Cybercrime

DLA Piper, Århus
Januar 2020

REST ASSURED

www.csis.dk

Hvem er CSIS og whois: Peter Kruse?

- Danskejet selskab, grundlagt, 2003
- Ca. 100 ansatte, 24 nationaliteter
- Datacentre over hele verden
- IT sikkerhedsleverandør til verdens største selskaber
- Advisory Board medlem hos Europol EC3, Interpol, medlem af CARO og OPS-Trust
- Vært for Copenhagen Cybercrime Conference
- Søsterselskaber Heimdal, Defendas og Agile Technologies
- Peter Kruse har arbejdet professionelt med it-sikkerhed i næsten 20 år og analyserede sin første computervirus i 1984

Den aktuelle cybertrussel mod Danmark

Agenda

1.00 Trends
2.00 Fra Anonymous til APT#
3.00 Phishing, Vishing, Smishing og spear phishing
4.00 Ransomware
5.00 Case study: MazarBOT
6.00 Bredspektrede angreb: IoT
7.00 Opsamling og gode råd
8.00 Spørgsmål

Cybercrime

REST ASSURED

1.00 Trends

Stadig flere afpresses af it-kriminelle over e-mail

Stadig flere afpresses af it-kriminelle over e-mail, viser tal fra Danmarks Statistik. Foto: Loic Venance / Scanpix Denmark

Det er et hastigt voksende problem, at it-kriminelle stjæler filer fra computere og bagefter kræver løsesum.

at bruge deres sunde fornuft, når de

(Arkivfoto).

06. sep 2017 kl. 07:0

→ Østjylland

MEST SETE PÅ TV2.DK

KRIMI

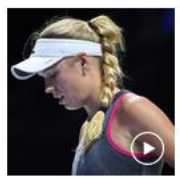
Shuaib Khan e
lukker LTF-lok

KURS MOD FJERN

Havana kan ikk
ekspedition - k
nye skib

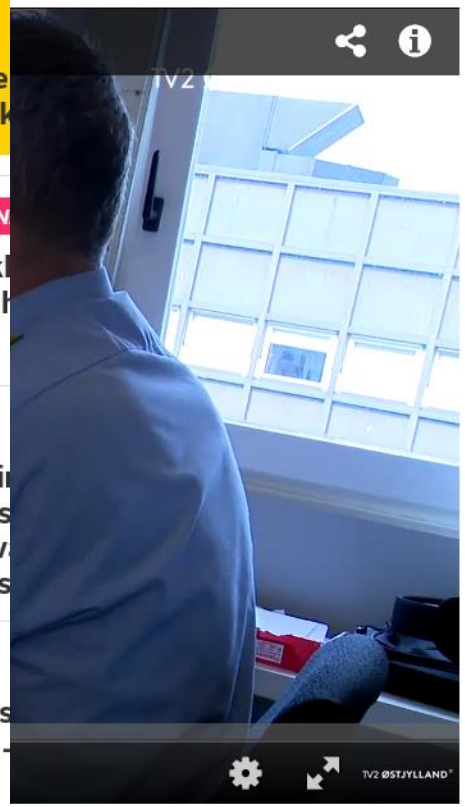
UDLAND

Kennedy-papi
frygtede stats
troede, drab v
Vietnam-præs



TENNIS

Wozniacki bes
gruppekamp: -
forskel



Direktørsvindel (CEO Fraud)

En af de største økonomiske trusler mod virksomheder

INDLAND

Kirkeråd franarret knap en million kroner via mailsvindel

Danske Kirkers Råd er blevet franarret halvdelen af sit årlige budget. Pengene er blevet sendt til udlandet.

Danske Kirkers Råd er blevet franarret et større beløb, der er endt på engelske og rumænske konti. (Foto: Betina Garcia © dr)

uncement

MPROMISE THE 12 BILLION

nt (PSA) is an update and companion to
EC) PSA 1-050417-PSA posted on
new Internet Crime Complaint Center (IC3)
ed statistical data for the time frame October

EC)/E-mail Account Compromise (EAC) is a
h businesses and individuals performing wire

ut when a subject compromises legitimate
h social engineering or computer intrusion
zed transfers of funds.

sociated with a request for transfer of funds. A
mpromising legitimate business e-mail
lly Identifiable Information (PII) or Wage and
mployees.[1]

Zoom

Zoom

etter of

Den aktuelle cybertrussel mod Danmark

Mål: Social og politisk mål. At demonstrere uenighed, udstille og synliggøre urimeligheder.

Metoder: DDOS, sociale medier recognisering, Sofistikerede angreb med målet at udtrække sensitive data.

Ideologiske grupperinger

Mål: Penge

Metoder: Spam , Malware, BotNets, DDOS, Sociale Medier hijacking , Black Market Cyber-crime toolkits, CAAS

Organiseret kriminalitet

Mål: Spionage. Indsamling af finansielle og økonomiske data, Teknologi/IP, strategi og militær information

Metoder: sociale medier, recognisering, social engineering, malware infektion og datatyveri.

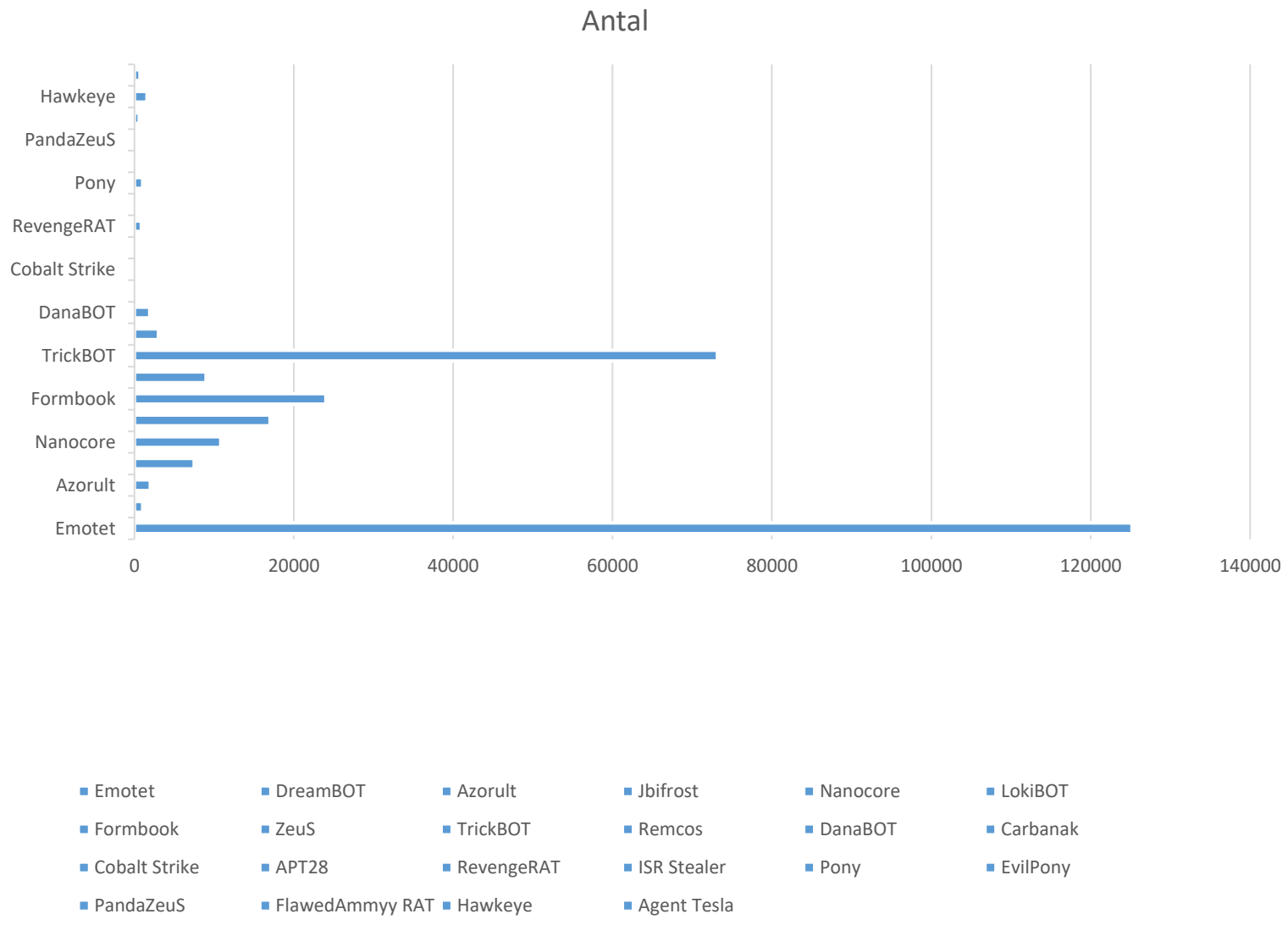
APT

Spamkampagner og payload mod Danmark

- Generelt er Danmark ramt af de samme store generiske malware familier som rammer vores nabolande. Payload i anden stadie varierer med afsæt i GeoIP
- Mere end 80 procent er dataindsamlende malware (!)
- Den største andel af malware båret via spammails er skabt med malware toolkits
- I 76 procent er både første og andet stadie af infektionen beskyttet ved brug af en cryptor og anvender bullet proof hosting som infrastruktur
- Makro- og exploit payload i dokumenter er mest hyppigt anvendte metode (DEMO)
- Mindre end 0,1 procent er APT relateret … men de er der …
- Den samlede økonomi i cybercrime har, ifølge FBI overhalet, den globale handel med narkotika

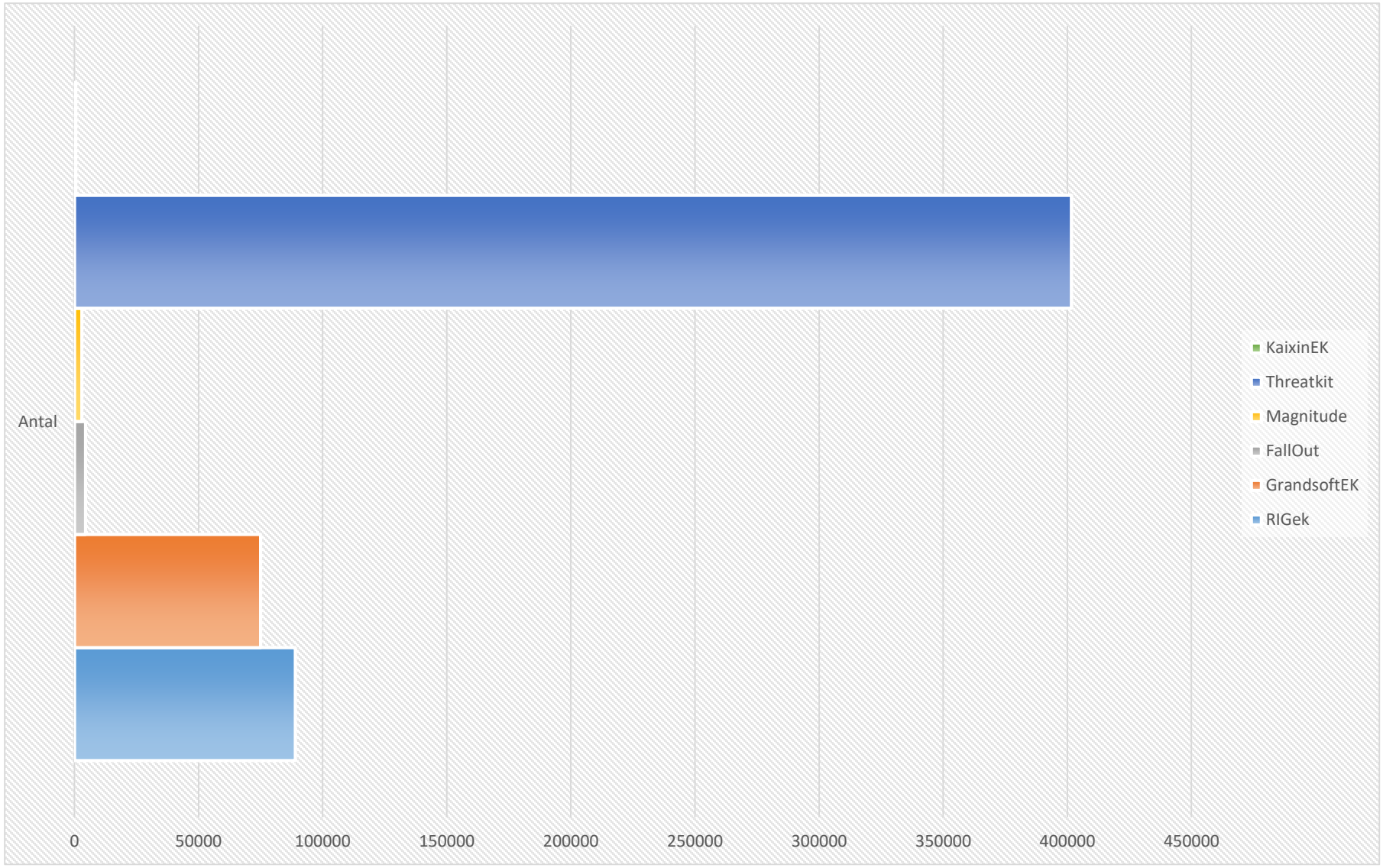
Spamkampagner og payload mod Danmark

Navn	Antal
Emotet	125191
DreamBOT	1042
Azorult	2001
Jbifrost	7511
Nanocore	10844
LokiBOT	17011
Formbook	24012
ZeuS	9013
TrickBOT	73181
Remcos	3011
DanaBOT	1911
Carbanak	141
Cobalt Strike	299
APT28	96
RevengeRAT	867
ISR Stealer	309
Pony	1039
EvilPony	200
PandaZeuS	104
FlawedAmmyy RAT	581
Hawkeye	1571
Agent Tesla	705



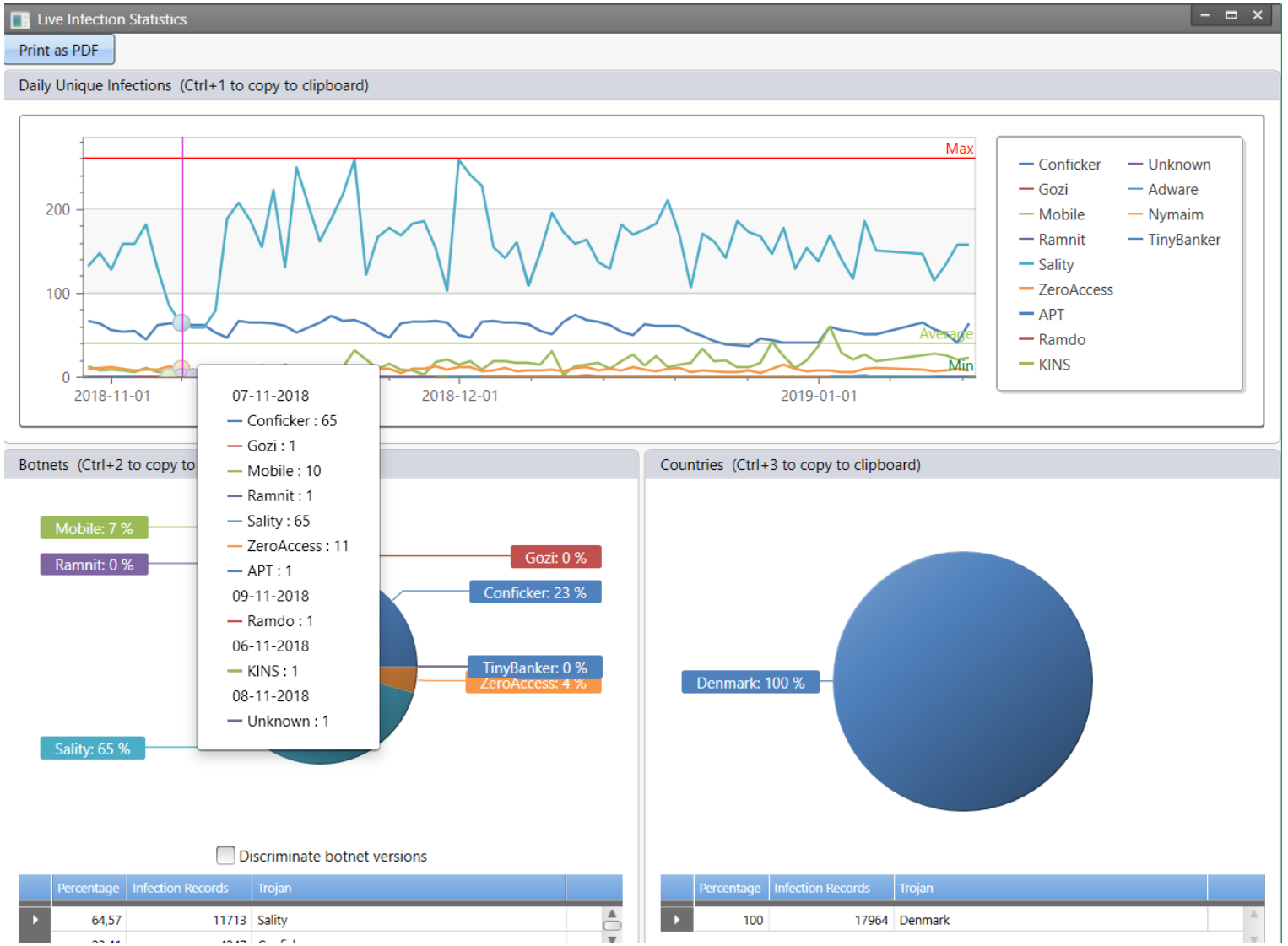
Exploitkits 2019 og payload mod Danmark

Exploitkit	Antal
RIGek	89005
GrandsoftEK	75005
FallOut	4519
Magnitude	3044
Threatkit	401655
KaixinEK	498



Danske hændelser i den forløbne måned

CONFICKER STADIG MED?

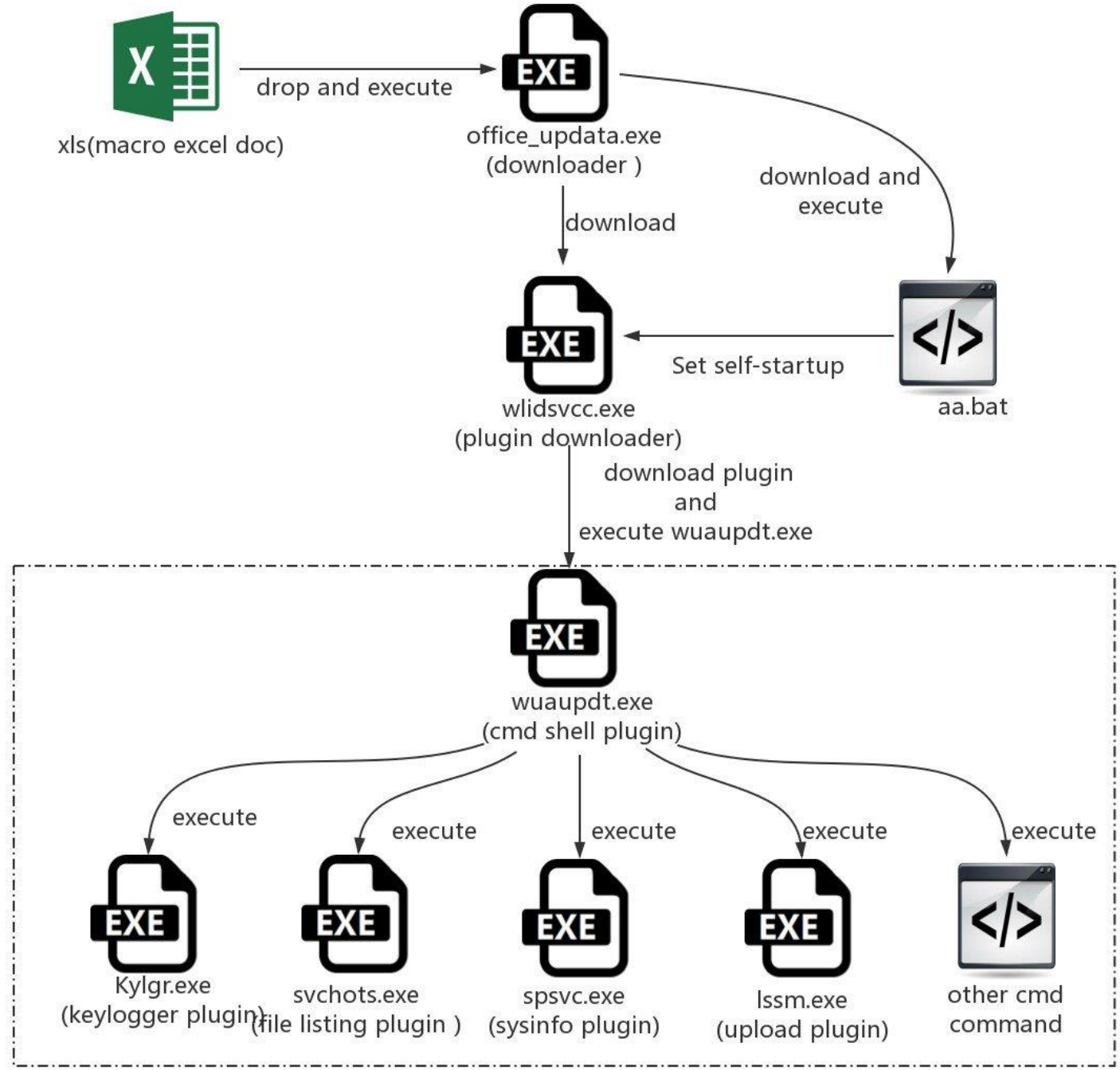


Den aktuelle cybertrussel mod Danmark

REST ASSURED

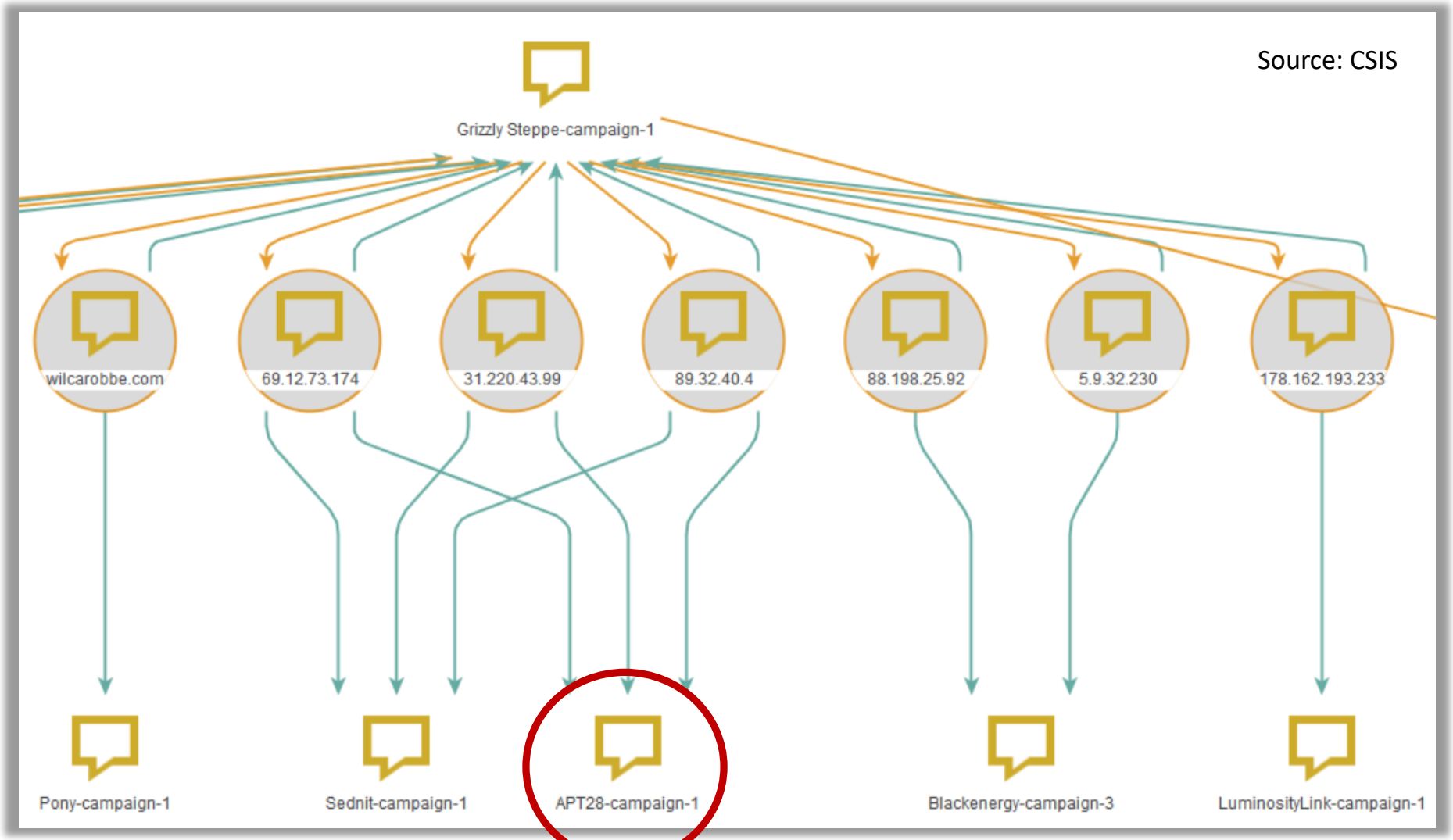
2.00 Fra Anonymous til APT#

APT cyklus i angreb mod Danmark

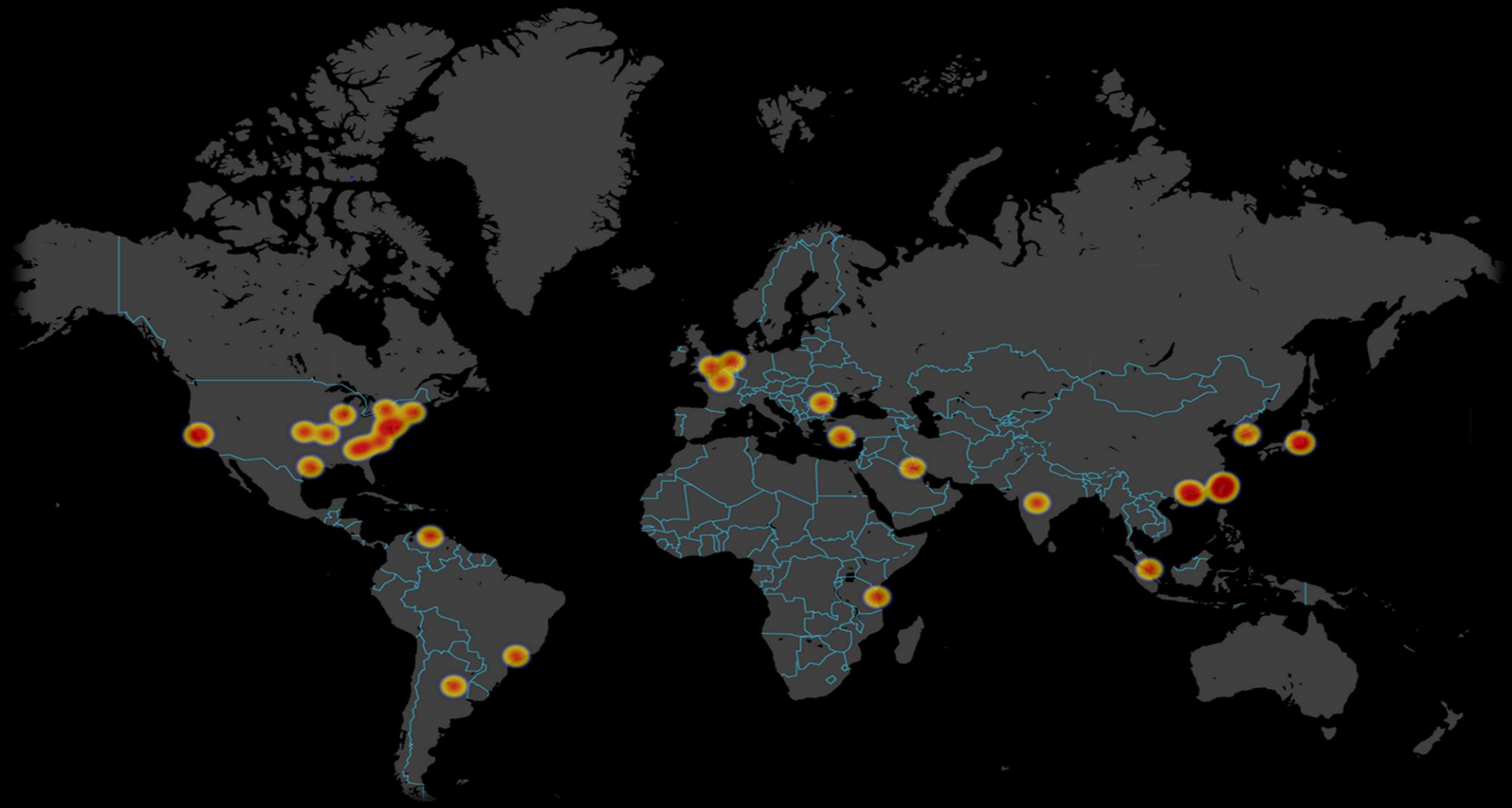

xls(macro excel doc)
drop and execute
office_updata.exe
(downloader)
download and
execute
download
wlidsvcc.exe
(plugin downloader)
Set self-startup
aa.bat
download plugin
and
execute wuaupdt.exe
wuaupdt.exe
(cmd shell plugin)
execute
execute
execute
execute
execute
Kylgr.exe
(keylogger plugin)
svchots.exe
(file listing plugin)
spsvc.exe
(sysinfo plugin)
lssm.exe
(upload plugin)
other cmd
command

APT aktører vokser i resourcer, kompleksitet og omfang

Russisk interferens i den amerikanske valgkamp? Helt sikkert.



APT C&C server lokation (GeoIP -> Heatmap)



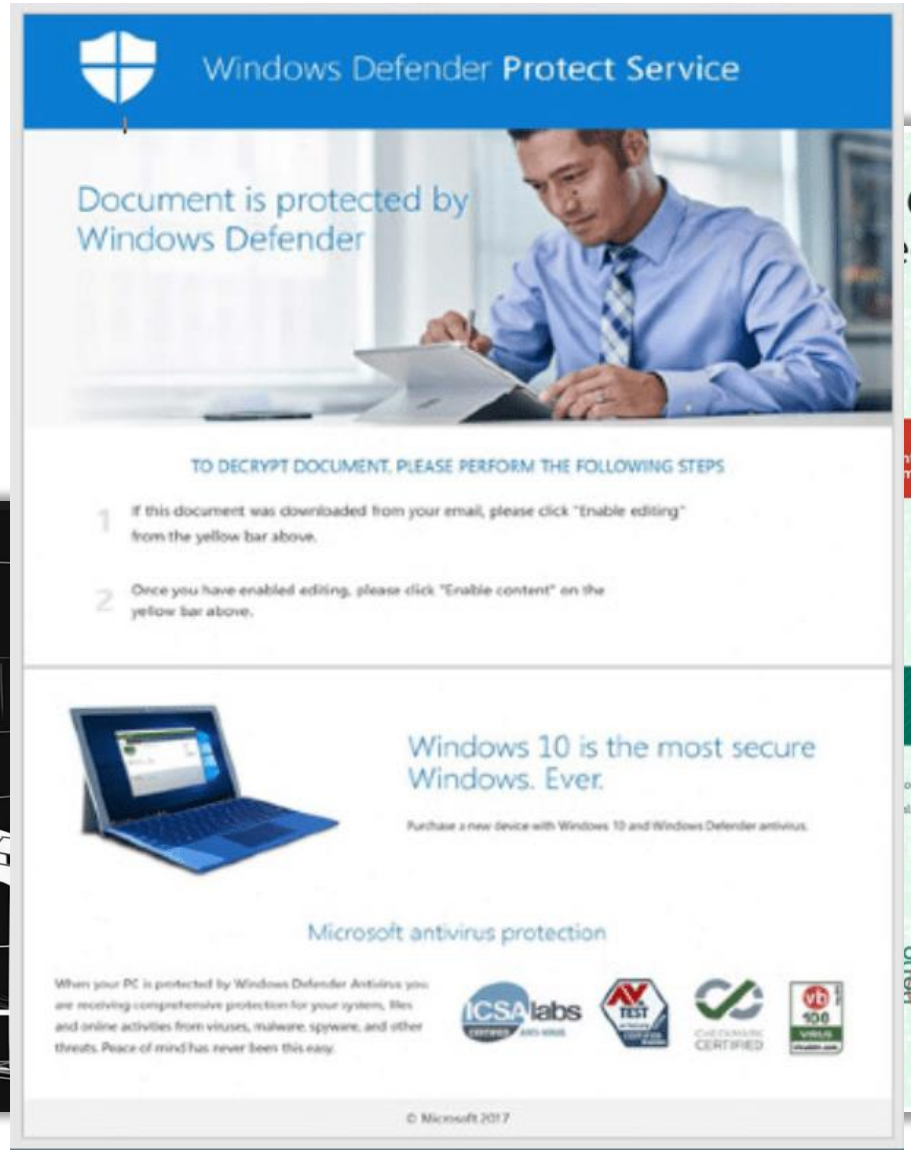
Emotet C&C Tier-1 (GeoIP -> Heatmap)

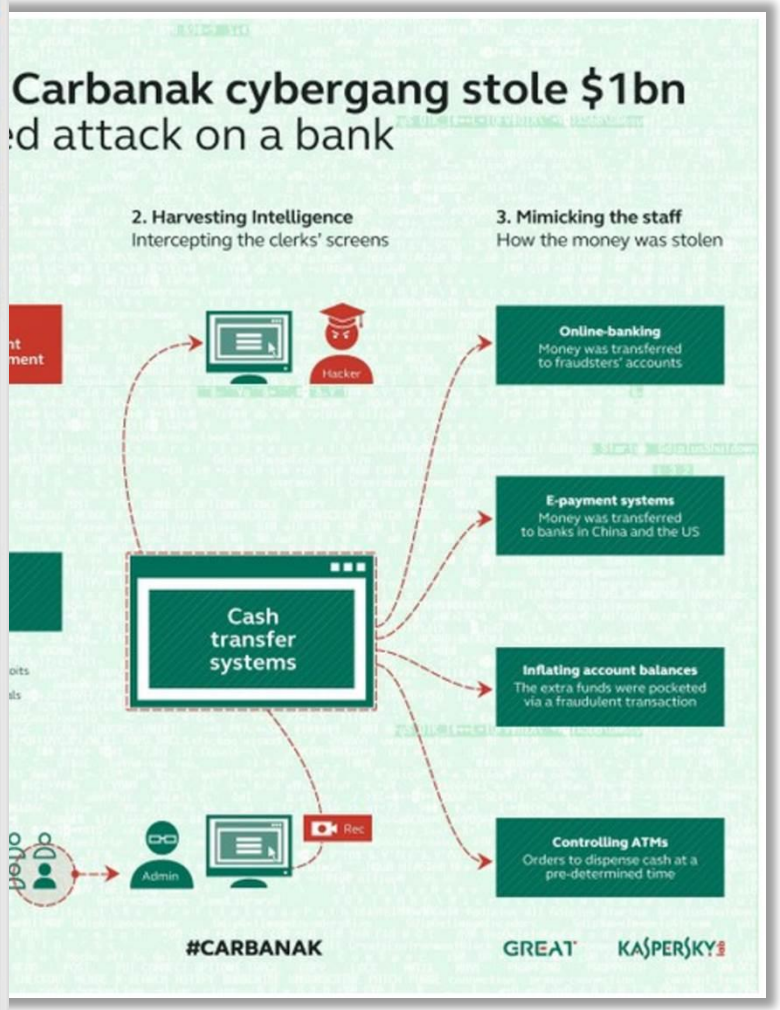
2019: Løbende APT aktivitet i Danmark

MÅLT OVER DEN SENESTE MÅNED

2018-12-27 15:55:00	Stofa	APT	Darkhotel	37.128.222.30	Denmark	Esbjerg	waldennetworks.co...
2018-12-29 13:10:35	Rakibul Islam t/a Dynamic...	APT	EquationDrug	103.85.200.86	Denmark	Copenhagen	monster-ads.net
2019-01-05 19:18:00	Rakibul Islam t/a Dynamic...	APT	EquationDrug	103.85.200.84	Denmark	Copenhagen	techsupportpwr.com
2019-01-02 03:16:16	Zen Systems A/S	APT	Stuxnet	94.18.214.122	Denmark	Brøndby Strand	best-advertising.net
2019-01-06 02:40:47	Rakibul Islam t/a Dynamic...	APT	EquationDrug	103.85.200.98	Denmark	Copenhagen	islamicmarketing.net
2019-01-05 13:54:53	M247 LTD Copenhagen Inf...	APT	Hangover	82.102.20.178	Denmark	Copenhagen	torqspot.org
2019-01-05 13:53:21	M247 LTD Copenhagen Inf...	APT	Hangover	82.102.20.167	Denmark	Copenhagen	torqspot.org
2019-01-14 10:07:28	Netic A/S	APT	Red October	77.243.61.193	Denmark	Ålborg	svchost-online.com
2019-01-14 10:07:28	Netic A/S	APT	Red October	77.243.61.193	Denmark	Ålborg	svchost-update.com

APT aktører som Carbanak jagter også penge





Crime as a Service

Crime as a Service

Prev 1 .. 121 122 123 124 .. 20745 Next

Group	Country	City	Version	Browser	OS	IP	Reg	Comment	Sys
1068	US	Gig Harbor	216989	Internet Explorer 8.0	Win_7_64	67.183.164.92	2018-03-07 19:29:02	Seabeck Pizza ...	details
1068	US	Bozeman	216989	Internet Explorer 8.0	Win_7	216.166.170.186	2018-03-07 18:19:13	Sacajawea Hotel	details
1070	UA	Kiev	216989	Internet Explorer 8.0	Win_7	176.37.132.185	2018-03-21 11:27:21	SECRETAR-INCOM	details
1070	UA	Lviv	216989	Internet Explorer 8.0	Win_XP x64 Edition_64	213.174.0.20	2018-03-21 12:25:21	POS lan - chec...	details
1065	US		216989	Internet Explorer 8.0	Win_10_64	73.119.139.150	2018-02-26 20:47:18	POS in LAN. Ja...	details
1065	US	New York	216989	Internet Explorer 8.0	Win_10_64	98.7.40.194	2018-02-26 18:58:03	POS in LAN	details
1052	BG	Pravda	216975	Internet Explorer 8.0	Win_7_64	95.43.223.40	2017-12-05 15:47:16	POS - check, w...	details
1068	US	Lexington	216989	Internet Explorer 8.0	Win_7_64	71.174.87.110	2018-02-26 18:57:39	Neillios Gourm...	details
1061	PL	Sopot	216989	Internet Explorer 8.0	Win_7_64	194.181.123.5	2018-02-14 16:41:31	Naukowa I Akad...	details
1000	BG	Plovdiv	216962	Internet Explorer 8.0	Win_XP	212.116.159.93	2017-11-28 15:07:13	Municipality o...	details

Den aktuelle cybertrussel mod Danmark

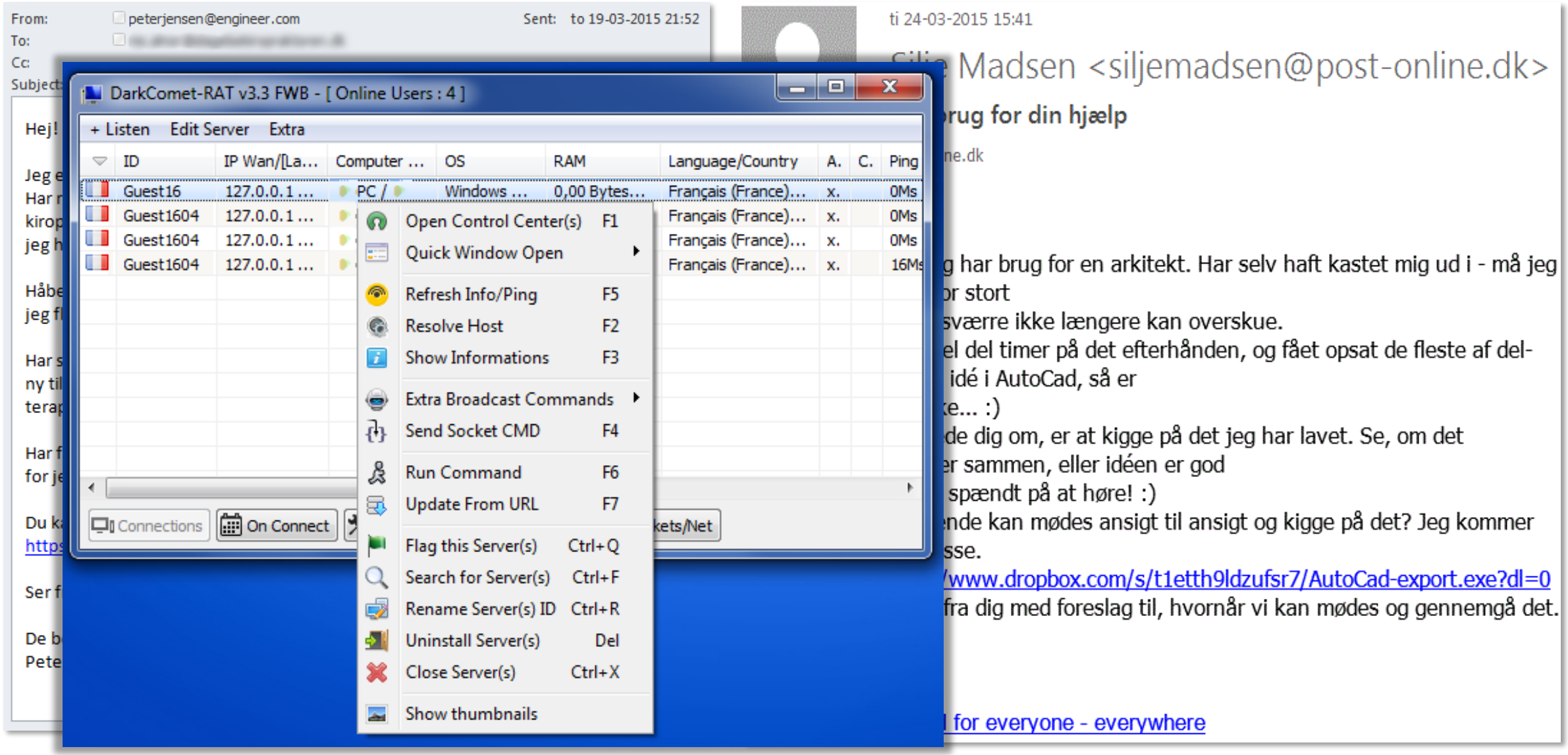
CSIS
REST ASSURED

3.00 Phishing, Vishing & Smishing

Phishing, V scam

Spear phishing tricks

Spear phishing



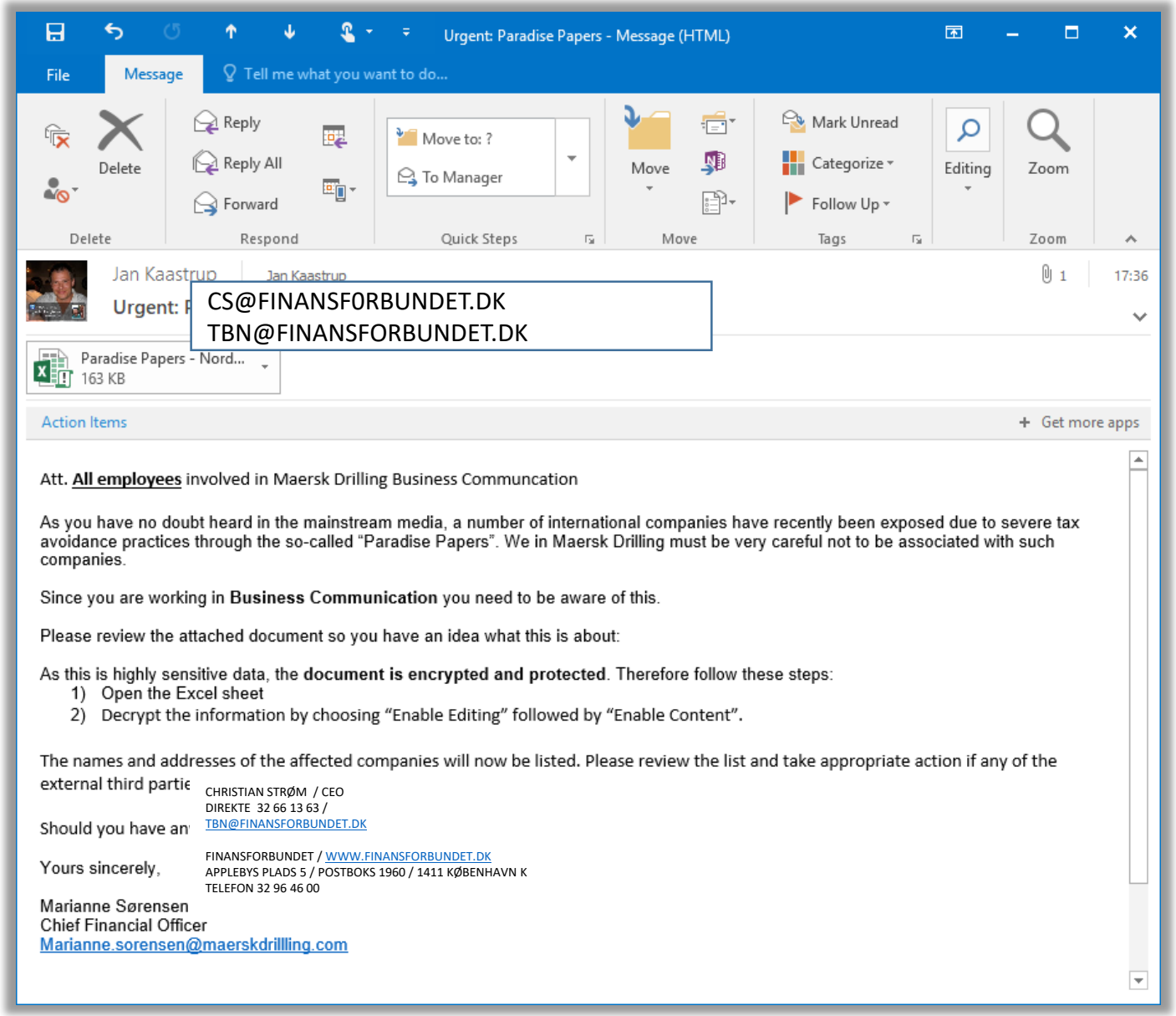
Spear phishing tricks: spoofing e-mail FROM

Kan du spotte forskellen?

cs@finansf**o**rbundet.dk
cs@finansf**0**rbundet.dk

eller

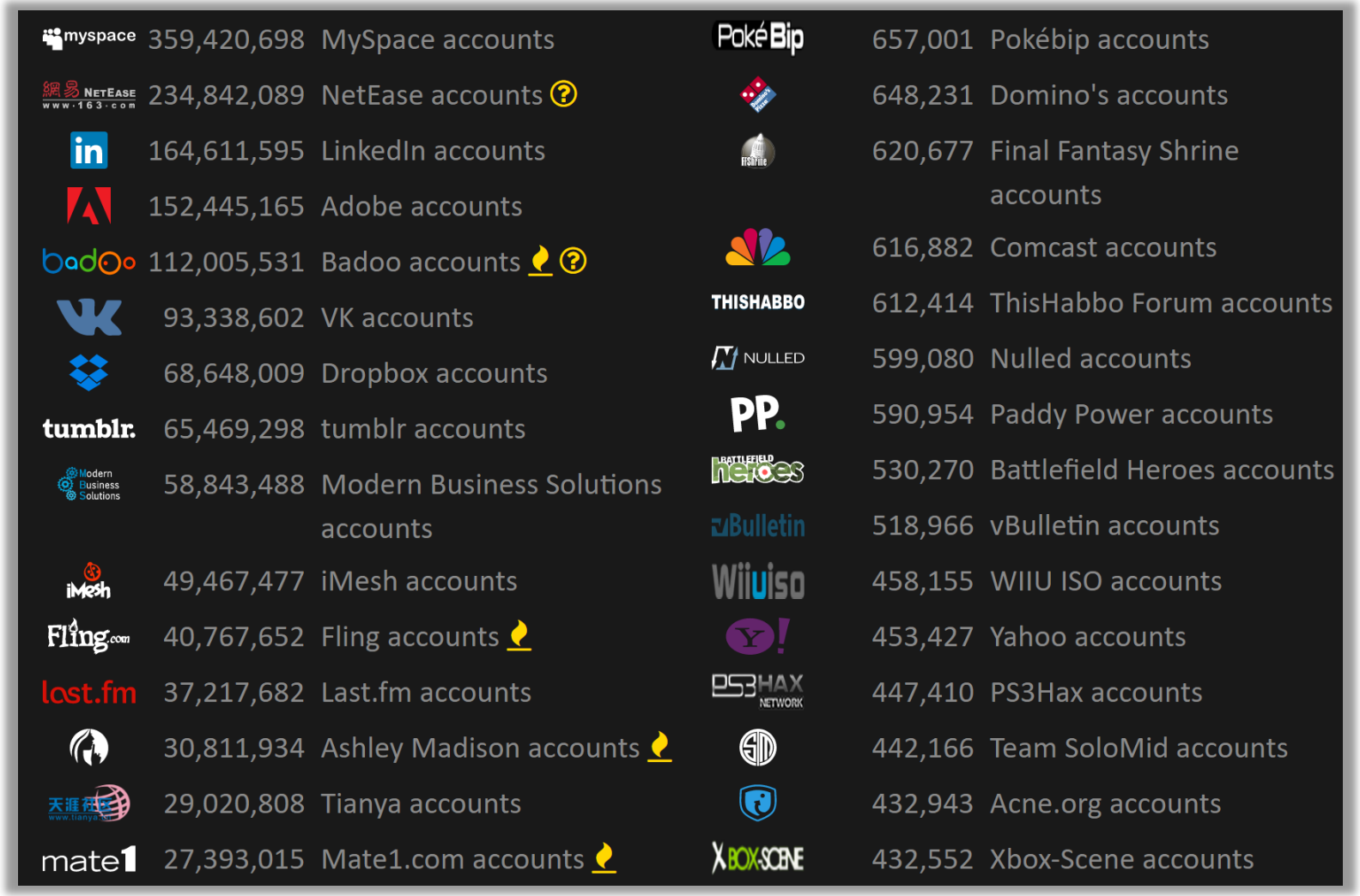
CS@FINANSF**O**RBUNDET.DK
CS@FINANSF**0**RBUNDET.DK



Datalækager

Hvilken værdi har dit brugernavn, email og password?

Har du skiftet password for NYLIGT og GENBRUGER du dit password andre steder?

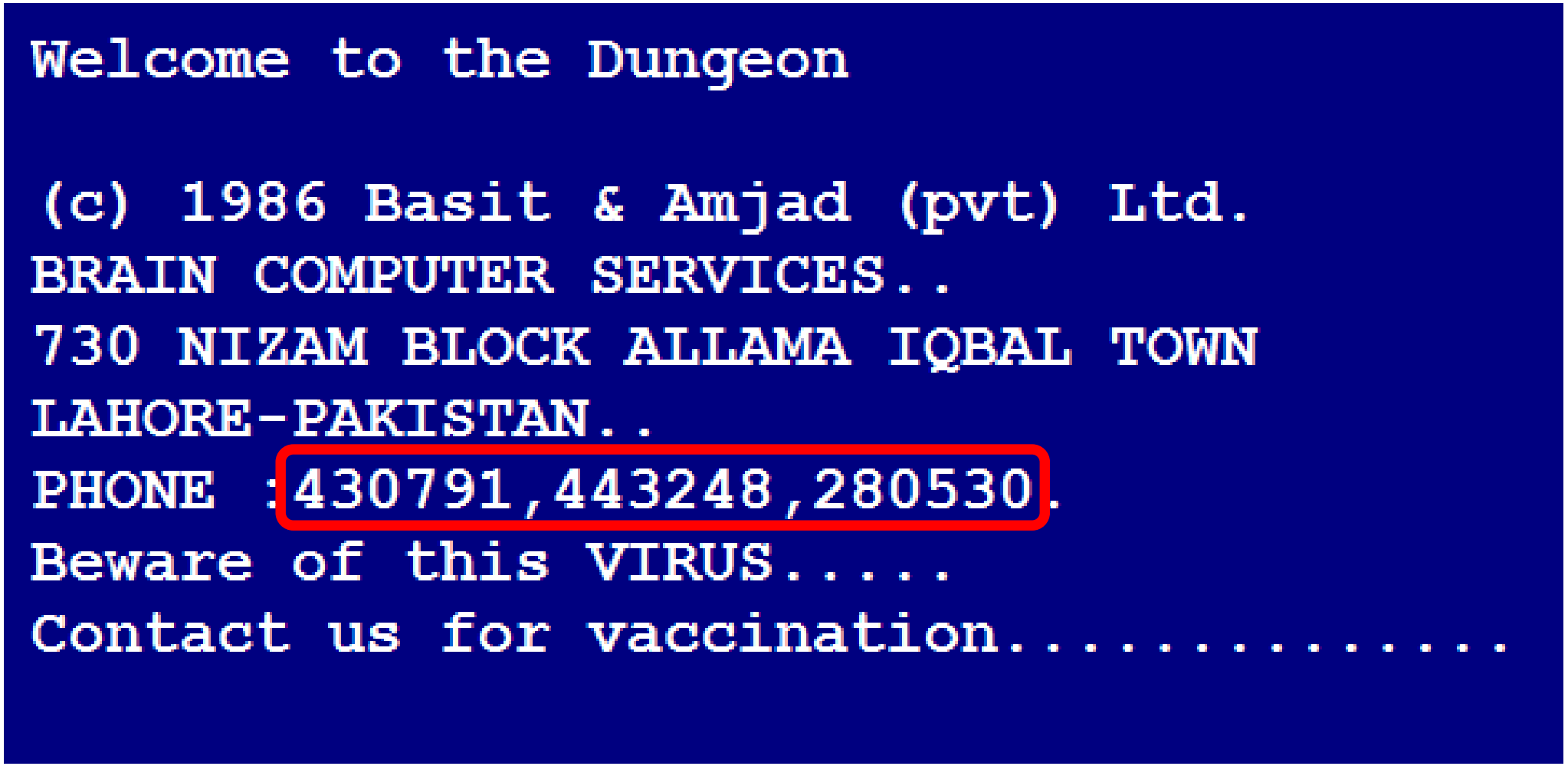


Det aktuelle trusselsbillede

REST ASSURED

4.00 Ransomware

Ransomware


Welcome to the Dungeon
(c) 1986 Basit & Amjad (pvt) Ltd.
BRAIN COMPUTER SERVICES..
730 NIZAM BLOCK ALLAMA IQBAL TOWN
LAHORE-PAKISTAN..
PHONE :430791,443248,280530.
Beware of this VIRUS.....
Contact us for vaccination.....

Ransomware


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immediately.
Contact
If you need our assistance, send a message by clicking <Contact Us>.
We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!
Payment will be raised on
1/4/1970 00:00:00
Time Left
00:00:00:00
Your files will be lost on
1/8/1970 00:00:00
Time Left
00:00:00:00
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $600 worth of bitcoin to this address:
Copy
Check Payment
Decrypt

Mærsk hændelsen

NotPetya

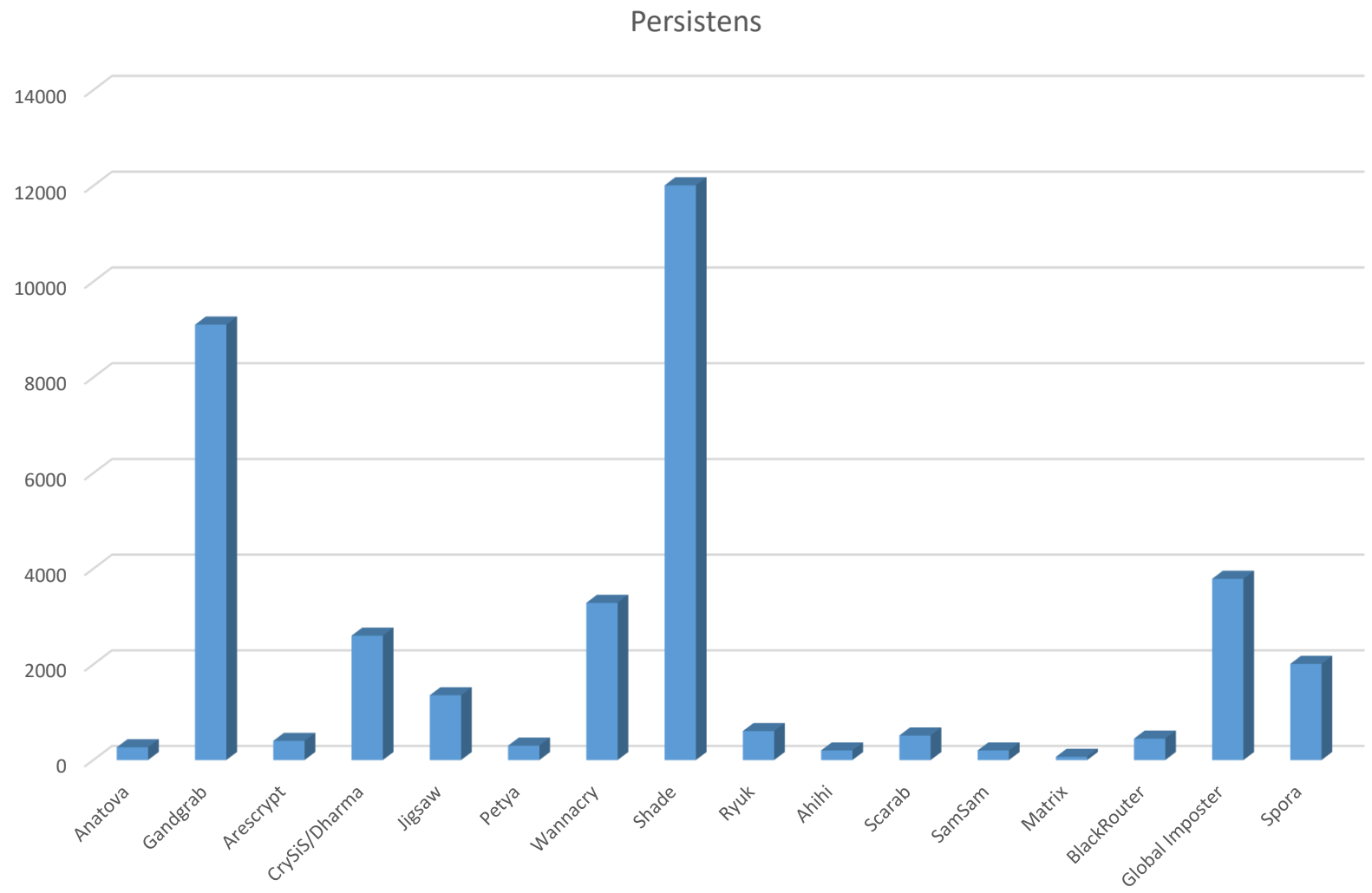
Trin 1: Software opdatering
- Patient-0 ← vanskeligt at beskytte sig imod

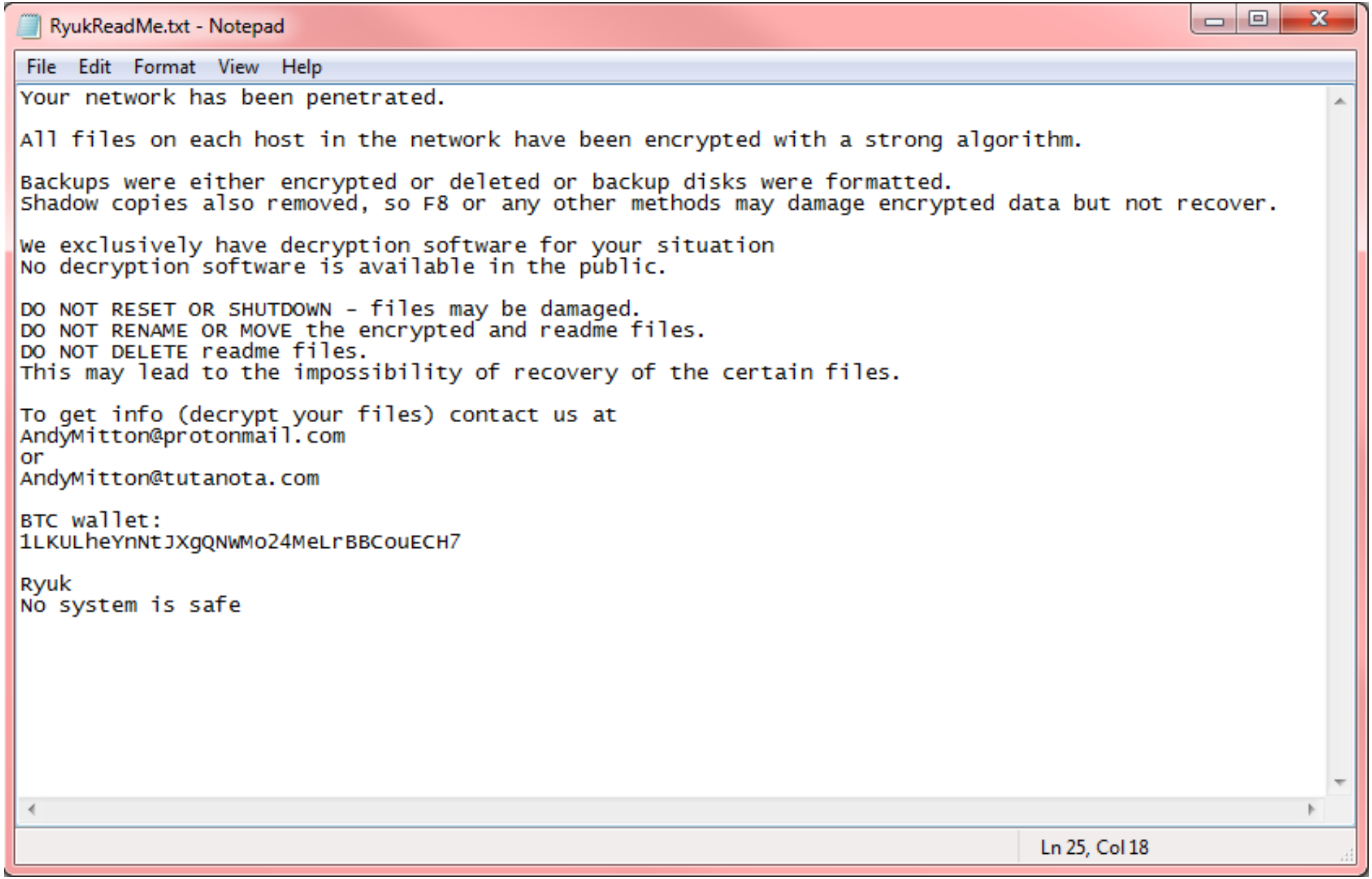
Trin 2: Automatisk spredning
- Exploit
- Høst af brugerkonto

```
TLP:AMBER

Related to Incident Response: #Petya (#NotPetya)

A Normal update from medoc would look like this:

2017-06-22 07:54:26 CLIENT 273
upd.me-doc.com.ua/last.ver?rnd=RNDSTRING
"medoc1001188"
2017-06-22 07:54:26 CLIENT 418
upd.me-doc.com.ua/update_list.ver?rnd=RNDSTRING "medoc1001188"
2017-06-22 07:54:26 CLIENT 198 upd.me-doc.com.ua/- "medoc1001188"
2017-06-22 08:11:40 CLIENT 273 upd.me-doc.com.ua/last.ver- -
2017-06-22 08:13:02 CLIENT *19367953*
upd.me-doc.com.ua*/ezvit.*10.01.188-10.01.189.upd- "medoc1001188"
2017-06-22 11:35:20 CLIENT 198 upd.me-doc.com.ua/- "medoc1001189"
2017-06-22 11:35:20 CLIENT *273*
upd.me-doc.com.ua/*last.ver*?rnd=RNDSTRING "medoc1001189"

Infected host receives this instead:

2017-06-???? CLIENT2 *332963*
upd.me-doc.com.ua/*last.ver*?rnd=RNDSTRING

CLIENT = CLient hostname.
RNDSTRING = a string that has been sanitized

So in a normal update, the *ezvit* is used to ship new code.
*last.ver* usually ships ~ 270 bytes, but in case of an malcrafted package
it is > 300 KB

It therefore looks like they did not use the update but the version check
mechanism to inject code.
```

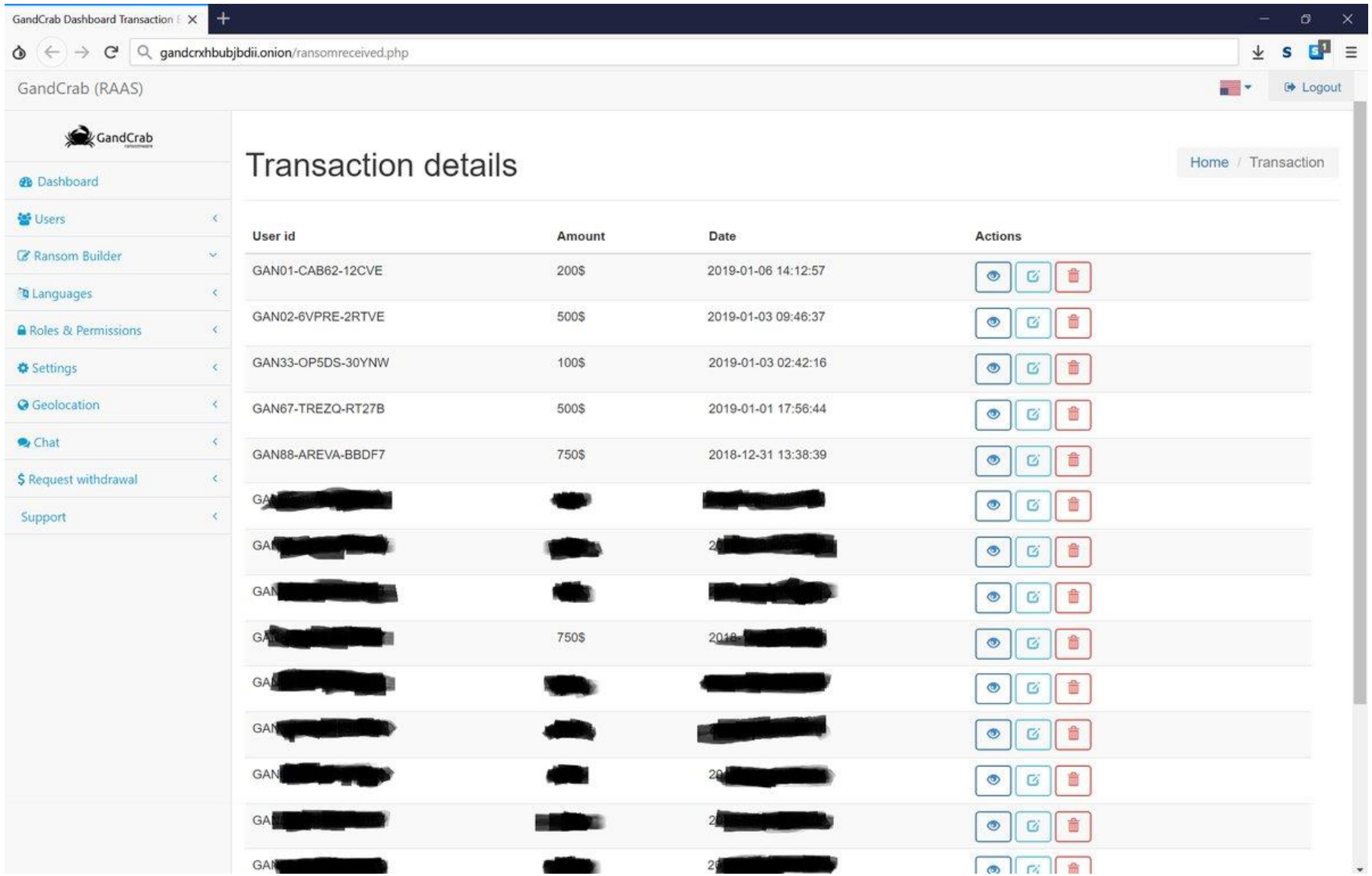
Ransomware

Ransomware	Antal
Anatova	267
Gandgrab	9102
Arescrypt	401
CrySiS/Dharma	2601
Jigsaw	1355
Petya	302
Wannacry	3288
Shade	12011
Ryuk	606
Ahihi	201
Scarab	514
SamSam	201
Matrix	68
BlackRouter	449
Global Imposter	3791
Spora	2012



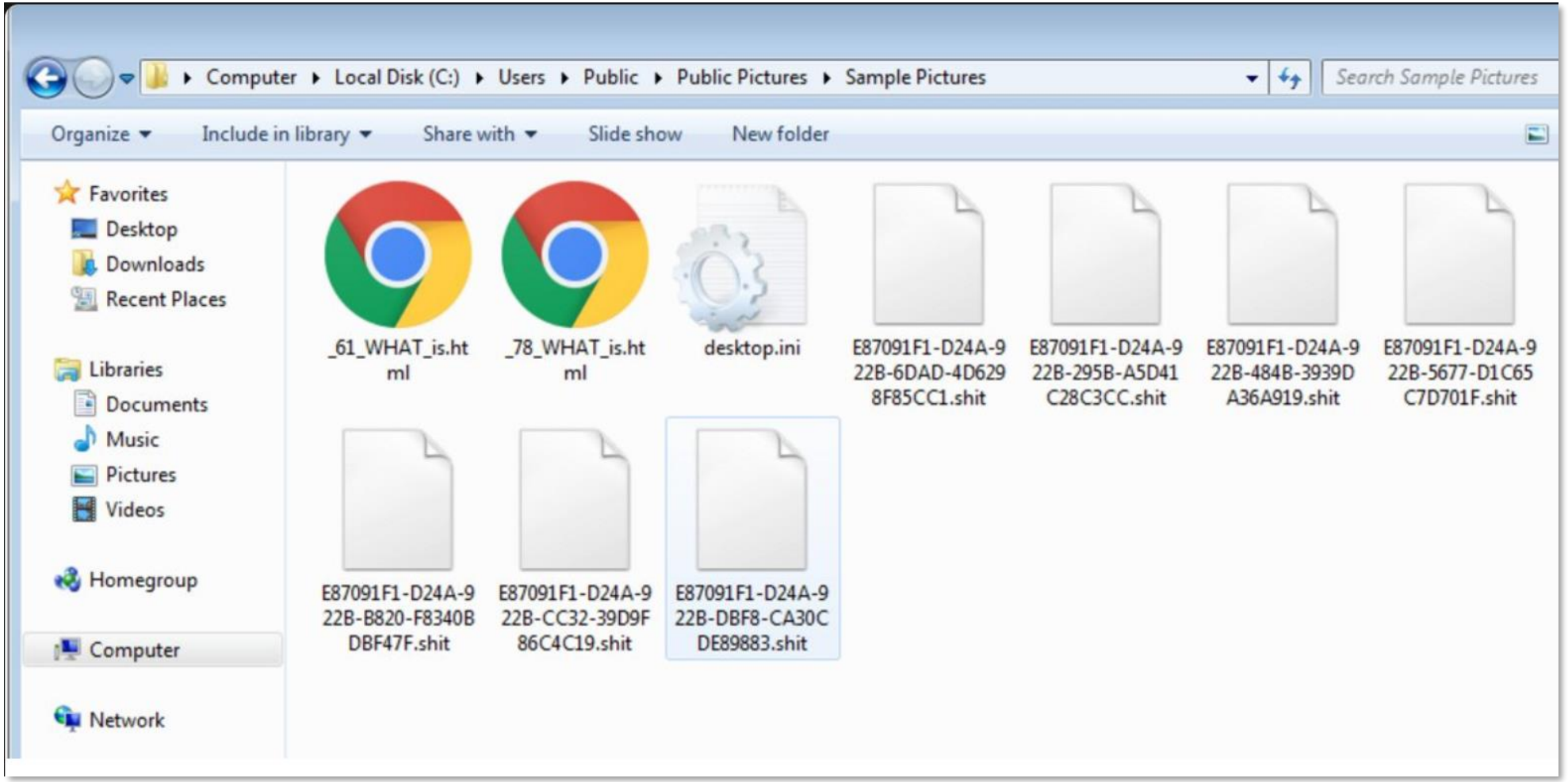

RyukReadMe.txt - Notepad
File Edit Format View Help
Your network has been penetrated.
All files on each host in the network have been encrypted with a strong algorithm.
Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.
We exclusively have decryption software for your situation
No decryption software is available in the public.
DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.
To get info (decrypt your files) contact us at
AndyMitton@protonmail.com
or
AndyMitton@tutanota.com
BTC wallet:
1LKULheYnNtJXgQNWMo24MeLrBBCouECH7
Ryuk
No system is safe
Ln 25, Col 18

GandGrab backend



Ransomware

Hvad sker der?



Den aktuelle cybertrussel mod Danmark

CSIS
REST ASSURED

6.00 Bredspektrede angreb

Fra IoT til SCADA

- Angreb mod eksempelvis webcams, routere, smartTVs, IHC, Elmålere, badevægte, køleskabe, biler, dørklokker, alarmsystemer og andre kontrol devices findes i PoC og mange har aldrig skiftet standard password! **#Mirai**
- Devices kan anvendes som platform for andre angreb som set med printer servere og andre ”storage devices”.
- I angreb mod IHC systemer kan en angriber lukke døre og porte, slukke lys, ændre temperatur, aktivere brandalarm osv. Det kan skabe panik i butikscentre og kontorkomplekser, gymnastikhaller m.v.
- Angreb mod industrielle systemer og produktion (PLC/SCADA)

Gode råd /opsummering

- Udvis sund fornuft. Klik ikke ukritisk på materiale som kommer uopfordret
- Sørg for at holde alt dit udstyr opdateret
- Læs manualen
- Tag backup – glem ikke clouden
- Installerer antivirus – de fleste til private er gratis. GRATIS er bedre end ingenting!
- Genbrug aldrig password. Vælg et godt password og en password manager
- Hvis i tvivl, så hellere tøv og ring til afsender eller en ven for bekræftelse eller hjælp
- Del ikke oplysninger ukritisk på nettet
- Slå 2FA (totrinsgodkendelse) til hvorend det er muligt (Facebook/Linkedin/Gmail osv)
- Slå din maskine med en skærmlås når du ikke bruger den
- Indtast aldrig sensitive oplysninger på en offentlig maskine
- Udvis kritisk sans og del ikke ukritisk nyheder og konkurrencer fra tvivlsomme kilder

REST ASSURED

Tak for Jeres tid!
- Er der nogen spørgsmål?

Kontaktoplysninger:

pkr@csis.dk

PGP-ID: 0x715FB4BD

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