Det aktuelle trusselsbillede

Dansk Standard

CSIS

REST ASSURED

www.csis.dk

SIS

aber

ARO, og medstifter af SIE-Europe

kkerhed i næsten 20 år og analyserede

Den aktuelle cybertrussel mod Danmark

Agenda

1.00 Trends i en Corona krise
2.00 Phishing, Vishing, Smishing og spear phishing
3.00 Crime as a Service & ransomware
4.00 APT i Danmark 2020
5.00 Gode råd & spørgsmål

Cybercrime

SIS
REST ASSURED

1.00 Trends under en Corona krise

Trends under en Corona krise

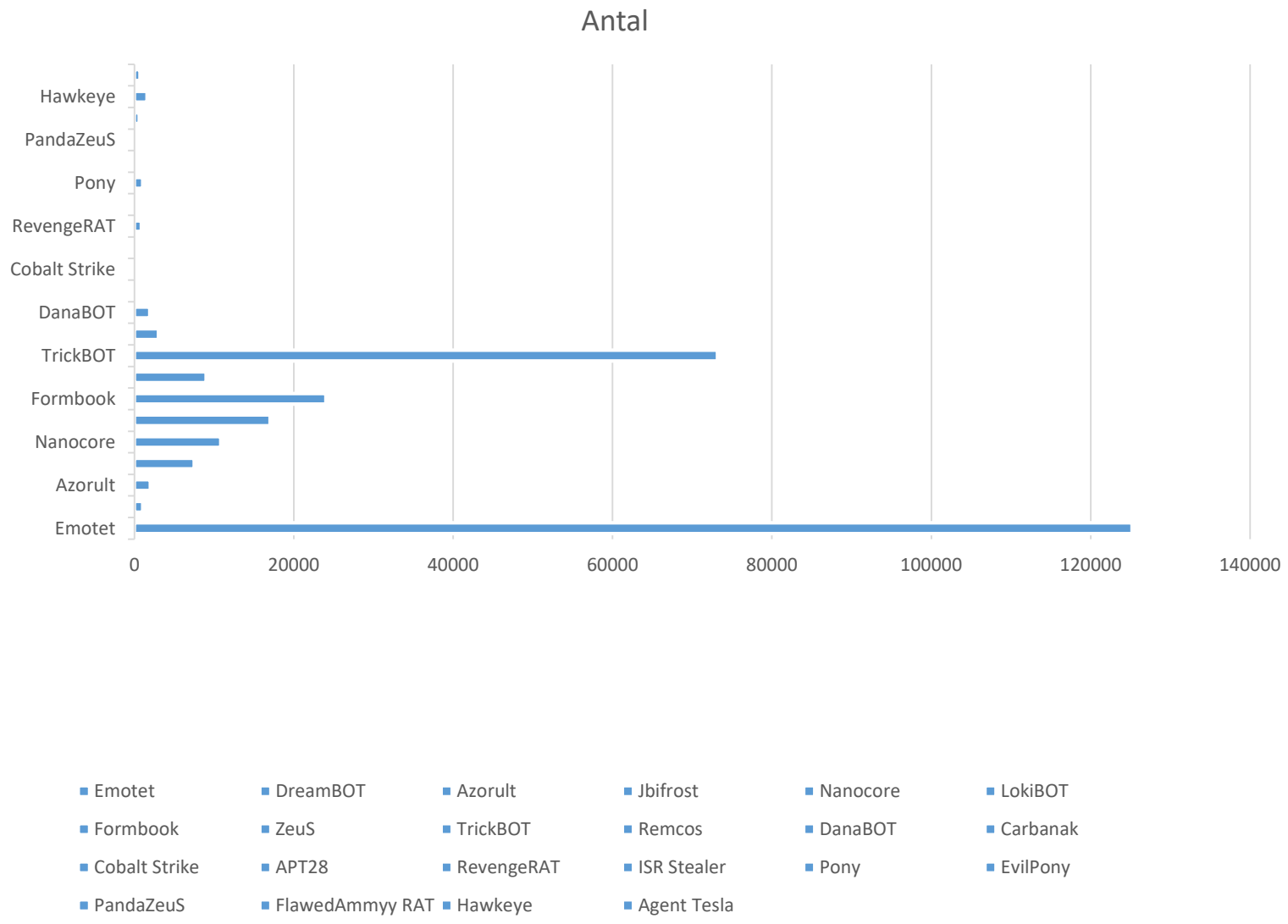
- Vi har vendt det digitale trusselsbillede på hovedet og decentraliseret endpoints
- Som med andre verdensomspændende nyheder, så misbruges sådanne af kriminelle
- I denne fase er både statsaktører og it-kriminelle helt opmærksomme på at vores perimeter er blevet udvidet, og nemmere at penetrere
- Når der arbejdes decentralt, så eksponeres nye services og flere angrebsvinkler introduceres.
- Enhver hjemmearbejdsplads, som er dårligt sikret, kan blive et springbræt ind i et netværk
- End of Life, opdateringer, router, sammenblanding af en masse trafik fra hjem til LAN og wifi konfiguration er en stor udfordring for alle virksomhedstyper
- Der laves phishing og smishing i en hidtil uset grad
- CEO og BEC svindel har kickstartet sommer tendensen

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
- Mindre end 0,5 procent er decideret APT relateret (men vent … det er slemt nok!)

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

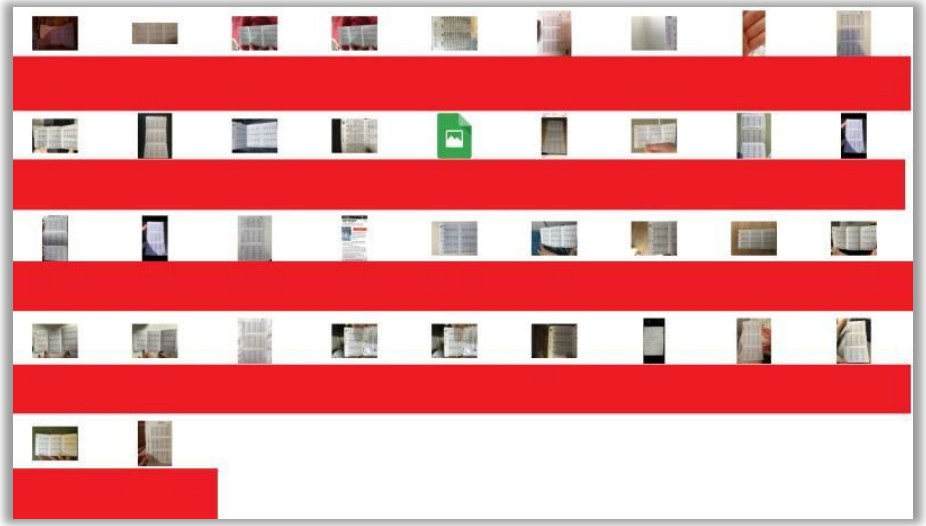


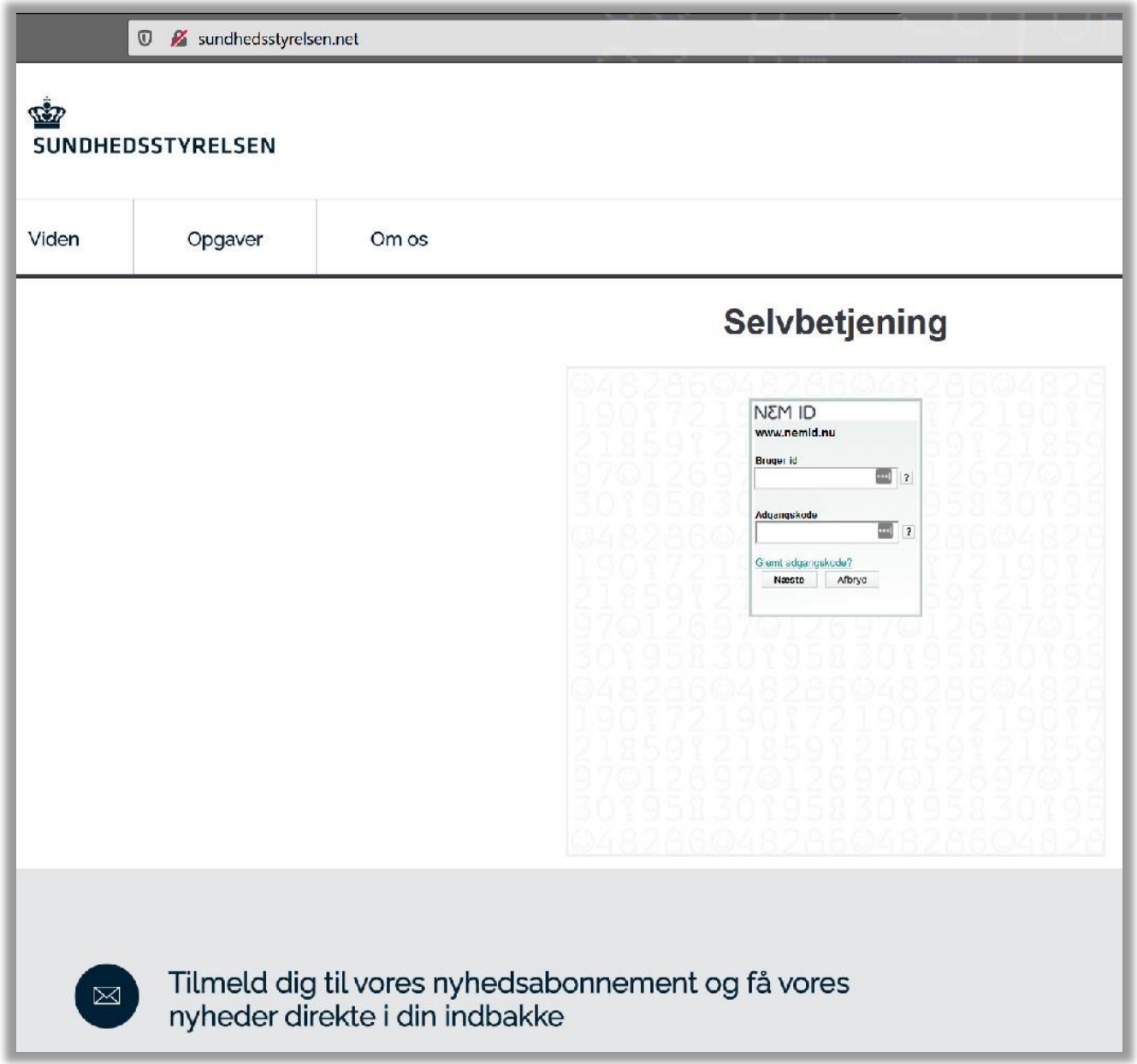
Den aktuelle cybertrussel mod Danmark

REST ASSURED

2.00 Phishing, Vishing, Smishing og spear phishing

Sundhedsstyrelsen misbruges





Spear phishing tricks

Spear phishing

Mærsk misbrugt i leverance af en Gh0stRAT

Wed 04/03/2020 11:03

MAERSK Operations (Customer service) <info@arakaturk.live>

MAERSK shipping notice on Corona Virus Impact

To it@pharmaffiliates.com

Message CoronaVirus impact on Shipment booking.doc (60 KB)

Dear it@pharmaffiliates.com,

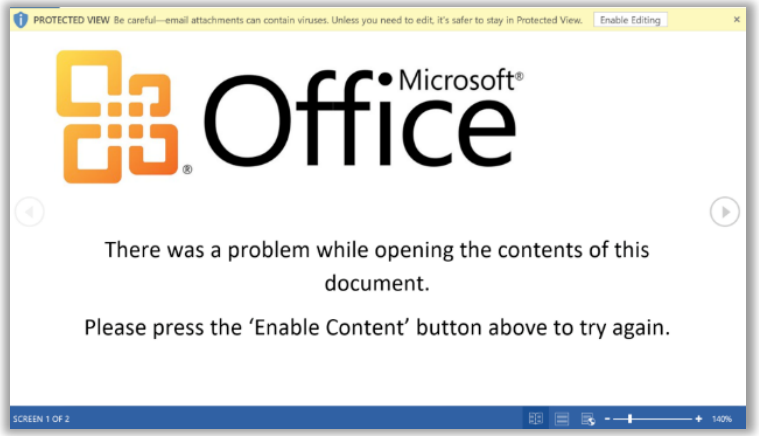
&n=sp;

<=P>

This is MAERSK SHIPPING=LINE. Enclosed is our important notice for Coronavirus and Impact on =ur Shipment booking.
Would you please kindly have=a second to read carefully as it may affect your on hand order lead time a=d your plan for shipment.

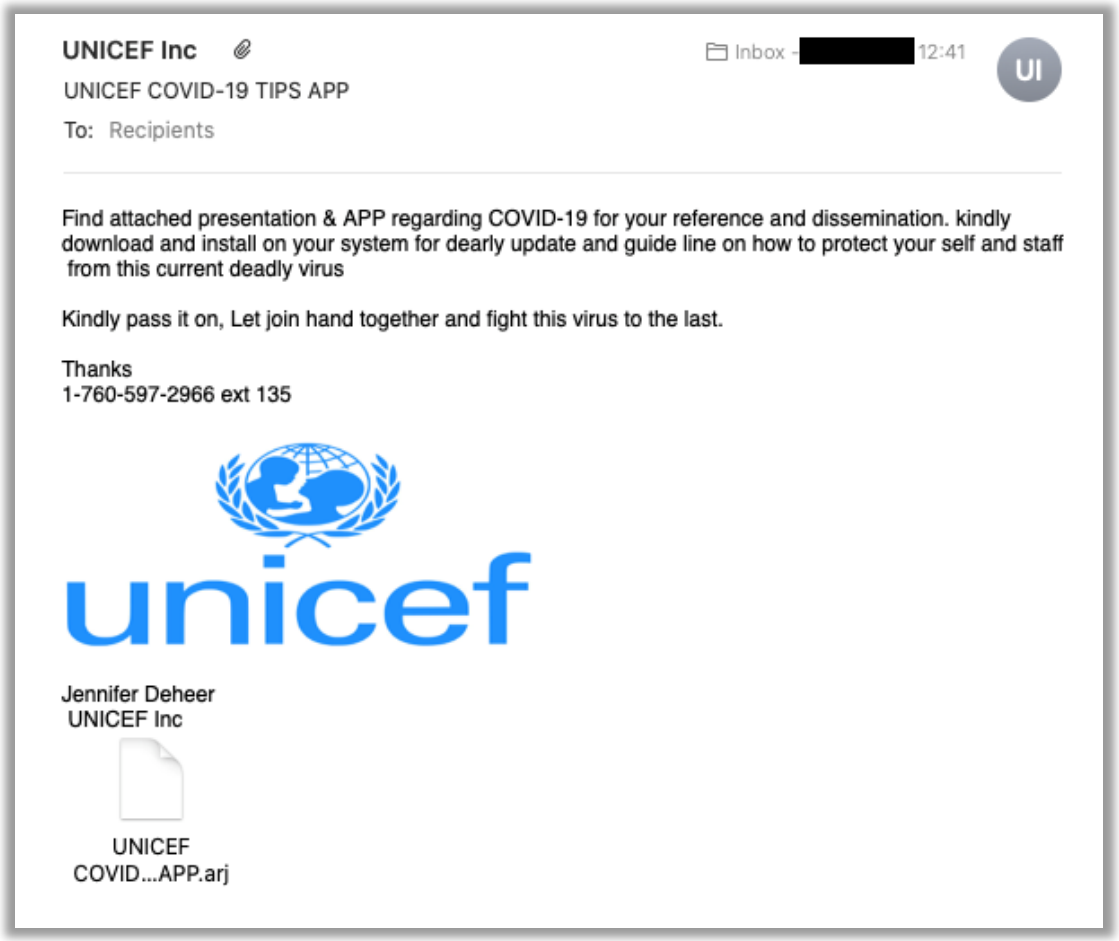
1. *Please note the attac=ed information is of Top Priority.*

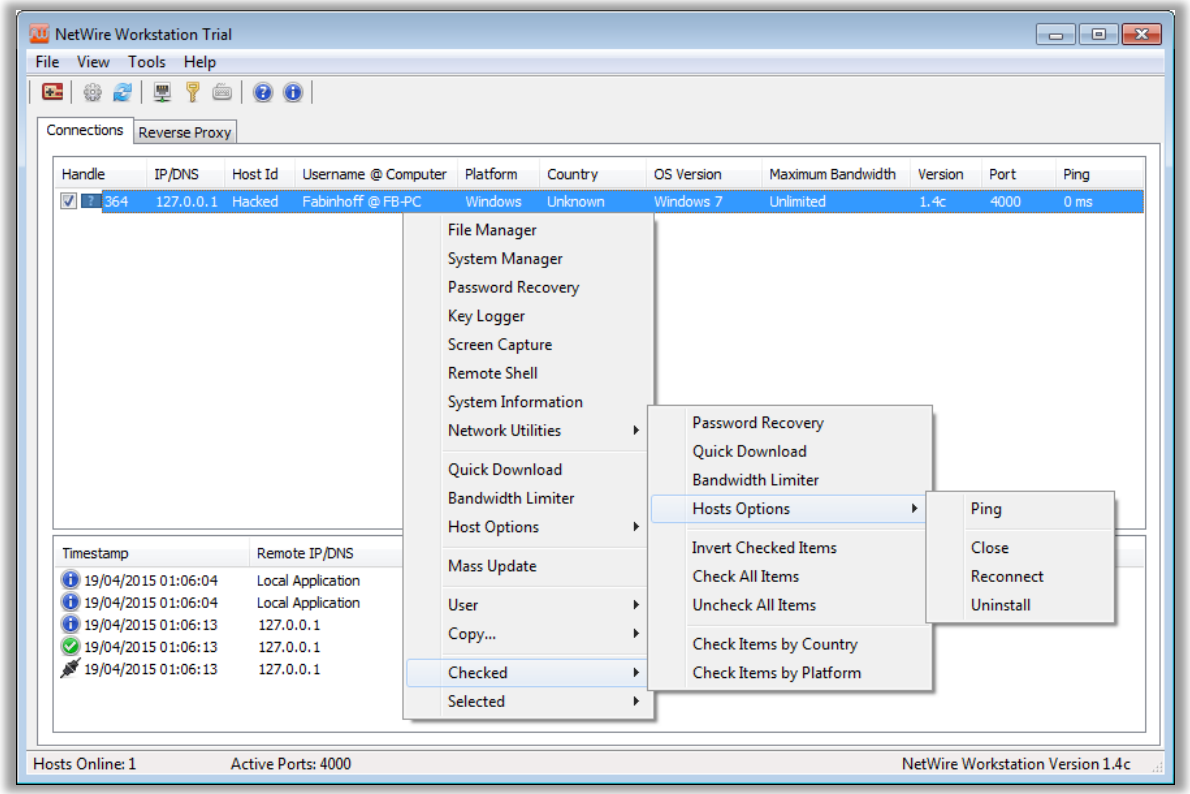
Thanks a=d best regards,
&nb=p;
MAERSK Operations=/SPAN>
SCM Oper=tions | Customer Se=vice | Maersk SCM
MAERSK
Maersk V=etnam Ltd., **Headquarters:** Copenhagen, DenmarkPhone: ~~+84 28 3520~~3871| =eb: ~~www.maersk.com=/SPAN~~>



Spear phishing

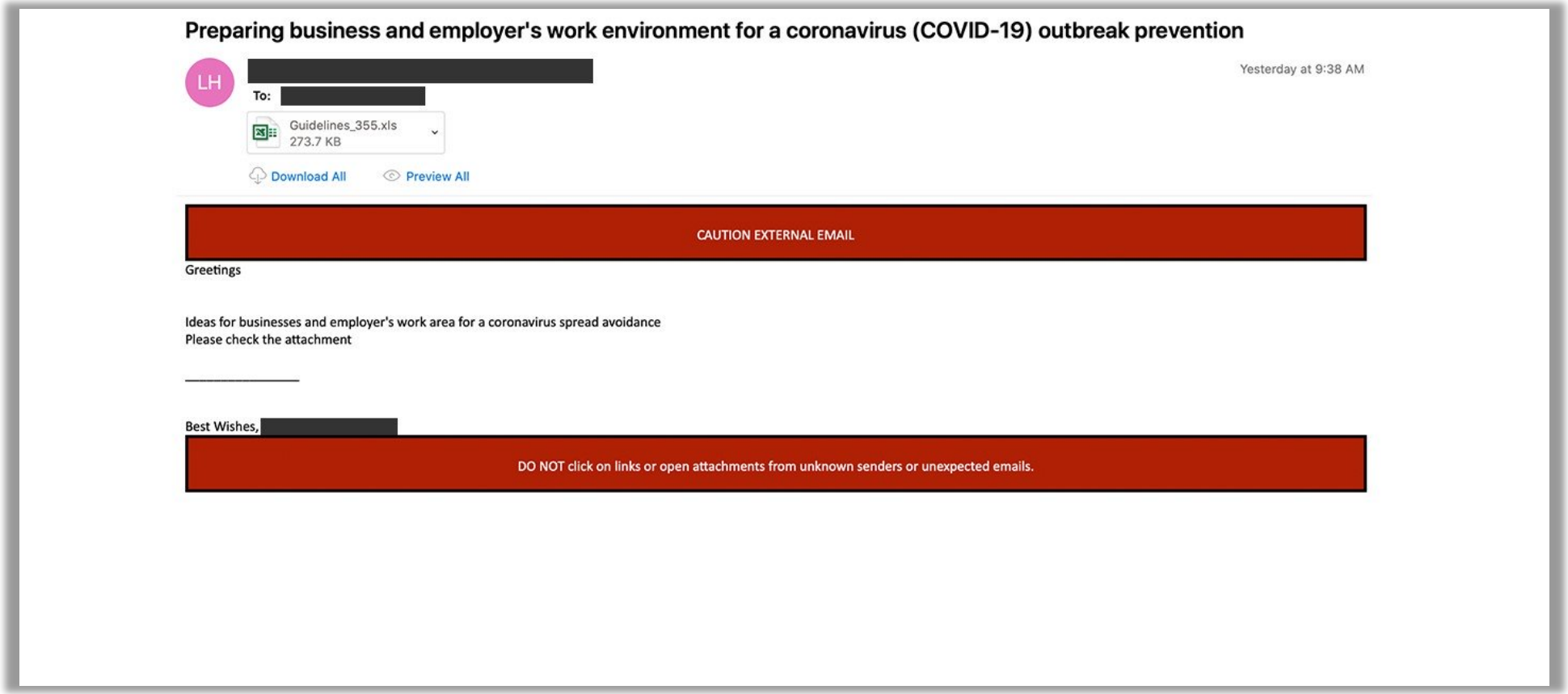
Payload: Netwire RAT





Spear phishing

Denne spear phishing kampagne vil ved åbning af dokumentet, og accept af makro/VBA kørsel, droppe “Zloader” til windows maskinen. Zloader er som navnet antager en første stadie infection som henter og kører – I dette tilfælde – en modificeret udgave af den udødlife datatyv ZeuS.



Spear phishing

Det tredje eksempel anvender også et Covid-19 tema og inkluderer et link som ofret skal klikke på: *http://gbud.webd[.]pl/images/COVID-19-04-01-2020.IMG*

Det pågældende image indeholder en binær fil som ved kørsel vil komproitteret maskinen med en RAT i Nanocore klassen.

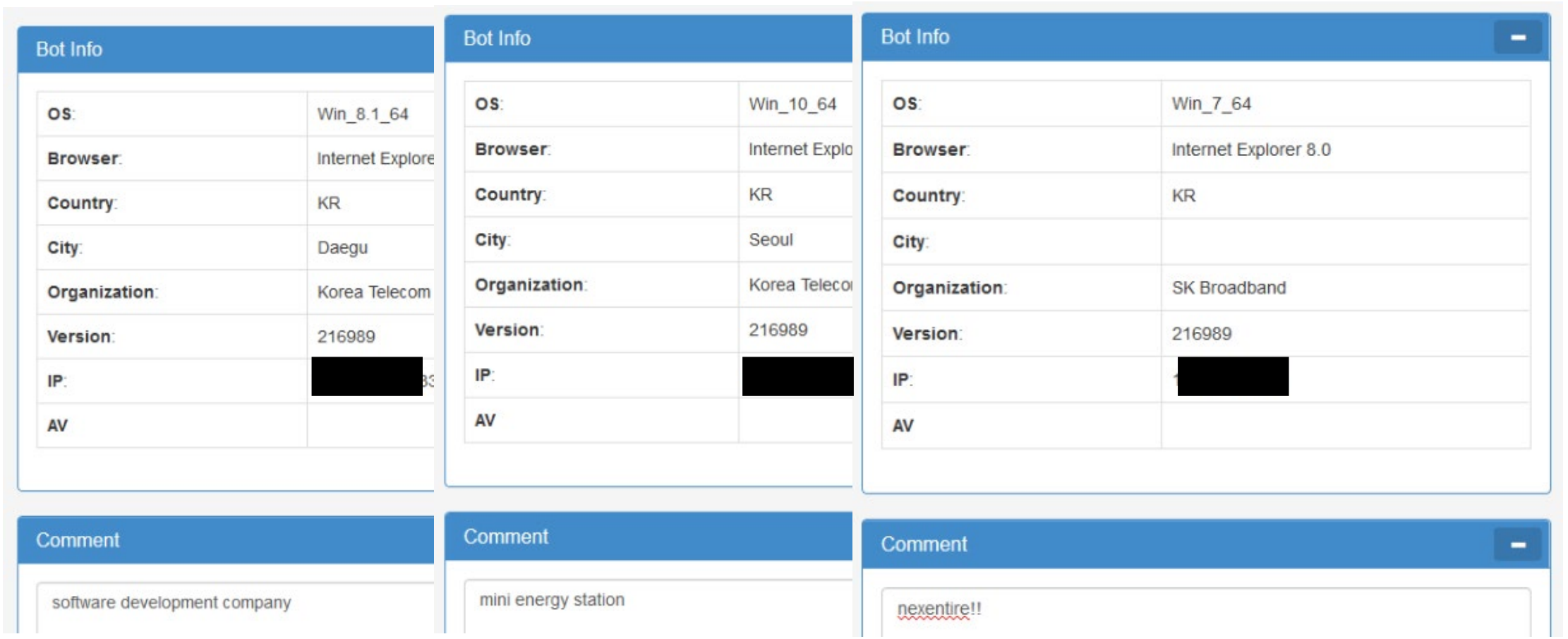
Det aktuelle trusselsbillede

REST ASSURED

3.00 Crime as a Service & ransomware

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

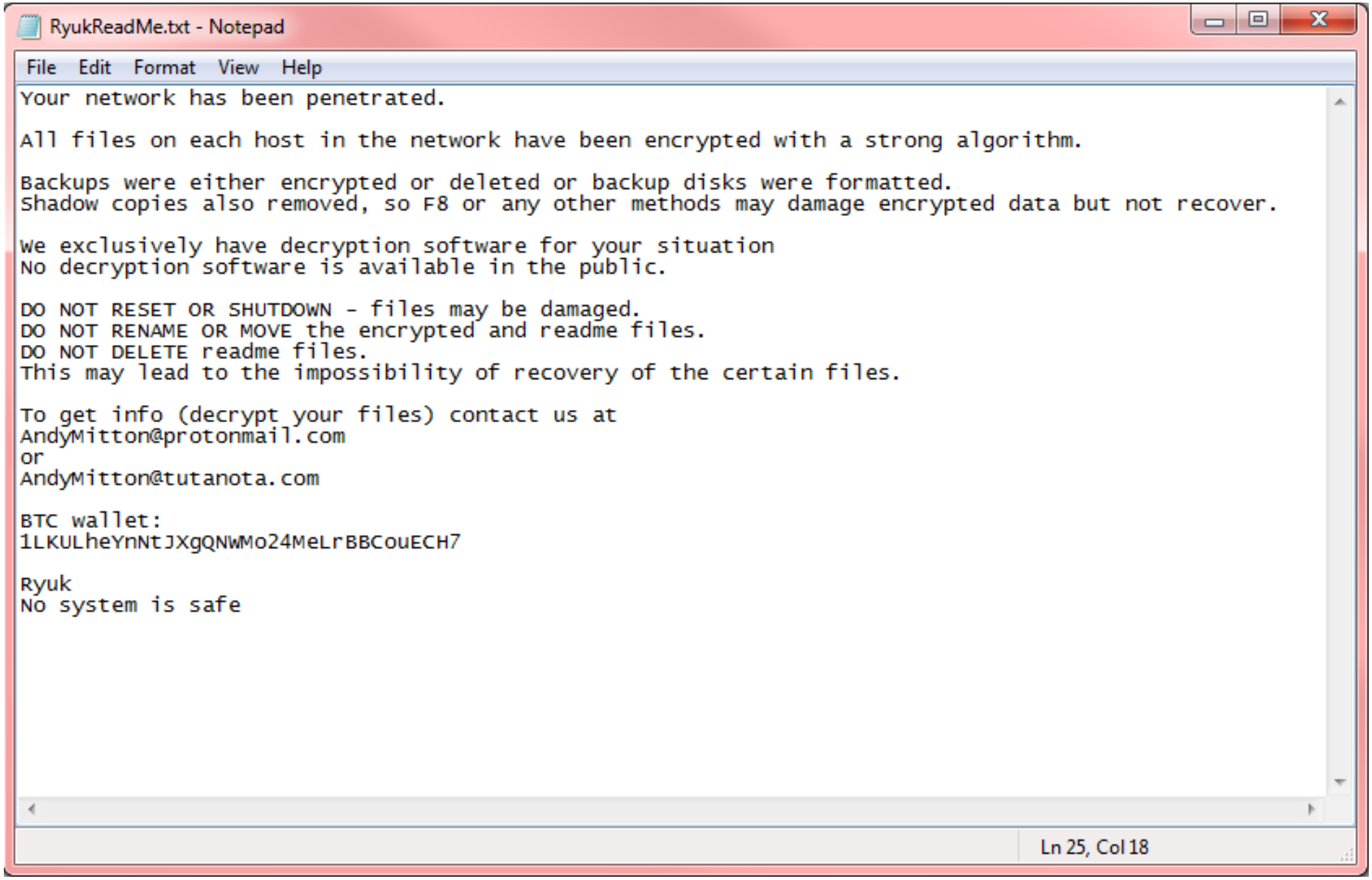
Crime as a Service



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		2018-03-07 19:29:02	Seabeck Pizza ...	details
1068	US	Bozeman	216989	Internet Explorer 8.0	Win_7		2018-03-07 18:19:13	Sacajawea Hotel	details
1070	UA	Kiev	216989	Internet Explorer 8.0	Win_7		2018-03-21 11:27:21	SECRETAR-INCOM	details
1070	UA	Lviv	216989	Internet Explorer 8.0	Win_XP x64 Edition_64		2018-03-21 12:25:21	POS lan - chec...	details
1065	US		216989	Internet Explorer 8.0	Win_10_64		2018-02-26 20:47:18	POS in LAN. Ja...	details
1065	US	New York	216989	Internet Explorer 8.0	Win_10_64		2018-02-26 18:58:03	POS in LAN	details
1052	BG	Pravda	216975	Internet Explorer 8.0	Win_7_64		2017-12-05 15:47:16	POS - check, w...	details
1068	US	Lexington	216989	Internet Explorer 8.0	Win_7_64		2018-02-26 18:57:39	Neillios Gourm...	details
1061	PL	Sopot	216989	Internet Explorer 8.0	Win_7_64		2018-02-14 16:41:31	Naukowa I Akad...	details
1000	BG	Plovdiv	216962	Internet Explorer 8.0	Win_XP		2017-11-28 15:07:13	Municipality o...	details


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

Case story: TrickBOT som elevator

- TrickBOT er en modulbaseret bank trojaner (Crime as a Service) og dele af basekoden udspringer fra forgængeren Dyreza/Dyre
- TrickBOT er særlig farlig da den bl.a. anvendes af ransomware grupper og særligt modulerne:
  worm(32|64)DLL: EternalBlue og EternalRomance. Scanner via IPC og Active Directory samt Net Share

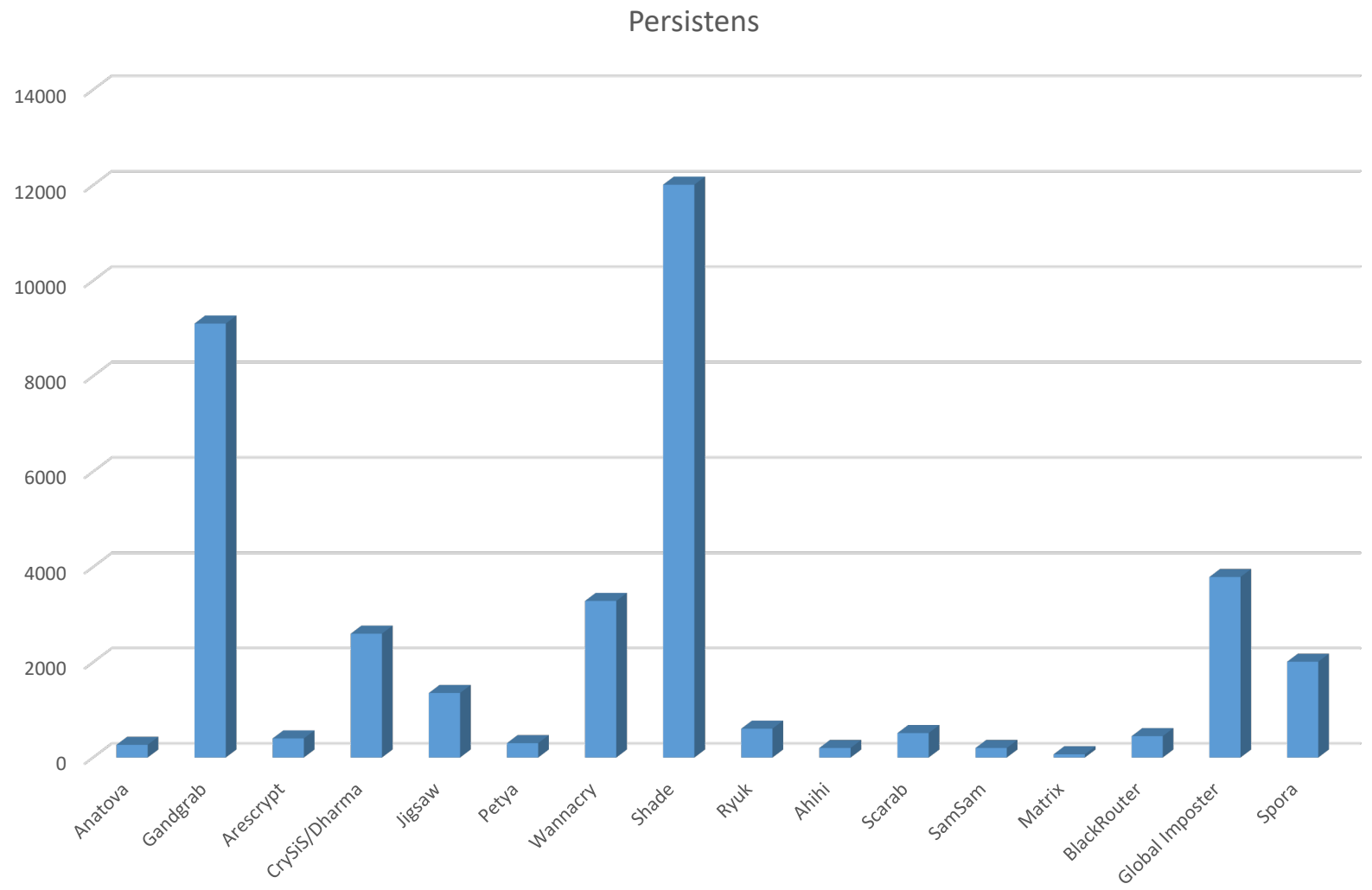
- ”adll(32|64)DLL” er en dumper til Active Directory via API'et "ntdsutil". Dumper endvidere KKM/SMA, HKLM/security samt HKLM/System. Dumps droppes lokalt og transporteres krypteret til C&C

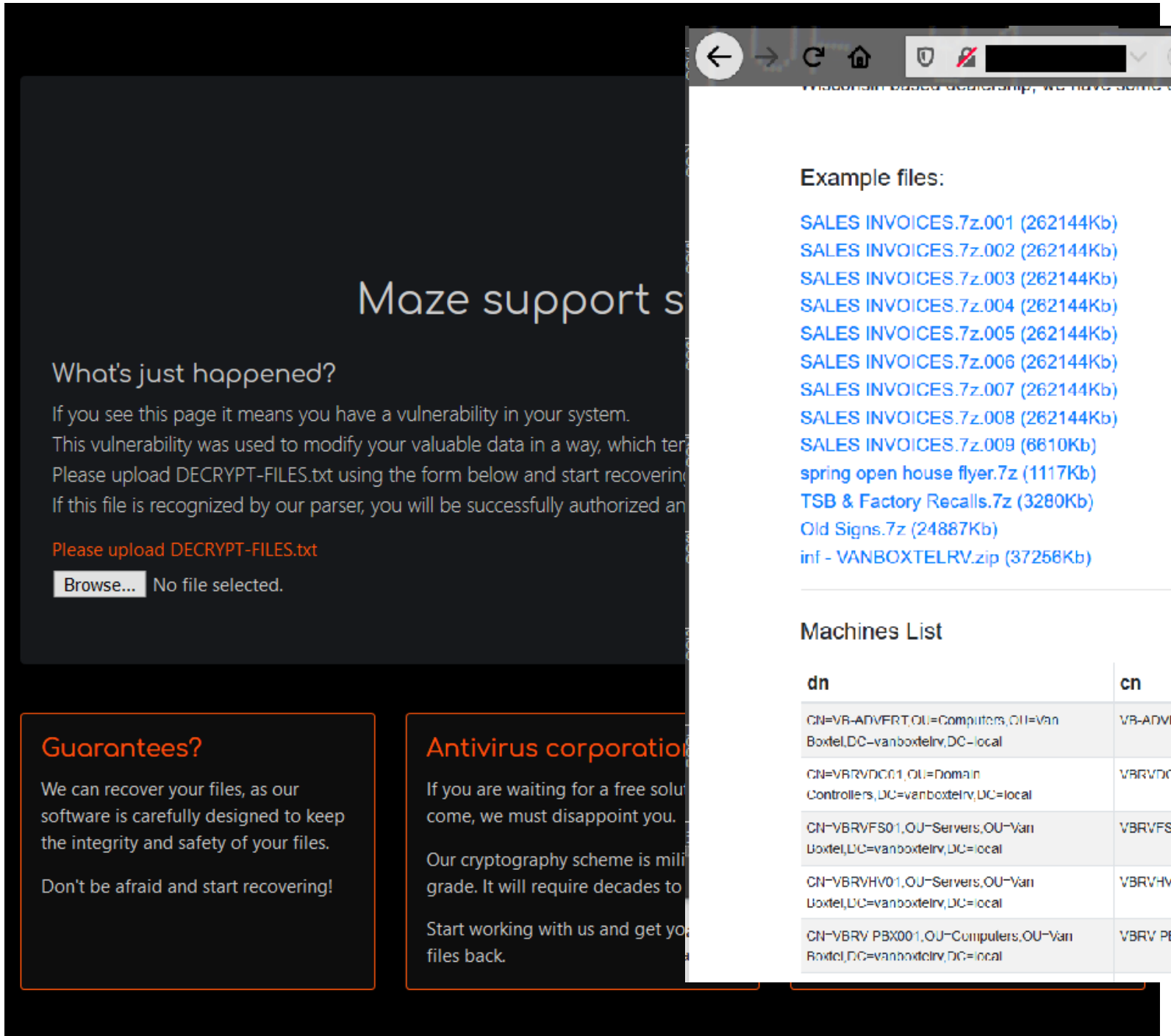
- ”network(32|64)DLL”: Netværk grabber
- ”domain(32|64) DLL”: Domæne grabber
- ”psfinDll(32|64)DLL”: Point-of-Sale grabber

[...]

Ransomware

Ransomware	Antal
Maze	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





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)

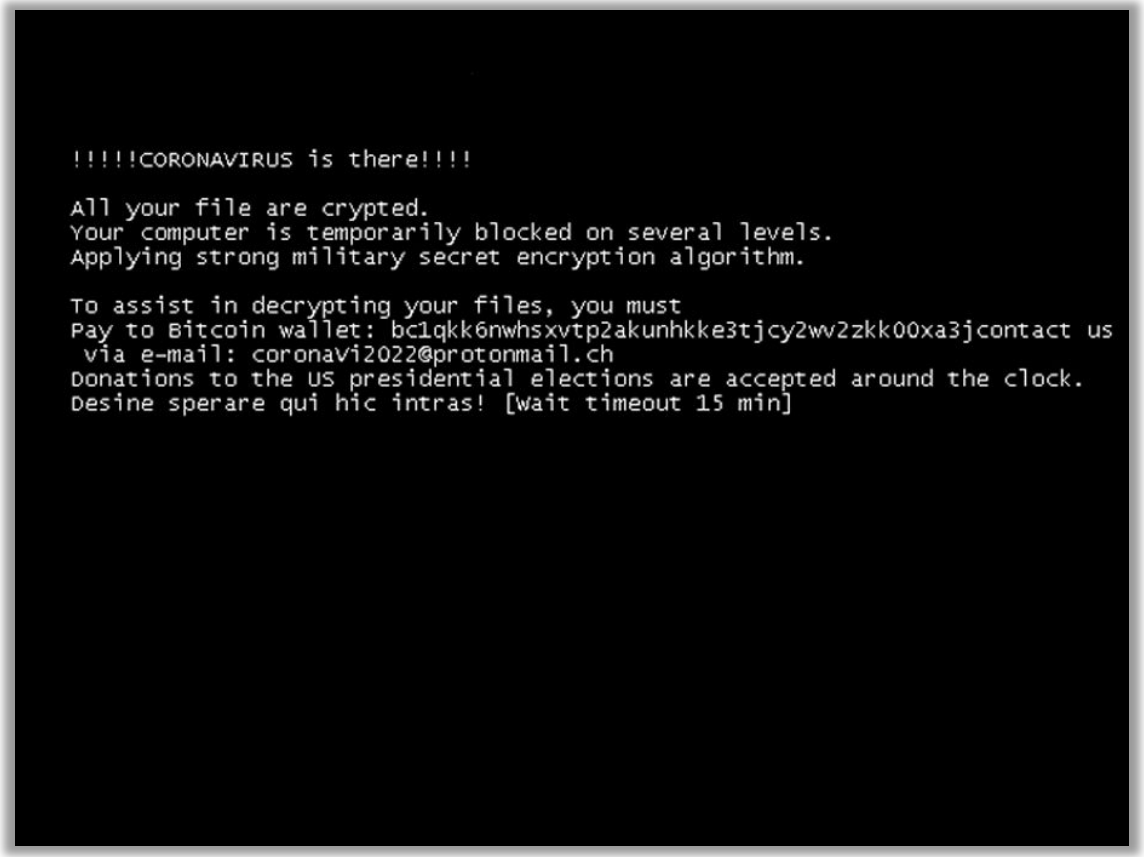
Machines List

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

teret

Ransomware

CORONAVIRUS (ransomware og datatyv)



Associated Files:

```
CoronaVirus.txt
```

Associated emails:

```
coronaVi2022@protonmail.ch
```

Ransom Note text:

```
                        CORONAVIRUS is there
                    All your file are crypted.
          Your computer is temporarily blocked on several levels.
           Applying strong military secret encryption algorithm.

To assist in decrypting your files, you must do the following:
1. Pay 0.008 btc to Bitcoin wallet bc1q8r42fm7kwg68dts3w70qah79n5emt5m76rus5u
or purchase the receipt Bitcoin;
2. Contact us by e-mail:  and tell us this your
unique ID: 94C492AD07F35492DA90CAAA25986929
and send the link to Bitcoin transaction generated or Bitcoin check number.
After all this, you get in your email the following:
1. Instructions and software to unlock your computer
2. Program - decryptor of your files.
Donations to the US presidential elections are accepted around the clock.
Desine sperare qui hic intras! [Wait to payment timeout 25 - 40 min]
```

Det aktuelle trusselsbillede

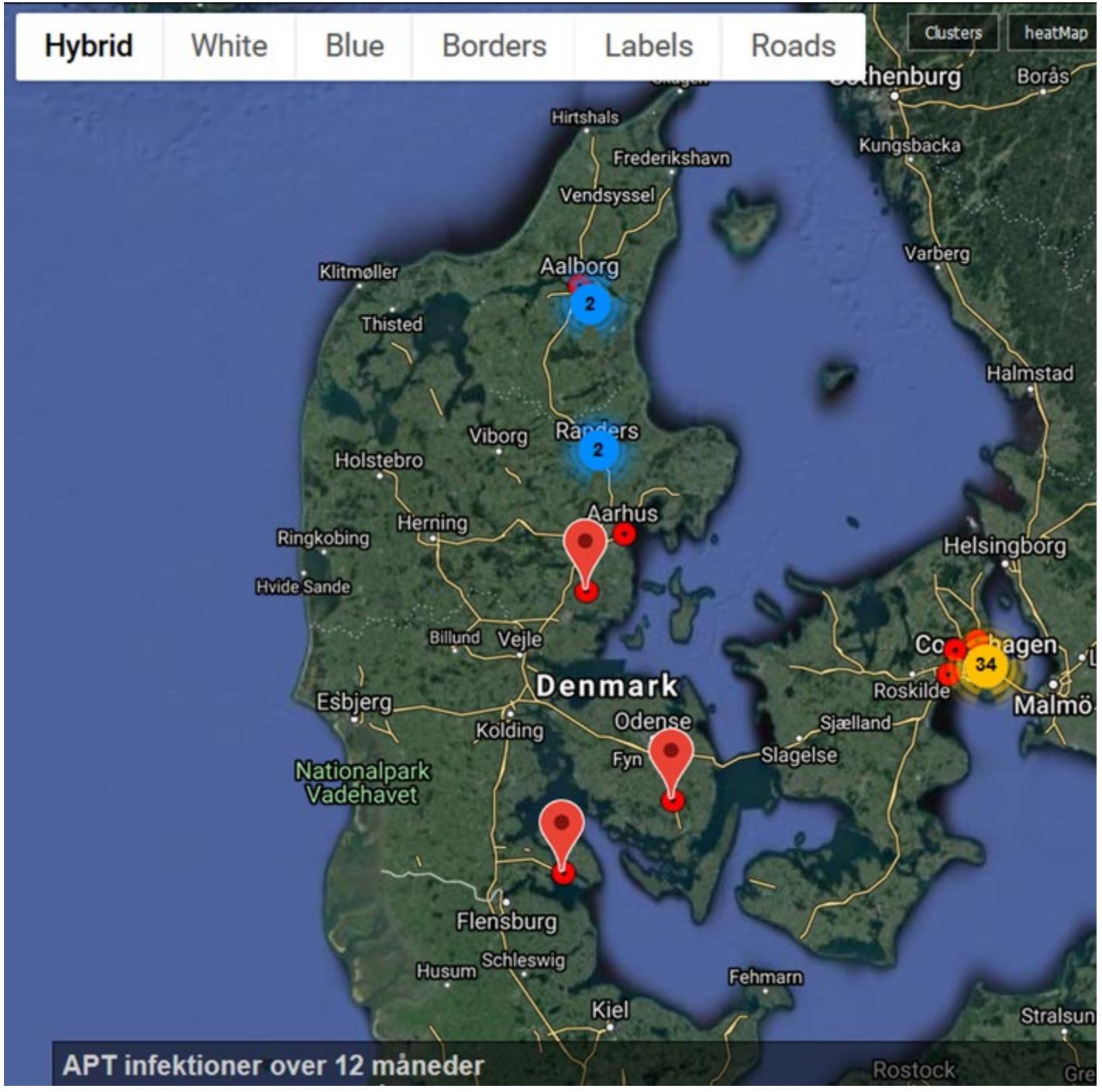
REST ASSURED

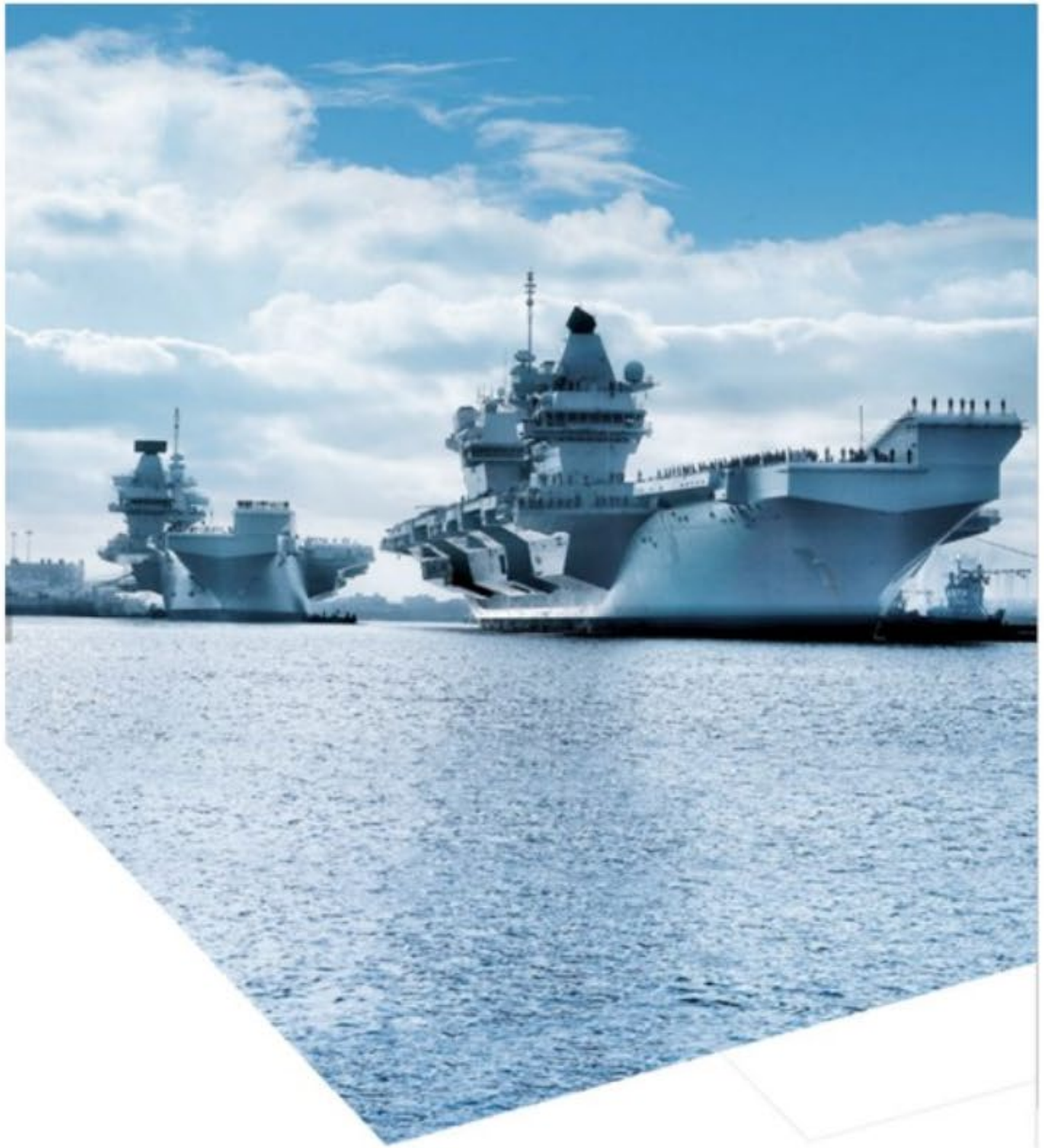
4.00 APT i Danmark 2020

APT i Danmark 2020

- Vi ser en stigning i APT aktivitet rettet mod infrastruktur og samfundskritiske funktioner og installationer
- Alene i 2020 kan vi, via vores unikke CSIS TI services bekræfte +20 succesfulde angreb
- APT familier observeret i relation til kampagner mod Danmark over 12 måneder omfatter følgende APT klasser:

- Stuxnet (legacy – oprydning savnes)
- DarkHotel
- APT1
- Pitty Tiger
- DoubleFantasy
- EquationDrug
- Dark Wetter (DK kampagne)
- FIN6/7
- Dino
- Black Vine
- TripleFantasy
- Putty Panda
- Carbanak
- Cobalt Strike
- APT28
- Comfoo


Hybrid
White
Blue
Borders
Labels
Roads
Clusters
heatMap
Hirtshals
Frederikshavn
Vendsyssel
Klitmøller
Aalborg
2
Thisted
Viborg
Randers
2
Holstebro
Herning
Aarhus
Ringkobing
Hvide Sande
Billund
Vejle
Denmark
Esbjerg
Kolding
Odense
Fyn
Nationalpark
Vadehavet
Flensburg
Husum
Schleswig
Kiel
Fehmarn
Kungsbacka
Varberg
Halmstad
Helsingborg
34
Roskilde
Malmö
Sjælland
Slagelse
Borås
Rostock
APT infektioner over 12 måneder



Description 2020

BAE Systems plc

BAE SYSTEMS

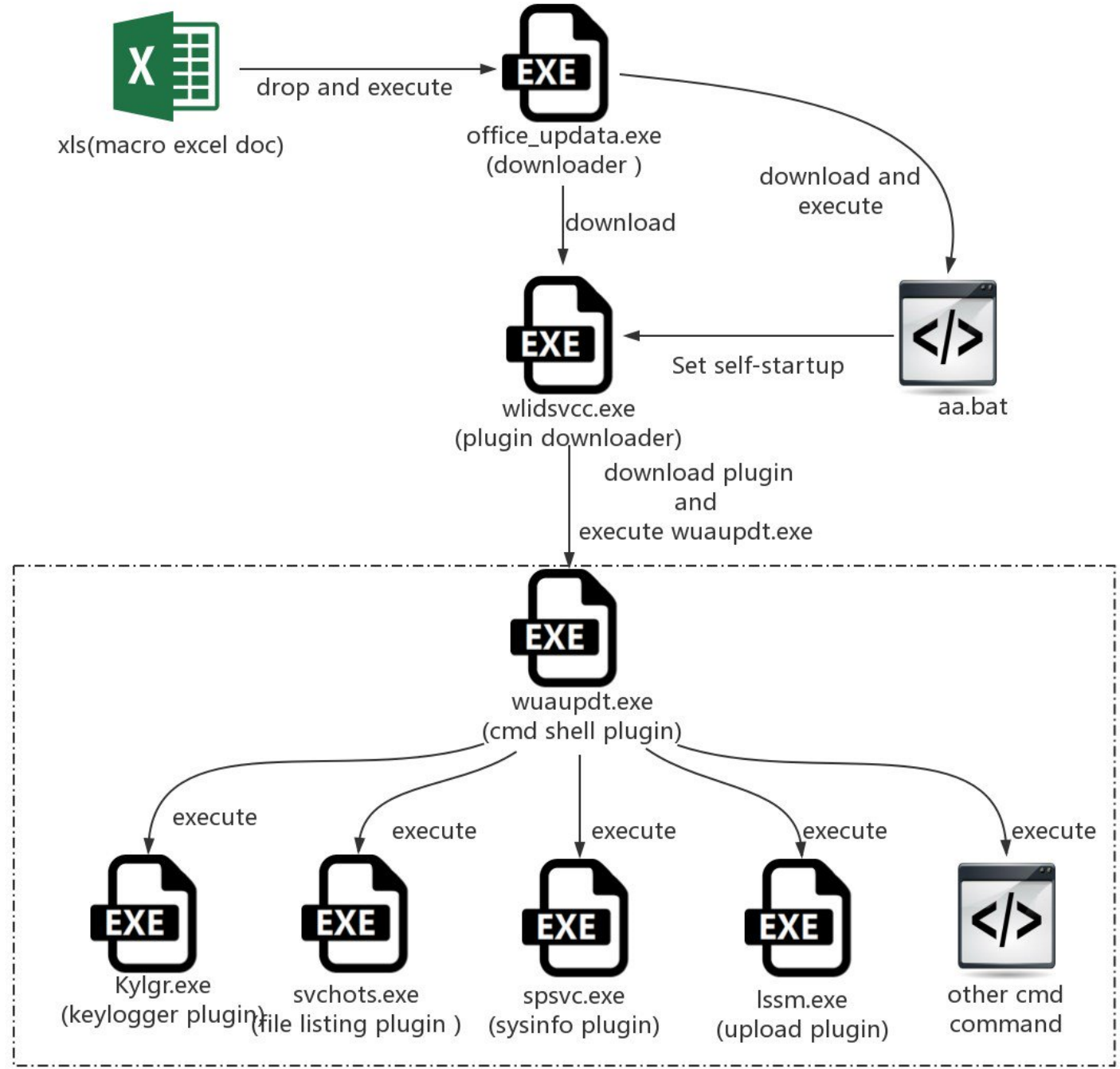
Senior Design Engineer

Job Location: London, UK
Employment Type: Full Time
Clearance Level Must Currently Possess: None
Clearance Level Must Be Able to Obtain: None
Telecommuting Options: Some Telecommuting Allowed
Annual Salary: $150k - $240K

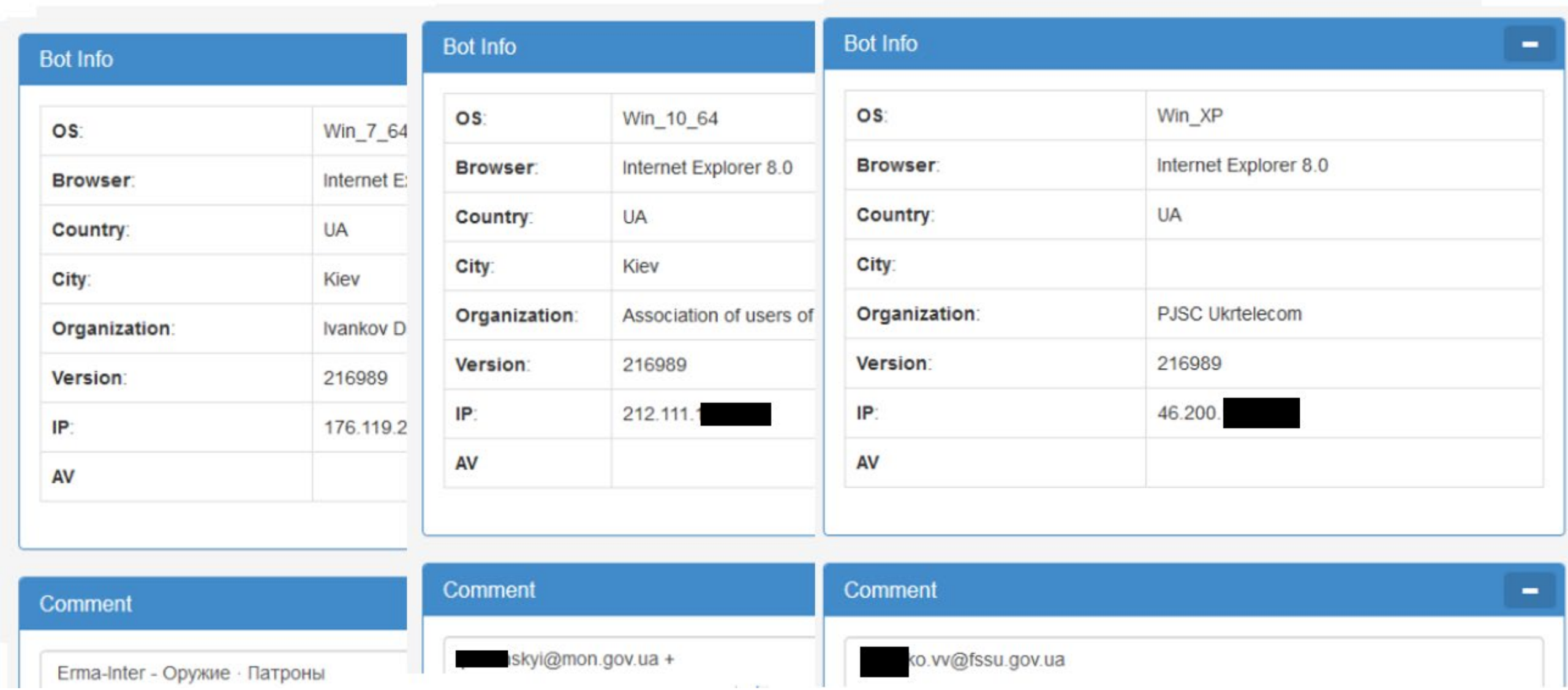
What we are made of

We are looking for experienced Senior Design Engineers to join our team following continuous growth and success in the UK Government and Law Enforcement sectors based in London. Behind great solutions there are great people: our employees. We pride ourselves on being able to solve some of our customers' most complex problems. Our people are what differentiate us, they are ingenious, innovative and dedicated. We have a mix of generalists and specialists and recognize that this diversity contributes to our success. In general, we work in teams. We recognize the benefits of forming teams from a mix of disciplines, which allows us to come up with balanced, high quality solutions.

We work hard and often go the extra mile, but we recognize people's efforts and that everyone has a life outside of work. We encourage people to speak up if they want to rotate to a new project in support of career development, or even just to face a new challenge. Our breadth across the UK Government and Law Enforcement sectors provides diverse opportunities for our people to develop their careers in new areas of expertise or with new clients.


drop and execute
xls(macro excel doc)
office_updata.exe
(downloader)
download and
execute
download
Set self-startup
aa.bat
wlidsvcc.exe
(plugin downloader)
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 i Danmark 2020 og trends



Bot Info

OS:	Win_7_64
Browser:	Internet E:
Country:	UA
City:	Kiev
Organization:	Ivankov D
Version:	216989
IP:	176.119.2
AV:	

Bot Info

OS:	Win_10_64
Browser:	Internet Explorer 8.0
Country:	UA
City:	Kiev
Organization:	Association of users of
Version:	216989
IP:	212.111.[redacted]
AV:	

Bot Info

OS:	Win_XP
Browser:	Internet Explorer 8.0
Country:	UA
City:	
Organization:	PJSC Ukrtelecom
Version:	216989
IP:	46.200.[redacted]
AV:	

Comment

Erma-Inter - Оружие · Патроны

Comment

[redacted]skyi@mon.gov.ua +

Comment

[redacted]ko.vv@fssu.gov.ua

Den aktuelle cybertrussel mod Danmark

CSIS
REST ASSURED

6.00 Opsamling og gode råd

Gode råd /opsummering

- Udvis sund fornuft. Klik ikke ukritisk på materiale som kommer uopfordret
- Sørg for at holde alt dit udstyr opdateret
- Etablerer en sikkerhed praksis omkring fjernsupport
- Tag backup – glem ikke clouden
- Endpoint sikkerhed (AV, FW, policies)
- Genbrug aldrig password. Vælg et godt password og evt 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 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.)
- Indtast aldrig sensitive oplysninger på en offentlig maskine

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