



Den usynlige fjende - Cyberangreb

GoLearn, 2026

Jan Kaastrup - CIO, CSIS

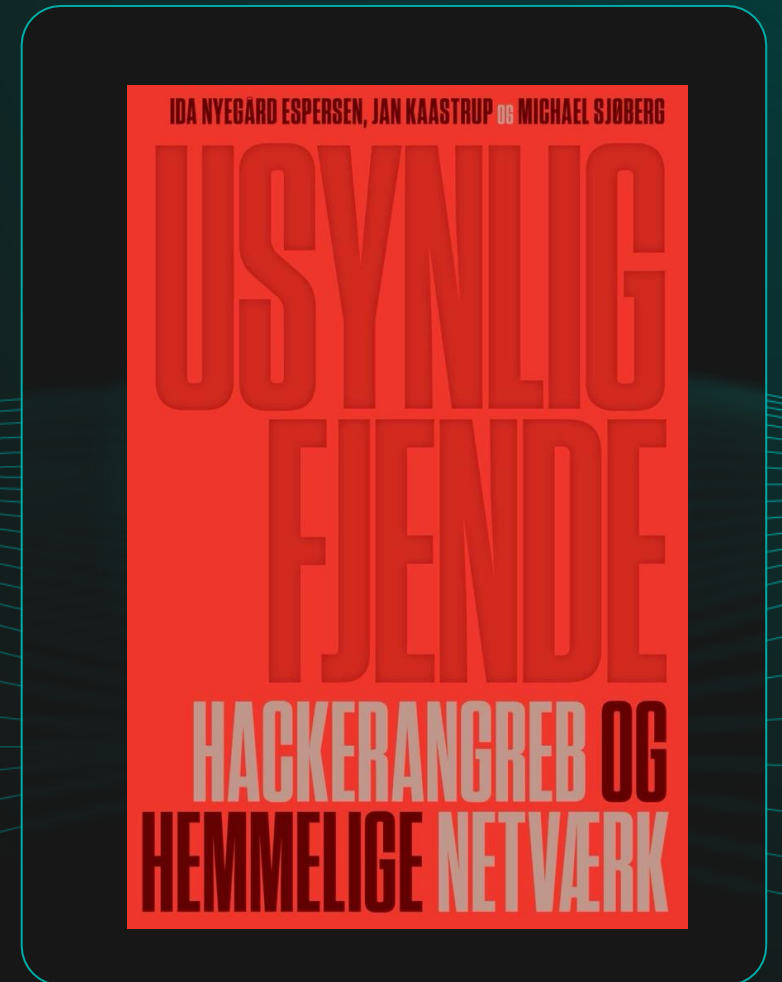
Profil og baggrund



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



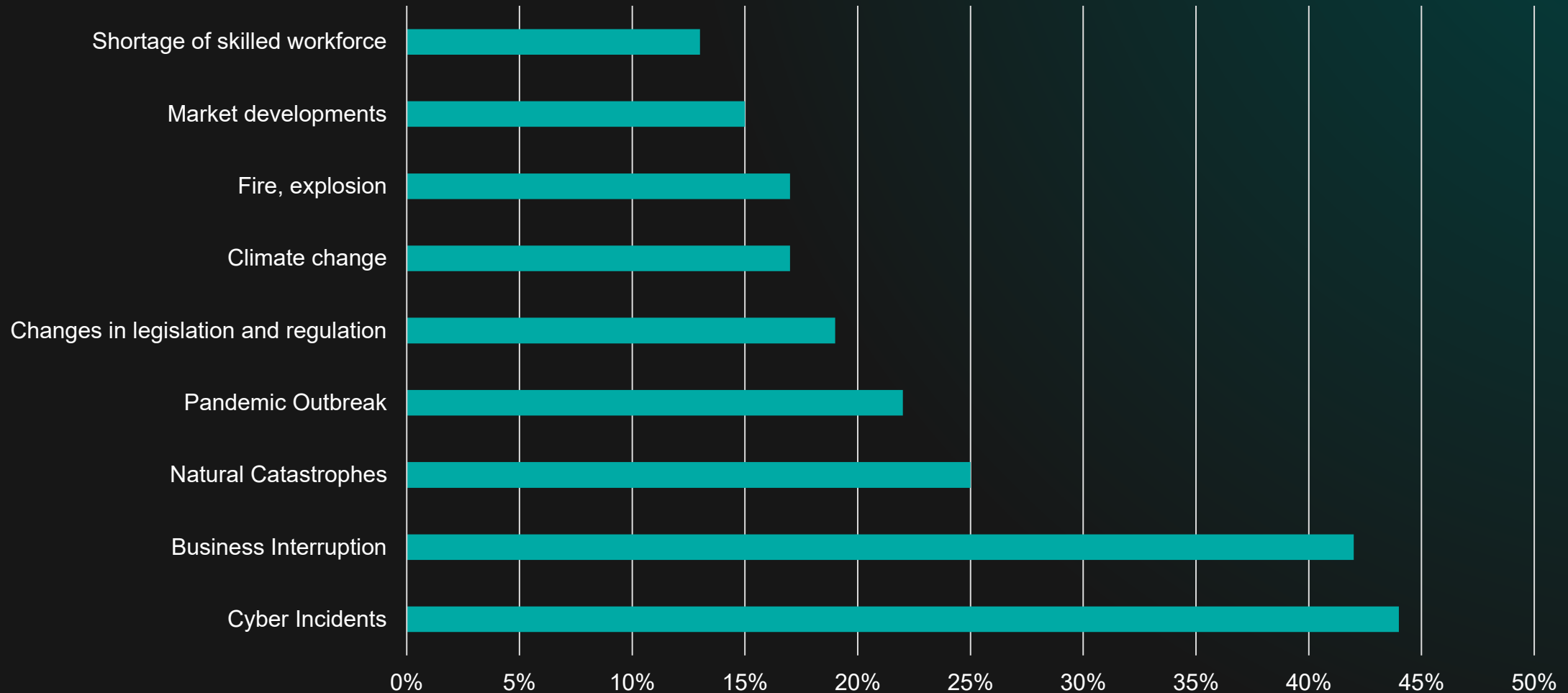
By **Bui Tyril** October 5, 2024

👁 1085

💬 0

Den væsentligste forretningsrisiko

CYBERANGREB



DE TRE TRUSSELAKTØRER I CYBERSPACE

Hacktivist



— Politiske Motiver —

Cyberkriminelle



— Økonomisk Gevinst —

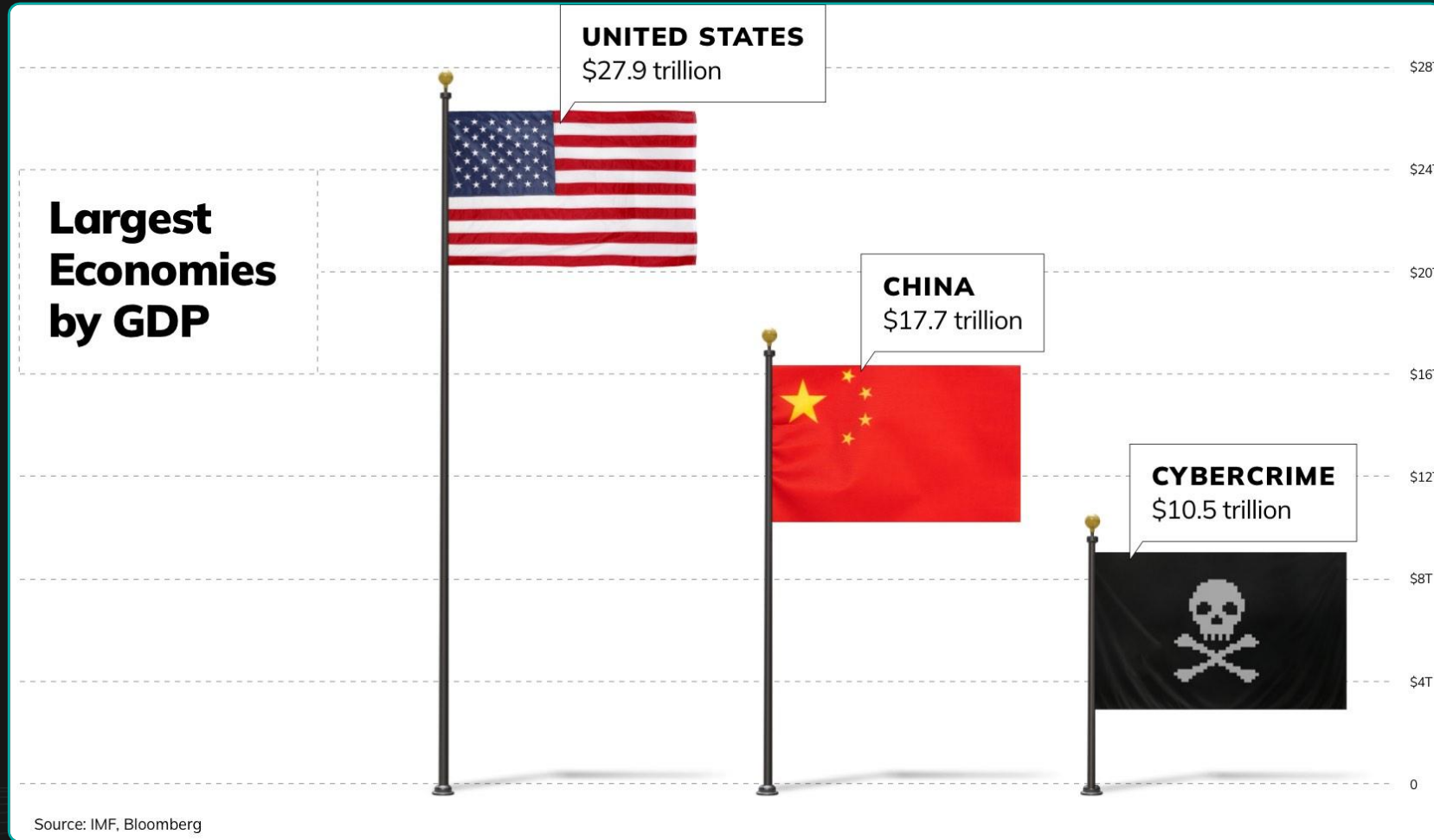
Statssponsoreret



— Nationale Interesser —

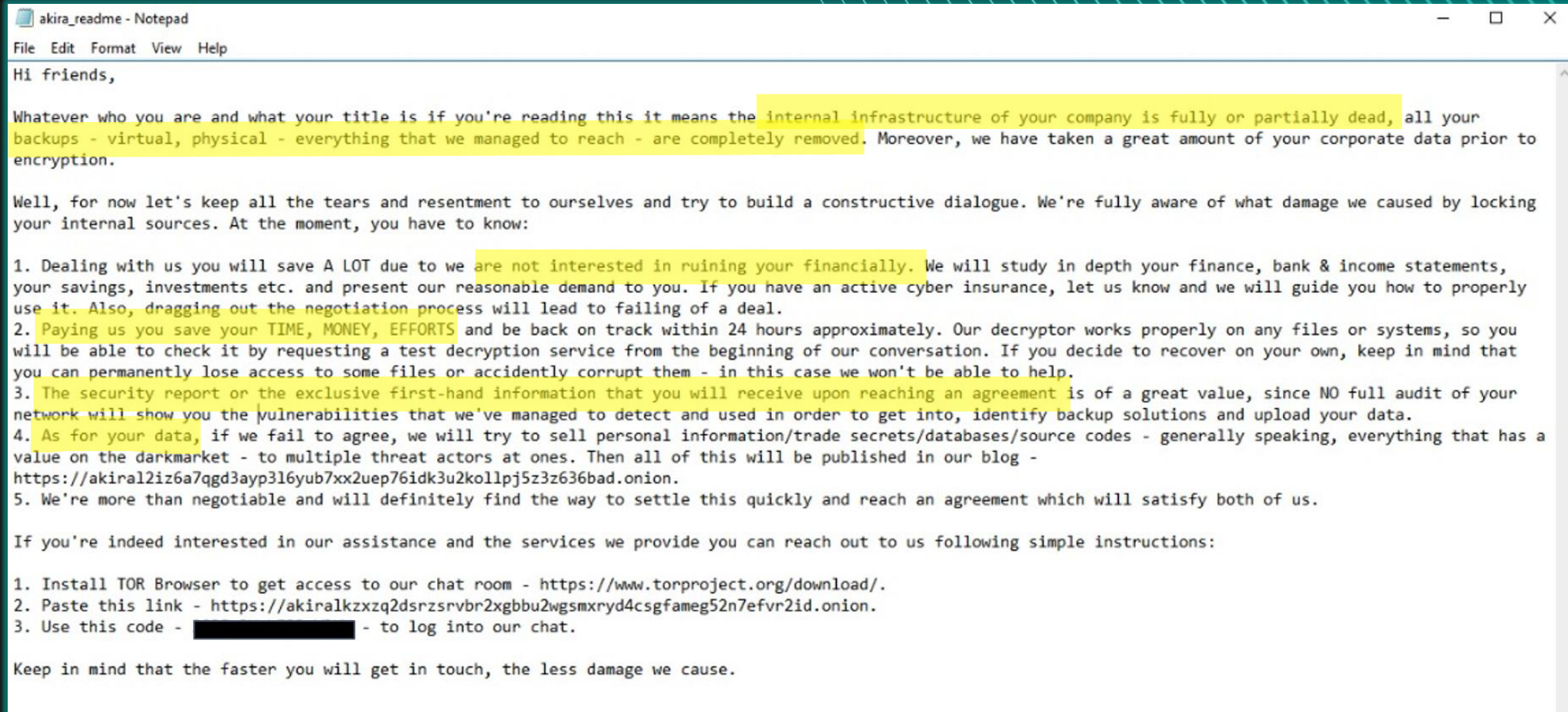
Cyberkriminalitet

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 accidentally 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://akiralkzqxq2dsrzsrivr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.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?



LEAKED DATA

[ENCRYPTING THE PLANET](#) >
 [HOW TO BUY BITCOIN](#) >
 [CONTACT US](#) >
 [PRESS ABOUT US](#) >
 [AFFILIATE RULES](#) >
 [MIRRORS](#)

fondonorma.org.ve

13d 21h 52m 53s

Fondonorma is a Venezuelan certification company that helps businesses prove they meet quality and s...

99 Apr, 2026, 06:31 UTC
579

comunidadandina.org

13d 21h 50m 45s

La Comunidad Andina (CAN) es un organismo internacional de integración subregional fundado el 26 de...

99 Apr, 2026, 06:28 UTC
575

wibeats.it

10d 1h 32m 29s

WIBEATS is an independent Asset Management and Loans Service groups, highly specialised in the selec...

05 Apr, 2026, 09:10 UTC
2607

earthprotect.co.jp

10d 0h 14m 47s

Earth Protect Co., Ltd Thinking about what we can do to protect and create tomorrow's global...

05 Apr, 2026, 07:03 UTC
2631

shunhinggroup.com

8d 8h 21m 43s

The Shun Hing Group (信興集團) is a prominent Hong Kong-based conglomerate founded in 1953, primarily kn...

03 Apr, 2026, 15:09 UTC
2731

aplast.ro

8d 8h 12m 29s

You are welcome in our offices across Central and Eastern Europe With international presence since...

03 Apr, 2026, 16:06 UTC
3380

seleniaravenna.it

8d 6h 29m 9s

Servizi all'avanguardia a Ravenna Nato nel 1992 dall'unione delle principali realtà coope...

03 Apr, 2026, 14:07 UTC
3353

vitexpharma.com

8d 6h 26m 40s

Vitex Pharmaceuticals is Australia's leading contract manufacturer specializing in vitamins, mi...

03 Apr, 2026, 14:04 UTC
3358

vitropor.pt

8d 6h 18m 3s

Tal como o nosso vidro, somos transparentes, seguros e resistentes. Com mais de 30 anos na indústri...

03 Apr, 2026, 13:06 UTC
3314

villa-romane.fr

8d 6h 14m 43s

Villa Romane, constructeur de maison à Perpignan Fondée en 1982, Villa Romane est une entreprise fa...

03 Apr, 2026, 13:02 UTC
3130

pegasussrl.com

8d 6h 11m 54s

Agenzia Unipol Assicurazioni 39547 Prato - Pegasus srl Agenzia 39547 Prato R.U.I.N. A000671187-P...

03 Apr, 2026, 13:00 UTC
3108

meyziptp.com

8d 5h 57m 10s

Fondée en 1954, l'entreprise MEYZIE TP est spécialisée dans les travaux de terrassements routiers et...

03 Apr, 2026, 13:38 UTC
2999

mesto-jemnice.cz

8d 5h 50m 44s

Historie města Jemnice Město Jemnice je správním, hospodářským a kulturním střediskem kraje mezi Da...

03 Apr, 2026, 13:28 UTC
2993

douglasstruckbodies.com

8d 5h 29m 45s

Douglass Truck Bodies specializes in the manufacturing and design of standard and custom truck bodie...

03 Apr, 2026, 13:07 UTC
2954

awygrazerfeld.at

8d 5h 28m 13s

Verwaltung Unter dem Motto "Weg vom Kostenumleger und hin zum Dienstleister" hat sich die Geschäfts...

03 Apr, 2026, 13:06 UTC
2356

contrar.it

8d 5h 22m 44s

Il consorzio CONTR.AR nasce nel 1985 dall' aggregazione di alcuni padroncini artigiani che sentiron...

03 Apr, 2026, 13:00 UTC
2986

zsfh.cz

8d 5h 15m 41s

Základní škola a Mateřská škola F. Hrubina Havířov-Podlesí

03 Apr, 2026, 12:53 UTC
2287

milanocavi.com

8d 5h 12m 23s

Wineuropa is a web agency based in Arezzo that specializes in web marketing, SEO services, and webst...

03 Apr, 2026, 13:00 UTC
2369

abuhatim.com

8d 5h 7m 23s

Abu Hatim Co LLC is an Excellent Grade Engineering Construction Company established in 1991, special...

03 Apr, 2026, 12:45 UTC
2991

gas.mercedes-benz.com.eg

8d 5h 5m 19s

Mercedes-Benz, founded in 1907 and headquartered in Giza, Egypt, is a automobile dealer and motor ve...

03 Apr, 2026, 12:43 UTC
3088

ikron.org

published

IKRON (Integration of Knowledge and Resources for Occupational Needs) was

montaury.com.br

published

Montaury Pimenta, Machado & Vieira de Mello is a leading Brazilian Intellectual

isoledilcappotti.it

published

La professionalità al Vostro servizio ISOLEDIL una garanzia di qualità ed

nandrin.be

published

Nandrin (French pronunciation: [nɑ̃dʁɛ̃]) is a municipality of Wallonia located in the

ombudsman.gov.ws

published

Ombudsman Western Australia is an impartial and independent office serving the

maasa.com.ar

published

Mega Alfalfa Argentina (MAA) is a family-oriented organization rooted in Argentina, comprising evol...

14 Dec, 2025, 15:06 UTC
21372

LEAKED DATA

[ENCRYPTING THE PLANET](#) >
 [HOW TO BUY BITCOIN](#) >
 [CONTACT US](#) >
 [PRESS ABOUT US](#) >
 [AFFILIATE RULES](#) >
 [MIRRORS](#)

Deadline: 29 Dec, 2025, 15:06:10 UTC

[no logo]

maasa.com.ar

Mega Alfalfa Argentina (MAA) is a family-oriented organization rooted in Argentina, comprising evolving enterprises employing over 5000 people

[no logo]

UPLOADED: 14 DEC 2025 15:06 UTC
UPDATED: 14 DEC 2025 15:06 UTC

Additional links with stolen data

[Link 11](#) [Link 22](#) [Link 33](#) [Link 44](#) [Link 55](#) [Link 66](#) [Link 77](#) [Link 88](#) [Link 99](#) [Link 00](#)

LEAKED DATA

[ENCRYPTING THE PLANET](#) >
 [HOW TO BUY BITCOIN](#) >
 [CONTACT US](#) >
 [PRESS ABOUT US](#) >
 [AFFILIATE RULES](#) >
 [MIRRORS](#)

File Name	File Size	Date
Parent Directory	-	-
unpack	-	December 11, 2025
maasa.com.ar?z	14.2 GiB	December 12, 2025
maasa.com.ar?z-file-tree.txt	628.2 KiB	December 12, 2025
maasa.com.ar?z.torrent	1.1 MiB	March 28, 2026

2025-12-06 03:23:12 ...A	28761066	unpack/rbravo/Downloads/Fwd_RECLAMO_CALIDAD_-_QINGDAO_AFA_IMPORT_&_EXPORT_-_recibido_ei_detalle_por_parte_del_cliente..zip
2025-12-06 03:22:58 ...A	534776	unpack/rbravo/Downloads/GHP+ 2020 FC Proposal MAASA - 2023 - FINAL.pdf
2025-12-06 03:22:58 ...A	533322	unpack/rbravo/Downloads/GHP+ 2020 FC Proposal MAASA - 2023 (1).pdf
2025-12-06 03:22:58 ...A	115652	unpack/rbravo/Downloads/GHP+ 2020 FC Proposal MAASA - GHP060059 - 2023_7 completo.pdf
2025-12-06 03:22:57 ...A	364156	unpack/rbravo/Downloads/GHP+ 2020 FC Proposal MAASA - GHP060059 - 2023.pdf
2025-12-06 03:22:57 ...A	106790	unpack/rbravo/Downloads/GHP+ 2020 FSA questionnaire MAASA - GHP060059 - 2023 completo.docx
2025-12-06 03:22:57 ...A	67247	unpack/rbravo/Downloads/GHP+ 2020 FSA questionnaire MAASA - GHP060059 - 2023.docx
2025-12-06 03:22:56 ...A	942124	unpack/rbravo/Downloads/GHP+2020 REPORT MAASA - GHP060059 - 2024 RESULTADOS.pdf
2025-12-06 03:22:57 ...A	1091845	unpack/rbravo/Downloads/GHP+2020 report - MAASA - GHP060059 - 2024 (1) (1).pdf
2025-12-06 03:22:57 ...A	346764	unpack/rbravo/Downloads/GHP+2020 report - MAASA - GHP060059 - 2024 (1).pdf
2025-12-06 03:22:56 ...A	346764	unpack/rbravo/Downloads/GHP+2020 report - MAASA - GHP060059 - 2024.pdf
2025-12-06 03:22:55 ...A	36945	unpack/rbravo/Downloads/GREENLAB.docx
2025-12-06 03:22:55 ...A	1736496	unpack/rbravo/Downloads/HACCP.pptx
2025-12-06 03:28:54 ...A	184620	unpack/rbravo/Downloads/Habilitacion de producto/anexo_7260888_1 (2).pdf
2025-12-06 03:28:54 ...A	327954	unpack/rbravo/Downloads/Habilitacion de producto/anexo_7260888_2 (2).pdf
2025-12-06 03:28:53 ...A	102642	unpack/rbravo/Downloads/Habilitacion de producto/anexo_7260888_3 (1).pdf
2025-12-06 03:28:53 ...A	116297	unpack/rbravo/Downloads/Habilitacion de producto/anexo_7260888_4.pdf
2025-12-06 03:28:53 ...A	164193	unpack/rbravo/Downloads/Habilitacion de producto/anexo_7260888_5.pdf
2025-12-06 03:28:53 ...A	215577	unpack/rbravo/Downloads/Habilitacion de producto/anexo_7260888_6.pdf
2025-12-06 03:28:53 ...A	107912	unpack/rbravo/Downloads/Habilitacion de producto/anexo_7260888_7.pdf
2025-12-06 03:28:53 ...A	108895	unpack/rbravo/Downloads/Habilitacion de producto/anexo_7260888_8.pdf
2025-12-06 03:28:53 ...A	222107	unpack/rbravo/Downloads/Habilitacion de producto/anexo_7260888_9 (1).pdf
2025-12-06 03:22:54 ...A	596505	unpack/rbravo/Downloads/Humedmetro - unlv_calif - lng.pdf
2025-12-06 03:22:54 ...A	862234	unpack/rbravo/Downloads/Humedmetro DELHORST (1).pdf
2025-12-06 03:22:55 ...A	4167308	unpack/rbravo/Downloads/Humedmetro DELHORST.docx
2025-12-06 03:22:53 ...A	758660	unpack/rbravo/Downloads/Humedmetro DELHORST.pdf

Hvordan arbejder politiet?

UTRADITIONELLE METODER ANVENDT AF EUROPOL, NCA OG FBI

THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

LOCKBIT

The graphic displays a central 'LOCKBIT' logo surrounded by circular icons of national flags from the United Kingdom, United States, Germany, France, Finland, Japan, Netherlands, Switzerland, Sweden, Australia, and Canada. To the right, a vertical column of police department logos includes the FBI, Department of Justice, and various international police forces. At the bottom, logos for the National Crime Agency (NCA), South West ROCU, Metropolitan Police, Europol, and other international law enforcement agencies are shown.

Hvilke tiltag iværksætter politiet?

OVERTOG LOCKBITS LEAKSITE OG OFFENTLIGGJORDE OPLYSNINGER OM LOCKBIT OG SAMARBEJDSPARTNERE

LOCKBIT 3.0 **LEAKED DATA** THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

NCA National Crime Agency **FBI** **EUROPOL**

Press Releases PUBLISHED
Updated: 01 Feb, 2024, 04:12 UTC 3947

LB Backend Leaks PUBLISHED
Updated: 31 Jan, 2024, 01:44 UTC 1182

Lockbitsupp PUBLISHED
Updated: 31 Jan, 2024, 01:44 UTC 1182

Who is LockbitSupp? 2D 17H 25M 18S
The \$10m question

Lockbit Decryption Keys PUBLISHED
Updated: 01 Feb, 2024, 04:12 UTC 3947

Recovery Tool PUBLISHED
Updated: 01 Feb, 2024, 04:12 UTC 3947

US Indictments PUBLISHED
Updated: 31 Jan, 2024, 01:44 UTC 1182

Sanctions 0D 1H 55M 18S
Updated: 31 Jan, 2024, 01:44 UTC 1182

Arrest in Poland PUBLISHED
On 20/02/2024 a suspected LockBit actor was arrested in Poland on the request of the French

Activity in Ukraine PUBLISHED
On 20/02/2024 a suspected Lockbit actor was arrested in Ternopil (UA) by the local authorities.

Report Cyber Attacks! PUBLISHED
Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive

Cyber Choices PUBLISHED
Activate Windows
Go to Settings to activate Windows features

Hvordan reagerede LockBit?

EFTER 4 DAGE

The screenshot displays a grid of 16 company profiles, each with a header, a status bar, a description, and a timestamp. The profiles are arranged in four rows and four columns. The 'fbi.gov' profile is circled in red.

Company	Status	Updated	Views
sundbirsta.com	6D 22h 54m 07s	28 Feb, 2024, 13:48 UTC	6703
vertdure.com	6D 22h 50m 35s	28 Feb, 2024, 13:44 UTC	6401
bmc-cpa.com	6D 22h 42m 39s	28 Feb, 2024, 13:37 UTC	6429
dunaway.com	5D 07h 49m 10s	27 Feb, 2024, 22:47 UTC	8766
npgandour.com	2D 05h 47m 32s	27 Feb, 2024, 17:41 UTC	6788
stemcor.com	PUBLISHED	26 Feb, 2024, 12:59 UTC	8143
mcs360.com	PUBLISHED	26 Feb, 2024, 12:58 UTC	8176
igs-inc.com	PUBLISHED	26 Feb, 2024, 12:57 UTC	8659
groupe-idea.com	PUBLISHED	26 Feb, 2024, 12:56 UTC	8901
apeagers.com.au	PUBLISHED	26 Feb, 2024, 12:52 UTC	8698
stsaviationgroup.com	5D 00h 57m 10s	26 Feb, 2024, 12:51 UTC	8324
gatesshields.com	PUBLISHED	26 Feb, 2024, 12:10 UTC	7981
aeromechinc.com	PUBLISHED	26 Feb, 2024, 11:48 UTC	8044
fbi.gov	PUBLISHED	24 Feb, 2024, 19:37 UTC	47008

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

Besked fra LockBit

TIL FBI



```
lockbit7z2jwvcskxpbokpemdxmltipntwlmkmdl2qirbu7ykg46eyd.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.
- **Cyberhaktivisme: 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://bastad5huzwkepdixedg2gek7jk22ato24zyl1p6lnjx7wdtyctgvyd.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

DAG 1



Kompromittering af medarbejder-pc

FRA BLACK BASTA-CHATLOGS, DER EFTERFØLGENDE BLEV LÆKKET

```

{
  timestamp: 2023-10-27 14:32:25,
  chat_id: !B0pqkyiMnBRfCPXwod: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:
  
```

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:

-----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$10240#885952#9d68d6e500109af814b278e4e6a0daaff
EDC.LOCAL/107988:$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:
Password
[*] DPAPI_SYSTEM
dpapi_machinekey: eaad7d457c55839ef09035fb6b048cb5bede29c
dpapi_userkey: f9bfd009d0e06d4d95e130670f867e7e0722521
[*] NL$KM
NL$KM:75e7d9923bac94523f265272e9274ac3a821fb521b4d1a3c7f9f417f8a8894d0b42679607894ce42d0fc48b1a3aa0da4e6b3eb03c4556c80660decccd2d138218
-----Script execution completed-----
  
```

DAG 1

A large, white, sans-serif number '3' centered within a circular graphic. The circle has a cyan-colored border and a background of a white circuit board pattern on a dark grey background.

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] ● [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 exfiltrate [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

 Basta Group, 09:50

Hello Thomas

We are Black Basta Group. We are here to inform that your company local network has been hacked and encrypted. We've downloaded over 2.5Tb of a sensitive information and data from your network.

Right now we're keeping it secret. However, if we don't come to an agreement within 10 days, it'll be posted on our news board.

We will let everyone who wants to connect to your network and get all the necessary data from your.

Decryption price is \$6,000,000. In case of successful negotiations we guarantee you will get:


- 1) Decryptor for all your Windows;
- 2) Non recoverable removal of all downloaded data from our side;
- 3) Security report on how you were hacked to fix your vulnerabilities and avoid such situations in future.

Hope you can correctly assess the risks for your company.


You can find more information about Black Basta Group in Google.

Hvordan blev hændelsen afsluttet?


DATABRUD

You, 







I have told them. Thank you for your understanding. I get the feeling that you have tried to argue that I was in a tough spot with your management. I appreciate you for that, even though we could not make it fly in the end.

 Basta Group, 18:52

That is fine, stay safe

 Basta Group, 19:21

Data published, please inform your management. Other than that, it was a pleasure working with you.

<p>arenaproducts.com</p>  <p>Reusable Bulk Packaging Solutions</p> <p><i>Arena Products is a leading packaging, design and pooling company in North America. With 30 years of experience, we provide a full spectrum of</i></p> <table border="1"> <tr> <td>Published</td> <td>Visits</td> </tr> <tr> <td>100%</td> <td>2058</td> </tr> </table> <p>Read more</p>	Published	Visits	100%	2058	<p>agrovi.dk</p>  <p><i>[EN] Agrovi provides finance, auditing, trade and counselling services for the agricultural sector.</i></p> <p><i>[DK] Agrovi yder rådgivning til landmænd, landboer og andre erhvervsdrivende. Vi er specialister i regenerativt landbrug og holder os selv og</i></p> <table border="1"> <tr> <td>Published</td> <td>Visits</td> </tr> <tr> <td>100%</td> <td>2155</td> </tr> </table> <p>Read more</p>	Published	Visits	100%	2155	<p>maytec.de</p>  <p>MayTec 100% privately owned family entity. LIT Group owns 17 companies across the USA, Canada, and Europe Company complex covering approximately 13,000 sq. m. Medium-sized international company with subsidiaries in</p> <table border="1"> <tr> <td>Published</td> <td>Visits</td> </tr> <tr> <td>100%</td> <td>3231</td> </tr> </table> <p>Read more</p>	Published	Visits	100%	3231
Published	Visits													
100%	2058													
Published	Visits													
100%	2155													
Published	Visits													
100%	3231													
<p>edc.dk</p>  <p><i>[EN] EDC is a real estate company that specializes in buying, selling and valuing real estate.</i></p> <p><i>[DK] Vi er Danmarks største ejendomsmæglerkæde, og det er i slutningen af Vinteren at det</i></p> <table border="1"> <tr> <td>Published</td> <td>Visits</td> </tr> <tr> <td>100%</td> <td>2678</td> </tr> </table> <p>Read more</p>	Published	Visits	100%	2678	<p>shopbentley.com</p>  <p><i>Bentley & Co LTD's great adventure began in 1987 in St. John's, Newfoundland, CA. Since that time, our growth and advancement has never stopped. We continue to reinvent ourselves to provide our customers with the best experience on the market and</i></p> <table border="1"> <tr> <td>Published</td> <td>Visits</td> </tr> <tr> <td>100%</td> <td>2745</td> </tr> </table> <p>Read more</p>	Published	Visits	100%	2745	<p>uchlogistics.co.uk</p>  <p><i>UCH Logistics is a dynamic, customer focused provider of specialist transport services to the airfreight industry. Having been established in this industry since the year 2000, we have built a reputation for</i></p> <table border="1"> <tr> <td>Published</td> <td>Visits</td> </tr> <tr> <td>100%</td> <td>2744</td> </tr> </table> <p>Read more</p>	Published	Visits	100%	2744
Published	Visits													
100%	2678													
Published	Visits													
100%	2745													
Published	Visits													
100%	2744													

Tidslinje

DAG 1 (morgen)

Medarbejder modtager en spear phishing-email indeholdende en ondsindet JavaScript-fil der klikkes på, og maskinen bliver dermed inficeret.

DAG 3

Black Basta eskalere rettigheder ved hjælp af ADCS-sårbarhed og omgår AD-tieringssikkerhedsforanstaltningerne. Fuld kompromittering.

DAG 4

2.5 TB eksfiltreret ved hjælp af værktøjet rclone. AV-advarsler udløst relateret til Black Basta.

DAG 5 (nat)

Ransomware-udrulning, men blokeret af AV i begyndelsen.

DAG 5 (morgen)

CSIS kontaktes for assistance med IR-sagen.

DAG 5 (eftermiddag)

CSIS anmoder Akamai om nedtagning af data-eksfiltrationsserveren

DAG 6 (morgen)

Data-eksfiltrationsserveren er blevet suspenderet.

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%

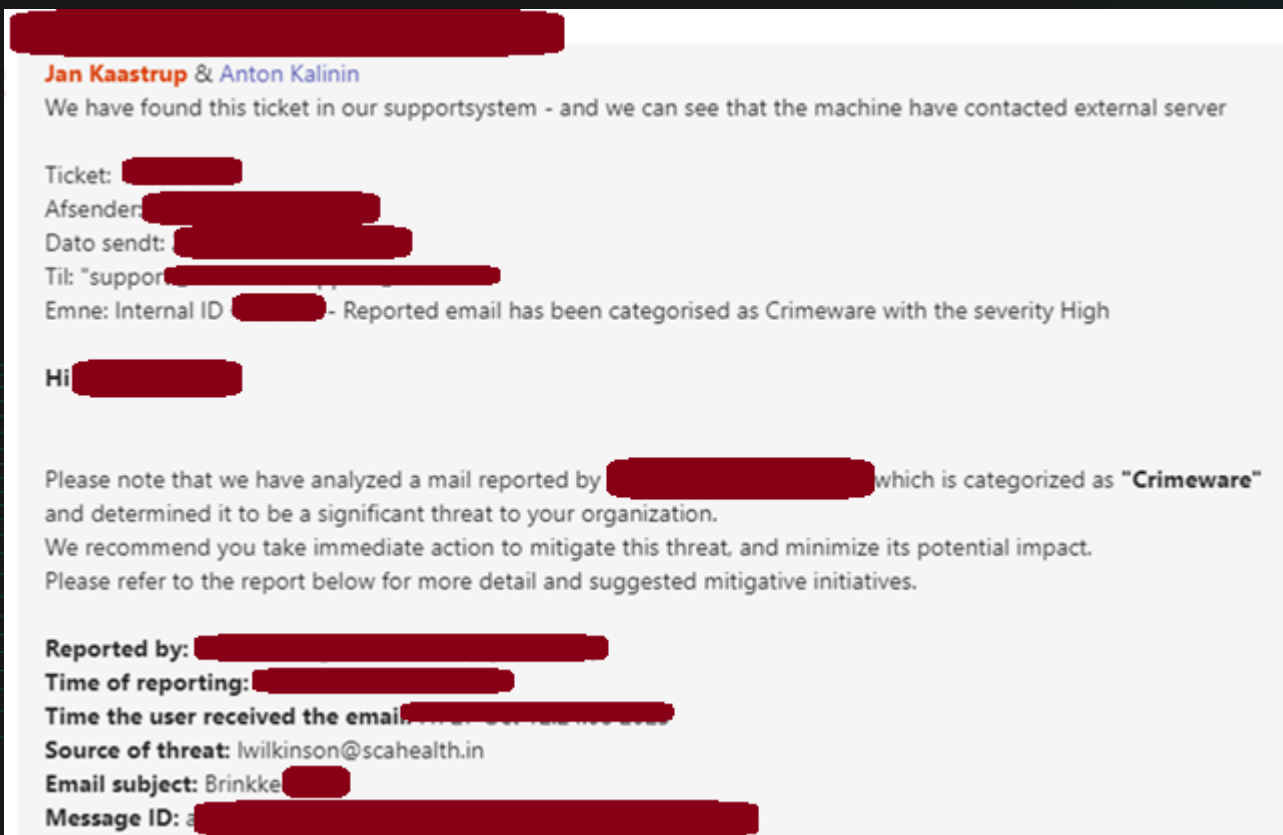
af organisationer har IKKE en formaliseret beredskabsplan

68%

af medarbejdere glemmer træningsindhold inden for en uge

Awareness-træning styrker beredskabet

DU KAN BEGRÆNSE KONSEKVENSERNE AF ET ANGREB



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

- Reager 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 alvorligere ransomware-hændelser er det sjældent angriberne, men ledelsen, der afgør, hvor omfanget af skaden bliver."

Spørgsmål

jka@csis.com

