1 Pro	N/A	Trend Micro Security Agent	8081 MB	450 / 1241 GB	84	27.11.2020, 11:36:24	Online	LW_JOB
804	62.[redacted]98.173		Microsoft Windows Server 2008 R2 Standard	User	N/A	8183 MB	103 / 274 GB	10	18.11.2020, 00:05:09	Online	BR_JOB
787	90.[redacted]114.74		Microsoft Windows Server 2016 Standard	User	N/A	40959 MB	507 / 948 GB	9	16.11.2020, 13:49:22	Online	LW_JOB
776	87.[redacted]89.211		Microsoft Windows 8.1 Pro	N/A	Windows Defender	8059 MB	2581 / 4655 GB	3	16.11.2020, 12:28:14	Online	LW_JOB
777	84.[redacted]51.87		Microsoft Windows 7 Professional	N/A	N/A	8081 MB	902 / 1789 GB	2	16.11.2020, 12:32:28	Online	LW_JOB
782	91.[redacted]0.148		Microsoft Windows 10 Pro	User	Managed Antivirus-Anti-Malware	16312 MB	875 / 1365 GB	0	16.11.2020, 13:02:20	Online	LW_JOB
775	82.[redacted]33.41		Microsoft Windows 10 Pro	User	TeamViewer Endpoint Protection (ITbrain Anti-Malware)	8191 MB	1410 / 1928 GB	0	16.11.2020, 12:26:20	Online	LW_JOB
778	188.[redacted]81.252		Microsoft Windows 10 Pro	User	Avast Antivirus	8030 MB	2261 / 2797 GB	0	16.11.2020, 12:32:52	Online	LW_JOB
781	80.[redacted]89.99		Microsoft Windows 10 Pro	User	Securepoint Antivirus Pro	8114 MB	896 / 2470 GB	0	16.11.2020, 12:49:04	Online	LW_JOB
783	84.[redacted]211.209		Microsoft Windows 10 Pro	User	Windows Defender	8077 MB	970 / 1117 GB	0	16.11.2020, 13:02:56	Online	LW_JOB
784	79.[redacted]248.13		Microsoft Windows 10 Pro	User	Windows Defender	8063 MB	1886 / 3223 GB	0	16.11.2020, 13:03:36	Online	LW_JOB
791	212.[redacted].49.177		Microsoft Windows 10 Pro	User	Trend Micro Security Agent	16255 MB	888 / 1630 GB	0	16.11.2020, 14:13:43	Online	LW_JOB
793	87.[redacted]55.59		Microsoft Windows 10 Pro	User	Windows Defender	3766 MB	14742 / 19789 GB	0	16.11.2020, 14:58:27	Online	BR_JOB
794	87.[redacted]57.232		Microsoft Windows 10 Home	User	Windows Defender	8006 MB	366 / 701 GB	0	16.11.2020, 15:18:53	Online	BR_JOB

Hvad er Conti?

- Conti kom på “scenen” i 2019 som “Ransomware as a Service”
- Conti er en one-stop-shop for cyberkriminelle og tilbyder en bred vifte af forskellige services f.eks. platform til management og distribution af høstet data
- Nøglepersonerne kan knyttes til Dyreza og TrickBOT og kendes som ”Wizard Spider”
- Wizard Spider er en sofistikeret kriminel organisation som operer fra Rusland (St Petersburg) og Ukraine. Organisationen har eksisteret siden 2008.
- Wizard Spider organisationen består af flere end 70 ansatte og rammer udelukkende mål udenfor det tidligere Sovjet
- Conti er et ”double sword”. Der leveres ransomware builders, bruger manualer, SLA, og høstes data som bruges til at true ofre.

Hvad er Conti?

- Det største mål indtil videre var Health Service Executive i Irland
- Conti er optimeret til multi-threading encryption som gør Conti hurtigere end konkurrenterne. Den anvender høj grad af beskyttelse af dens kode hvor den f.eks. Anvender 277 forskellige algoritmer – en per streng. Af dem er 230 subrutiner. Conti anvender endvidere en udviklket AES-256 og ChaCha implementering med 32 individuelle CPU trade og en master RSA-4096 nøgle.
- Når Conti køres dræber den først processer relateret til backup (og meget andet!):

net stop “Acronis VSS Provider” /y
net stop “Enterprise Client Service” /y
net stop “SQLsafe Backup Service” /y
net stop “SQLsafe Filter Service” /y
net stop “Veeam Backup Catalog Data Service” /y ("start C:\locker.exe -m -net -size 10 -nomutex -p \\VEEAM.dc.local”)
net stop AcronisAgent /y

Acronis VSS Provider
Enterprise Client Service
SQLsafe Backup Service
SQLsafe Filter Service
Veeam Backup Catalog Data Service
AcronisAgent
AcrSch2Svc
Antivirus
ARSM
BackupExecAgentAccelerator
BackupExecAgentBrowser
BackupExecDeviceMediaService
BackupExecJobEngine
BackupExecManagementService
BackupExecRPCService
BackupExecVSSProvider
bedbg
DCAgent
EPSecurityService
EPUpdateService
EraserSvc11710
EsgShKernel
FA_Scheduler
IISAdmin
IMAP4Svc
McShield
McTaskManager
mfemms
mfevtp
MMS
mozyprobackup
MsDtsServer
MsDtsServer100
MsDtsServer110
MSExchangeES
MSExchangeIS
MSExchangeMGMT
MSExchangeMTA
MSExchangeSA
MSExchangeSRS
MSOLAP$SQL_2008
MSOLAP$SYSTEM_BGC
MSOLAP$TPS
MSOLAP$TPSAMA
MSSQL$BKUPEXEC
MSSQL$SBSMONITORING
MSSQL$SHAREPOINT
MSSQL$SQL_2008
MSSQL$SYSTEM_BGC

MSSQL$TPS
MSSQL$TPSAMA
MSSQL$VEEAMSQL2008R2
MSSQL$VEEAMSQL2012
MSSQLFDLauncher
MSSQLFDLauncher$PROFXENGAGEMENT
MSSQLFDLauncher$SBSMONITORING
MSSQLFDLauncher$SHAREPOINT
MSSQLFDLauncher$SQL_2008
MSSQLFDLauncher$SYSTEM_BGC
MSSQLFDLauncher$TPS
MSSQLFDLauncher$TPSAMA
MSSQLSERVER
MSSQLServerADHelper100
MSSQLServerOLAPService
MySQL57
ntrtscan
OracleClientCache80
PDVFSService
POP3Svc
ReportServer
ReportServer$SQL_2008
ReportServer$SYSTEM_BGC
ReportServer$TPS
ReportServer$TPSAMA
RESvc
sacsvr
SamSs
SAVAdminService
SAVService
SDRSVC
SepMasterService
ShMonitor
Smcinst
SmcService
SMTPSvc
SQLAgent$BKUPEXEC
SQLAgent$ECWDB2
SQLAgent$PRACTTICEBGC
SQLAgent$PRACTTICEMGT
SQLAgent$PROFXENGAGEMENT
SQLAgent$SBSMONITORING
SQLAgent$SHAREPOINT
SQLAgent$SQL_2008
SQLAgent$SYSTEM_BGC
MSSQL$PRACTICEMGT

SQLAgent$TPS
SQLAgent$TPSAMA
SQLAgent$VEEAMSQL2008R2
SQLAgent$VEEAMSQL2012
SQLBrowser
SQLSafeOLRService
SQLSERVERAGENT
SQLTELEMETRY
SQLTELEMETRY$ECWDB2
SQLWriter
VeeamBackupSvc
VeeamBrokerSvc
VeeamCatalogSvc
VeeamCloudSvc
VeeamDeploymentService
VeeamDeploySvc
VeeamEnterpriseManagerSvc
VeeamMountSvc
VeeamNFSSvc
VeeamRESTSvc
VeeamTransportSvc
W3Svc
wbengine
WRSVC
MSSQL$VEEAMSQL2008R2
SQLAgent$VEEAMSQL2008R2
VeeamHvIntegrationSvc
swi_update
SQLAgent$CXDB
SQLAgent$CITRIX_METAFRAME
SQL Backups
MSSQL$PROD
Zoolz 2 Service
MSSQLServerADHelper
SQLAgent$PROD
msftesql$PROD
NetMsmqActivator
EhttpSrv
ekrn
ESHASRV
MSSQL$SOPHOS
SQLAgent$SOPHOS
AVP
klnagent
MSSQL$SQLEXPRESS
SQLAgent$SQLEXPRESS
wbengine
mfefire
MSSQL$PROFXENGAGEMENT
MSSQL$ECWDB2
MSSQL$PRACTTICEBGC

Conti bruger manualer

Passwords anvendt i RDP og andre perimeter services:

Password1, Hello123, password, Welcome1, banco@1, training, Password123, job12345, spring, food1234, June2020, July2020, August20, August2020, Summer20, Summer2020, June2020!, July2020!, August20!, August2020!, Summer20!, Summer2020!

Lækket data

Inden Conti ransomware aktiveres fremhæver manualer følgende tiltag:

- Dumping password hashes
- Deaktivere Windows Defender
- Metasploit
- Scanning af netværk/cloud for backup devices/redundans
- Aktivering af “legitime” bagdøre I form af Remote Support værktøjer
- Elevatering af privilegier

Conti annoncerer deres død …

- Men frem træder: Silent Ransom, Quantum, og Roy/Zeon
- Anvender BazarCall til kompromittering af enterprise kunder
- Bazarcall gør brug af spear phishing og et nummer til et dedikeret callcenter som henviser til en webside hvorfra der tilbydes et Excel dokument. Hvis makrokode tillades så droppes BazarLoader og Bazar Backdoor
- Der fokuseres på en bred vifte af brancher bl.a. Finans, teknologi, kommuner, skoler, uddannelsesinstitutioner, advokat og revision samt forsikring og pensionsselskaber

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:

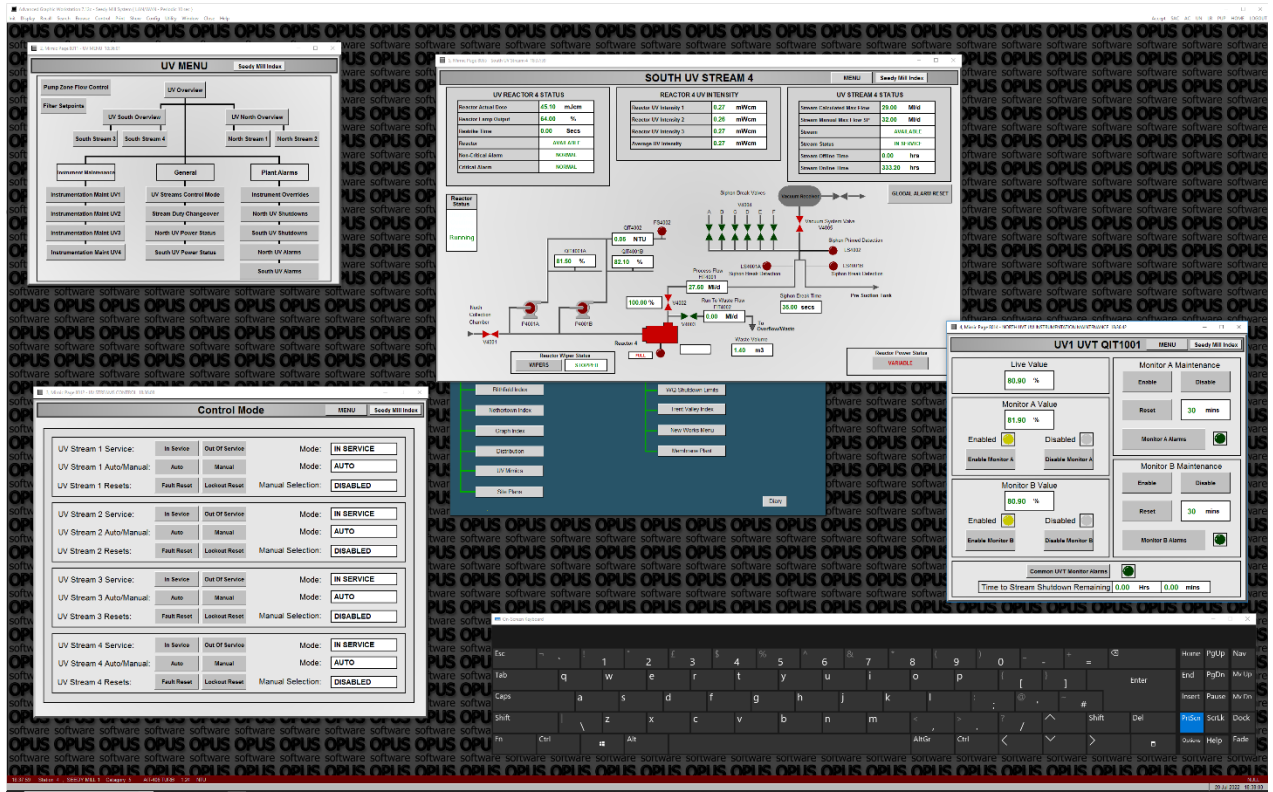
- 10AuditsFY23.zip.001
- 11FY21YrEnd.zip.001
- 13Investigations.zip.001
- 14FY22Projects.zip.001
- 15MasterCard.zip.001
- 16Visa.zip.001
- 17CAD.zip.001
- 18ArchiveProcesses.zip.001

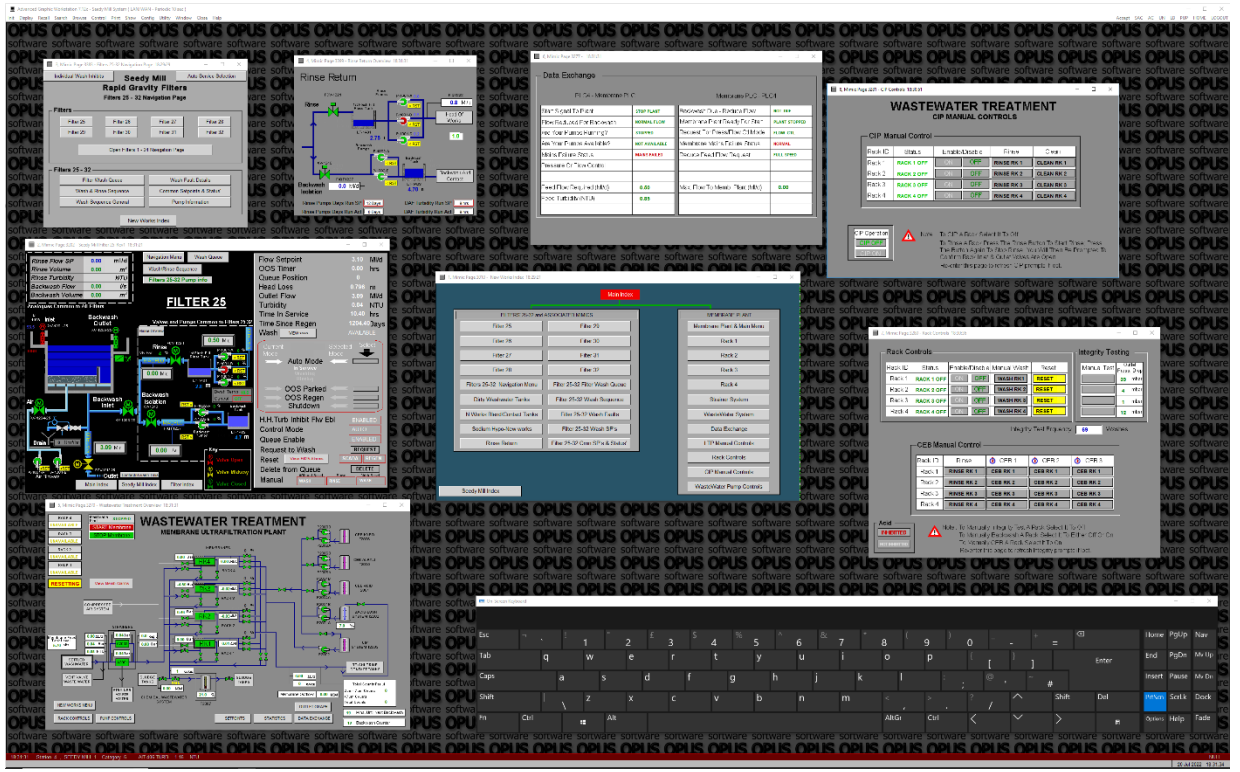
About the DDoS it was shared on this way

```
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"
```

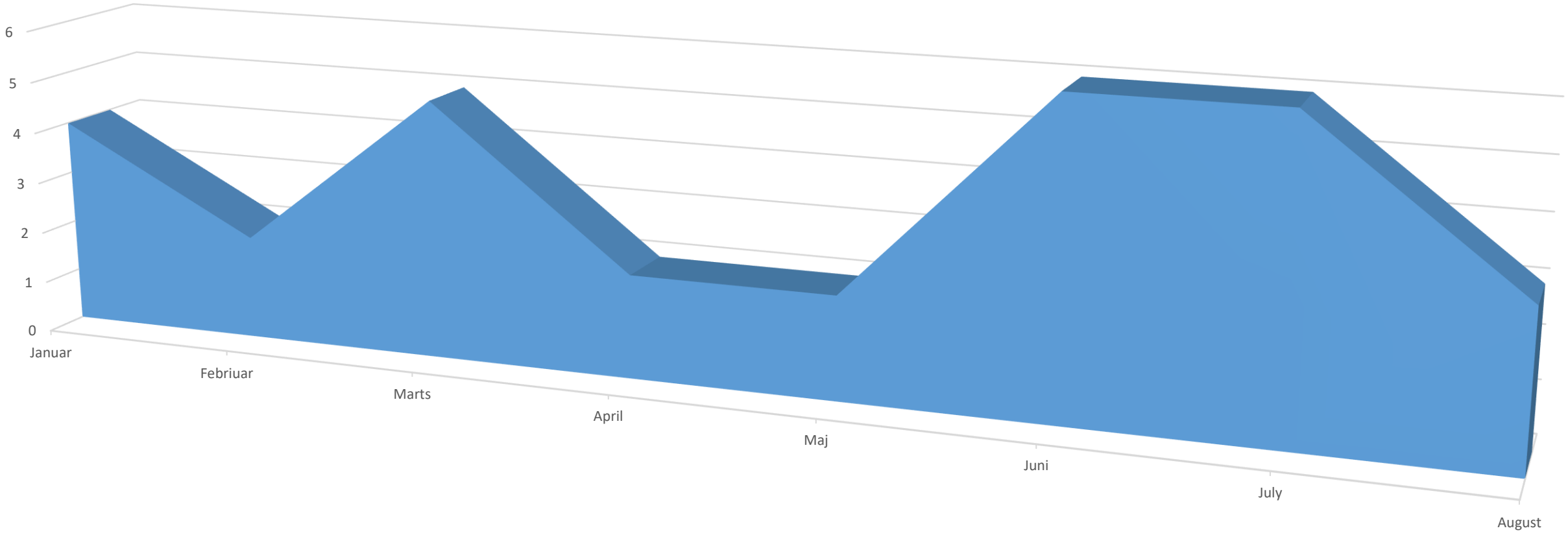
Cl0p hacker vandforsyning og poster billeder af PLC

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



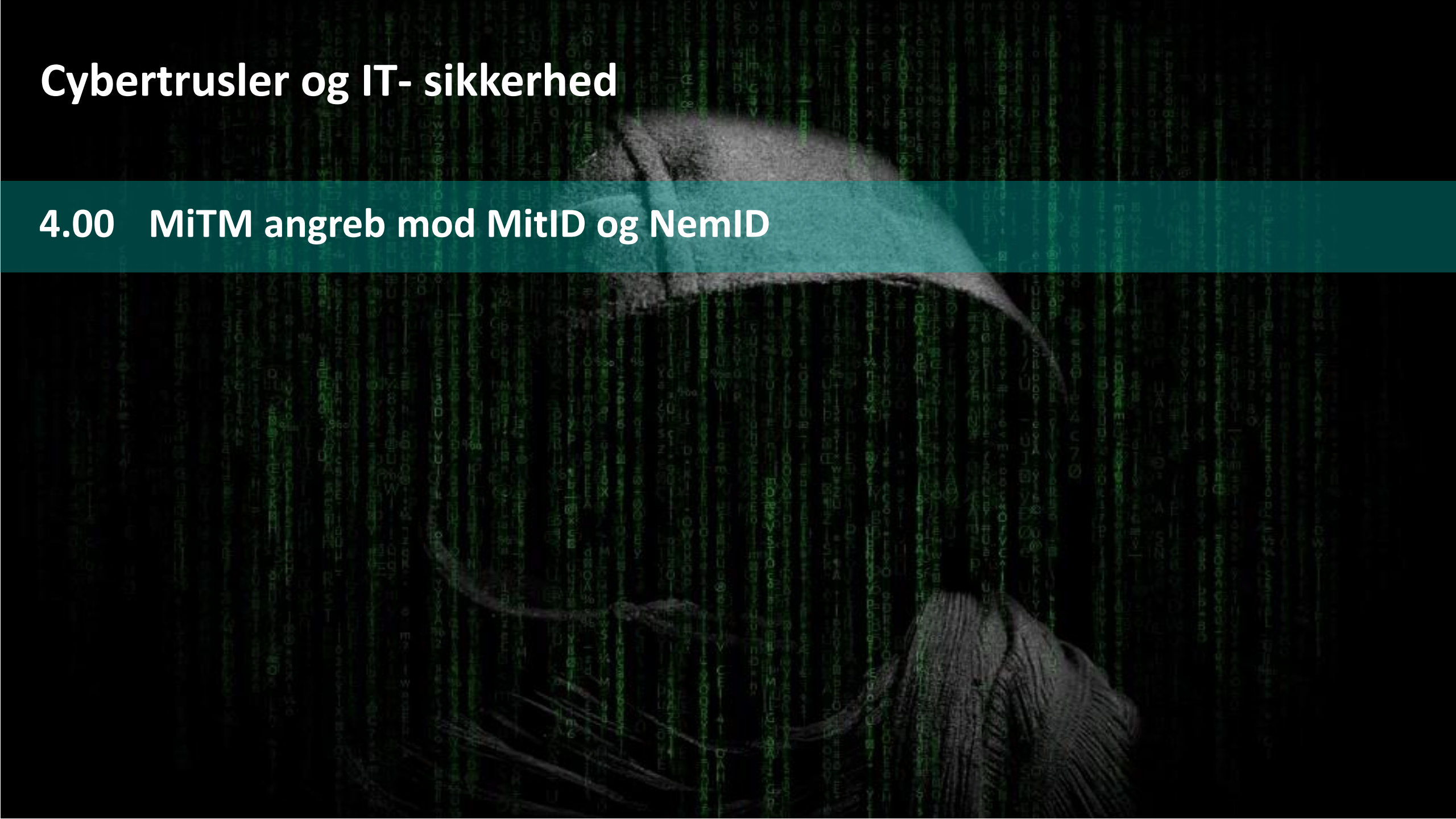


CSIS IR sager relateret til ransomware i 2022

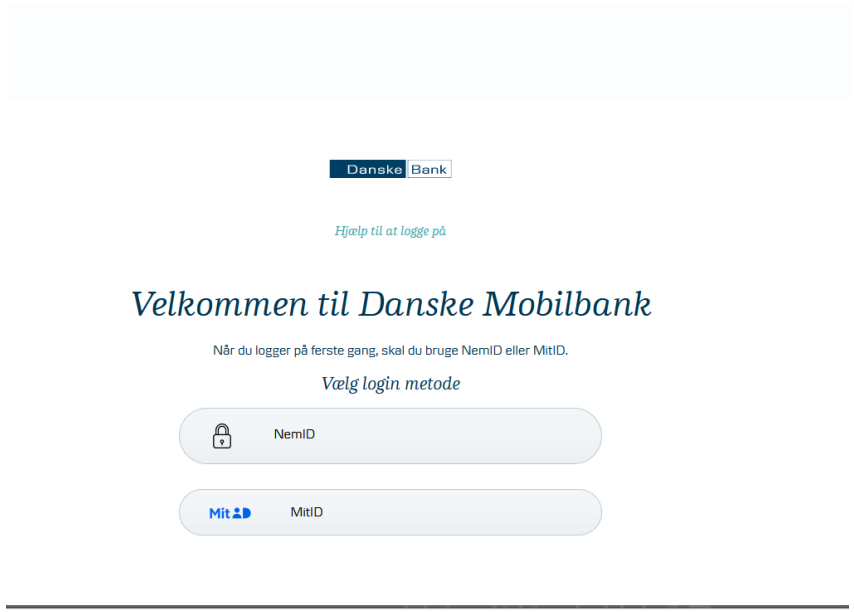


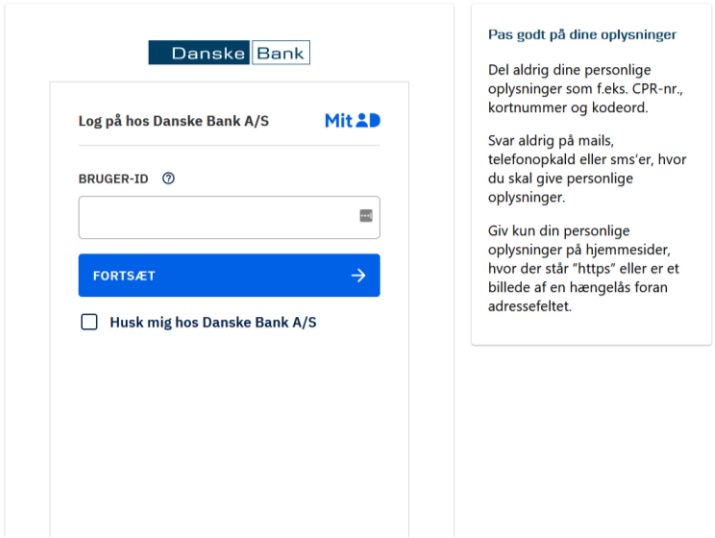
Cybertrusler og IT- sikkerhed

4.00 MiTM angreb mod MitID og NemID



Det starter med en SMS!


Danske Bank
Hjælp til at logge på
Velkommen til Danske Mobilbank
Når du logger på ferste 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

Smishing domæner

- I løbet af en måned har vi set flere end 100 domæner oprettet med formålet at lave smishing mod danske borgere og viksomheder. Der misbruges primært varemærker fra Danske Bank og eBoks. De 6 er på TLD .dk
- Hovedparten (98%) af disse skadelige domæner opsamles igennem SIE Europe pDNS sensor net
- DNS bloking skal ske på telecarrier niveau da trafik løber over 4/5G net
- Vi kan nedskyde og eksfiltrere data men ikke blokere. SMS'er kan spoofes

Phishing domain	bankdanske.dk
Phishing domain	opdatering-dkdanskerring.online

```
actionable-identifier: true
date added:
- 2022-04-23 10:37:34 UTC
ips:
- ip: 141.136.39.35
  timestamp: 2022-04-23 10:37:34 UTC
```

Phishing domain	sikkerenhedbekraeftelse-danskekunde.com
Phishing domain	opdatering-mitdanske.online
Phishing domain	1danskebank.com
Phishing domain	enhedsbekraeftelse-danske.com
Phishing domain	danskeuautoriseretlogpa.com
Phishing domain	mydanske-auth.com
Phishing domain	danske-dk.net
Phishing domain	danskesbank.dk
Phishing domain	sikker-danskeonline.com
Phishing domain	sikkerdanske-dk.com
Phishing domain	sikkerdanske-konto.com
Phishing domain	sikkerdanske-konto.net
Phishing domain	verificere-danske.com
Phishing domain	bankdanske.com
Phishing domain	danske-bank.online
Phishing domain	danskesbank.com
Phishing domain	danskebank-review.com
Phishing domain	danskebank-help.com
Phishing domain	danskesikkerhed-dk.com

Phishing aktører

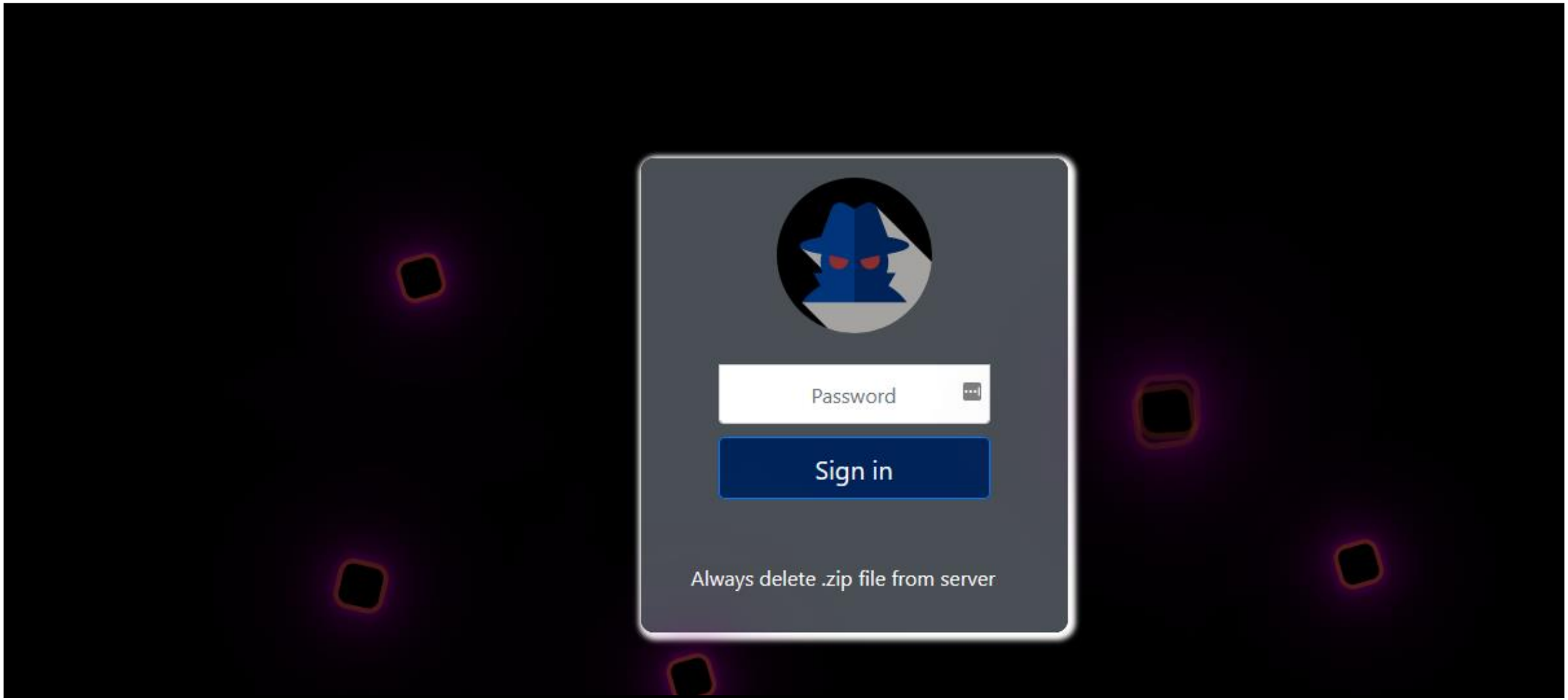
- Vi har pt at gøre med 5 forskellige grupper. Flere end 3000 kliks på 24 timer I gennemsnit!!
- De 2 mest aktive sporer vi som ”SST actor” (dansker) og ”Mr Vito” og ”Billy Jackson” som er den ene og same
- Mr Vito og Billy Jackson anvender et kommercielt phish kit som vi kender som “Zeroc0d3r”.
- Angrebene mod Danmark vil fortsætte. De it-kriminelle har lugtet blod!
- DK Hostmaster mener det godt, men har ikke helt forstået teknikken … (se svar på abuse herunder)

```
Domain:                 bankdanske.dk
DNS:                    bankdanske.dk
Registered:             2022-04-12
Expires:                2023-04-11
Registrar:              Dynadot LLC
Registration period:    1 year
VID:                    no
DNSSEC:                 Unsigned delegation, DNSSEC disabled, no records
Status:                 Active

Registrant
Handle:                 ***N/A***
Name:                   Vito Aloisio
Address:                Piazza Umberto 1,12
Postalcode:             90010
City:                   Ustica
Country:                IT
Phone:                  +39 3512076256

Nameservers
Hostname:               ns1.dynadot.com
Hostname:               ns2.dynadot.com
```

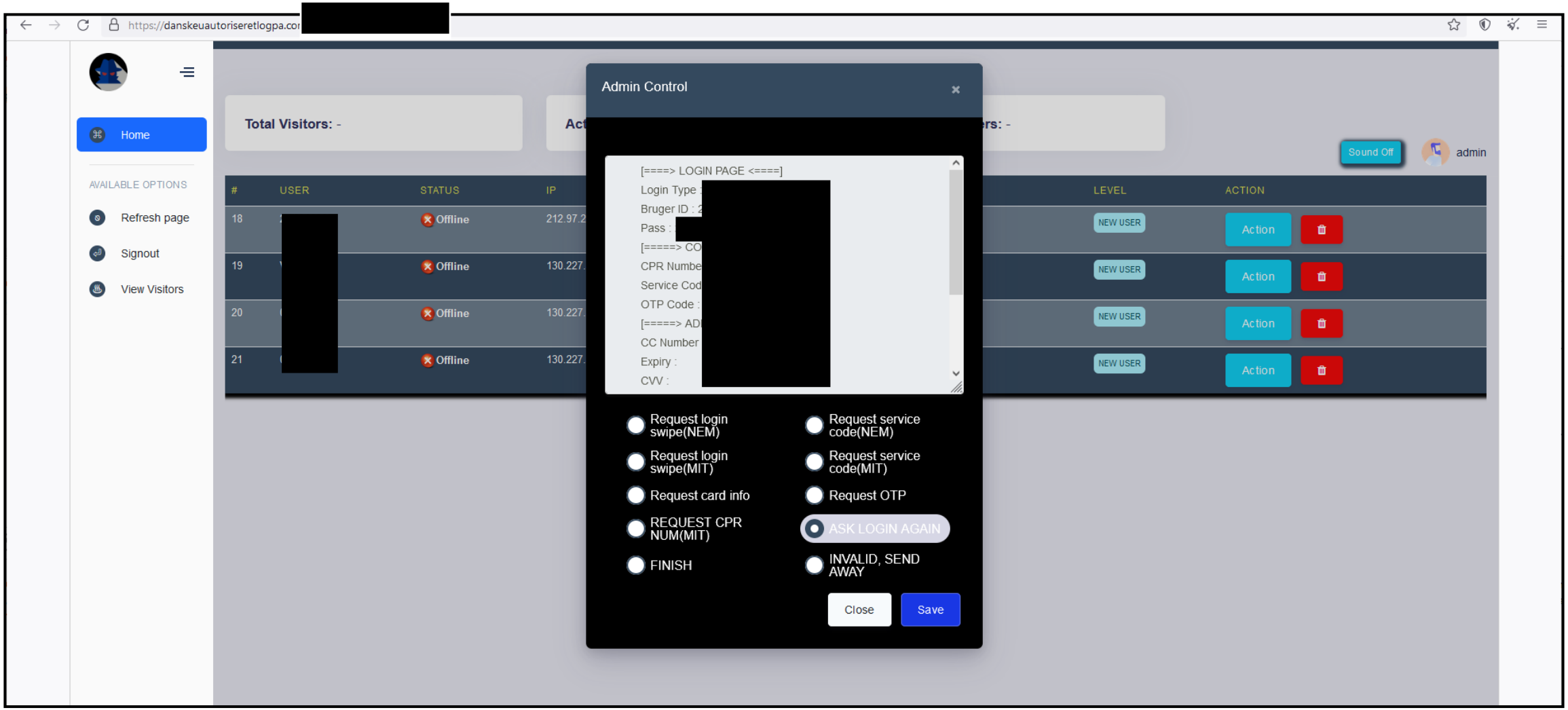
```
Domain:                 danskesbank.dk
DNS:                    danskesbank.dk
Registered:             2022-04-15
Expires:                2023-04-14
Registration period:    1 year
VID:                    no
DNSSEC:                 Unsigned delegation, DNSSEC disabled, no records
Status:                 Active

Registrant
Handle:                 ***N/A***
Name:                   billy jackson
Address:                frankfut 12,
Postalcode:             60313
City:                   Frankfurt am Main
Country:                DE
Phone:                  +49 1744191597

Nameservers
Hostname:               ns61.domaincontrol.com
Hostname:               ns62.domaincontrol.com
```

Vi har gennem de seneste dage flere gange forsøgt at tilgå hjemmesiden under domænenavnet. Det er ikke lykkedes at konstatere, at der foretages phishing fra siden, og dermed er grundlaget for at suspendere domænenavnet ikke til stede.

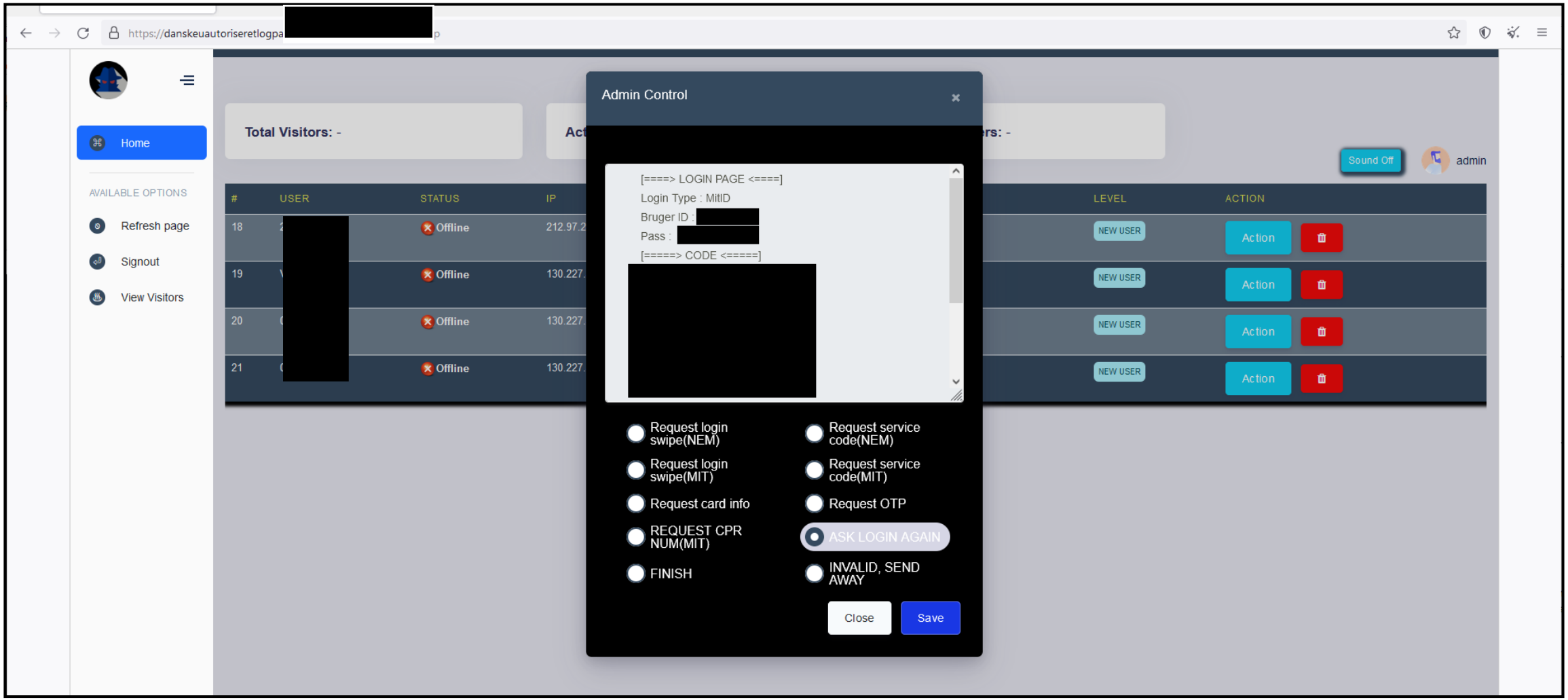
Vores beslutning er derfor, at domænenavnet ikke suspenderes.



MiTM - Zeroc0d3r kit



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

Truslen fra ransomware og potentielle datalæk

CSIS
REST ASSURED

5.00 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
- Lås din maskine med en skærmlås når du ikke bruger den, begræns adgang til hjemmearbejdspladsen i hjemmet. Del den ikke med børn
- Sikre hardware (routere/wifi, firmware, passwords osv.)
- Cyberforsikring?

REST ASSURED

Spørgsmål

pkr@csis.dk

PGP-ID: 0x715FB4BD

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