Den usynlige fjende
- Cyberangreb

GoLearn, 2026

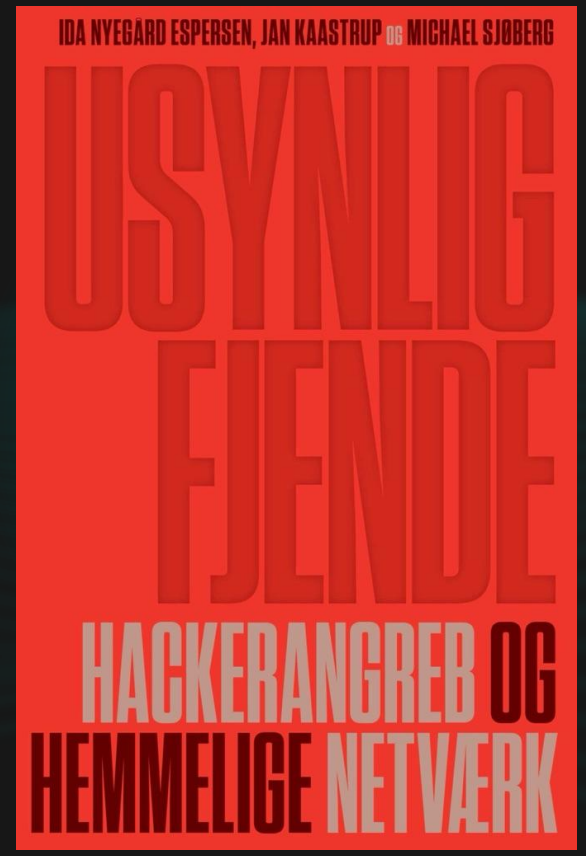
Jan Kaastrup - CIO, CSIS

Profil og baggrund

Jan Kaastrup

Chief Information Officer (CIO) og cybersikkerhedsekspert

1. Mere end 25 års erfaring med analyse af cybertrusler og avancerede cyberangreb
2. Rådgiver organisationer om at forstå og håndtere komplekse cybertrusler
3. Fokus på statsstøttede aktører, cyberkriminelle grupper, hybridkrigsførelse og informationspåvirkning
4. Medforfatter til Usynlig fjende



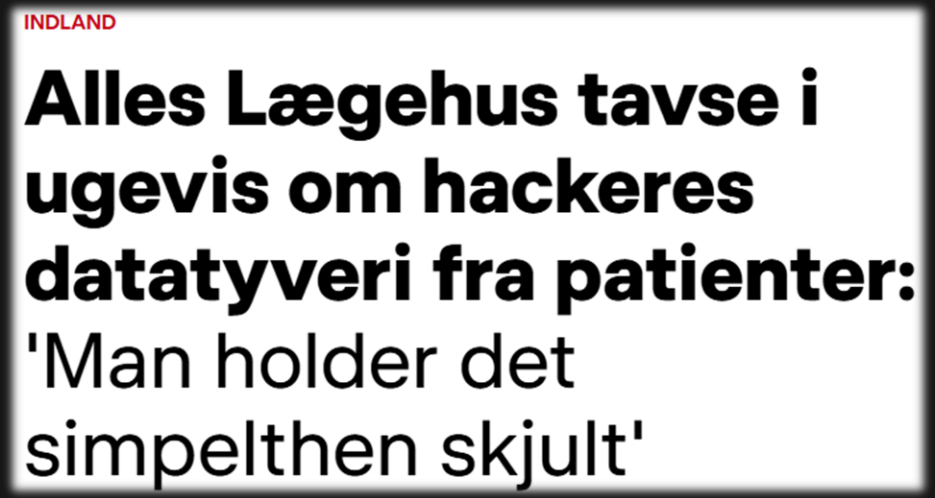
Dagsorden

1. Trusselsbilledet
2. Pause
3. Gennemgang af ransomware-sag
4. Centrale læringspunkter og anbefalinger

1. Det aktuelle trusselsbillede

Vi er under angreb

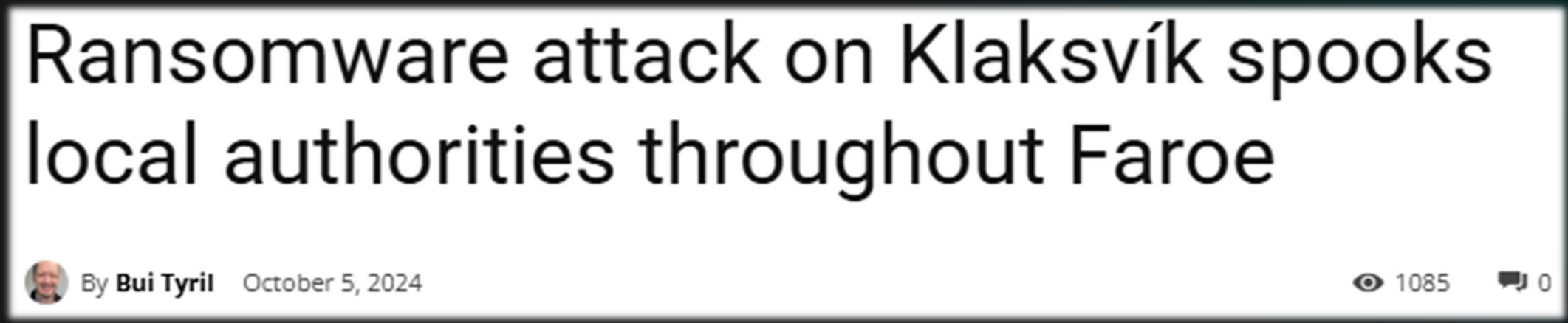
ALLE SEKTORER RAMMES


INDLAND

Alles Lægehus tavse i ugevis om hackeres datatyveri fra patienter: 'Man holder det simpelthen skjult'


Softwareleverandør til det offentlige er blevet ramt af omfattende ransomwareangreb

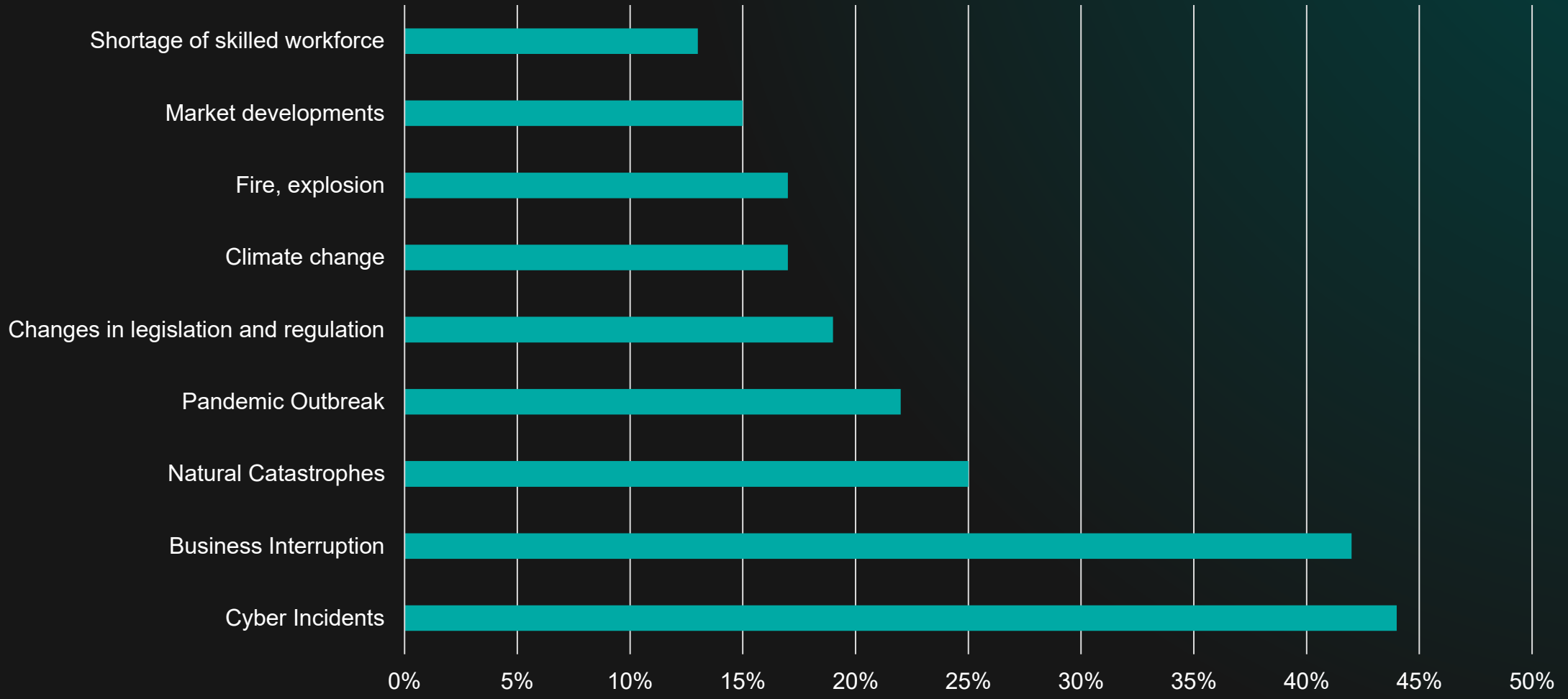
Cyberkriminalitet | 28. november 2024 kl. 10:45


Ransomware attack on Klaksvík spooks local authorities throughout Faroe

By **Bui Tyril** October 5, 2024 1085 0

Den væsentligste forretningsrisiko

CYBERANGREB



DE TRE TRUSSELAKTØRER I CYBERSPACE

Hacktivister

— Politiske Motiver —

Cyberkriminelle

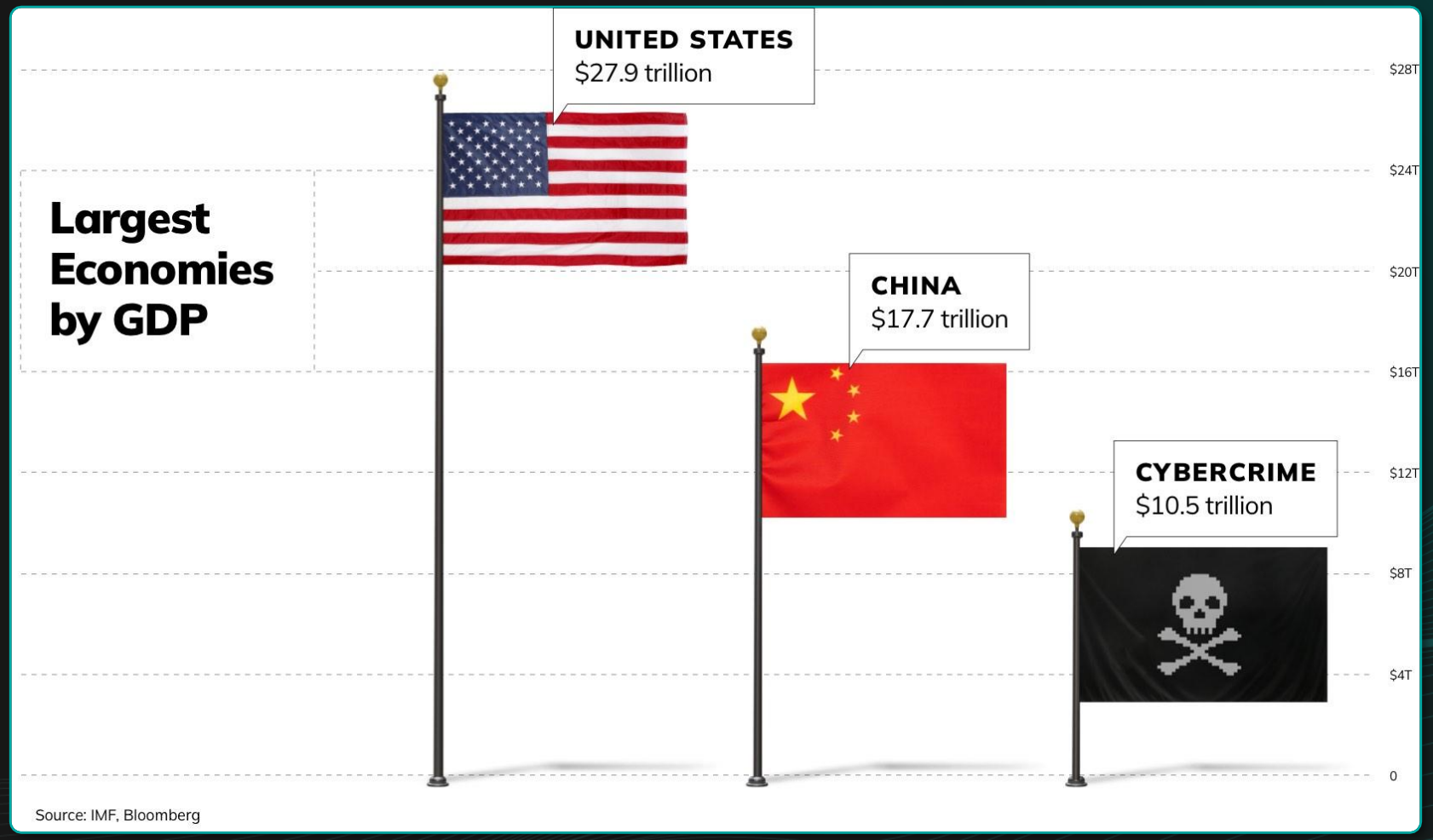
— Økonomisk Gevinst —

Statssponsoreret

— Nationale Interesser —

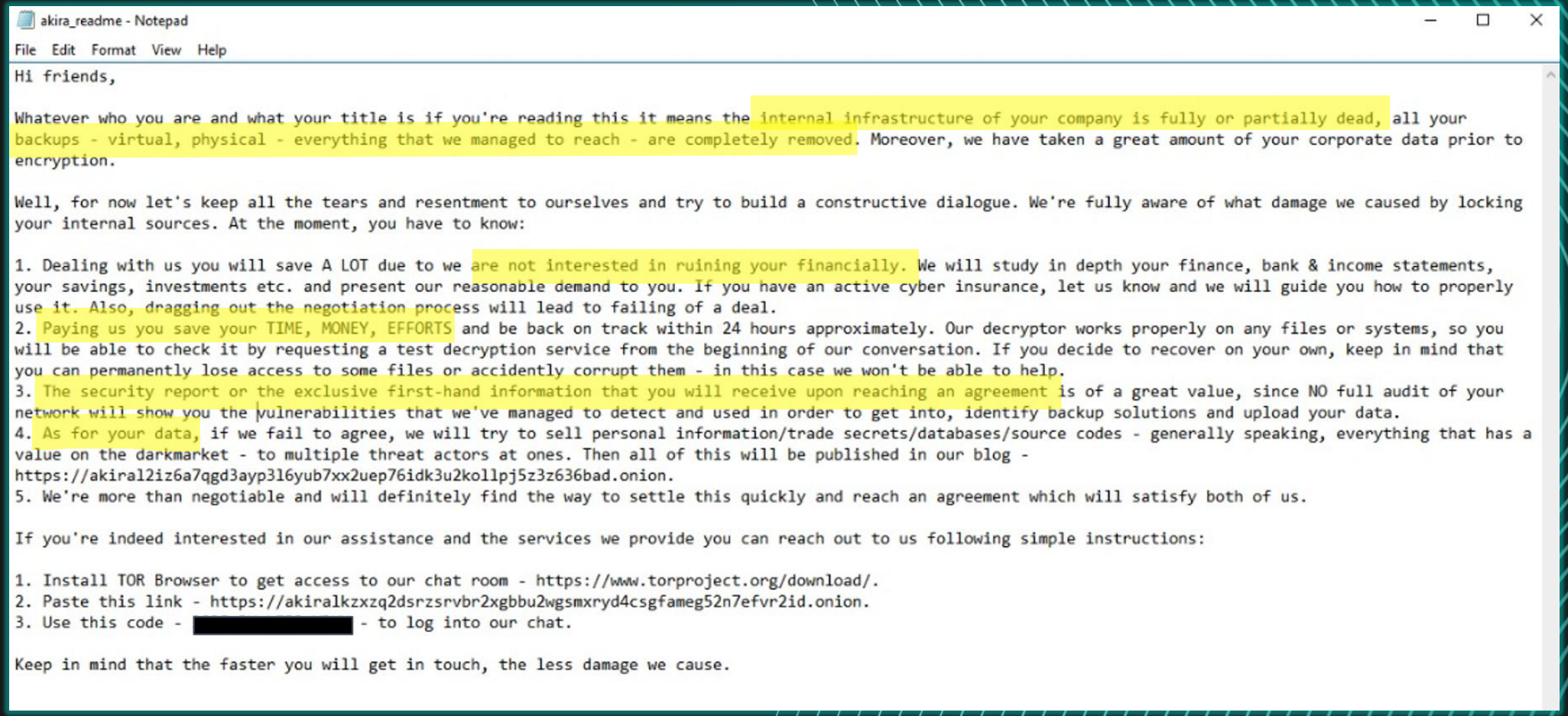
Cyberkriminalitet

VERDENS TREDJESTØRSTE ØKONOMI



Hvem er den usynlige fjende?

PRÆSENTATION



akira_readme - Notepad

File Edit Format View Help

Hi friends,

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal.
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files or accidently corrupt them - in this case we won't be able to help.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data.
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog - https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion.
5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:

1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.
2. Paste this link - https://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion.
3. Use this code - [redacted] - to log into our chat.

Keep in mind that the faster you will get in touch, the less damage we cause.

Hvilke ydelser tilbyder de?

OVERSIGT OVER YDELSER

We

> We're preparing the list of files currently and will be done in an hour. We offer:

1) full decryption assistance;

2) evidence of data removal;

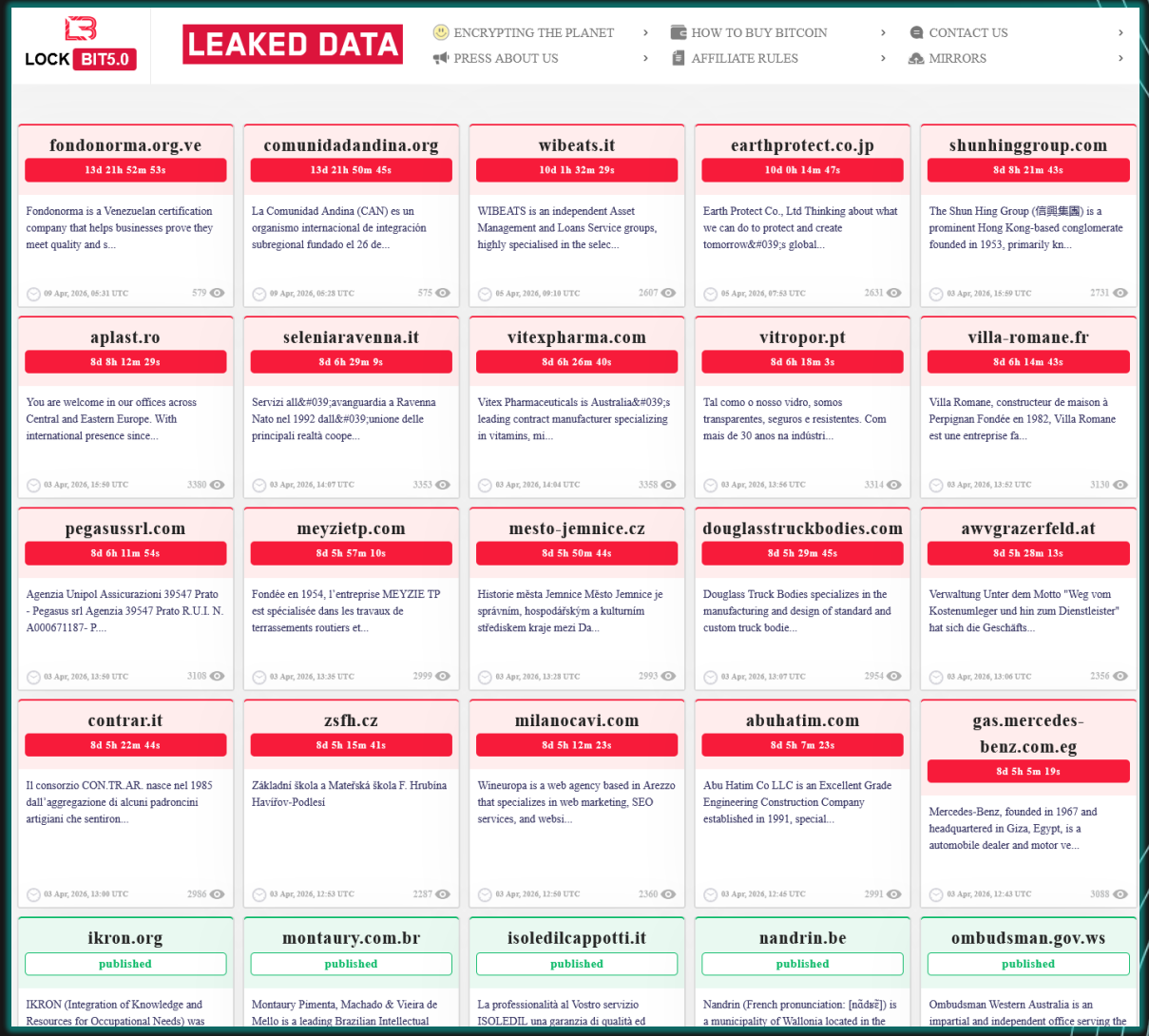
3) security report on vulnerabilities we found;

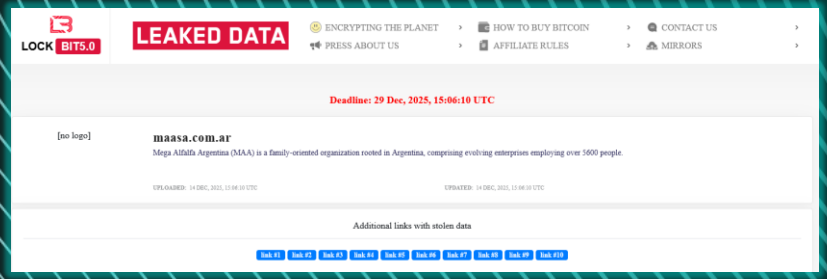
4) guarantees not to publish or sell your data;

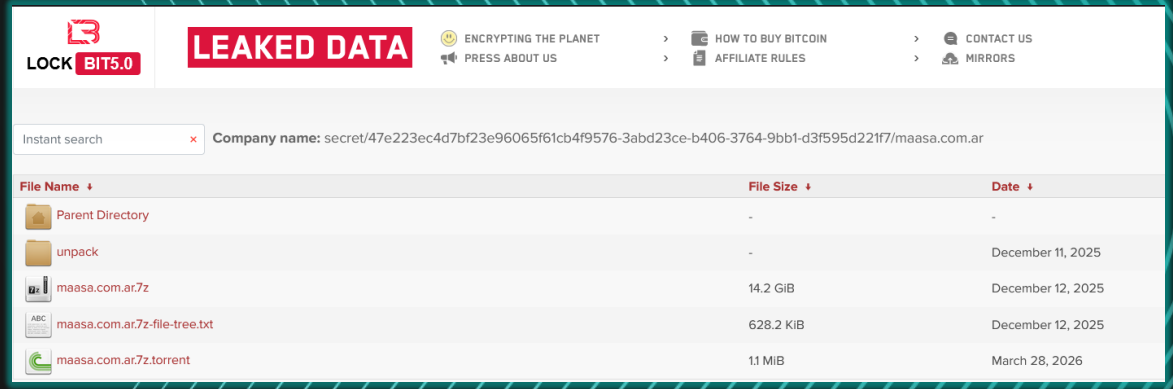
5) guarantees not to attack you in the future.

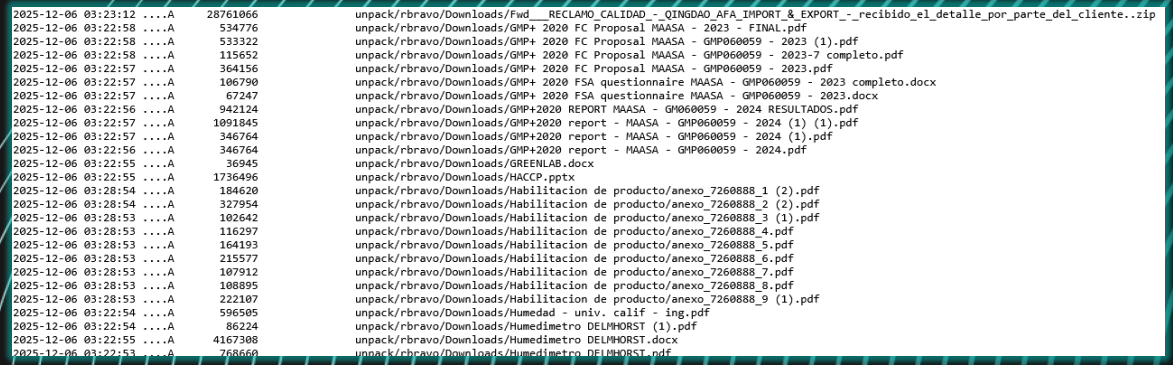
Let me know whether you're interested in a whole deal or in parts. This will affect the final price.

Hvordan gennemfører de afpresning?







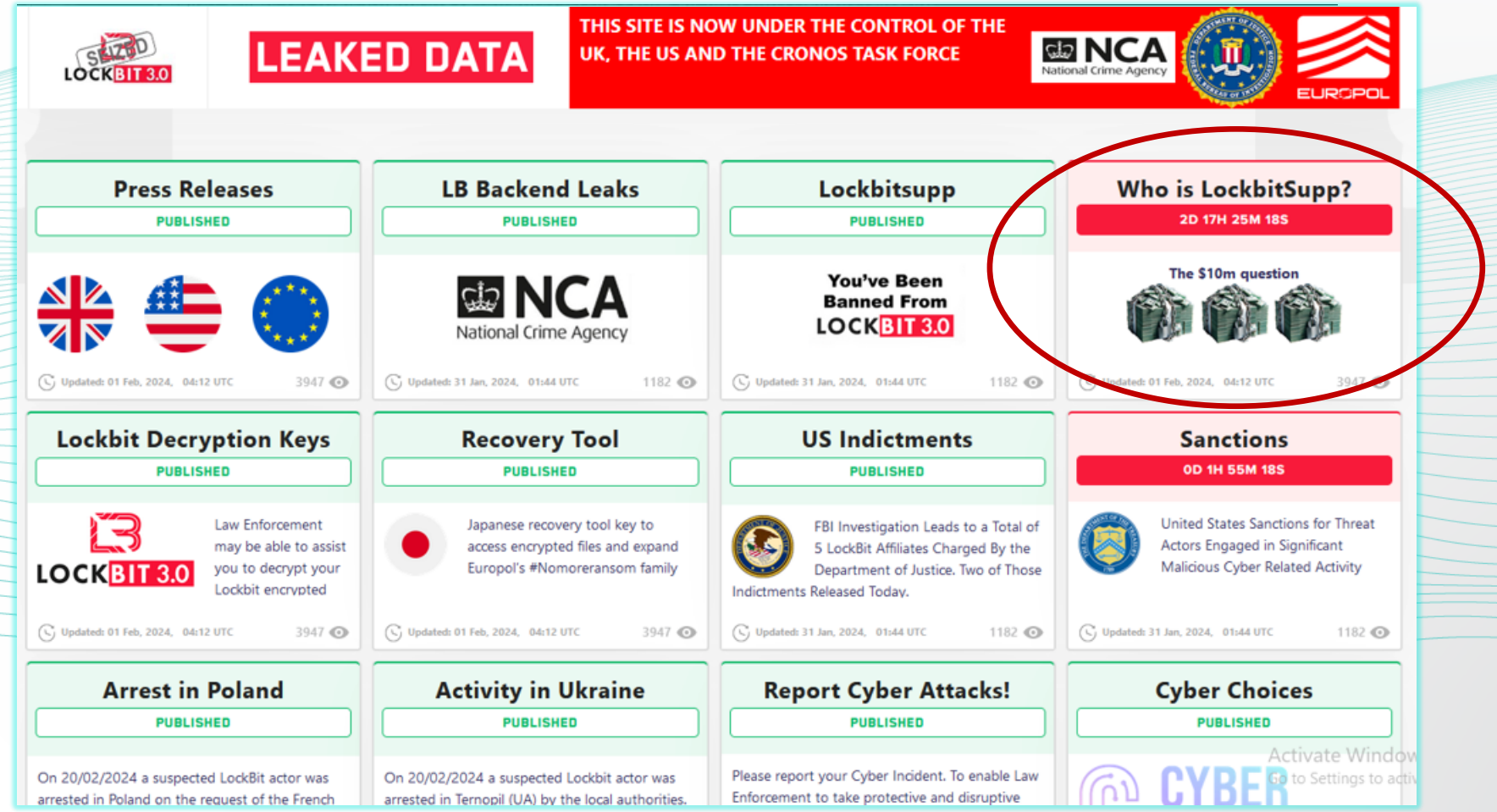


Hvordan arbejder politiet?

UTRADITIONELLE METODER ANVENDT AF EUROPOL, NCA OG FBI

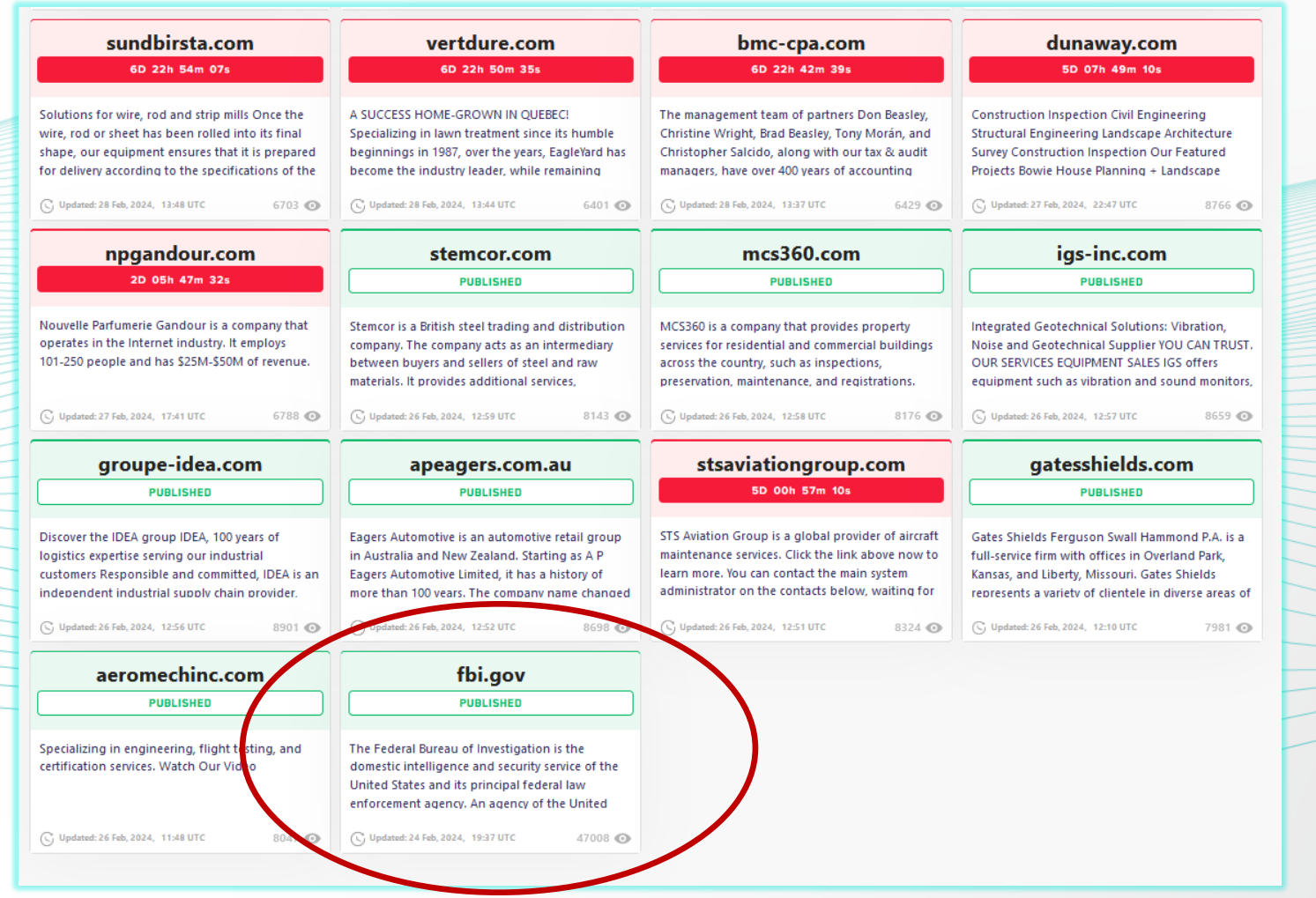
Hvilke tiltag iværksætter politiet?

OVERTOG LOCKBITS LEAKSITE OG OFFENTLIGGJORDE OPLYSNINGER OM LOCKBIT OG SAMARBEJDSPARTNERE



Hvordan reagerede LockBit?

EFTER 4 DAGE



- LockBit reetablerede infrastrukturen efter 4 dage
- Det første opslag, der blev offentliggjort, havde: FBI.gov

Besked fra LockBit

TIL FBI

lockbit7z2jwcskxpbokpemdxmltipntwlkmidcll2qirbu7ykg46eyd.onion/fbi.gov/fbi.gov_en.txt

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

What happened.

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

Due to my personal negligence and irresponsibility I relaxed and did not update PHP in time, the servers had PHP 8.1.2 version installed, which was successfully penetration tested most likely by this CVE https://www.cvedetails.com/cve/CVE-2023-3824/ , as a result of which access was gained to the two main servers where this version of PHP was installed. I realize that it may not have been this CVE, but something else like 0day for PHP, but I can't be 100% sure, because the version installed on my servers was already known to have a known vulnerability, so this is most likely how the victims' admin and chat panel servers and the blog server were accessed. The new servers are now running the latest version of PHP 8.3.3. If anyone recognizes a CVE for this version, be the first to let me know and you will be rewarded.

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

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

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

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

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

The only thing that is of value and potential threat is the source code of the panel, because of it is probably possible future hacks if you let everyone into the panel, but now the panel

Trusselsvurdering Danmark

STYRELSEN FOR SAMFUNDSSIKKERHED

- Cyberkriminalitet: MEGET HØJ – konstante angreb, herunder ransomware, datatyveri og svindel.
- Cyberspionage: MEGET HØJ – Rusland og Kina målretter danske organisationer for at få adgang til følsomme politiske oplysninger og forsvarsoplysninger.
- Cyberhacktivisme: HØJ – hovedsageligt prorussiske hackere, der bruger DDoS og manipulation af OT-systemer (f.eks. angreb på et vandværk i slutningen af 2024). Nogle er sandsynligvis knyttet til den russiske stat.
- Destruktive cyberangreb: MIDDEL – hovedsageligt Rusland, der anvender hybride metoder (wipers, begrænset forstyrrelse af OT).
- Cyberterrorisme: INGEN – ingen ekstremistiske grupper er i øjeblikket i stand til eller har intention om at angribe Danmark digitalt.

3. Ransomware-sag

Hvordan blev hændelsen opdaget?

RANSOMWARE-NOTE / VISITKORT

DAG 5

```
ATTENTION!
Your network has been breached and all data was encrypted. Please contact us at:
https://bastad5huzwkepdixedg2gekg7jk22ato24zyllp6lnjx7wdtyctgvyd.onion/


Login ID: 44daac10-982f-4961-af32-33964ffe86d4


! To access .onion websites download and install Tor Browser at:

   https://www.torproject.org/ (Tor Browser is not related to us)

! To restore all your PCs and get your network working again, follow these instructions:

- Any attempts to modify, decrypt or rename the files will lead to its fatal corruption. It doesn't matter, who are trying to do this, either it will be your IT guys or a recovery agency.

Please follow these simple rules to avoid data corruption:

- Do not modify, rename or delete files. Any attempts to modify, decrypt or rename the files will lead to its fatal corruption.

- Do not hire a recovery company. They can't decrypt without the key.
They also don't care about your business. They believe that they are
good negotiators, but it is not. They usually fail. So speak for yourself.


Waiting you in a chat.
```

Hvordan fik gerningsmændene adgang?

SPEARPHISHING VIA EKSISTERENDE E-MAILTRÅD

Kompromittering af medarbejder-pc

FRA BLACK BASTA-CHATLOGS, DER EFTERFØLGENDE BLEV LÆKKET

DAG 1

```
{
    timestamp: 2023-10-27 14:32:25,
    chat_id: !BOpqkyiMnBRfCPXwod:matrix.bestflowers247.online,
    sender_alias: @usernamevv:matrix.bestflowers247.online,
    message: ```
List of domain trusts:

    0: EDC edc.local (NT 5) (Forest Tree Root) (Primary Domain) (Native)


Domain Admins
-------------------------------------------------------------------------------
t0-globeteam-hans


Domain Controllers
-------------------------------------------------------------------------------
EDCDC01$                EDCDC02$                EDCDC03$
EDCDC04$

Processing 5465 computers


System Boot Time:          26-10-2023, 16:07:21

local credentials just for REQ47105421
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3883c2fe3e0aa4d394ac121295947edb:::

Global credentials:
EDC\291963 14d8e59e5990af1ab00dae4da9a7db8e



PROMK@EDC.LOCAL 9WEzM4Zg

Original Install Date:     23-06-2022, 15:07:23



[RESULT]  Username: Administrator (built-in)
[RESULT]  Changed:  2014-04-04 08:17:19
[RESULT]  Password:[redacted]
```

DAG 1

```
Global credentials:
EDC\291963 14d8e59e5990af1ab00dae4da9a7db8e


PROMK@EDC.LOCAL 9WEzM4Zg

Original Install Date:     23-06-2022, 15:07:23



[RESULT]  Username: Administrator (built-in)
[RESULT]  Changed:  2014-04-04 08:17:19
[RESULT]  Password:[redacted]


----------Results from 127.0.0.1----------

[*] SAM hashes
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3883c2fe3e0aa4d394ac121295947edb
[*] Cached domain logon information(domain/username:hash)
EDC.LOCAL/291963:$DCC2$10240#291963#f431147f498dd1ef4159f699c7bcef96
EDC.LOCAL/edcdocumentwriter:$DCC2$10240#edcdocumentwriter#934f4638eb082a2d294f899e3e666763
EDC.LOCAL/885952:$DCC2$10240#885952#9d68d6e500109af814b278e4e6a0daff
EDC.LOCAL/107988:$DCC2$10240#107988#eddea9910eb9a79ea398b1cb98b83f7f
EDC.LOCAL/EDCDKMEDIAWRITER:$DCC2$10240#EDCDKMEDIAWRITER#f4e6353cf323ccc8089d7e21f65b9deb
[*] LSA Secrets
[*] $MACHINE.ACC
edc.local\REQ47105421$:aad3b435b51404eeaad3b435b51404ee:251d5986a95199f5c9a0d4b305152d30
[*] DefaultPassword
[!] Secret type not supported yet - outputing raw secret as unicode:
Passw0rd
[*] DPAPI_SYSTEM
dpapi_machinekey:eaad7d457c55839ef09035bfb6b048cb5bede29c
dpapi_userkey:f9bfdd009d0e06d4d95e130670f867e7e0722521
[*] NL$KM
NL$KM:75e7d9923bac94523f265272e9274ac3a821fb521b4d1a3c7f9f417f8a8894d0b42679607894ce42d0fc48b1a3aa0da4e6b3eb03c4556c80660deccd2d138218
----------Script execution completed----------
```


3
DAGE SENERE
SOM FØLGE AF HØJT SIKKERHEDSNIVEAU

Hele netværket er kompromitteret

EFTER 3 DAGE

Fakta:

- Initial adgang: Spearphishing-mail i eksisterende mailtråd
- Lateral bevægelse: Medarbejderens pc => Domain Controller (ADCS-sårbarhed)
- Persistens: Software- og brugerbaseret bagdør (lokal administrator og RDP)
- Backup: Intakt

Den mest alvorlige konsekvens for kunden

DATAEKSFILTRATION

Fakta:

- Program: Rclone, et legitimt backup- og synkroniseringsværktøj
- Konfigurationsfil: Rclone.conf, som indeholdt oplysninger om gerningsmændenes dataeksfiltrationsserver (brugernavn, kodeord og IP-adresse)

Forsøg på at lukke dataeksfiltrationsserveren

AKAMAI

CSIS anmodede om, at dataeksfiltrationsserveren blev suspenderet hos Akamai (dag 1 i efterforskningen).
Serveren blev suspenderet inden for 12 timer efter, at nedenstående anmodning om nedtagning blev sendt.
Desværre svarede Akamai aldrig tilbage til os.

DAG 5

Data exfiltration from Black Basta to a server in Akamai with IP: 172.104.144[.]97 (Urgent)!

Jan Kaastrup
To abuse@akamai.com
Cc [redacted]

Reply | Reply All | Forward

Wed 01/11/2023 22.45

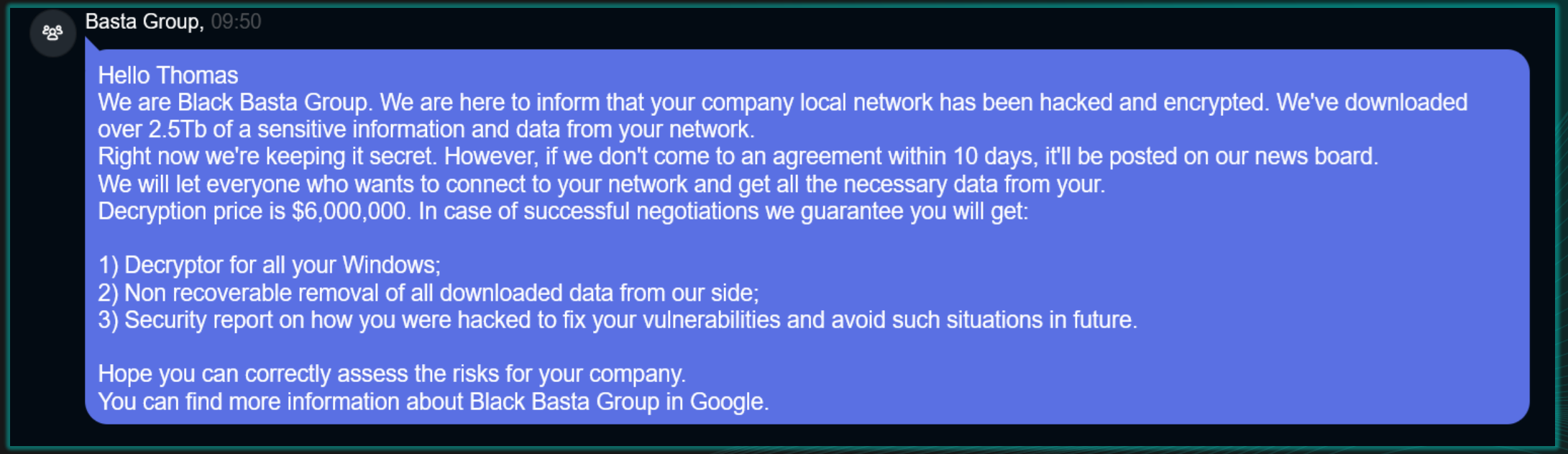
Dear support

Our customer [redacted] has been victim to a ransomware attack by the group Black Basta.
They have exfiltrated [redacted] data to the server IP: 1[redacted]
Data exfiltration started around 31/10 17.45 UTC+1

Can we please ask you to suspend the server and secure evidence?
We will inform Danish police tomorrow who will then reach out to you to get the details.
Meanwhile please keep us updated when the server is suspended and if data already was uploaded somewhere else or we can consider the data exfiltration contained.

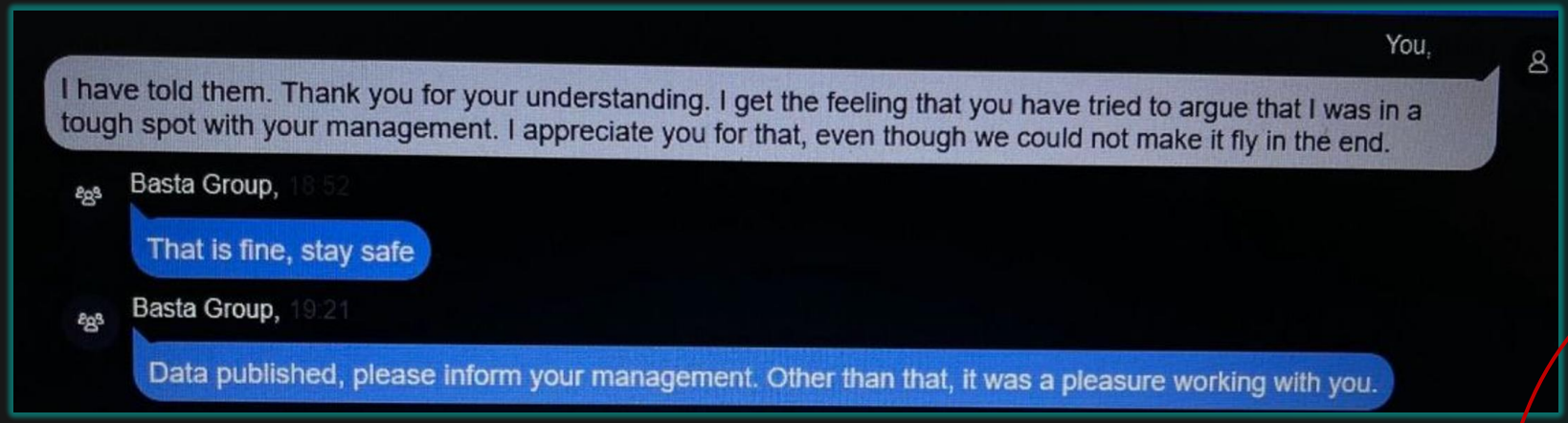
Forhandlinger med Black Basta

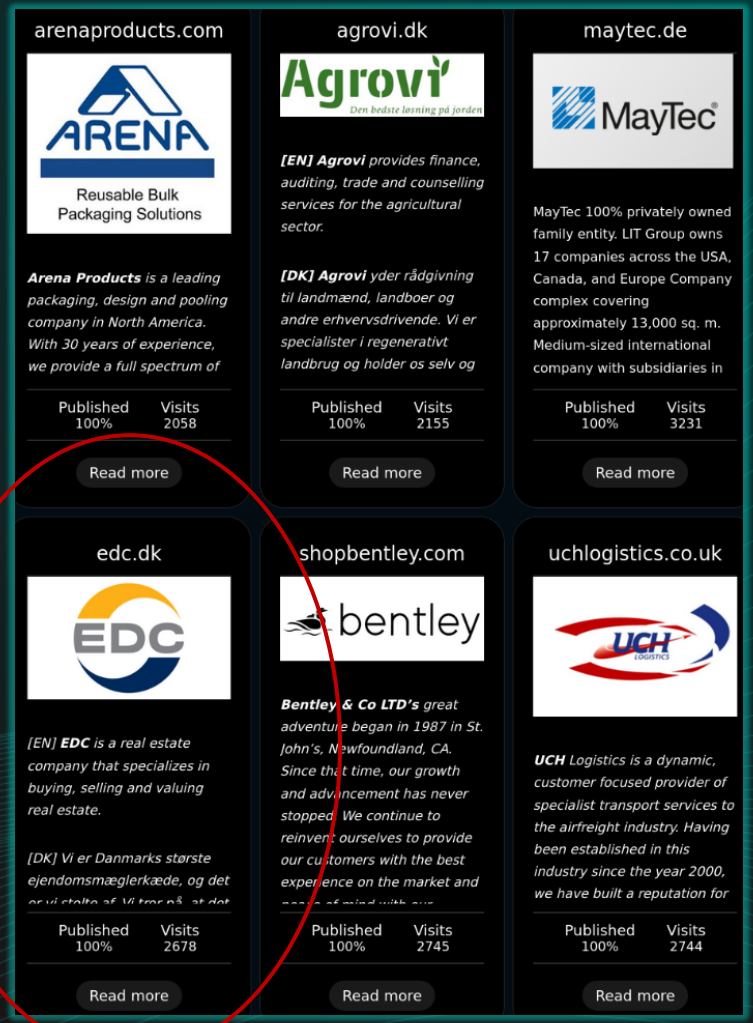
HÅNDTERING AF TRUSSELSAKTØRERNE



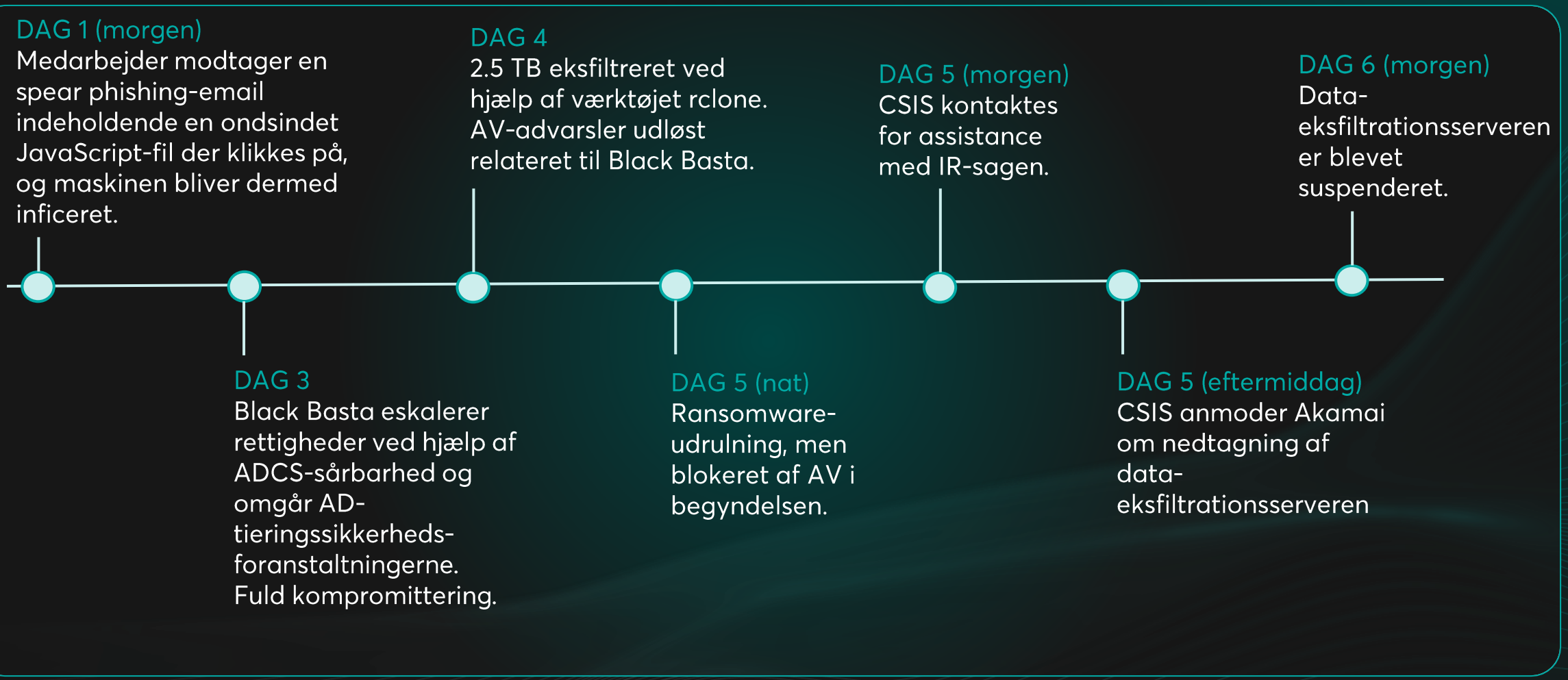
Hvordan blev hændelsen afsluttet?

DATABRUD





Tidslinje



4. Centrale læringspunkter?

4,5M EURO

Den gennemsnitlige omkostning ved et databrud for en virksomhed

82%

af brud involverer både menneskelige og organisatoriske forhold

80%

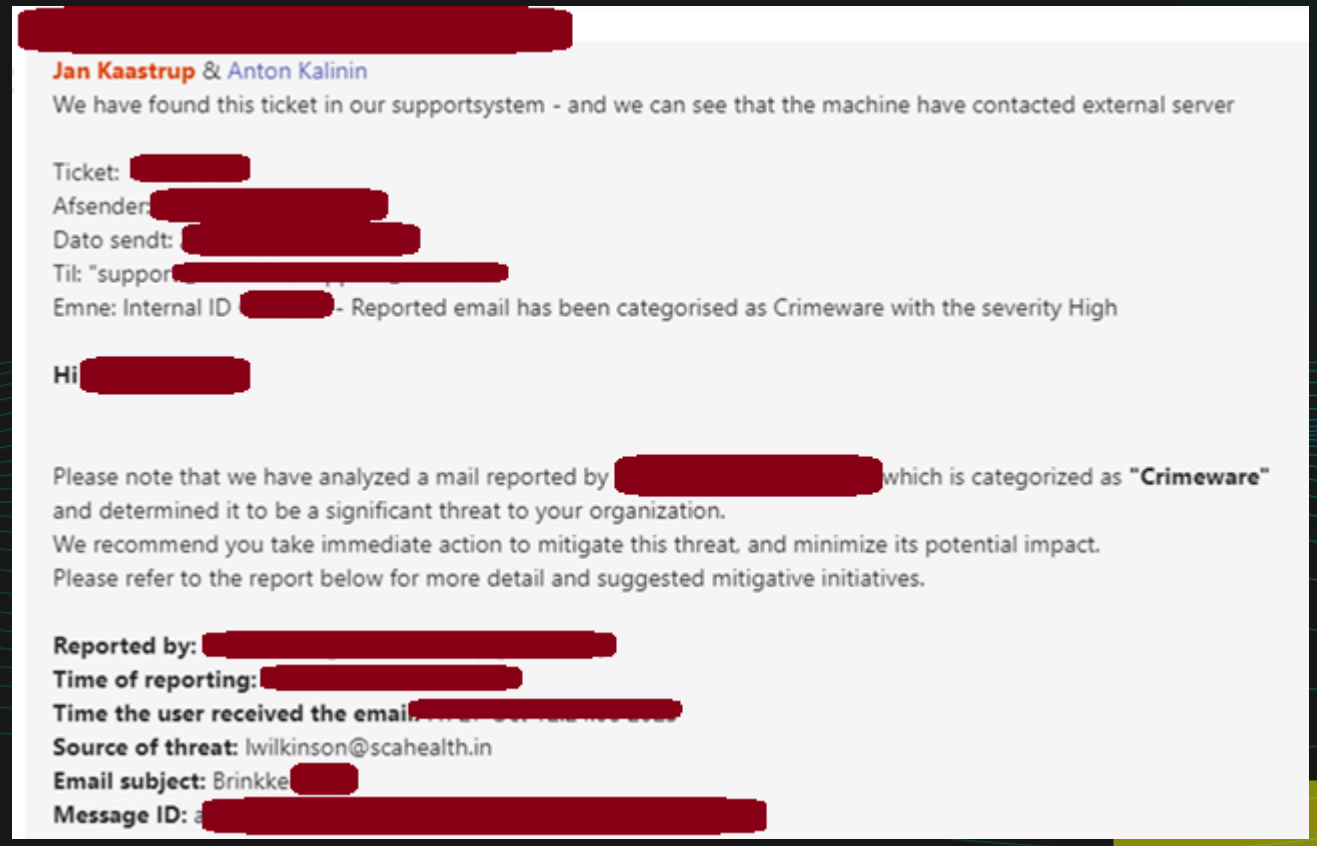
af organisationer har IKKE en formaliseret beredskabsplan

68%

af medarbejdere glemmer træningsindhold inden for en uge

Awareness-træning styrker beredskabet

DU KAN BEGRÆNSE KONSEKVENSERNE AF ET ANGREB



[redacted]

Jan Kaastrup & Anton Kalinin

We have found this ticket in our supportsystem - and we can see that the machine have contacted external server

Ticket: [redacted]
Afsender [redacted]
Dato sendt: [redacted]
Til: "suppor[redacted]
Emne: Internal ID [redacted]- Reported email has been categorised as Crimeware with the severity High

Hi [redacted]

Please note that we have analyzed a mail reported by [redacted] which is categorized as **"Crimeware"** and determined it to be a significant threat to your organization.
We recommend you take immediate action to mitigate this threat, and minimize its potential impact.
Please refer to the report below for more detail and suggested mitigative initiatives.

Reported by: [redacted]
Time of reporting: [redacted]
Time the user received the email: [redacted]
Source of threat: lwilkinson@scahealth.in
Email subject: Brinkke[redacted]
Message ID: [redacted]

Kilde: CSIS IR CASES

- Rapportér mistænkelig aktivitet, også hvis du har klikket på et link, har indtastet dine legitimationsoplysninger på et phishing-site eller har observeret unormal adfærd.

Anbefalede tiltag for virksomheden?

FORLÆNG TIDEN TIL KOMPROMITTERING, FORBEDR TIDEN TIL OPDAGELSE OG REDUCÉR TIDEN TIL REAKTION

Time-to-hack

- Gør det vanskeligere for hackere at kompromittere virksomhedens netværk ved at styrke sikkerheden i virksomhedens systemer.

Time-to-detect

- Opdag angrebet så tidligt som muligt ved at etablere og styrke virksomhedens detektionskapacitet.

Time-to-respond

- Reagér på sikkerhedsalarmer så hurtigt som muligt (24/7), og sørg for, at det er tydeligt, hvem der skal kontaktes, hvis der opstår behov for ekstern assistance.
- Gennemfør kriseøvelser for hele virksomheden.

Hvilke foranstaltninger kan du selv iværksætte?

ANBEFALEDE TILTAG

Anvend ikke din arbejdsmail til private tjenester.	Rapportér mistænkelig aktivitet, e-mails, SMS'er og telefonopkald.	Vær opmærksom på, at ondsindede e-mails også kan fremstå som afsendt af venner og samarbejdspartnere.
Vær forsigtig ved installation af software, aktivering af makroer og kørsel af JavaScript-filer.	Anvend en password manager	Anvend multifaktorgodkendelse, når det er muligt.
Vær bevidst om, hvilke oplysninger du deler på sociale medier.	Vær opmærksom på, at e-mails, SMS'er, telefonnumre, lyd og video kan forfalskes og manipuleres.	Etablér en robust procedure for verifikation af betalinger.

Ledelsen skal ligeledes være forberedt

HYPOTESE

=

"I de fleste alvorligeransomware-hændelser er det sjældent angriberne, men ledelsen, der afgør, hvor omfanget af skaden bliver."

Spørgsmål

jka@csis.com