# Welcome to Bernstorff Slot

orange Cyberdefense

# Cyberdefense, operational resilience, and crisis preparedness in a time of hybrid warfare

## What's on the agenda?

| | |
|---|---|
| 13:15-13:30: | **Presentation of the Program, Speakers, and Orange Cyberdefense.**<br>- Sanne Aagaard, Marketing Manager, Orange Cyberdefense Denmark<br>- Christian Juhl, Sales Director, Orange Cyberdefense Denmark |
| 13:30-14:10: | **Threat Intelligence – Introduction to Today's Threat Landscape.**<br>- Peter Larsson, CTO, Orange Cyberdefense Sweden |
| 14:10-15:10: | **Vestas' Journey From Attack to Enhanced Security.**<br>- Morten Duus, SVP, CISO, Vestas |
| 15:10-15:30: | **Coffee break and networking** |
| 15:30-16:10: | **Cyber Attack Readiness – Fail to Prepare, Prepare to Fail.**<br>- Hampus Glantz, CSIRT Technical Leader, Orange Cyberdefense Sweden |
| 16:10-16:50: | **Maintain Operational Resilience.**<br>- Bo Drejer, GRC Manager, Orange Cyberdefense Denmark<br>- Mats Lindblad, GRC Manager, Orange Cyberdefense Sweden |
| 16:50-17:50: | **The Hostage Negotiator:**<br>**My life in a War Room. Go Behind the Scenes of a Hostage Negotiation.**<br>- Michael Andersen, Data Hostage Negotiator, Psychologist, and Leadership Philosopher |
| 17:50-18:00: | **The professional program ends** |
| 18:00-18:30: | **Before-dinner drink and networking** |
| 18:30-21:00: | **3-course gourmet dinner** |
| 21:00-... | **The bar in the basement is open** |

# A part of Orange

- 137.000 employees

- 296 billion customers
- world wide

- **Global revenue:**
- €44 billion in 2023

**HQ in Paris**

# A part of Orange

Orange Cyberdefense HQ at La Défense in Paris

# We are Orange Cyberdefense

**We are the leading security services provider, supporting your business globally.**

**€1.072 billion**
turnover
in 2023
**+11% YtoY**

**Over 3,000**
multi-skilled cybersecurity experts.

**+8,700**
customers worldwide,
best in class in all verticals.

**Leader** in European Managed Security Services Providers.

FORRESTER

**500+**
sources continuously feed into our threat intelligence datalake.

**Leader** European Managed Security Services.

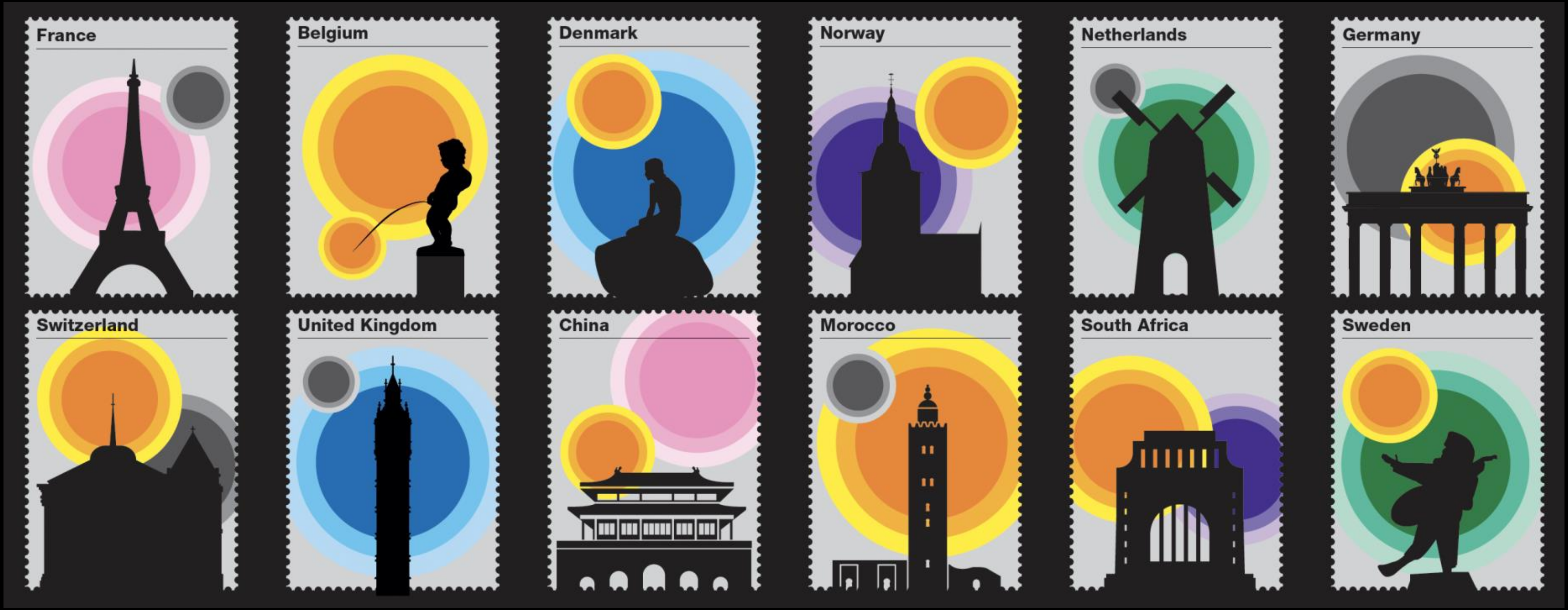
IDC

**24/7/365**
continuous monitoring of security systems worldwide.

**Listed vendor in five reports**
Managed Detection and Response, Incident Response and Digital Forensics, OT Security, Threat Intelligence & Managed Security Services

Gartner

# Orange Cyberdefense’s Local Offices



# Orange Cyberdefense Denmark

We deliver:

- Solution Sales
- Managed Security Services
- Consulting & Trusted Advisery
- 24/7 Monitoring & Support

Offices in
Brøndby
& Aarhus.

SOC
Cyber SOC
CERT

Local
Presence.

Global
Protection.

55 Dedicated and Highly Certified Employees.

Close Nordic & International Collaboration with Diverse Multi-skilled Cybersecurity Expert Teams.

Threat Intelligence Research.

We build a safer digital society

orange™ Cyberdefense

# Hello

## Management

Cyberdefense

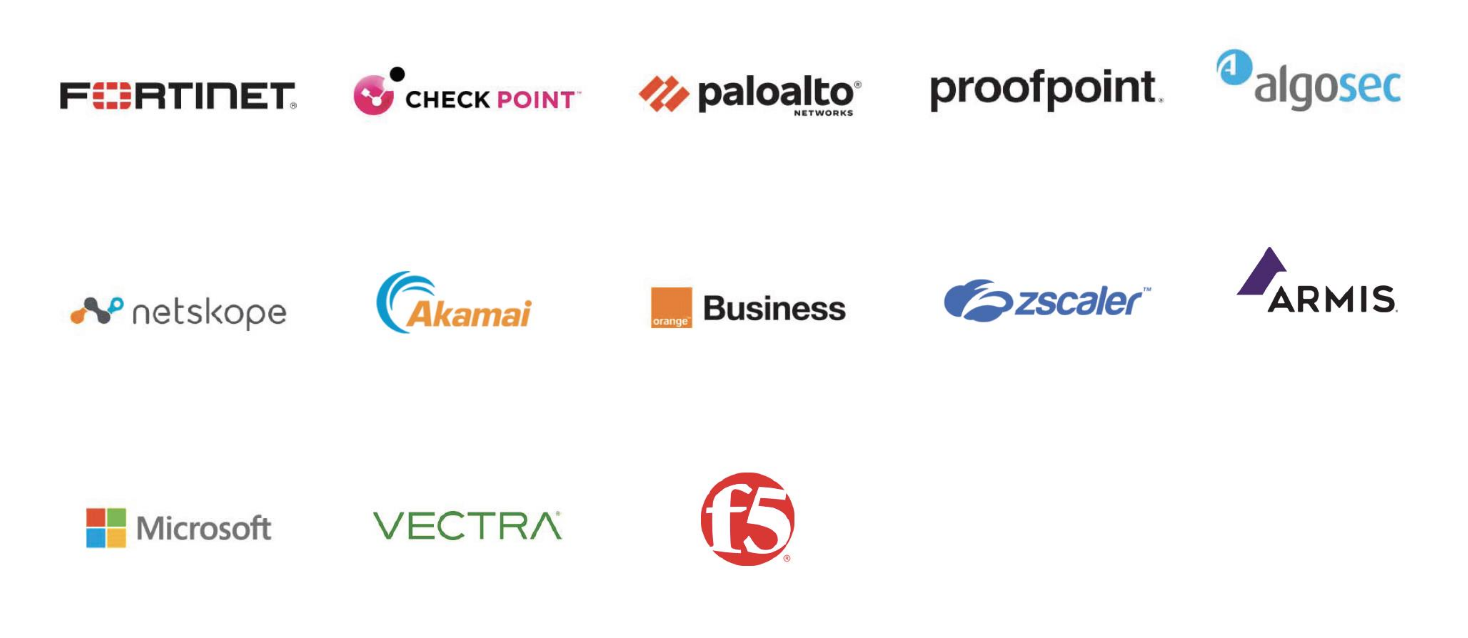
Nice to meet you!

Hugues Foulon
CEO
Orange Cyberdefense

Kaja Narum
EVP Nordic
Orange Cyberdefense

Mårten Toll-Söderblom
Managing Director Denmark
Orange Cyberdefense

# Some of our partners



# Cyberdefense

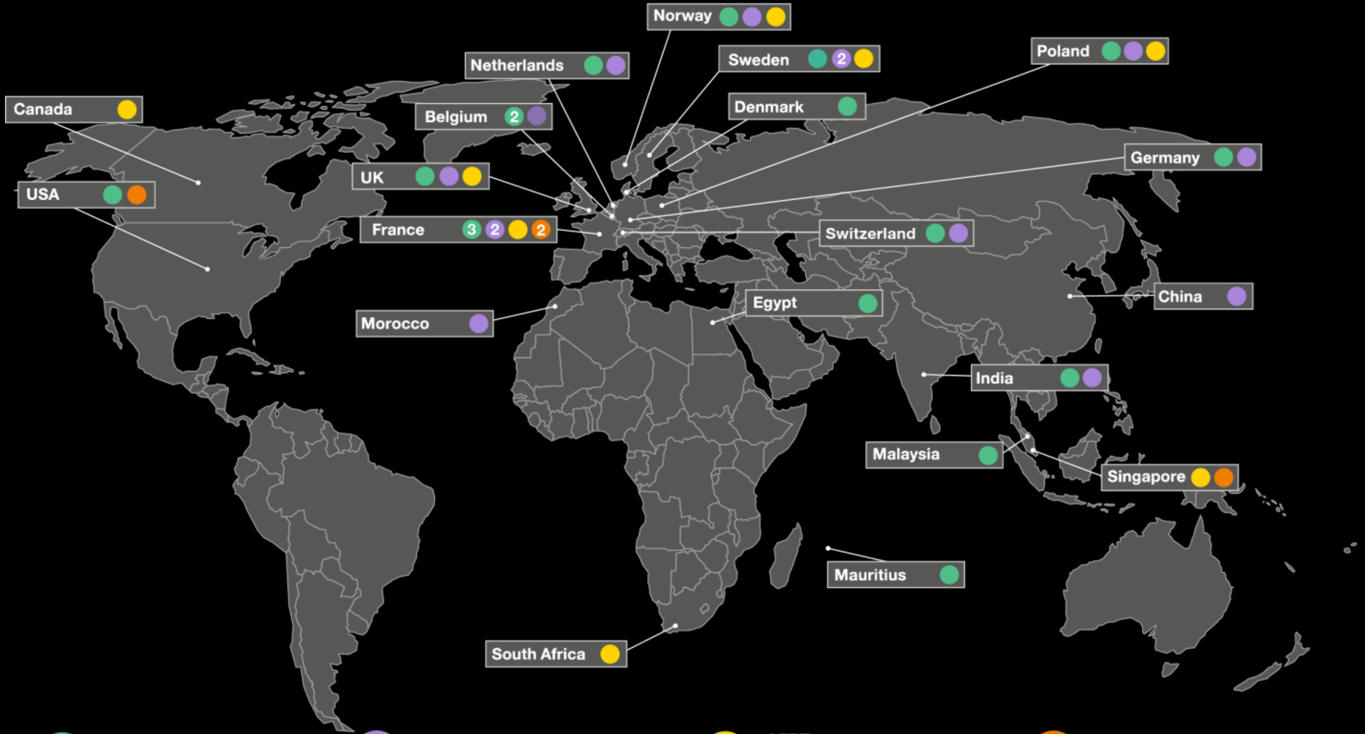
## Our core business

Solution Sales

Consulting & GRC

Managed Security Services

# Global protection with local presence



🟢 18 points of presence of our SOC

🟣 14 points of presence of our CyberSOC

🟡 CERTs operate continuously in 8 locations

🟠 4 scrubbing centers to mitigate DDoS attacks

**ANTICIPATE**
**the latest cyber threats and prevent digital risk.**

- Vulnerability Intelligence
- Threat Advisory

**IDENTIFY**
**your risks and prepare your security strategy.**

- Advisory Consulting
- Cybersecurity Training
- Ethical Hacking
- Penetration Testing
- Vulnerability Scanning

**PROTECT**
**your organization with the right technology and expertise.**

- Cloud Security
- Data-centric Security
- Endpoint Security
- Identity and Access Management
- Infrastructure Security
- Network Security
- OT/ICS Security
- Security Intelligence

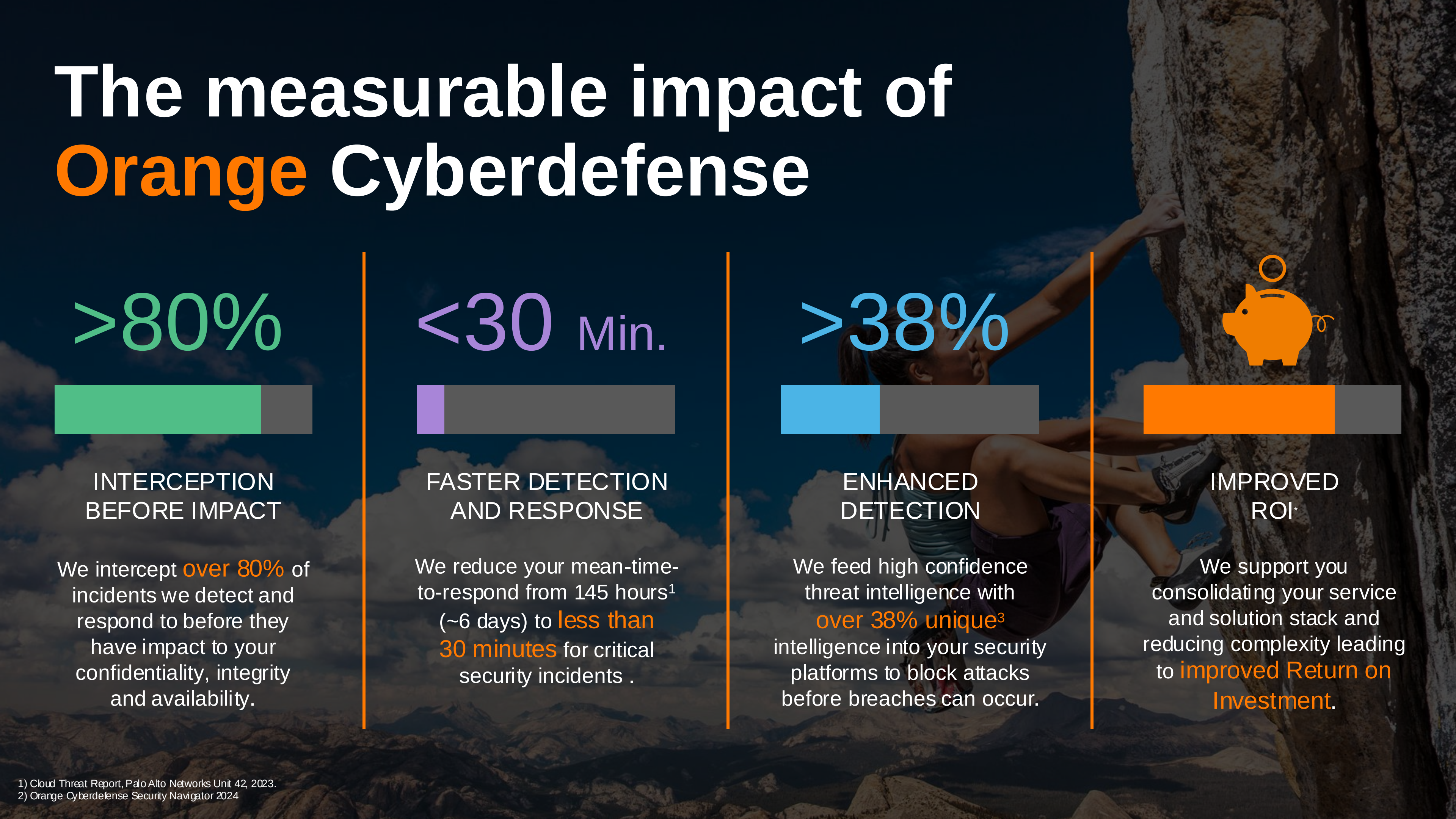
**DETECT**
**cyber attack through analysis of alerts and behavior anomalies.**

- Cybercrime Monitoring
- Threat Detection
  - Endpoint
  - Log
  - Network
  - XDR

**RESPOND**
**to cyber attacks with proper containment and remediation plans.**

- Compromise Assessment
- Digital Forensics
- Emergency Response
- Incident Response
- Threat Response
  - Isolation
  - Takedown

# The measurable impact of Orange Cyberdefense



>80%

INTERCEPTION BEFORE IMPACT

We intercept over 80% of incidents we detect and respond to before they have impact to your confidentiality, integrity and availability.

<30 Min.

FASTER DETECTION AND RESPONSE

We reduce your mean-time-to-respond from 145 hours[1] (~6 days) to less than 30 minutes for critical security incidents .

>38%

ENHANCED DETECTION

We feed high confidence threat intelligence with over 38% unique[3] intelligence into your security platforms to block attacks before breaches can occur.

IMPROVED ROI*

We support you consolidating your service and solution stack and reducing complexity leading to improved Return on Investment.

1) Cloud Threat Report, Palo Alto Networks Unit 42, 2023.
2) Orange Cyberdefense Security Navigator 2024

orange™ Cyberdefense

# Decoding Today's Cyber *Thread*

## A critical analysis of ongoing operations

Peter Larsson – CTO, Orange Cyberdefense Sweden

Diana Selck-Paulsson – Lead Security Researcher, Orange Cyberdefense Group

# 1 Agenda

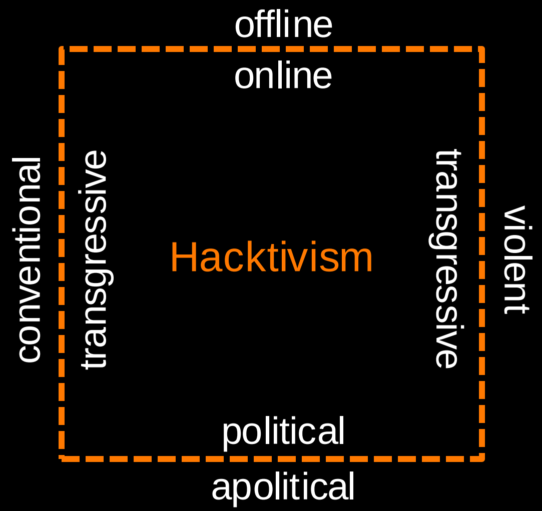
- Several forms of cybercrime
- What’s & Who’s
- Research Findings
- Defenders

# Cyber Threat Against Denmark

**Threat assessment by the Centre for Cyber Security**

- The threat of **cyber crime** against Denmark remains **VERY HIGH**. Cyber crime affects all levels of society.
- The threat of **cyber espionage** against Denmark is **VERY HIGH**. Organizations with access to information on matters of Danish foreign and security policy are often singled out as potential targets of cyber espionage. Danish critical infrastructure and the Danish Defence are also prime targets for foreign cyber espionage. […]primarily comes from **Russia** and **China**.
- The threat of **cyber activism** against Denmark is **HIGH.** The cyber activist attacks that have regularly struck Danish targets emphasize that cyber threats against Danish companies and public authorities have become the norm. […] primarily comes from pro-Russian cyber activists, with some of them being linked to the Russian state.
- The threat of **destructive cyber attacks** is **MEDIUM.** (2023: LOW) Several foreign states have the capabilities to launch destructive cyber attacks against Denmark. The threat of destructive cyber attacks can increase with little or no warning if foreign states decide to strike Danish targets.
- The threat of cyber terrorism is **NONE**. […] there are no actors with the capability
- and intent to conduct cyber terrorism against Denmark.

# 2 Cyber Activism / Hacktivism



offline

online

conventional

transgressive

Hacktivism

transgressive

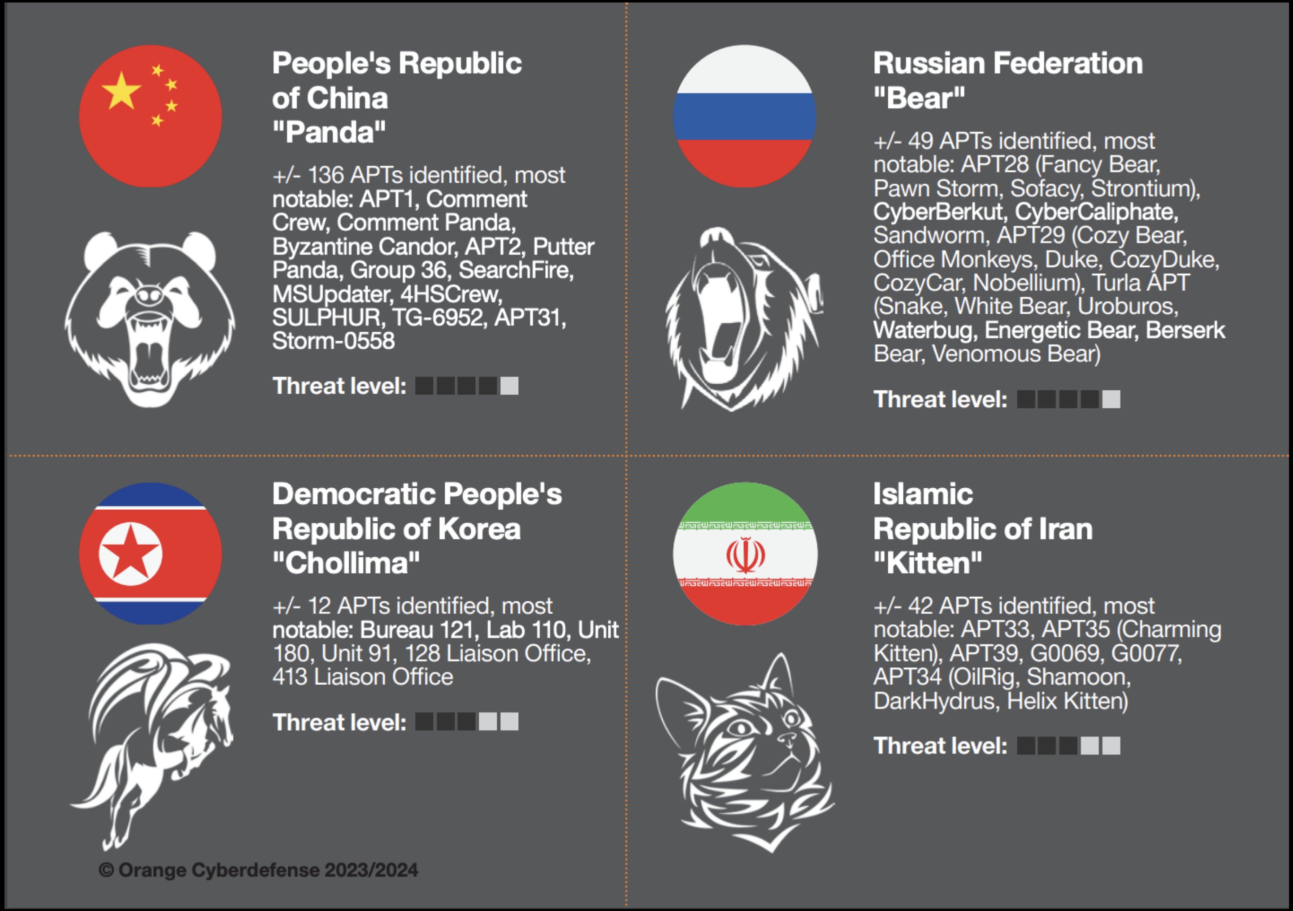
violent

political

apolitical

https://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf

# Cyber Warfare & The Most Active Countries



## People's Republic of China "Panda"

+/- 136 APTs identified, most notable: APT1, Comment Crew, Comment Panda, Byzantine Candor, APT2, Putter Panda, Group 36, SearchFire, MSUpdater, 4HSCrew, SULPHUR, TG-6952, APT31, Storm-0558

**Threat level:** ■■■■□

## Russian Federation "Bear"

+/- 49 APTs identified, most notable: APT28 (Fancy Bear, Pawn Storm, Sofacy, Strontium), CyberBerkut, CyberCaliphate, Sandworm, APT29 (Cozy Bear, Office Monkeys, Duke, CozyDuke, CozyCar, Nobellium), Turla APT (Snake, White Bear, Uroburos, Waterbug, Energetic Bear, Berserk Bear, Venomous Bear)

**Threat level:** ■■■■□

## Democratic People's Republic of Korea "Chollima"

+/- 12 APTs identified, most notable: Bureau 121, Lab 110, Unit 180, Unit 91, 128 Liaison Office, 413 Liaison Office

**Threat level:** ■■■□□

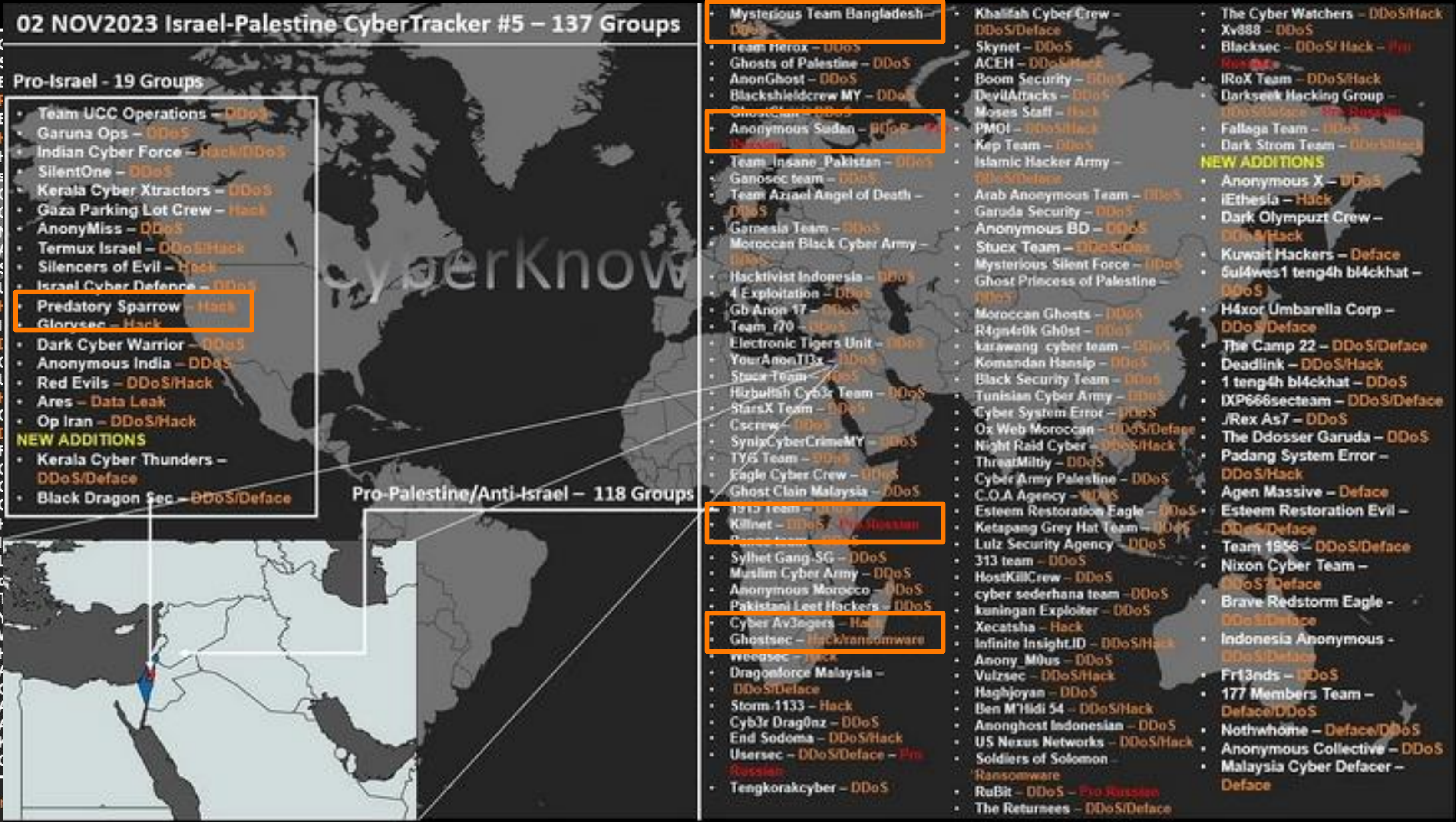
## Islamic Republic of Iran "Kitten"

+/- 42 APTs identified, most notable: APT33, APT35 (Charming Kitten), APT39, G0069, G0077, APT34 (OilRig, Shamoon, DarkHydrus, Helix Kitten)

**Threat level:** ■■■□□

© Orange Cyberdefense 2023/2024

# Hacktivism | Ongoing geopolitical conflicts



## 02 NOV2023 Israel-Palestine CyberTracker #5 – 137 Groups

### Pro-Israel - 19 Groups

- Team UCC Operations – DDoS
- Garuna Ops – DDoS
- Indian Cyber Force – Hack/DDoS
- SilentOne – DDoS
- Kerala Cyber Xtractors – DDoS
- Gaza Parking Lot Crew – Hack
- AnonyMiss – DDoS
- Termux Israel – DDoS/Hack
- Silencers of Evil – Hack
- Israel Cyber Defence – DDoS
- Predatory Sparrow – Hack
- Glorysec – Hack
- Dark Cyber Warrior – DDoS
- Anonymous India – DDoS
- Red Evils – DDoS/Hack
- Ares – Data Leak
- Op Iran – DDoS/Hack

NEW ADDITIONS

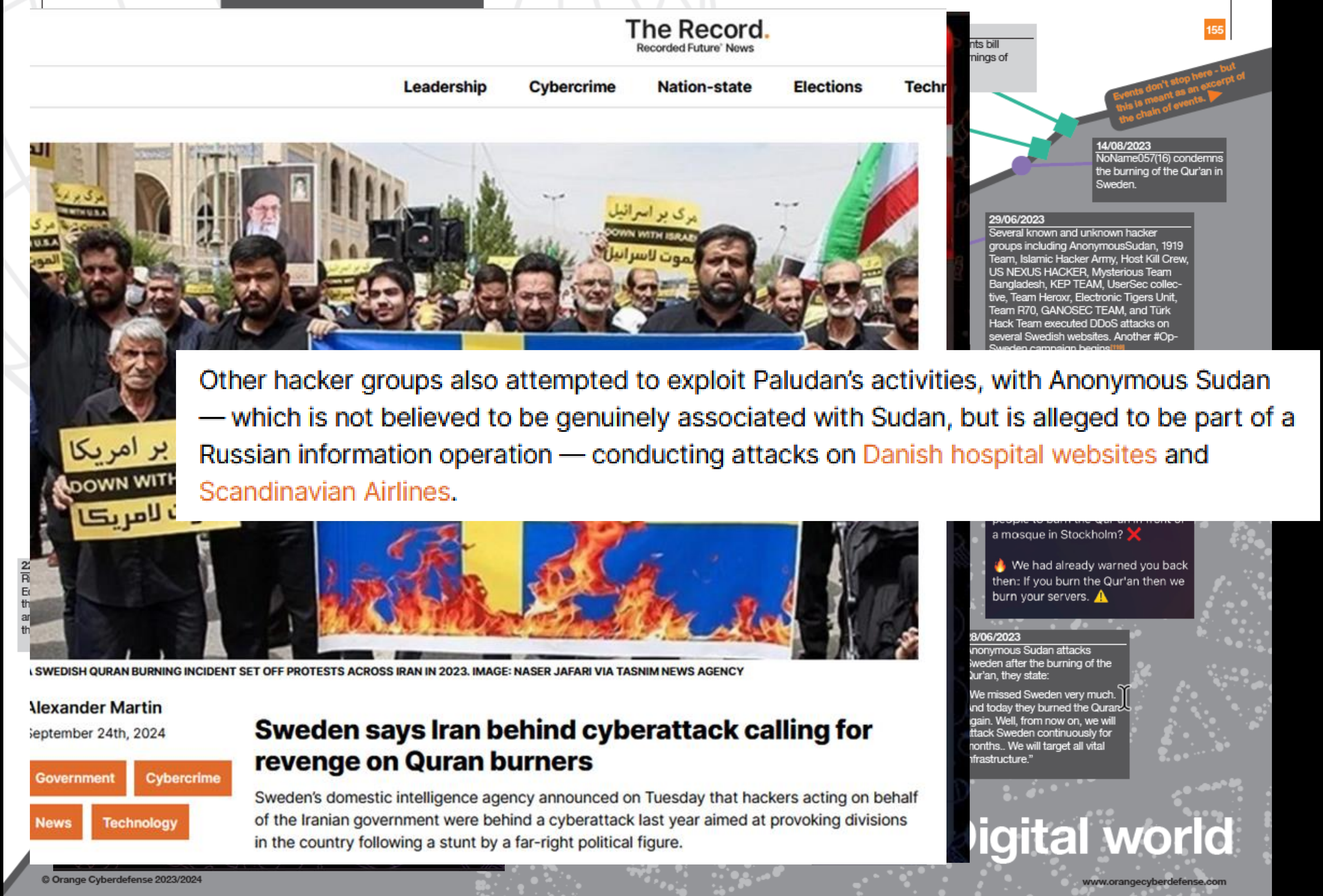
- Kerala Cyber Thunders – DDoS/Deface
- Black Dragon Sec – DDoS/Deface

### Pro-Palestine/Anti-Israel – 118 Groups

- Mysterious Team Bangladesh – DDoS
- Team Herox – DDoS
- Ghosts of Palestine – DDoS
- AnonGhost – DDoS
- Blackshieldcrew MY – DDoS
- GhostClan – DDoS
- Anonymous Sudan – DDoS – Pro-Russian
- Team_Insane_Pakistan – DDoS
- Ganosec team – DDoS
- Team Azrael Angel of Death – DDoS
- Garnesia Team – DDoS
- Moroccan Black Cyber Army – DDoS
- Hacktivist Indonesia – DDoS
- 4 Exploitation – DDoS
- Gb Anon 17 – DDoS
- Team_r70 – DDoS
- Electronic Tigers Unit – DDoS
- YourAnonT13x – DDoS
- Stucx Team – DDoS
- Hizbulla̲h Cyb3r Team – DDoS
- StarsX Team – DDoS
- Cscrew – DDoS
- SynixCyberCrimeMY – DDoS
- TYG Team – DDoS
- Eagle Cyber Crew – DDoS
- Ghost Clain Malaysia – DDoS
- 1915 Team – DDoS
- Killnet – DDoS – Pro-Russian
- Ponce team – DDoS
- Sylhet Gang-SG – DDoS
- Muslim Cyber Army – DDoS
- Anonymous Morocco – DDoS
- Pakistani Leet Hackers – DDoS
- Cyber Av3ngers – Hack
- Ghostsec – Hack/ransomware
- Weedsec – Hack
- Dragonforce Malaysia – DDoS/Deface
- Storm-1133 – Hack
- Cyb3r Drag0nz – DDoS
- End Sodoma – DDoS/Hack
- Usersec – DDoS/Deface – Pro-Russian
- Tengkorakcyber – DDoS
- Khalifah Cyber Crew – DDoS/Deface
- Skynet – DDoS
- ACEH – DDoS/Hack
- Boom Security – DDoS
- DevilAttacks – DDoS
- Moses Staff – Hack
- PMOI – DDoS/Hack
- Kep Team – DDoS
- Islamic Hacker Army – DDoS/Deface
- Arab Anonymous Team – DDoS
- Garuda Security – DDoS
- Anonymous BD – DDoS
- Stucx Team – DDoS/Data
- Mysterious Silent Force – DDoS
- Ghost Princess of Palestine – DDoS
- Moroccan Ghosts – DDoS
- R4gn4r0k Gh0st – DDoS
- karawang cyber team – DDoS
- Komandan Hansip – DDoS
- Black Security Team – DDoS
- Tunisian Cyber Army – DDoS
- Cyber System Error – DDoS
- 0x Web Moroccan – DDoS/Deface
- Night Raid Cyber – DDoS/Hack
- ThreatMiltiy – DDoS
- Cyber Army Palestine – DDoS
- C.O.A Agency – DDoS
- Esteem Restoration Eagle – DDoS
- Ketapang Grey Hat Team – DDoS
- Lulz Security Agency – DDoS
- 313 team – DDoS
- HostKillCrew – DDoS
- cyber sederhana team – DDoS
- kuningan Exploiter – DDoS
- Xecatsha – Hack
- Infinite Insight.ID – DDoS/Hack
- Anony_M0us – DDoS
- Vulzsec – DDoS/Hack
- Haghjoyan – DDoS
- Ben M'Hidi 54 – DDoS/Hack
- Anonghost Indonesian – DDoS
- US Nexus Networks – DDoS/Hack
- Soldiers of Solomon – Ransomware
- RuBit – DDoS – Pro-Russian
- The Returnees – DDoS/Deface
- The Cyber Watchers – DDoS/Hack
- Xv888 – DDoS
- Blacksec – DDoS/ Hack – Pro-Russian
- IRoX Team – DDoS/Hack
- Darkseek Hacking Group – DDoS/Deface – Pro-Russian
- Fallaga Team – DDoS
- Dark Strom Team – DDoS/Hack

NEW ADDITIONS

- Anonymous X – DDoS
- iEthesia – Hack
- Dark Olympuzt Crew – DDoS/Hack
- Kuwait Hackers – Deface
- 6ul4wes1 teng4h bl4ckhat – DDoS
- H4xor Umbarella Corp – DDoS/Deface
- The Camp 22 – DDoS/Deface
- Deadlink – DDoS/Hack
- 1 teng4h bl4ckhat – DDoS
- IXP666secteam – DDoS/Deface
- ./Rex As7 – DDoS
- The Ddosser Garuda – DDoS
- Padang System Error – DDoS/Hack
- Agen Massive – Deface
- Esteem Restoration Evil – DDoS/Deface
- Team 1956 – DDoS/Deface
- Nixon Cyber Team – DDoS/Deface
- Brave Redstorm Eagle - DDoS/Deface
- Indonesia Anonymous - DDoS/Deface
- Fr13nds – DDoS
- 177 Members Team – Deface/DDoS
- Nothwhome – Deface/DDoS
- Anonymous Collective – DDoS
- Malaysia Cyber Defacer – Deface



Other hacker groups also attempted to exploit Paludan's activities, with Anonymous Sudan — which is not believed to be genuinely associated with Sudan, but is alleged to be part of a Russian information operation — conducting attacks on Danish hospital websites and Scandinavian Airlines.

**The Record.**
Recorded Future® News

Leadership | Cybercrime | Nation-state | Elections | Techn

A SWEDISH QURAN BURNING INCIDENT SET OFF PROTESTS ACROSS IRAN IN 2023. IMAGE: NASER JAFARI VIA TASNIM NEWS AGENCY

Alexander Martin
September 24th, 2024

Government | Cybercrime | News | Technology

## Sweden says Iran behind cyberattack calling for revenge on Quran burners

Sweden's domestic intelligence agency announced on Tuesday that hackers acting on behalf of the Iranian government were behind a cyberattack last year aimed at provoking divisions in the country following a stunt by a far-right political figure.

155

nts bill
nings of

Events don't stop here - but this is meant as an excerpt of the chain of events.

**14/08/2023**
NoName057(16) condemns the burning of the Qur'an in Sweden.

**29/06/2023**
Several known and unknown hacker groups including AnonymousSudan, 1919 Team, Islamic Hacker Army, Host Kill Crew, US NEXUS HACKER, Mysterious Team Bangladesh, KEP TEAM, UserSec collective, Team Heroxr, Electronic Tigers Unit, Team R70, GANOSEC TEAM, and Türk Hack Team executed DDoS attacks on several Swedish websites. Another #OpSweden campaign begins[118]

a mosque in Stockholm? ❌

🔥 We had already warned you back then:: If you burn the Qur'an then we burn your servers. ⚠️

**28/06/2023**
Anonymous Sudan attacks Sweden after the burning of the Qur'an, they state:

We missed Sweden very much. And today they burned the Quran again. Well, from now on, we will attack Sweden continuously for months.. We will target all vital infrastructure."

Digital world

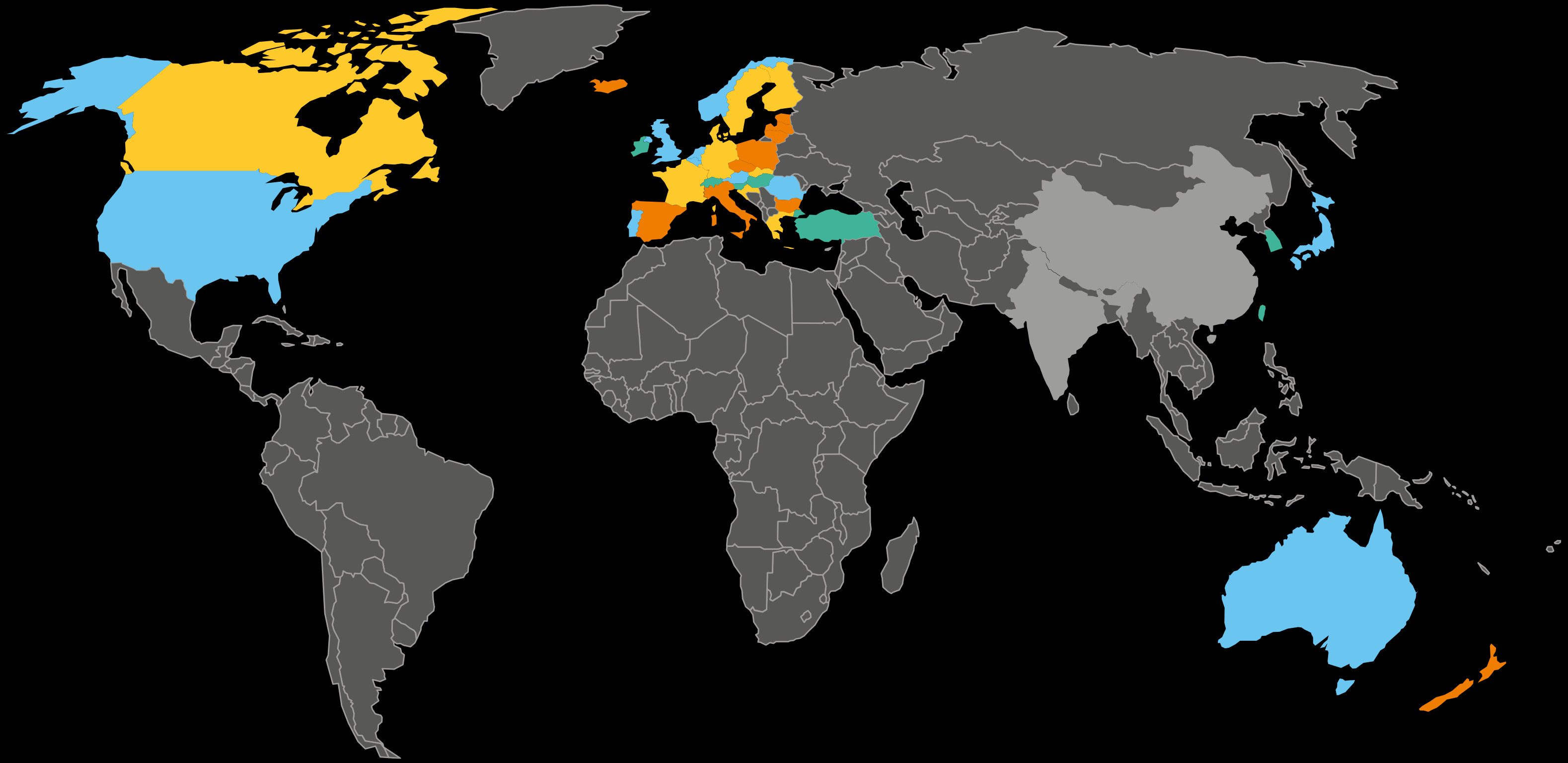
© Orange Cyberdefense 2023/2024

www.orangecyberdefense.com

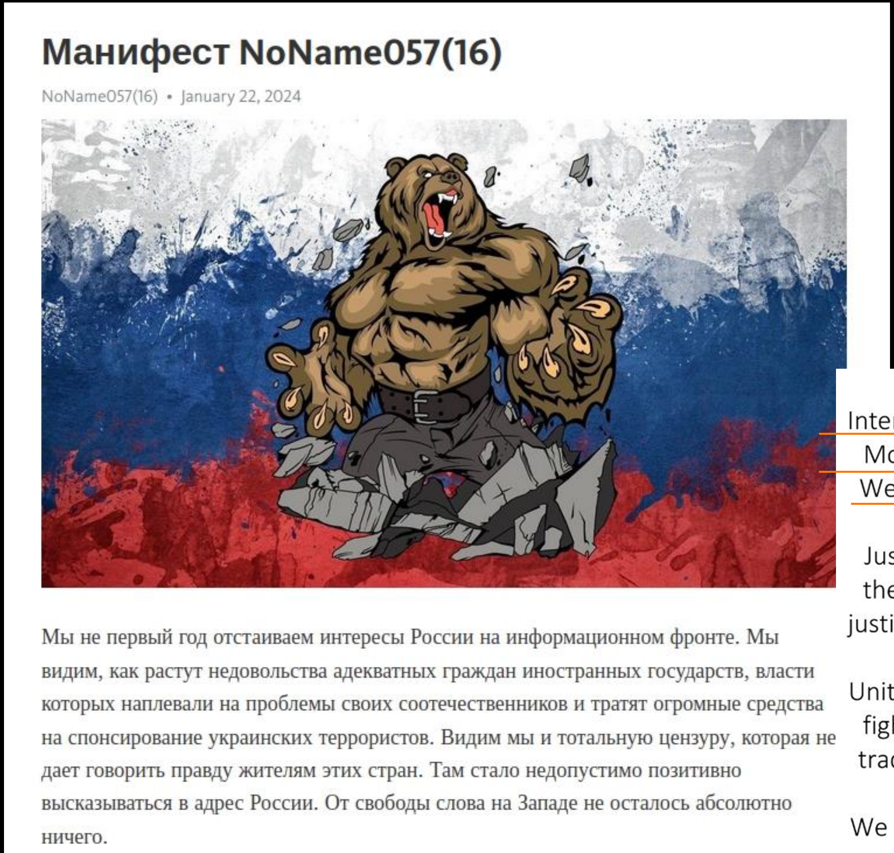
# NoName057(16): victim rank vs. donations (Map)

Difference in terms of the relation of attacks by NoName057(16) to donations of the victim country for Ukraine

🟩 1. Under-attacked/involved 🟧 2. Over-attacked/involved 🟨 3. Proportionate/involved ⬜ 4. Proportionate/uninvolved 🟦 5. Under-attacked/heavily involved



# NoName057(16)'s Manifesto



## Манифест NoName057(16)

NoName057(16) • January 22, 2024

Мы не первый год отстаиваем интересы России на информационном фронте. Мы видим, как растут недовольства адекватных граждан иностранных государств, власти которых наплевали на проблемы своих соотечественников и тратят огромные средства на спонсирование украинских террористов. Видим мы и тотальную цензуру, которая не дает говорить правду жителям этих стран. Там стало недопустимо позитивно высказываться в адрес России. От свободы слова на Западе не осталось абсолютно ничего.

'This is not the first year that we have been defending Russia's interests on the information front. We see how the discontent of adequate citizens of foreign countries is growing, whose authorities do not care about the problems of their compatriots and spend huge amounts of money on sponsoring Ukrainian terrorists. We also see total censorship, which prevents the residents of these countries from telling the truth. There it has become unacceptable to speak positively about Russia. There is absolutely nothing left of freedom of speech in the West[…].

Our project has long gone beyond the concept of a hacker group. We believe that you don't have to be a hacker to be a warrior - we have tasks for all volunteers, regardless of their competencies. Western elites have become a symbol of total unprincipled lies. The goal of the West is only endless power over the world and, as a result, its oppression. We must fight this! There is power in truth, that's what we stand for!

Our values:

Internationalism - we firmly believe in the greatness of Russia in the international arena. Our Motherland is a bastion of justice, rebelling against the lies and hypocrisy of the collective West. The fighters of our cyber army may live in different countries, but they must respect Russia.

Justice - one of our slogans is: "Justice has no name. "NoName". We are ready to come to the aid of our like-minded people anywhere in the world and make every effort to restore justice and punish their offenders. We help those who are weaker and learn from those who are stronger.

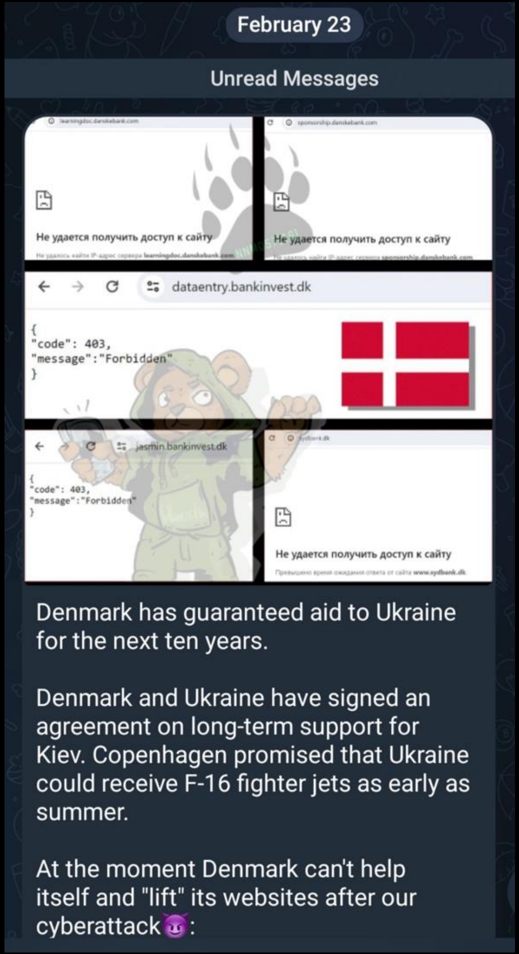
Unity - it doesn't matter to us what skin color, eye shape, language or place of residence our fighters have. One thing is important - that they are our like-minded people and share the traditional values of Russia. The word "Russian" has ceased to be a nationality. "Russian" is now an ideology. The ideology of a just world order and freedom.

We remain ready to cooperate with other pro-Russian hacker groups and free shooters who share our values listed in the Manifesto.'

# Cyber Activism/Hacktivism

> "Hvis danske myndigheder tror, at vi vil stoppe vores cyberangreb, så tager de fejl. Så længe de støtter Zelenskyjs kriminelle regime, vil vi fortsætte med at teste deres internetinfrastruktur til det yderste.
>
> NoName057(16)
> Pro-russisk hackergruppe

NoName057(16) har taget ansvaret for en række af de DDoS-angreb, der bl.a. ramte Forsvarsministeriets, Københavns lufthavns, Movias, DOT's, Trafikstyrelsens og en række kommuners hjemmesider i slutningen af februar 2024. Angrebene kommer i kølvandet på regeringens udmelding om, at Danmark garanterer økonomisk støtte til Ukraine de næste 10 år.



February 23

Unread Messages

Не удается получить доступ к сайту

Не удается получить доступ к сайту

dataentry.bankinvest.dk

```
{
"code": 403,
"message":"Forbidden"
}
```

jasmin.bankinvest.dk

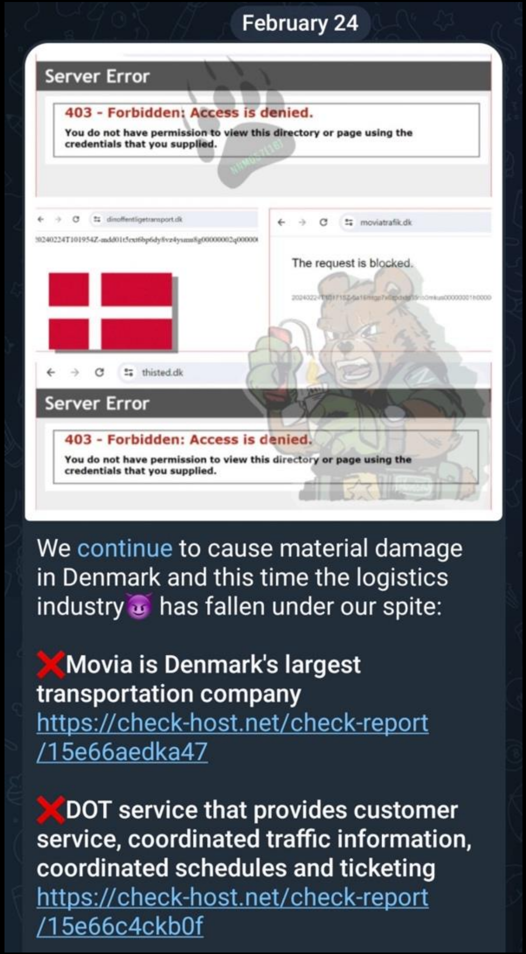
```
{
"code": 403,
"message":"Forbidden"
}
```

Не удается получить доступ к сайту

Denmark has guaranteed aid to Ukraine for the next ten years.

Denmark and Ukraine have signed an agreement on long-term support for Kiev. Copenhagen promised that Ukraine could receive F-16 fighter jets as early as summer.

At the moment Denmark can't help itself and "lift" its websites after our cyberattack😈:



February 24

Server Error

403 - Forbidden: Access is denied.

You do not have permission to view this directory or page using the credentials that you supplied.

dinoffentligetransport.dk

moviatrafik.dk

The request is blocked.

thisted.dk

Server Error

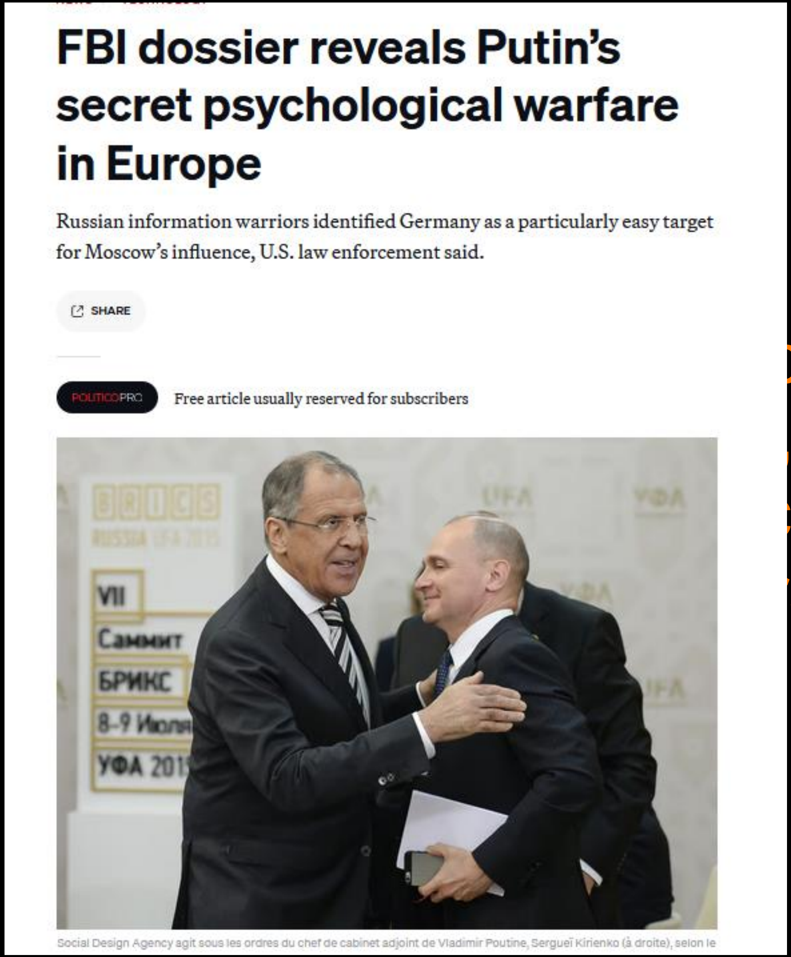
403 - Forbidden: Access is denied.

You do not have permission to view this directory or page using the credentials that you supplied.

We continue to cause material damage in Denmark and this time the logistics industry😈 has fallen under our spite:

❌Movia is Denmark's largest transportation company
https://check-host.net/check-report/15e66aedka47

❌DOT service that provides customer service, coordinated traffic information, coordinated schedules and ticketing
https://check-host.net/check-report/15e66c4ckb0f

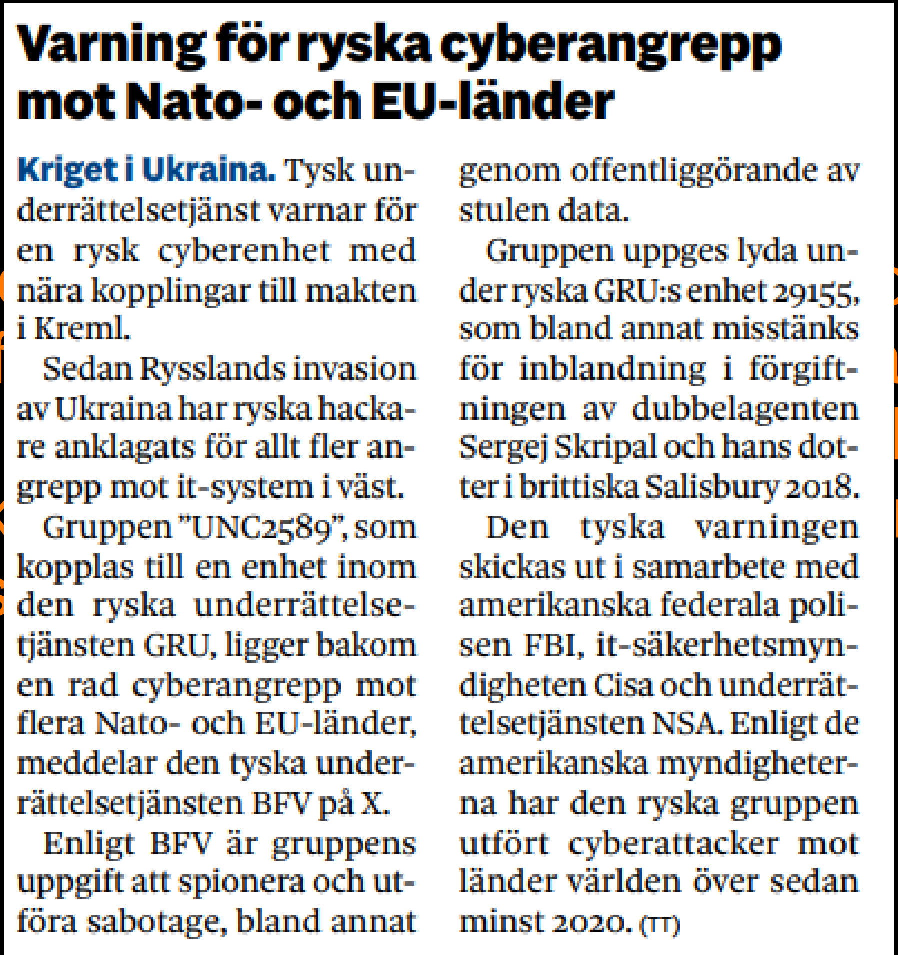


# FBI dossier reveals Putin's secret psychological warfare in Europe

Russian information warriors identified Germany as a particularly easy target for Moscow's influence, U.S. law enforcement said.

Free article usually reserved for subscribers

Social Design Agency agit sous les ordres du chef de cabinet adjoint de Vladimir Poutine, Sergueï Kirienko (à droite), selon le



# Varning för ryska cyberangrepp mot Nato- och EU-länder

**Kriget i Ukraina.** Tysk underrättelsetjänst varnar för en rysk cyberenhet med nära kopplingar till makten i Kreml.

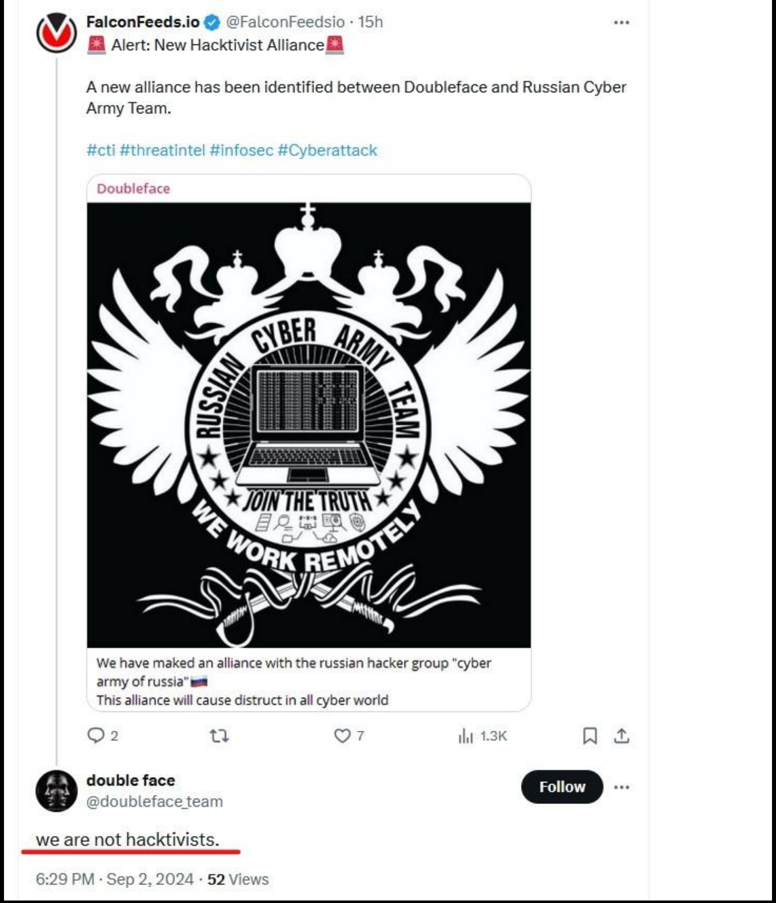
Sedan Rysslands invasion av Ukraina har ryska hackare anklagats för allt fler angrepp mot it-system i väst.

Gruppen "UNC2589", som kopplas till en enhet inom den ryska underrättelsetjänsten GRU, ligger bakom en rad cyberangrepp mot flera Nato- och EU-länder, meddelar den tyska underrättelsetjänsten BFV på X.

Enligt BFV är gruppens uppgift att spionera och utföra sabotage, bland annat genom offentliggörande av stulen data.

Gruppen uppges lyda under ryska GRU:s enhet 29155, som bland annat misstänks för inblandning i förgiftningen av dubbelagenten Sergej Skripal och hans dotter i brittiska Salisbury 2018.

Den tyska varningen skickas ut i samarbete med amerikanska federala polisen FBI, it-säkerhetsmyndigheten Cisa och underrättelsetjänsten NSA. Enligt de amerikanska myndigheterna har den ryska gruppen utfört cyberattacker mot länder världen över sedan minst 2020. (TT)



FalconFeeds.io @FalconFeedsio · 15h

🚨 Alert: New Hacktivist Alliance🚨

A new alliance has been identified between Doubleface and Russian Cyber Army Team.

#cti #threatintel #infosec #Cyberattack

Doubleface

We have maked an alliance with the russian hacker group "cyber army of russia"🇷🇺
This alliance will cause distruct in all cyber world

double face
@doubleface_team

we are not hacktivists.

6:29 PM · Sep 2, 2024 · 52 Views

Cyber Militia?

**Information warfare?**

**Hybrid Warfare?**

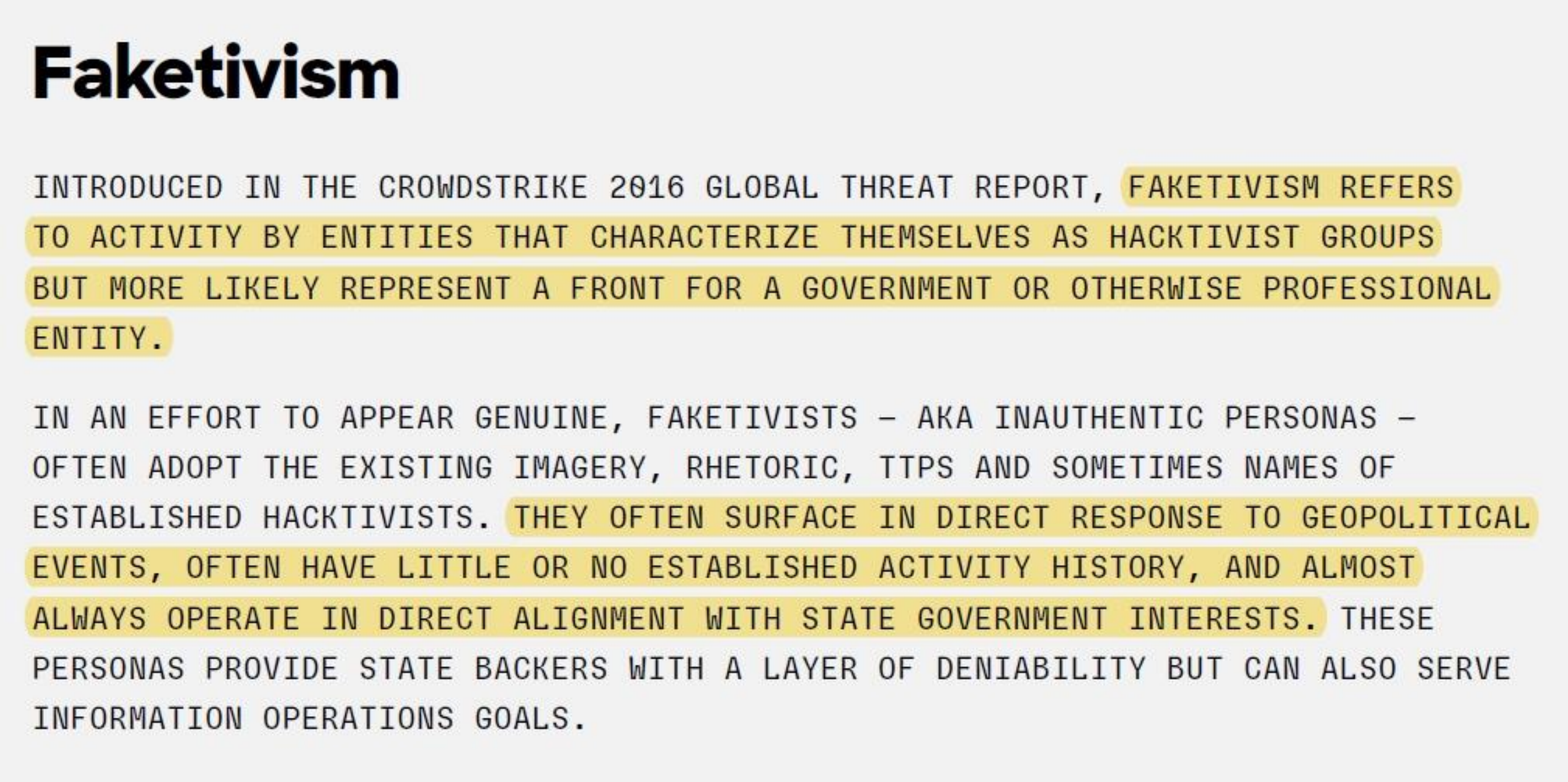
**Cyber Terrorism?**

**E-crime / cybercrime?**

**Hacktivism?**

**Cyber Vigilantism?**

**Faketivism?**



# Faketivism

INTRODUCED IN THE CROWDSTRIKE 2016 GLOBAL THREAT REPORT, FAKETIVISM REFERS TO ACTIVITY BY ENTITIES THAT CHARACTERIZE THEMSELVES AS HACKTIVIST GROUPS BUT MORE LIKELY REPRESENT A FRONT FOR A GOVERNMENT OR OTHERWISE PROFESSIONAL ENTITY.

IN AN EFFORT TO APPEAR GENUINE, FAKETIVISTS – AKA INAUTHENTIC PERSONAS – OFTEN ADOPT THE EXISTING IMAGERY, RHETORIC, TTPS AND SOMETIMES NAMES OF ESTABLISHED HACKTIVISTS. THEY OFTEN SURFACE IN DIRECT RESPONSE TO GEOPOLITICAL EVENTS, OFTEN HAVE LITTLE OR NO ESTABLISHED ACTIVITY HISTORY, AND ALMOST ALWAYS OPERATE IN DIRECT ALIGNMENT WITH STATE GOVERNMENT INTERESTS. THESE PERSONAS PROVIDE STATE BACKERS WITH A LAYER OF DENIABILITY BUT CAN ALSO SERVE INFORMATION OPERATIONS GOALS.

# 3 Cy-X / Ransomware

Cyberdefense

# Cy-Xplorer 2024

When bits turn to blackmail: navigating the ecosystem of cyber extortion and ransomware

Reposting Activity

Current Threat Lands

Cy-X over time

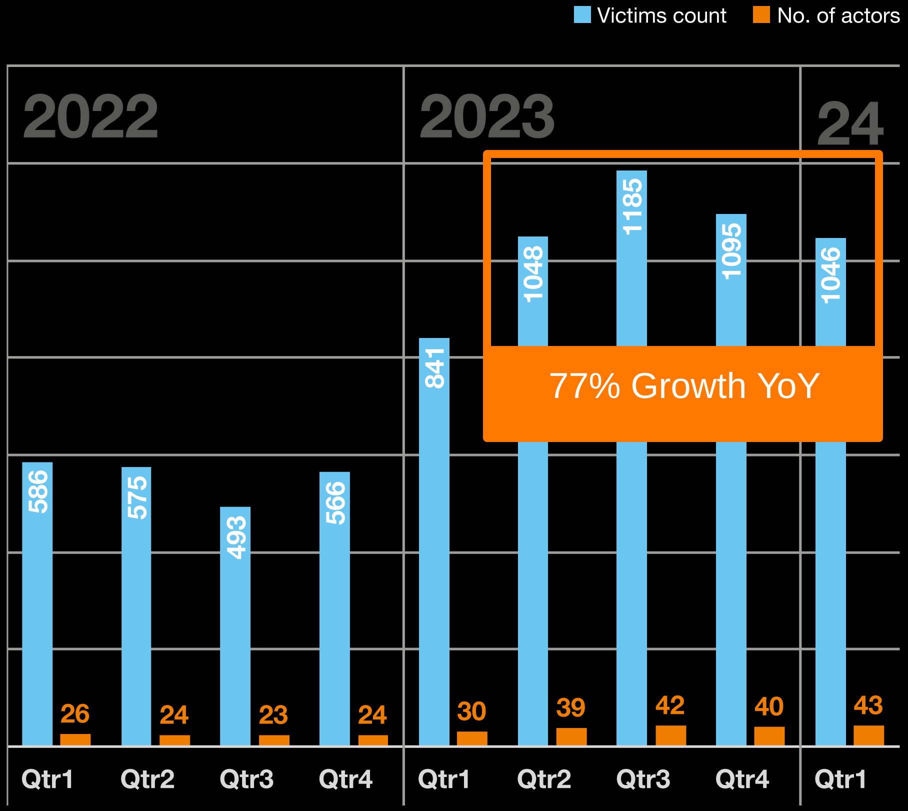
Cyberdefense

Cy-Xplorer 2024

When bits turn to blackmail: navigating the ecosystem of cyber extortion and ransomware

# Cy-X trends – past 24 months

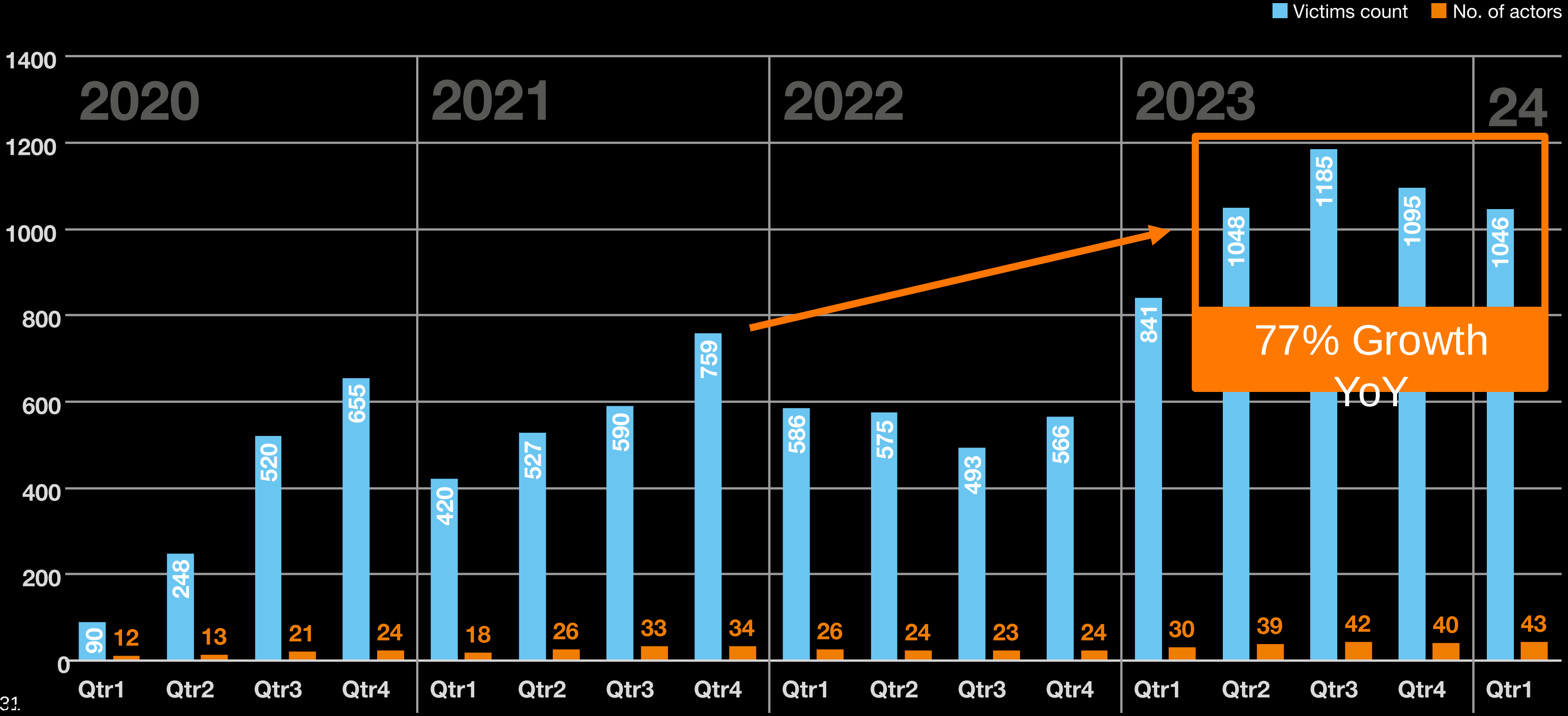
Victims and actors count observed on double-extortion leak sites over time



77% Growth YoY

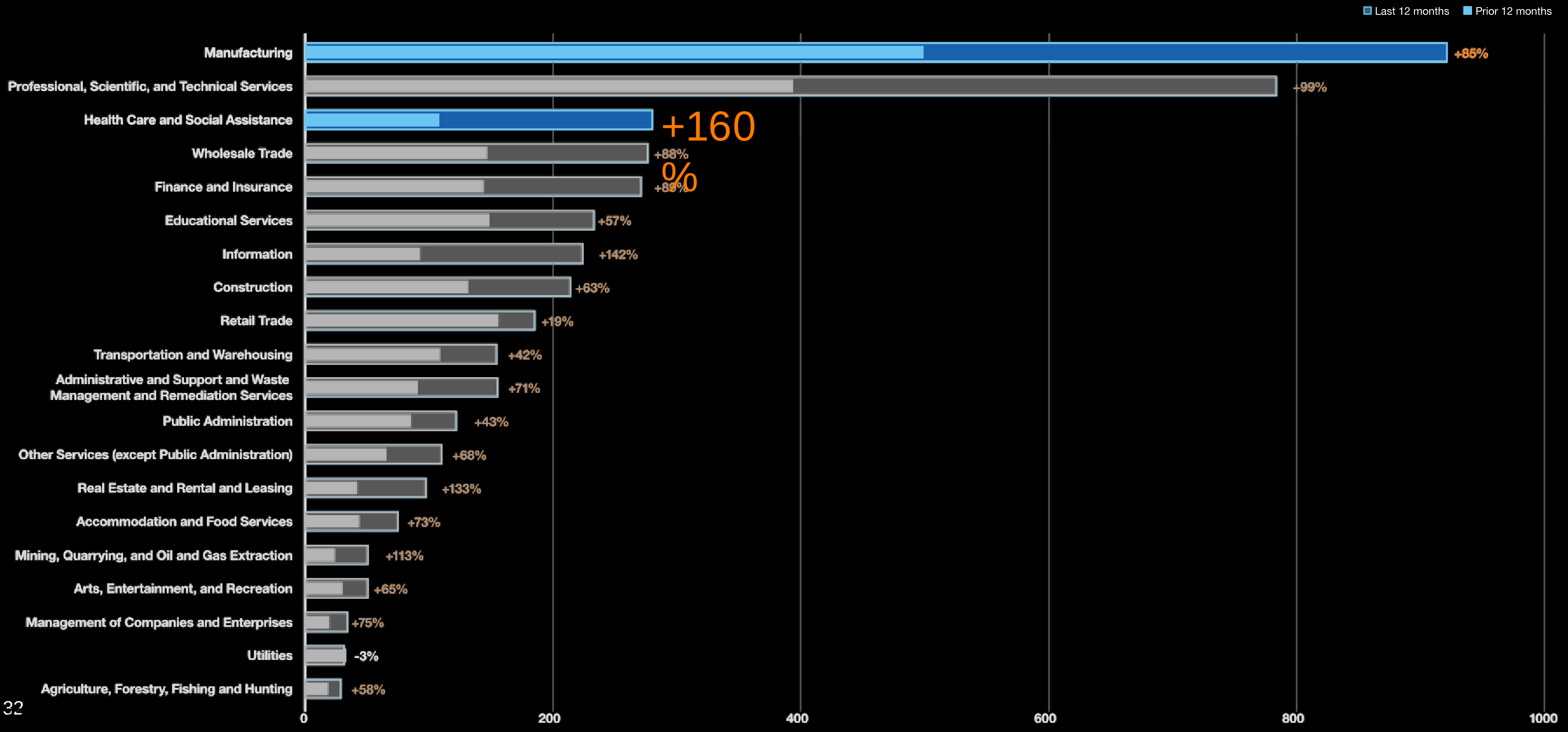
# Cy-X over time

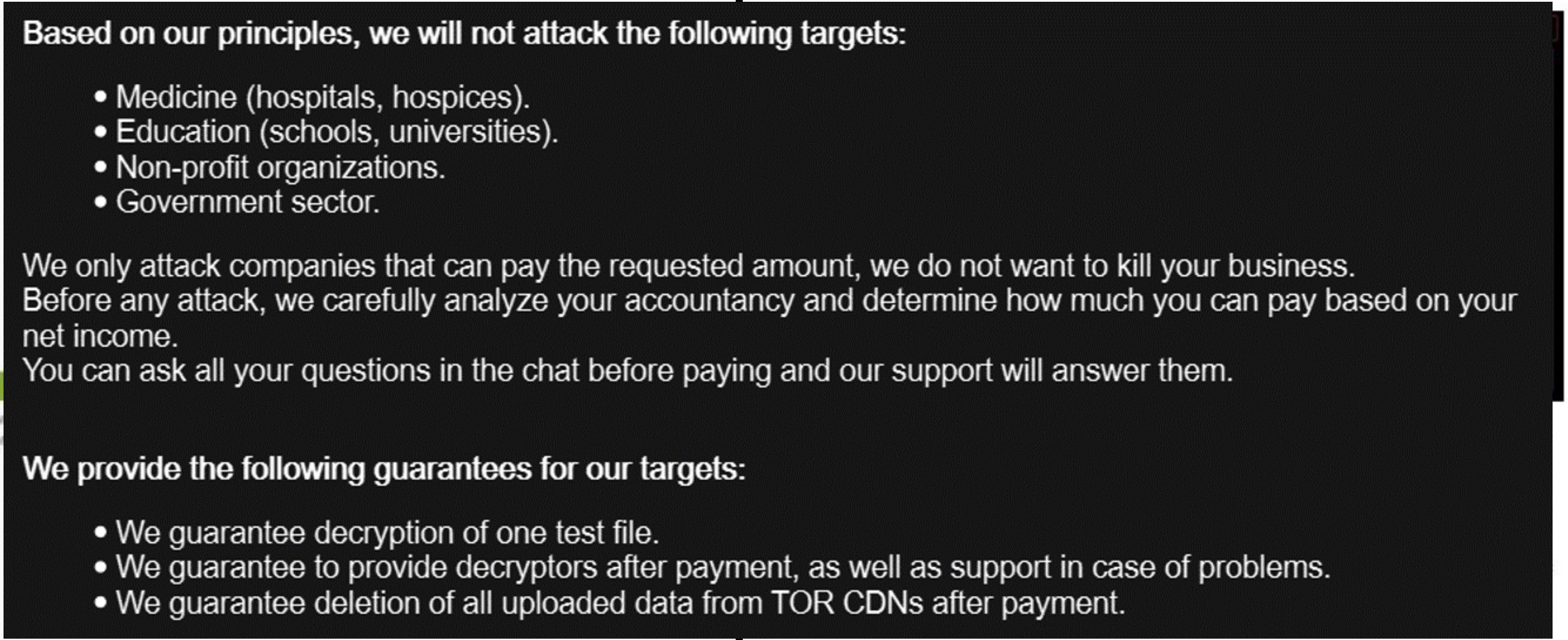
Victims and actors count observed on double-extortion leak sites over time



# Shift in victims by industry

## Industry breakdown: comparison between the last and prior year





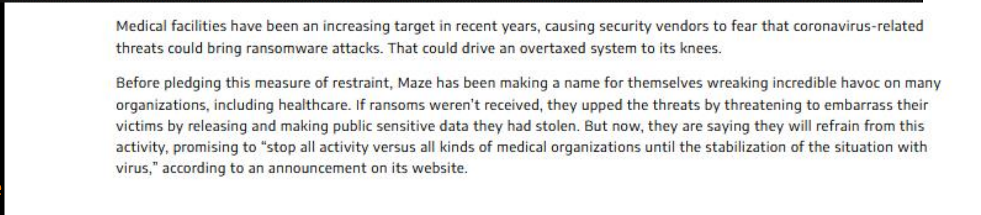
**Based on our principles, we will not attack the following targets:**

- Medicine (hospitals, hospices).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business.
Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income.
You can ask all your questions in the chat before paying and our support will answer them.

**We provide the following guarantees for our targets:**

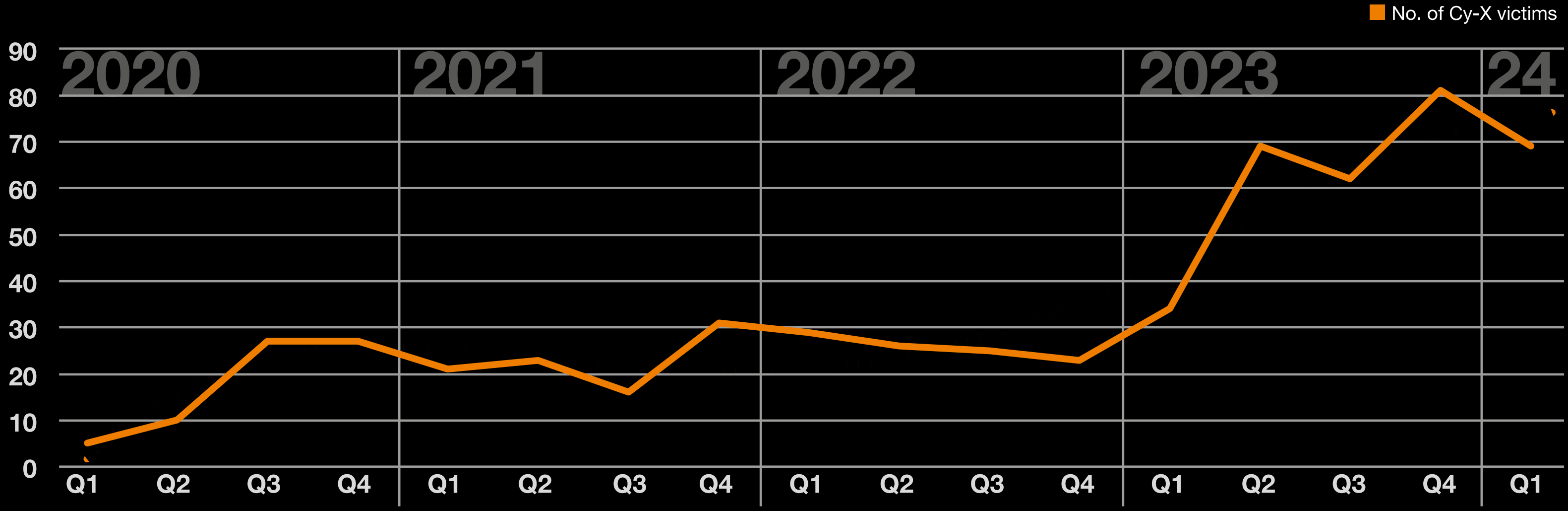
- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.



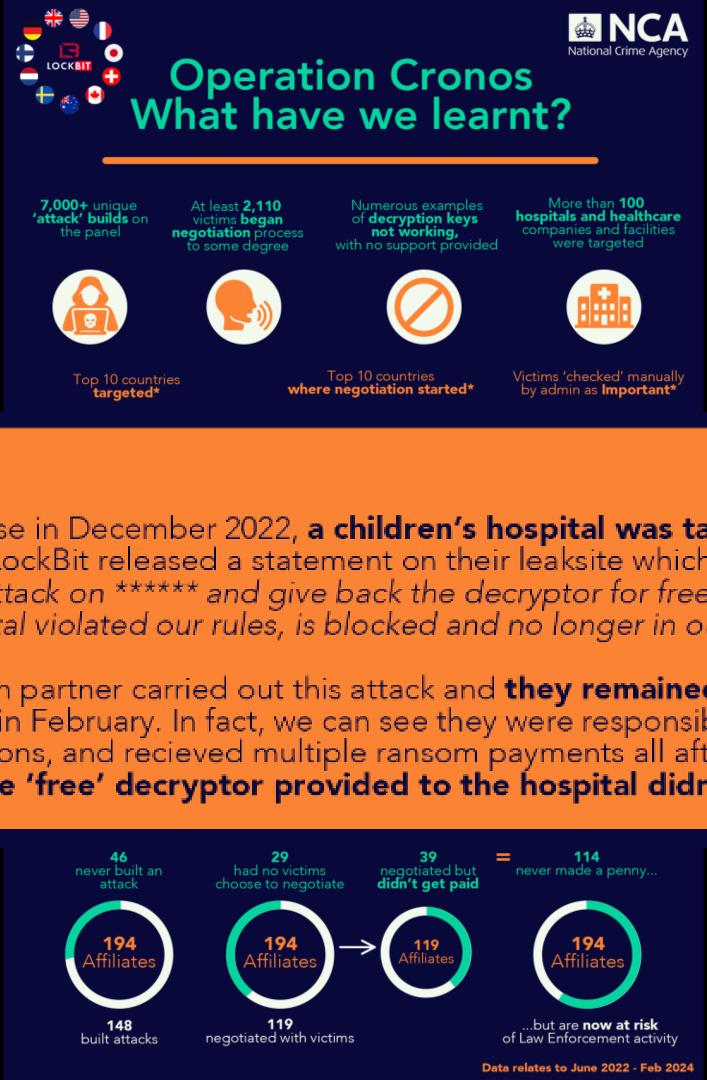
Medical facilities have been an increasing target in recent years, causing security vendors to fear that coronavirus-related threats could bring ransomware attacks. That could drive an overtaxed system to its knees.

Before pledging this measure of restraint, Maze has been making a name for themselves wreaking incredible havoc on many organizations, including healthcare. If ransoms weren't received, they upped the threats by threatening to embarrass their victims by releasing and making public sensitive data they had stolen. But now, they are saying they will refrain from this activity, promising to "stop all activity versus all kinds of medical organizations until the stabilization of the situation with virus," according to an announcement on its website.

# Healthcare



| Subindustry | % of victims |
|---|---|
| Ambulatory Health Care Services | 37.37% |
| Hospitals | 16.73% |
| Offices of Physicians | 9.61% |
| Social Assistance | 7.47% |
| Nursing and Residential Care Facilities | 7.12% |



# Operation Cronos What have we learnt?

**7,000+** unique **'attack' builds** on the panel

At least **2,110** victims **began negotiation** process to some degree

Numerous examples of **decryption keys not working,** with no support provided

More than **100 hospitals and healthcare** companies and facilities were targeted

Top 10 countries **targeted***

Top 10 countries **where negotiation started***

Victims 'checked' manually by admin as **Important***

## Case study

In one particular case in December 2022, **a children's hospital was targeted** by the group. After a complaint, LockBit released a statement on their leaksite which said *"We formally apologise for the attack on ****** and give back the decryptor for free. The partner who attacked this hospital violated our rules, is blocked and no longer in our affiliate program"*.
**This was a lie.**
We now know which partner carried out this attack and **they remained an active LockBit actor** until our operation in February. In fact, we can see they were responsible for 127 unique attack builds, 50 negotiations, and recieved multiple ransom payments all after apparently being fired by LockBit. **The 'free' decryptor provided to the hospital didn't work** properly either.

**46** never built an attack

**29** had no victims choose to negotiate

**39** negotiated but **didn't get paid**

= **114** never made a penny...

**148** built attacks

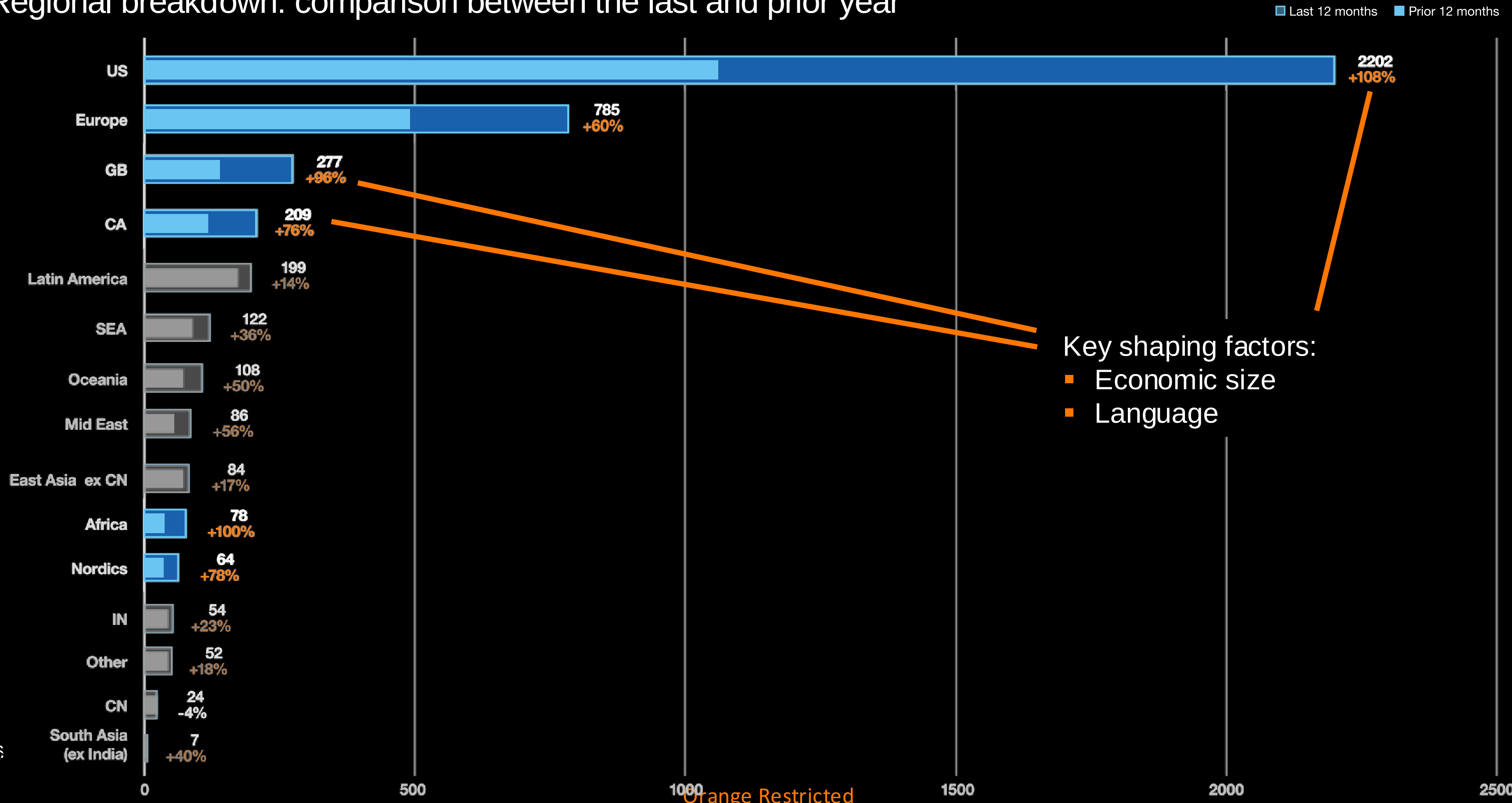
**119** negotiated with victims

...but are **now at risk** of Law Enforcement activity

**Data relates to June 2022 - Feb 2024**

# Shift in victims by region

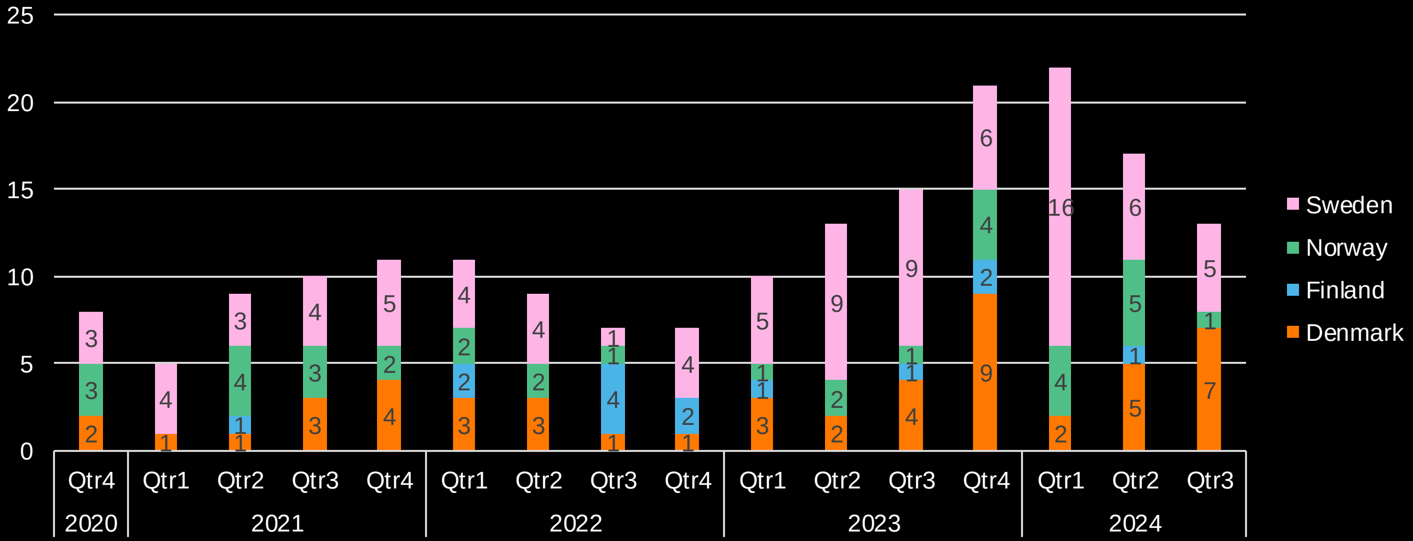
## Regional breakdown: comparison between the last and prior year

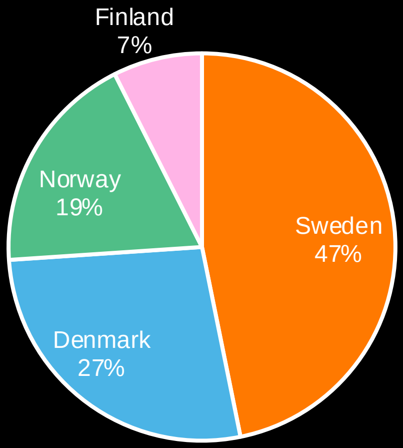


Key shaping factors:

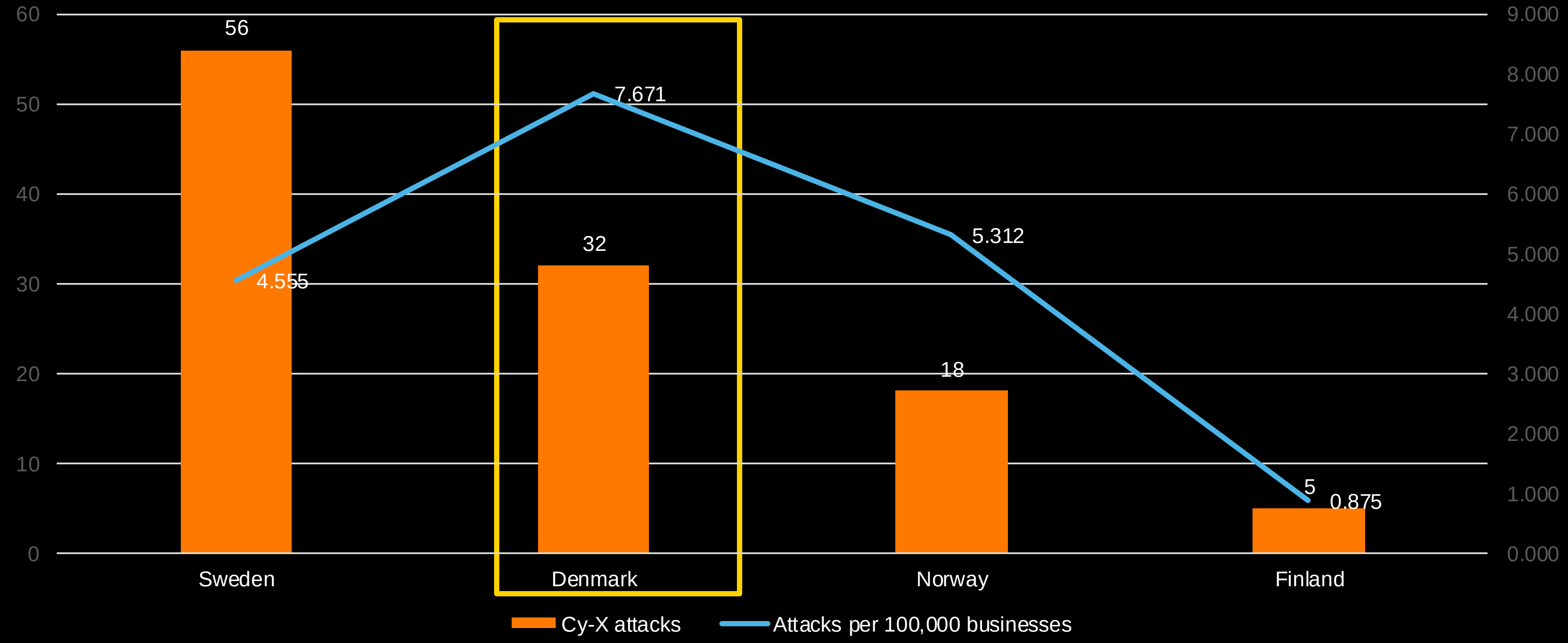
- Economic size
- Language

# Profile : Nordics





# Denmark in context – Attacks per 100,000 businesses



# Denmark 2023 – 2024 (Sep)

LockBit

BlackBasta

Cactus

Akira

Ransomhub

ALPHVM / BlackCat

Cloak

Cicada3301

Cl0p

Rhysida

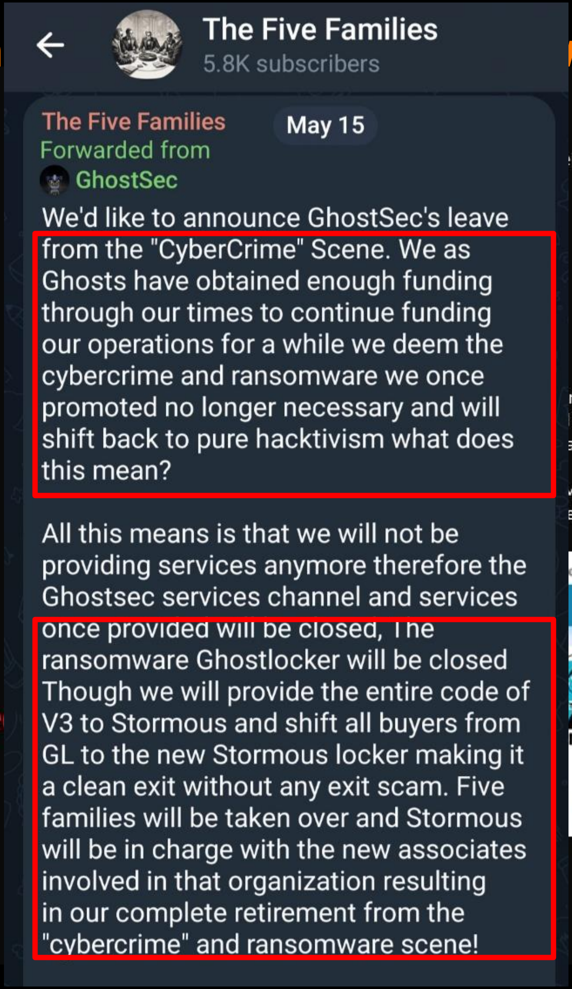
# 4 Why are we still struggeling with this?

# Hacktivism ... ware & vice versa

Blurry lir

- 
- 
- 
- 
-

Hacke



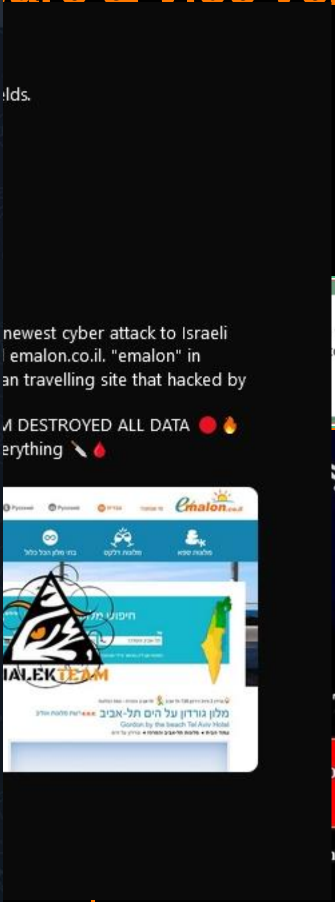
The Five Families
5.8K subscribers

The Five Families
Forwarded from
GhostSec

May 15

We'd like to announce GhostSec's leave from the "CyberCrime" Scene. We as Ghosts have obtained enough funding through our times to continue funding our operations for a while we deem the cybercrime and ransomware we once promoted no longer necessary and will shift back to pure hacktivism what does this mean?

All this means is that we will not be providing services anymore therefore the Ghostsec services channel and services once provided will be closed, The ransomware Ghostlocker will be closed Though we will provide the entire code of V3 to Stormous and shift all buyers from GL to the new Stormous locker making it a clean exit without any exit scam. Five families will be taken over and Stormous will be in charge with the new associates involved in that organization resulting in our complete retirement from the "cybercrime" and ransomware scene!



elds.

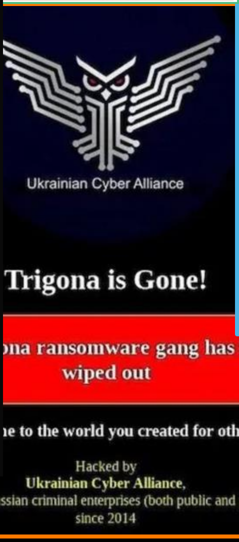
newest cyber attack to Israeli
emalon.co.il. "emalon" in
an travelling site that hacked by

M DESTROYED ALL DATA 🔴🔥
erything 🔪🩸

emalon.co.il
חיפוש מלון
IALEK TEAM
מלון גורדון על הים תל-אביב
Gordon by the beach Tel Aviv Hotel

the following countries: Iran 🇮🇷,
ountries. Message

👁 112 📌 7:20 AM



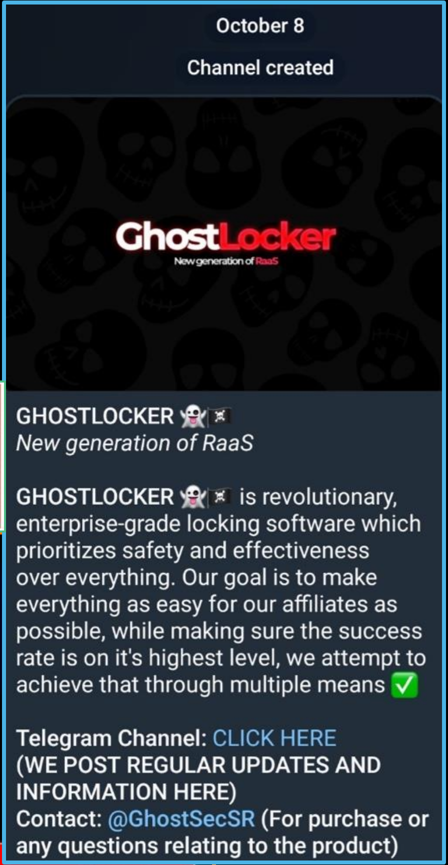
Ukrainian Cyber Alliance

Trigona is Gone!

ona ransomware gang has been exfiltrated and wiped out

ne to the world you created for others

Hacked by
Ukrainian Cyber Alliance,
disrupting russian criminal enterprises (both public and private)
since 2014



October 8

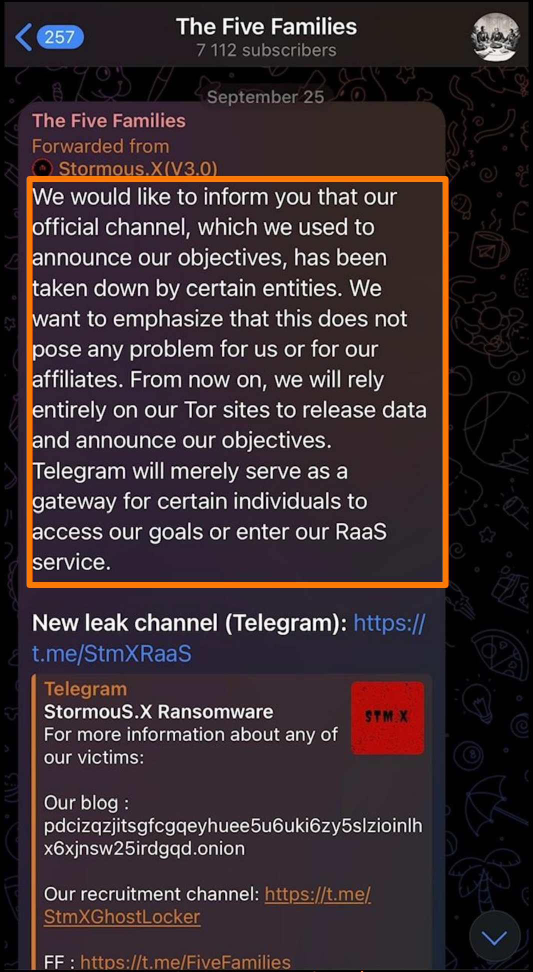
Channel created

GHOSTLOCKER 👻☠
*New generation of RaaS*

GHOSTLOCKER 👻☠ is revolutionary, enterprise-grade locking software which prioritizes safety and effectiveness over everything. Our goal is to make everything as easy for our affiliates as possible, while making sure the success rate is on it's highest level, we attempt to achieve that through multiple means ✅

Telegram Channel: CLICK HERE
(WE POST REGULAR UPDATES AND INFORMATION HERE)
Contact: @GhostSecSR (For purchase or any questions relating to the product)

# What’s it to us?



The Five Families
Forwarded from
Stormous.X(V3.0)

We would like to inform you that our official channel, which we used to announce our objectives, has been taken down by certain entities. We want to emphasize that this does not pose any problem for us or for our affiliates. From now on, we will rely entirely on our Tor sites to release data and announce our objectives. Telegram will merely serve as a gateway for certain individuals to access our goals or enter our RaaS service.

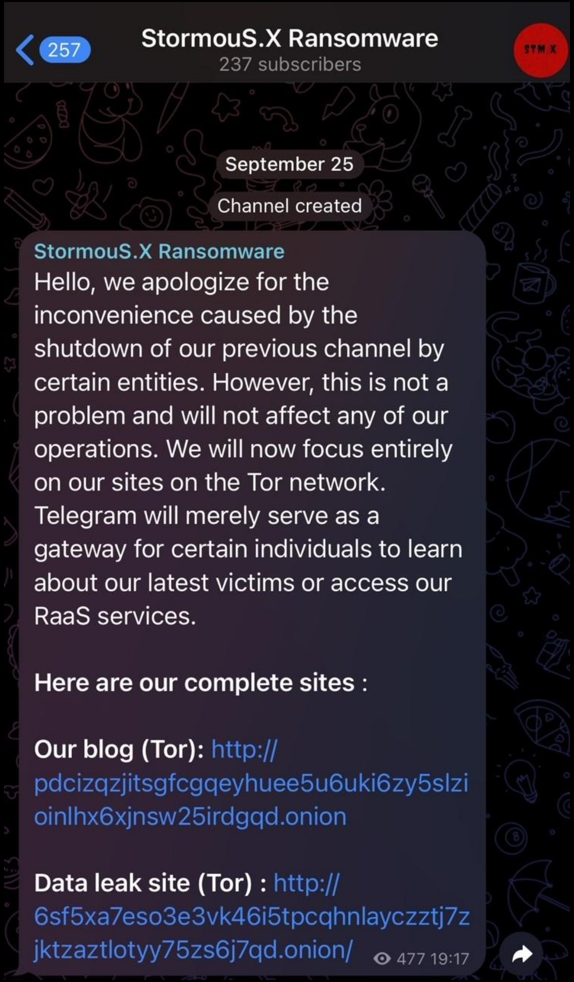
**New leak channel (Telegram):** https://t.me/StmXRaaS

Telegram
**StormouS.X Ransomware**
For more information about any of our victims:

Our blog : pdcizqzjitsgfcgqeyhuee5u6uki6zy5slzioinlhx6xjnsw25irdgqd.onion

Our recruitment channel: https://t.me/StmXGhostLocker

FF : https://t.me/FiveFamilies



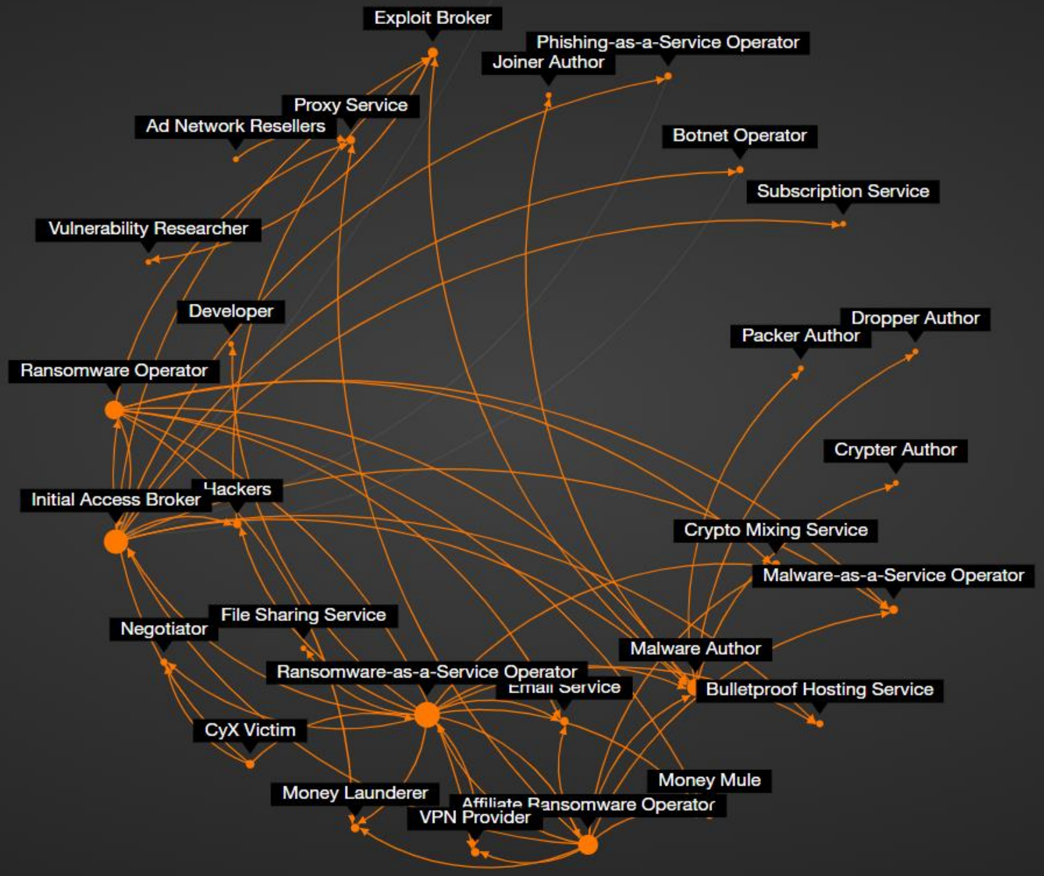
StormouS.X Ransomware

Hello, we apologize for the inconvenience caused by the shutdown of our previous channel by certain entities. However, this is not a problem and will not affect any of our operations. We will now focus entirely on our sites on the Tor network. Telegram will merely serve as a gateway for certain individuals to learn about our latest victims or access our RaaS services.

**Here are our complete sites :**

**Our blog (Tor):** http://pdcizqzjitsgfcgqeyhuee5u6uki6zy5slzioinlhx6xjnsw25irdgqd.onion

**Data leak site (Tor) :** http://6sf5xa7eso3e3vk46i5tpcqhnlayczztj7zjktzaztlotyy75zs6j7qd.onion/

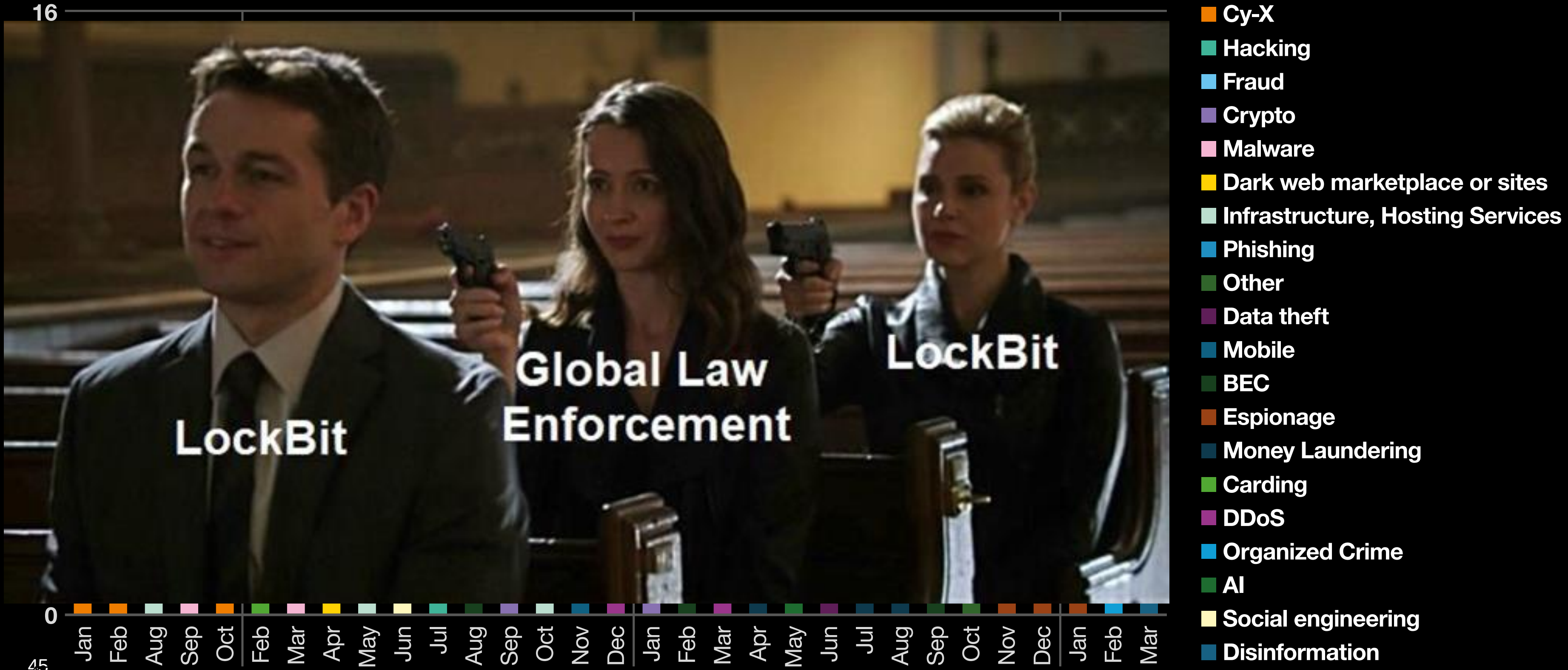

Exploit Broker
Phishing-as-a-Service Operator
Joiner Author
Proxy Service
Ad Network Resellers
Botnet Operator
Subscription Service
Vulnerability Researcher
Developer
Dropper Author
Packer Author
Ransomware Operator
Crypter Author
Hackers
Initial Access Broker
Crypto Mixing Service
Malware-as-a-Service Operator
File Sharing Service
Negotiator
Malware Author
Ransomware-as-a-Service Operator
Email Service
Bulletproof Hosting Service
CyX Victim
Money Mule
Money Launderer
Affiliate Ransomware Operator
VPN Provider

# 5 Action by law enforcement

- Takedown and disruption by law enforcement

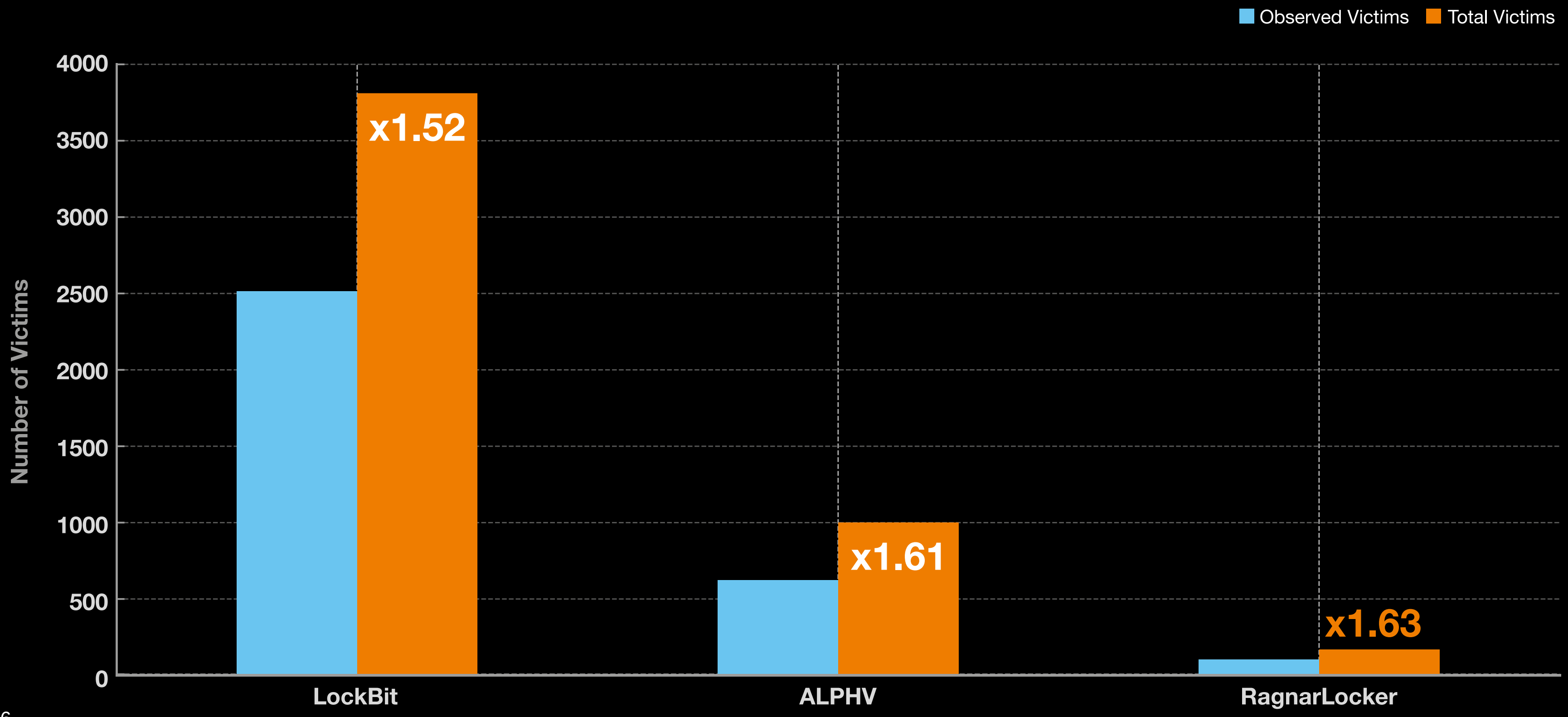
# Focus of Law Enforcement

Types of cyber crime Law Enforcement activities targeted in recent years



# Observed vs. Total reported victims

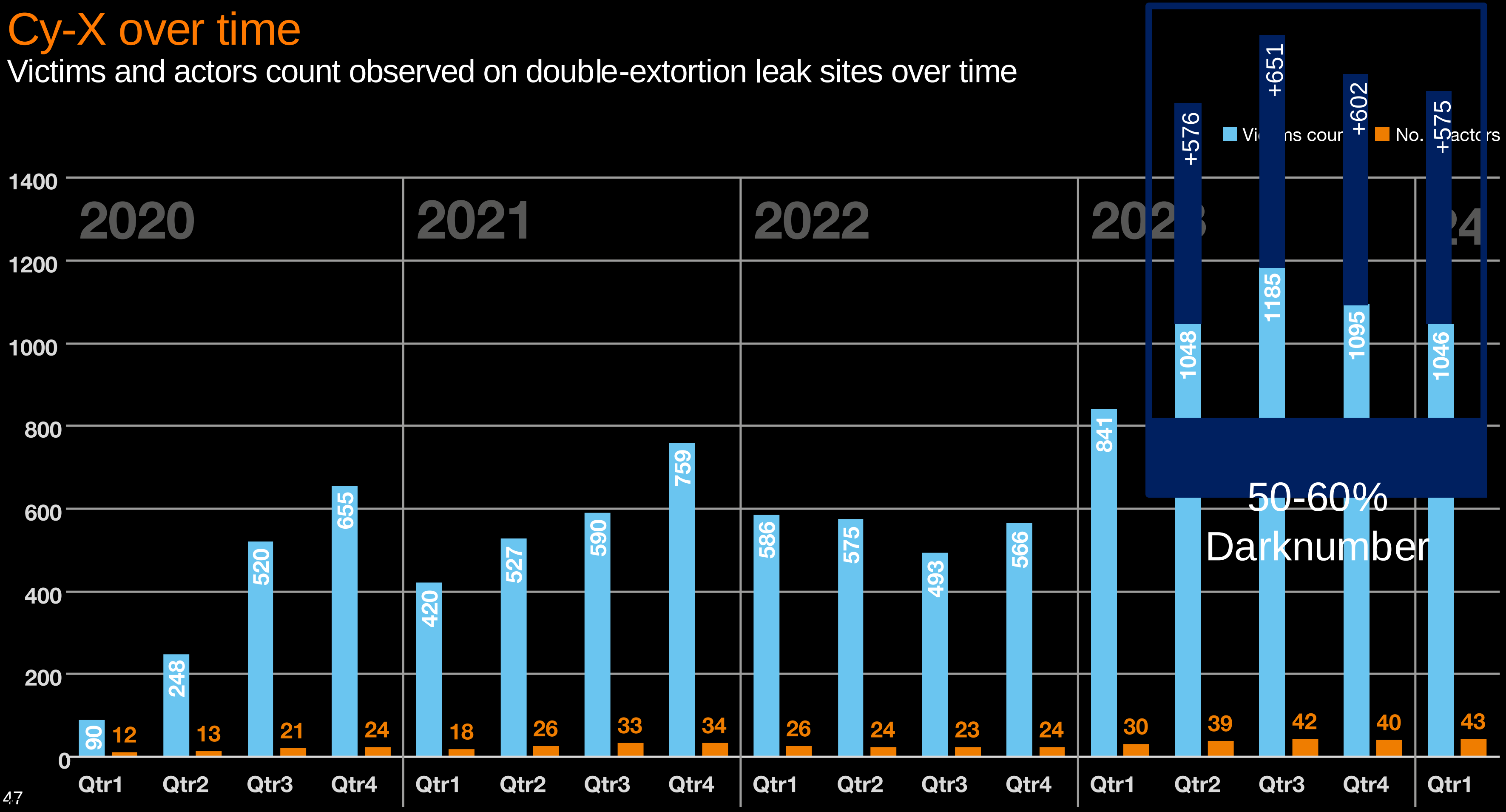
## Dark figures: count of victims of example ransomware actors (observed vs. law enforcement)



Orange Restricted

# Cy-X over time

Victims and actors count observed on double-extortion leak sites over time



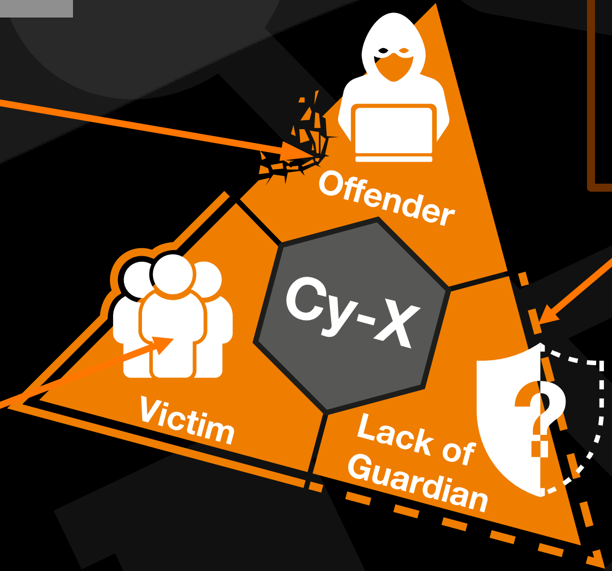
Orange Cyberdefense

Demotivate offenders:

- Coordinated law enforcement effort
- Reducing the flow of funds from victims
- Targeted efforts to reduce criminals' neutralization techniques

Get suitable guardians in place:

- Technical controls
- 'Social' guardians – government, individuals, teams and groups



Attractiveness as victim:

- **V**isibility. A large attack surface
- **V**ulnerability. Poor cybersecurity practices
- **I**nertia: 'Data' is easy to access and exfiltrate
- **V**alue: The value of the data to the victim
- **A**ccess: The amount of time and space allowed to the attacker

Orange
Cyberdefense

Beating ransomware

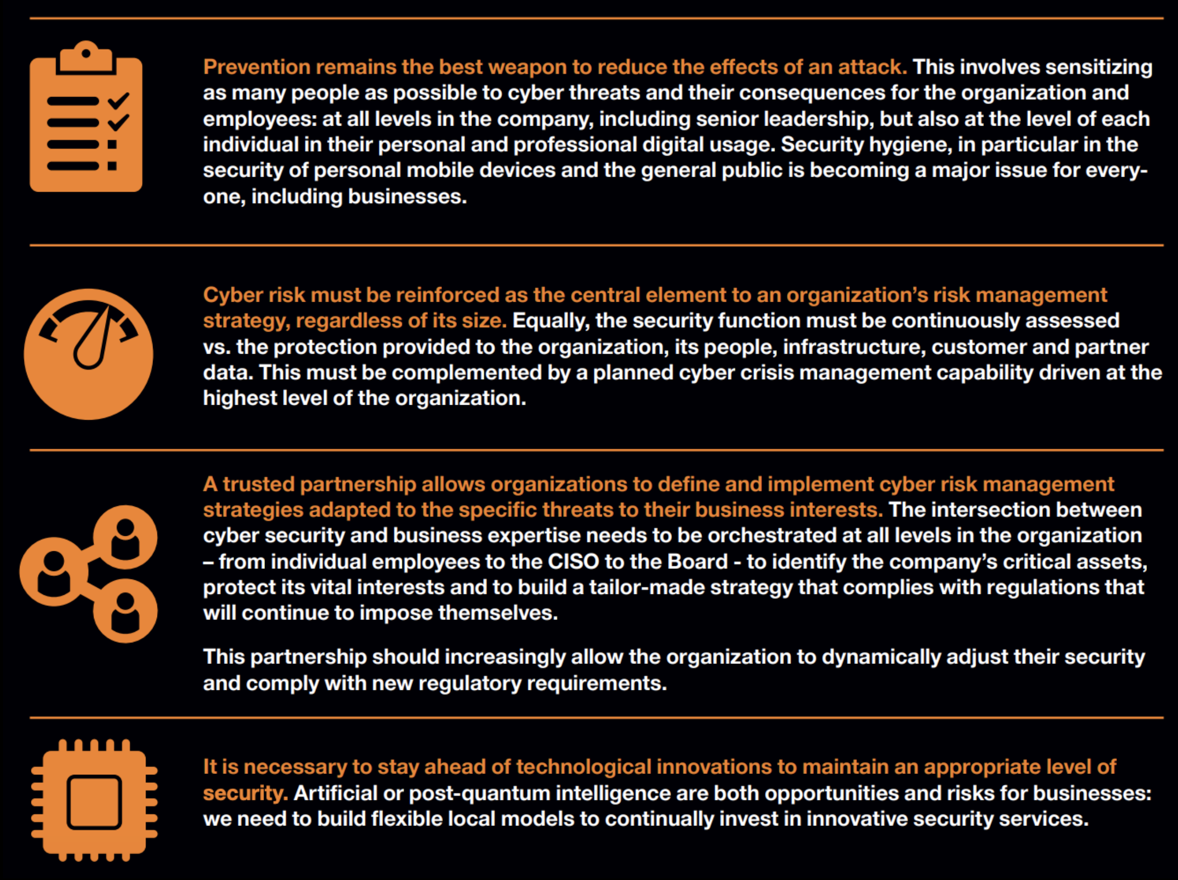
A comprehensive guide to tackling the cyber extortion threat

## Good news!

**AWARENESS!**

Downloadable on our website:
https://www.orangecyberdefense.com/global/white-papers/beating-ransomware

# Orange Cyberdefense’s recommendations:



**Prevention remains the best weapon to reduce the effects of an attack.** This involves sensitizing as many people as possible to cyber threats and their consequences for the organization and employees: at all levels in the company, including senior leadership, but also at the level of each individual in their personal and professional digital usage. Security hygiene, in particular in the security of personal mobile devices and the general public is becoming a major issue for everyone, including businesses.

**Cyber risk must be reinforced as the central element to an organization’s risk management strategy, regardless of its size.** Equally, the security function must be continuously assessed vs. the protection provided to the organization, its people, infrastructure, customer and partner data. This must be complemented by a planned cyber crisis management capability driven at the highest level of the organization.

**A trusted partnership allows organizations to define and implement cyber risk management strategies adapted to the specific threats to their business interests.** The intersection between cyber security and business expertise needs to be orchestrated at all levels in the organization – from individual employees to the CISO to the Board - to identify the company’s critical assets, protect its vital interests and to build a tailor-made strategy that complies with regulations that will continue to impose themselves.

This partnership should increasingly allow the organization to dynamically adjust their security and comply with new regulatory requirements.

**It is necessary to stay ahead of technological innovations to maintain an appropriate level of security.** Artificial or post-quantum intelligence are both opportunities and risks for businesses: we need to build flexible local models to continually invest in innovative security services.

orange™ Cyberdefense

# Thank you

orangecyberdefense.com

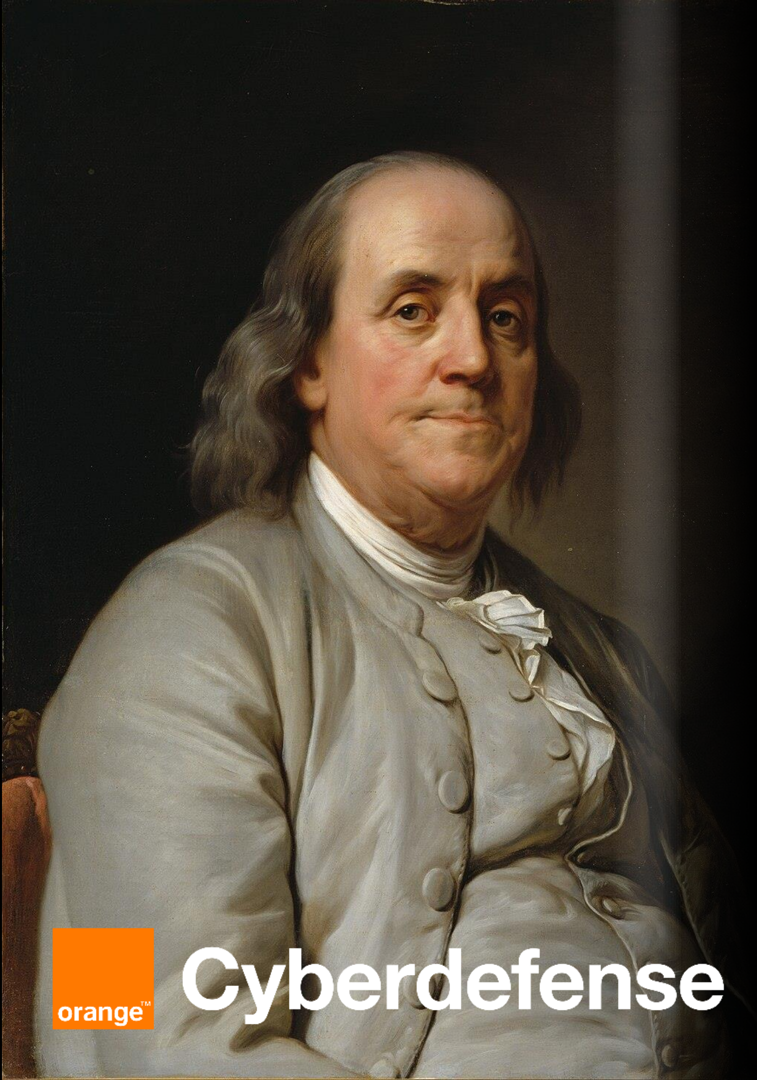
# Cyber Attack Rediness

Fail to prepare, Prepare to Fail.

orange™ Cyberdefense

# About me...

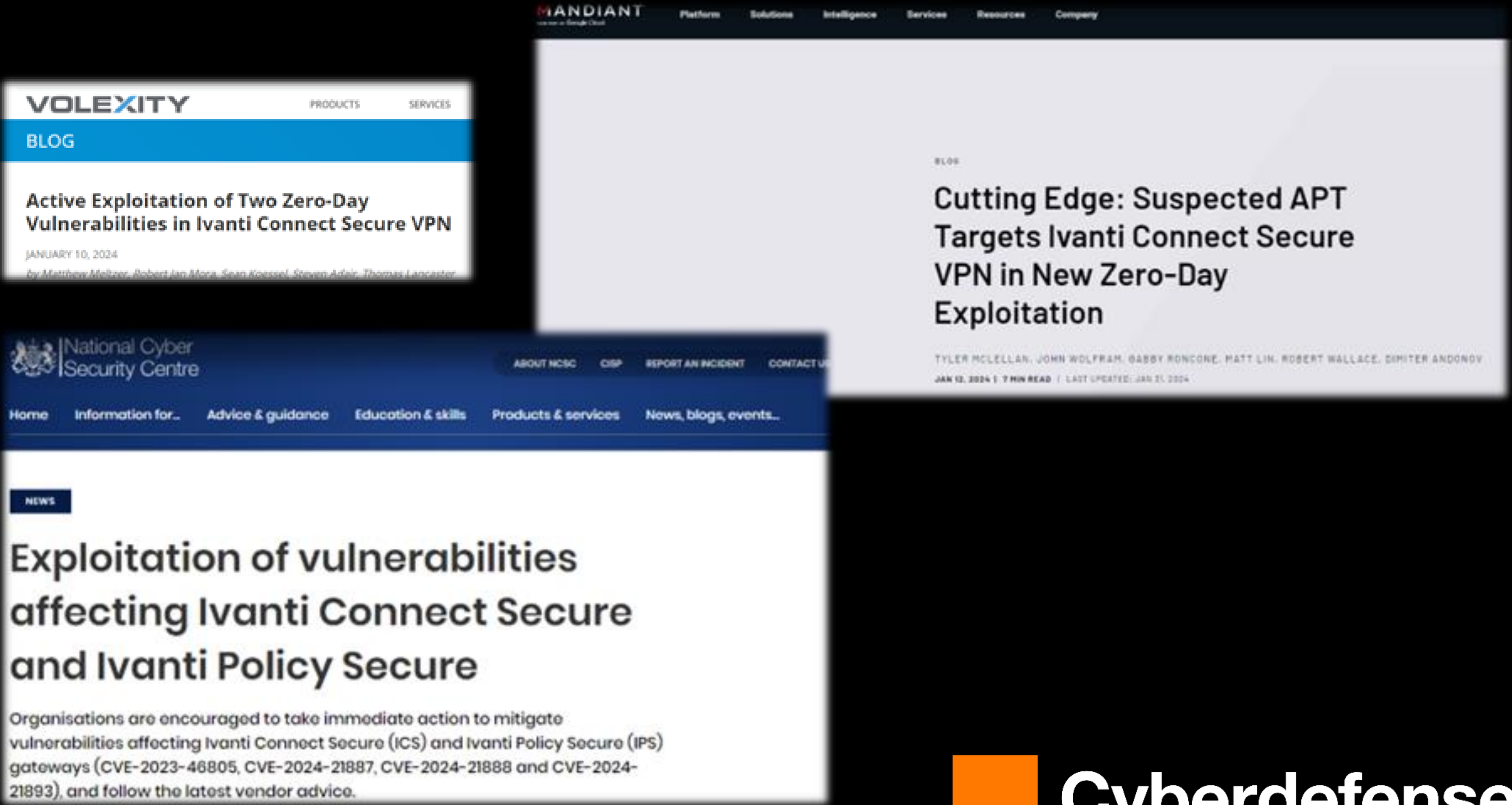
- CSIRT Country Lead Nordics region at Orange Cyberdefense.
- At Orange Cyberdefense CSIRT since 2019
- Worked on multiple major cybersecurity incidents, including ransomware, network-wide compromises and business fraud.
- Loves Sailing and Motorbiking.



By failing to **prepare,** you are preparing to **fail.**

Benjamin Franklin

orange™ Cyberdefense



Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN

JANUARY 10, 2024

by Matthew Meltzer, Robert Jan Mora, Sean Koessel, Steven Adair, Thomas Lancaster

Cutting Edge: Suspected APT Targets Ivanti Connect Secure VPN in New Zero-Day Exploitation

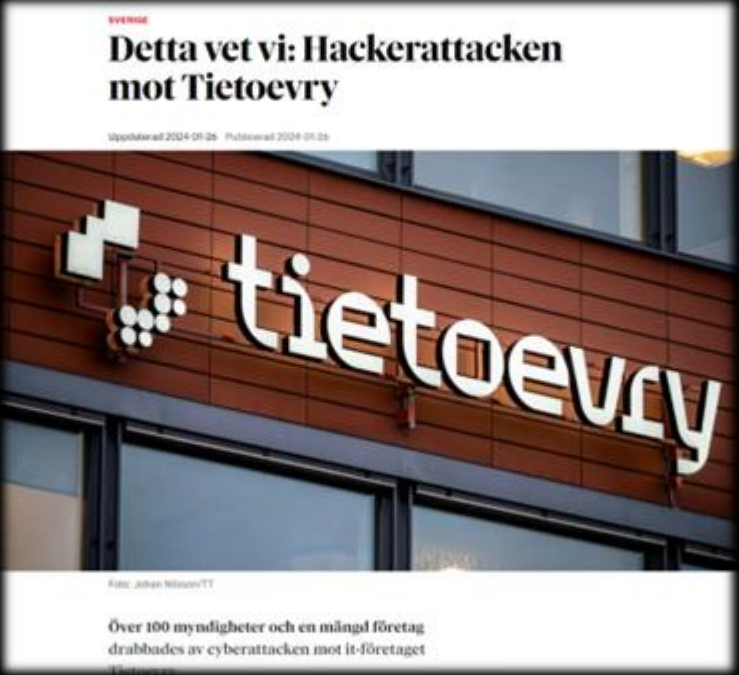
TYLER MCLELLAN, JOHN WOLFRAM, GABBY RONCONE, MATT LIN, ROBERT WALLACE, DIMITER ANDONOV

JAN 12, 2024 | 7 MIN READ / LAST UPDATED: JAN 31, 2024

Exploitation of vulnerabilities affecting Ivanti Connect Secure and Ivanti Policy Secure

Organisations are encouraged to take immediate action to mitigate vulnerabilities affecting Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS) gateways (CVE-2023-46805, CVE-2024-21887, CVE-2024-21888 and CVE-2024-21893), and follow the latest vendor advice.

orange™ Cyberdefense



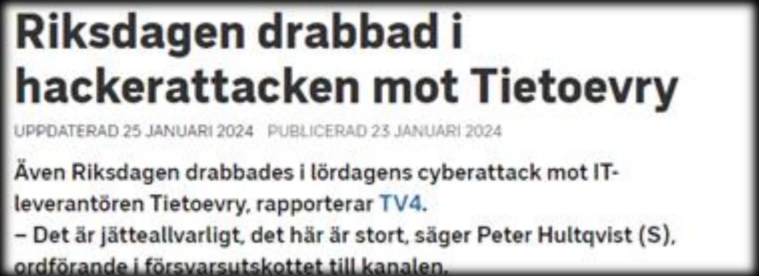
SVERIGE

## Detta vet vi: Hackerattacken mot Tietoevry

Uppdaterad 2024-01-26 Publicerad 2024-01-26

Foto: Johan Nilsson/TT

**Över 100 myndigheter och en mängd företag** drabbades av cyberattacken mot it-företaget Tietoevry.

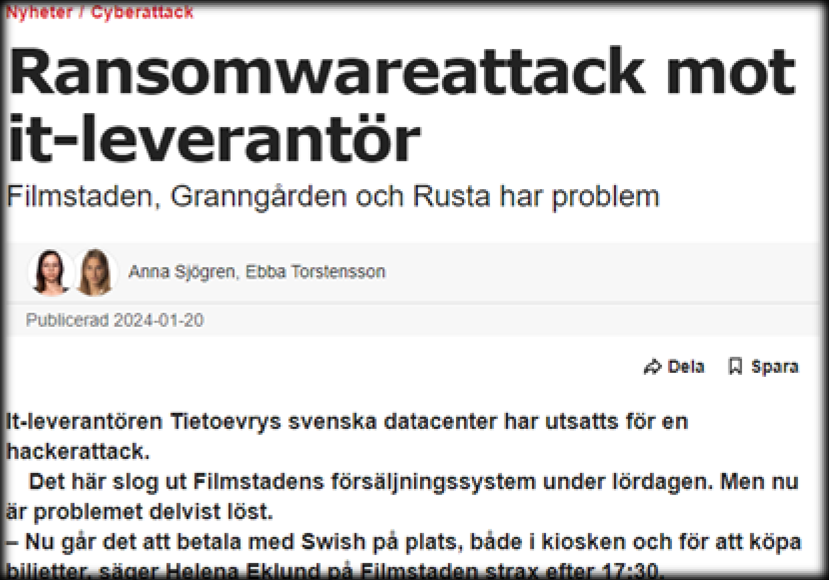


## Riksdagen drabbad i hackerattacken mot Tietoevry

UPPDATERAD 25 JANUARI 2024 PUBLICERAD 23 JANUARI 2024

Även Riksdagen drabbades i lördagens cyberattack mot IT-leverantören Tietoevry, rapporterar TV4.

– Det är jätteallvarligt, det här är stort, säger Peter Hultqvist (S), ordförande i försvarsutskottet till kanalen.



Nyheter / Cyberattack

## Ransomwareattack mot it-leverantör

Filmstaden, Granngården och Rusta har problem

Anna Sjögren, Ebba Torstensson

Publicerad 2024-01-20

**It-leverantören Tietoevrys svenska datacenter har utsatts för en hackerattack.**

Det här slog ut Filmstadens försäljningssystem under lördagen. Men nu är problemet delvist löst.

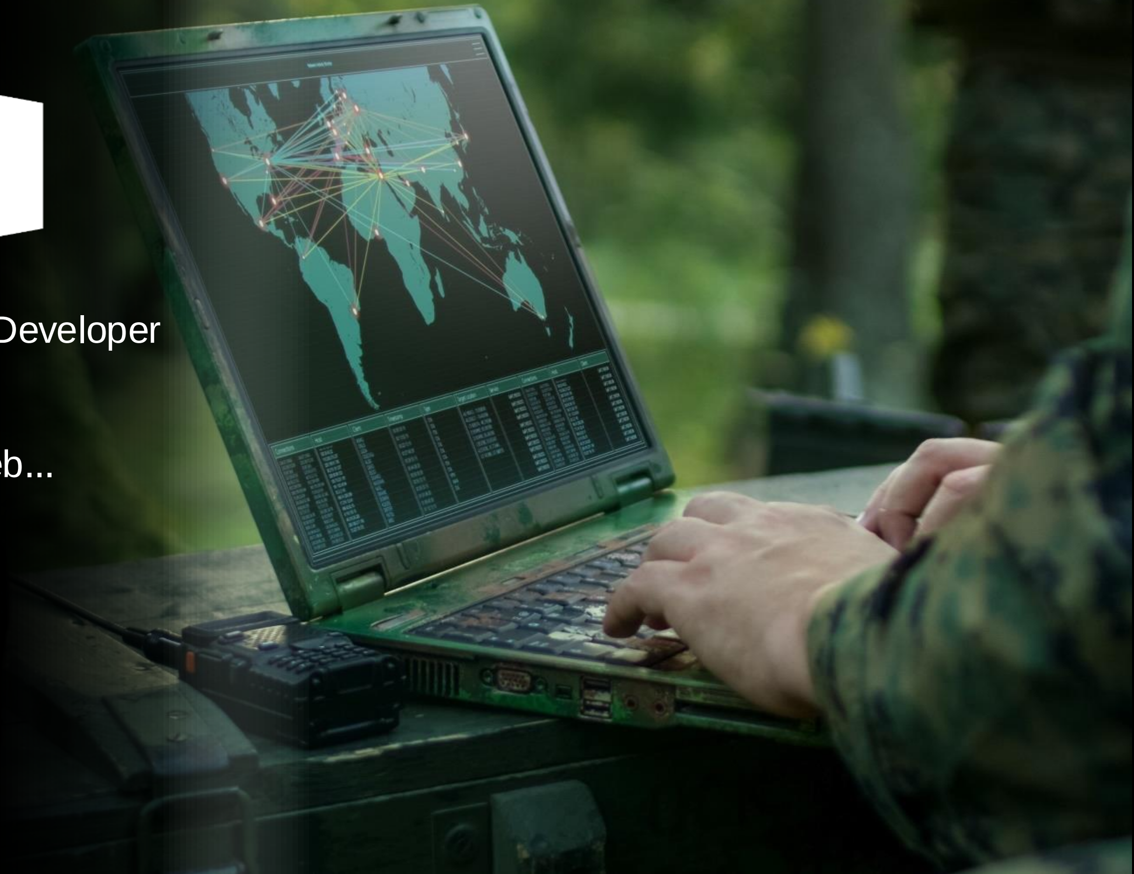
– Nu går det att betala med Swish på plats, både i kiosken och för att köpa biljetter, säger Helena Eklund på Filmstaden strax efter 17:30.

# Ett Nato-medlemskap kan generera cybersäkerhetsattacker mot svenska verksamheter

25 January 2024 Cybersäkerhet Nyheter

# War story

- Real-world example.
- Client was an international Software Developer and retailer.
- Data Exfiltration.
- Started with an open server to the web...



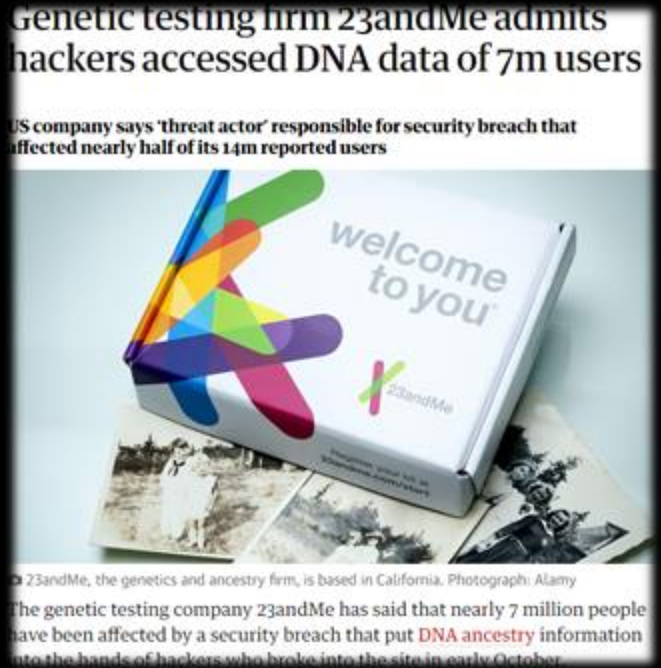
Cyberdefense

# Proper planning and preparation prevents Piss Poor Performance.

British Royal Marines

orange™ Cyberdefense

# The Morning started like this…

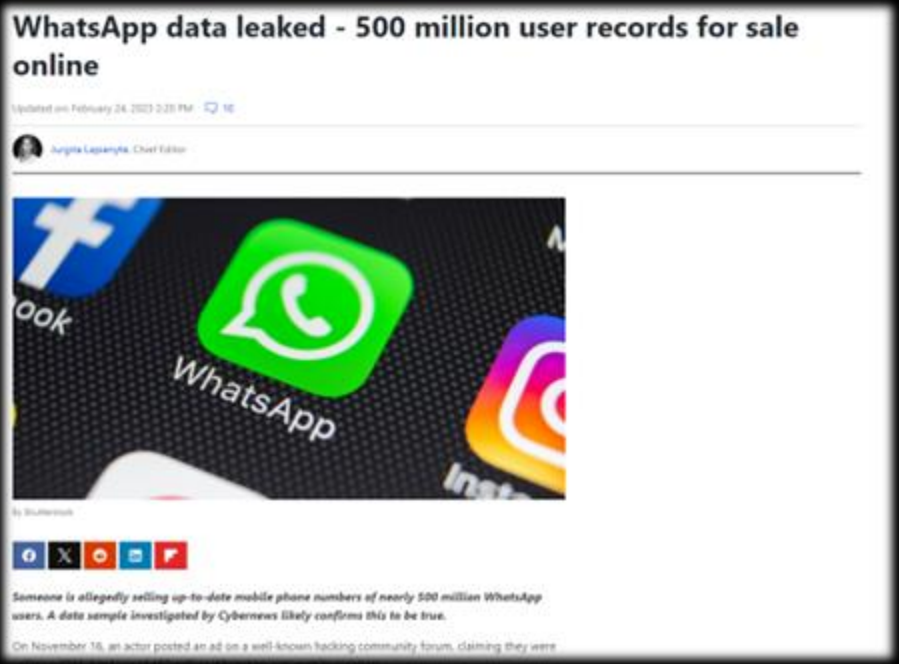


## Genetic testing firm 23andMe admits hackers accessed DNA data of 7m users

**US company says 'threat actor' responsible for security breach that affected nearly half of its 14m reported users**

23andMe, the genetics and ancestry firm, is based in California. Photograph: Alamy

The genetic testing company 23andMe has said that nearly 7 million people have been affected by a security breach that put DNA ancestry information into the hands of hackers who broke into the site in early October



## WhatsApp data leaked - 500 million user records for sale online

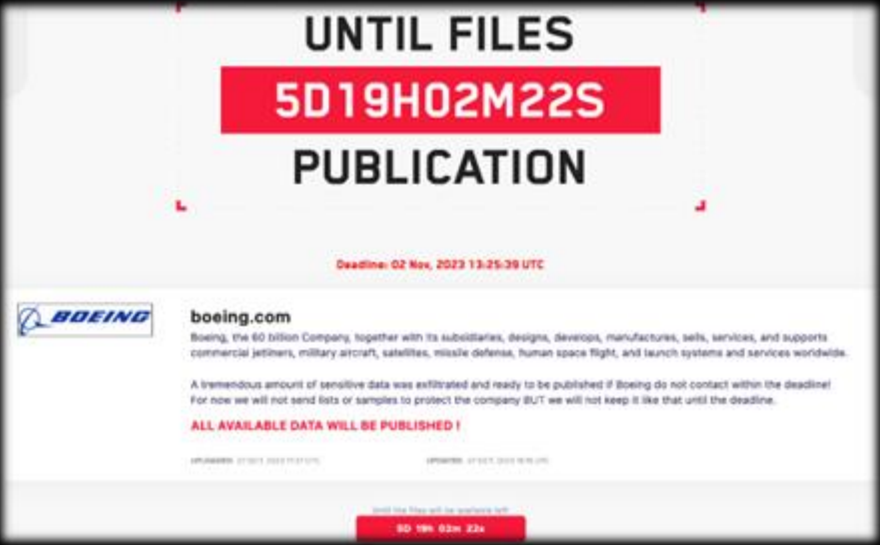
Updated on February 24, 2023 2:20 PM 16

Jurgita Lapienytė, Chief Editor

By Shutterstock

***Someone is allegedly selling up-to-date mobile phone numbers of nearly 500 million WhatsApp users. A data sample investigated by Cybernews likely confirms this to be true.***

On November 16, an actor posted an ad on a well-known hacking community forum, claiming they were



UNTIL FILES

5D19H02M22S

PUBLICATION

Deadline: 02 Nov, 2023 13:25:39 UTC

**boeing.com**

Boeing, the 60 billion Company, together with its subsidiaries, designs, develops, manufactures, sells, services, and supports commercial jetliners, military aircraft, satellites, missile defense, human space flight, and launch systems and services worldwide.

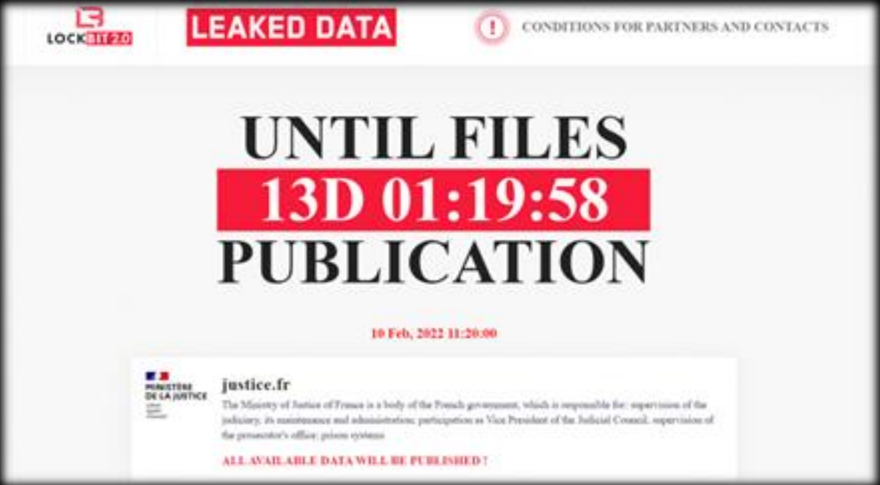
A tremendous amount of sensitive data was exfiltrated and ready to be published if Boeing do not contact within the deadline! For now we will not send lists or samples to protect the company BUT we will not keep it like that until the deadline.

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: [illegible]    UPDATED: [illegible]

Until the files will be available left:

5D 19h 02m 22s



UNTIL FILES

13D 01:19:58

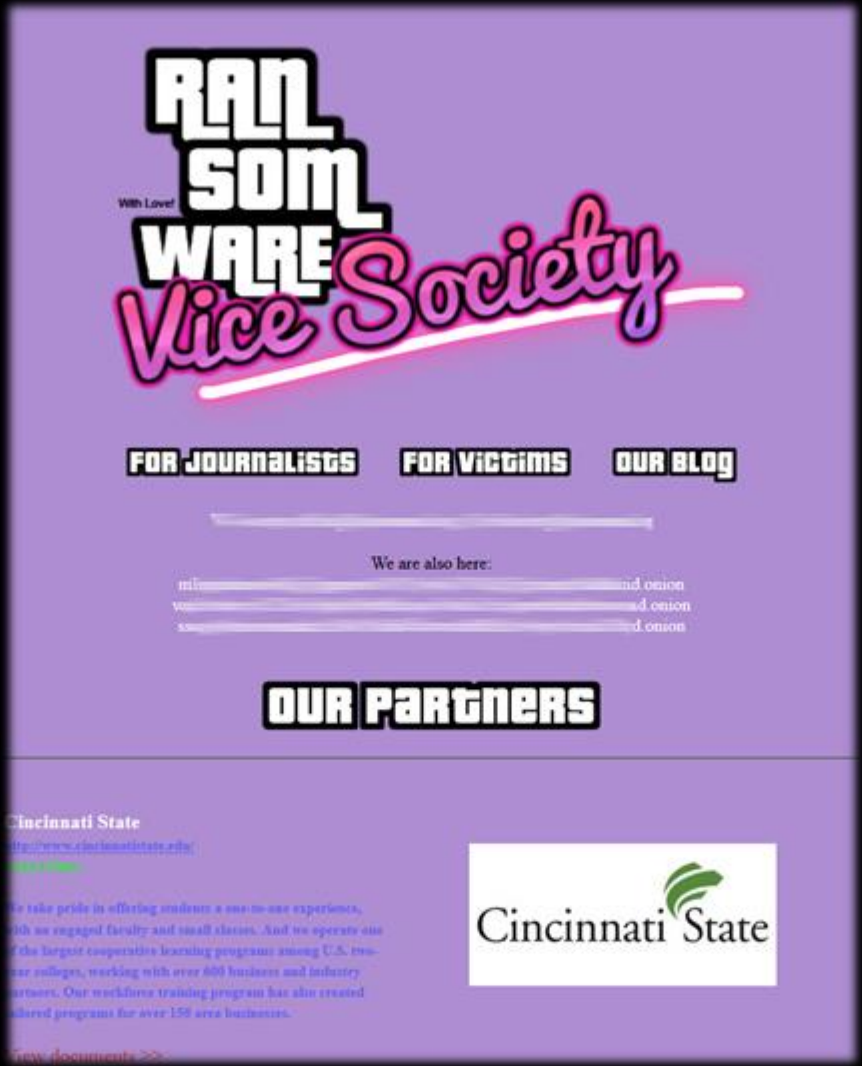
PUBLICATION

10 Feb, 2022 11:20:00

**justice.fr**

The Ministry of Justice of France is a body of the French government, which is responsible for: supervision of the judiciary, its maintenance and administration; participation as Vice President of the Judicial Council, supervision of the prosecutor's office; prison systems

ALL AVAILABLE DATA WILL BE PUBLISHED !



[redacted]

We are also here:

mi[redacted]d.onion
v[redacted]d.onion
s[redacted]d.onion

**Cincinnati State**

http://www.cincinnatistate.edu/

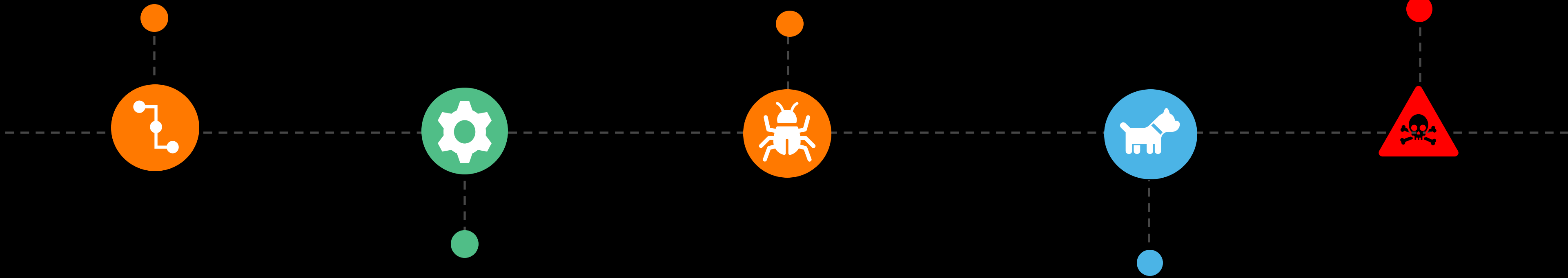
[illegible]

e take pride in offering students a one-to-one experience, ith an engaged faculty and small classes. And we operate one f the largest cooperative learning programs among U.S. two-ear colleges, working with over 600 business and industry artners. Our workforce training program has also created ailored programs for over 150 area businesses.

iew documents >>

# Attack timeline

Cyberdefense



## April 13 13:38

**LATERAL MOVEMENT**

Movement inside the network to several critical servers, such as **Domain Controllers**.

## May 1-2

**MALWARE EXECUTION:**

Threat Actor executes the infamous commercial hacking toolkit “**Cobalt Strike**” to the network.

## May 2-7

**DISCOVERY:**

Industry-recognised administration programs “**Advanced Port Scanner**” were downloaded and installed.

## May 5

**CONTINUED RECONNAISSANCE:**

Threat Actor deploys the attack tool **Bloodhound**

## May 8-9

**RANSOMWARE DEPLOYMENT**

# CSIRT

orange™ Cyberdefense

# Quis, quid, ubi, quibus auziliis, cur, quomodo, quando.

### What happened?

**For example:**

- Files encrypted
- Suspicious login
- Phishing email interaction
- Strange file execution
- Unauthorized traffic in firewall log
- What containment actions have you done?

### Who was involved?

**For example:**

- Which user accounts?
- Who would be able to give more (technical) context?

### When did it happen?

**For example:**

- Date/time of first indication that something was wrong?
- When did you perform containment activity?
- How far back do your logs/data set go?

### Where did it happen?

**For example:**

- Which systems were involved?
- Domain controllers?
- Servers or workstations?
- Which operating systems?
- Microsoft 365 environment?
- Network/firewall traffic?

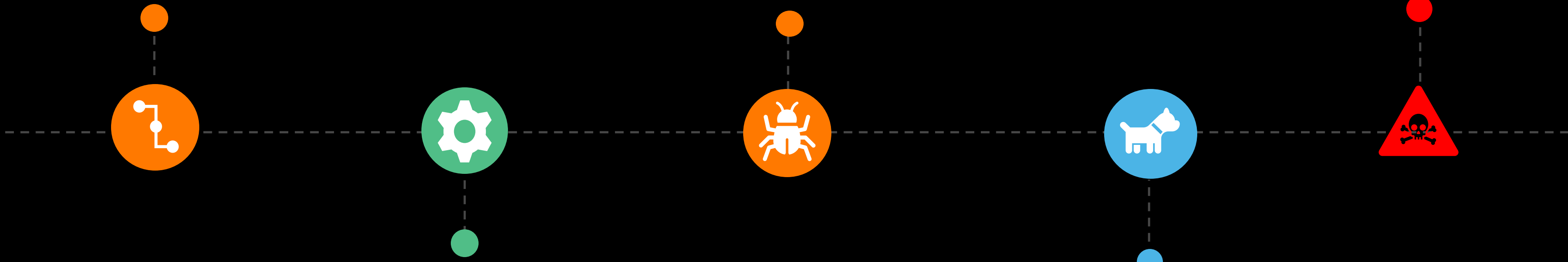
### Why did you realize it happened?

**For example:**

- I received a detection from CSOC.
- I noticed it myself while doing ‘X’.
- I got a call from a user.
- I got a call from an MSP/3rd party.

# CSIRT

orange™ Cyberdefense



## April 13 13:38

**LATERAL MOVEMENT**

Movement inside the network
to several critical servers,
such as **Domain Controllers**.

## May 1-2

**MALWARE EXECUTION:**

Threat Actor executes the infamous commercial hacking toolkit “**Cobalt Strike**” to the network.

## May 2-7

**DISCOVERY:**

Industry-recognised administration programs “**Advanced Port Scanner**” were downloaded and installed.

## May 5

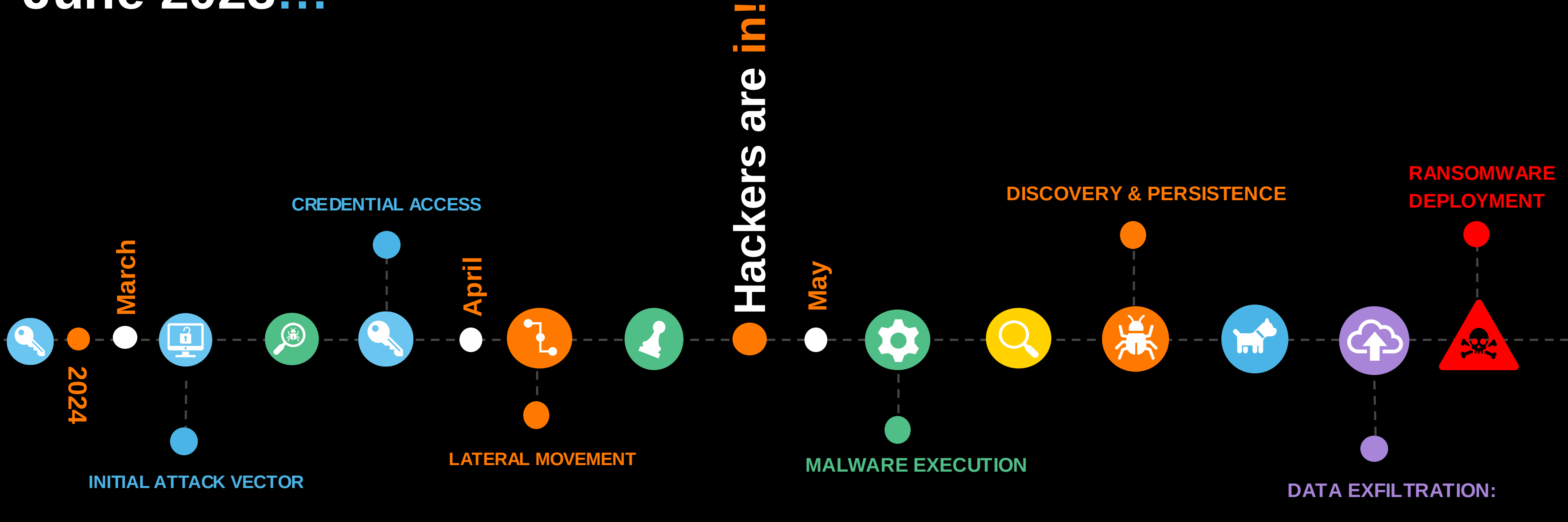
**CONTINUED RECONNAISSANCE:**

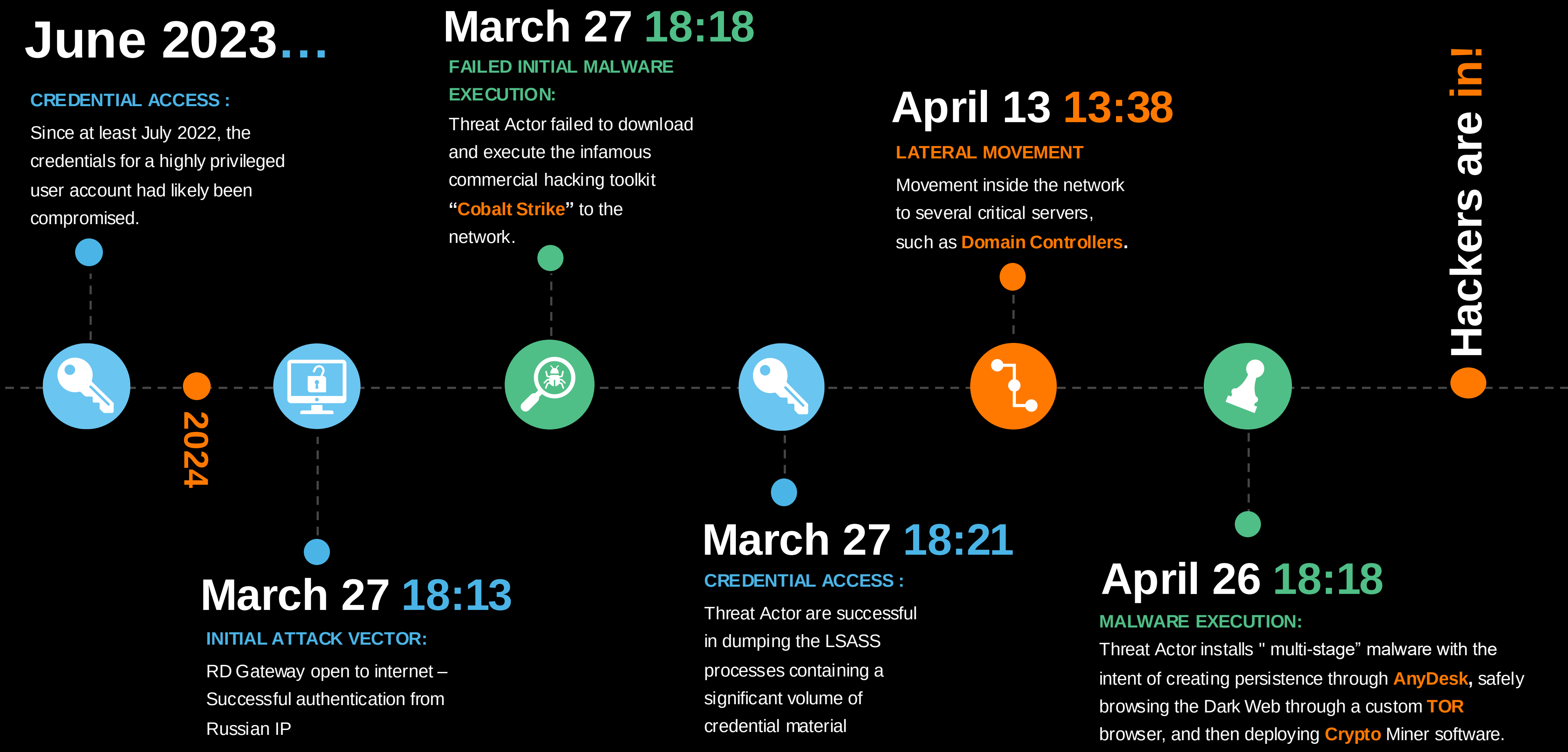
Threat Actor deploys the attack tool **Bloodhound**

## May 8-9

**RANSOMWARE DEPLOYMENT**

# June 2023…


2024
March
INITIAL ATTACK VECTOR
CREDENTIAL ACCESS
April
LATERAL MOVEMENT
Hackers are in!
May
MALWARE EXECUTION
DISCOVERY & PERSISTENCE
DATA EXFILTRATION:
RANSOMWARE DEPLOYMENT



## June 2023…

**CREDENTIAL ACCESS :**

Since at least July 2022, the credentials for a highly privileged user account had likely been compromised.

**2024**

## March 27 18:13

**INITIAL ATTACK VECTOR:**

RD Gateway open to internet – Successful authentication from Russian IP

## March 27 18:18

**FAILED INITIAL MALWARE EXECUTION:**

Threat Actor failed to download and execute the infamous commercial hacking toolkit **“Cobalt Strike”** to the network.

## March 27 18:21

**CREDENTIAL ACCESS :**

Threat Actor are successful in dumping the LSASS processes containing a significant volume of credential material

## April 13 13:38

**LATERAL MOVEMENT**

Movement inside the network to several critical servers, such as **Domain Controllers.**

## April 26 18:18

**MALWARE EXECUTION:**

Threat Actor installs " multi-stage” malware with the intent of creating persistence through **AnyDesk**, safely browsing the Dark Web through a custom **TOR** browser, and then deploying **Crypto** Miner software.

**Hackers are in!**

## May 1-2

**MALWARE EXECUTION:**

Threat Actor executes the infamous commercial hacking toolkit “**Cobalt Strike**” to the network.

## May 1 23:59

**CONTINUED DISCOVERY:**

Data and Access Discovery through typed paths in Microsoft Windows Explorer. Results output to a text file.

## May 2-7

**DISCOVERY & PERSISTENCE :**

Industry-recognised data discovery, collection “**Velociraptor**”, and administration programs “**ScreenConnect**” and “**Advanced Port Scanner**” were downloaded and installed.

## May 5

**CONTINUED RECONNAISSANCE:**

Threat Actor deploys the attack tool **Bloodhound**

## May 5

**DATA EXFILTRATION:**

The attackers deployed the commercial file copying tool **Rclone**, exfiltrating data of approximately 1.2TB…

# Hackers are in and they have your data!

orange Cyberdefense

# War story - PAUSE

## Situation:

Attackers have Access to the Network.

## Immediate Business Risk:

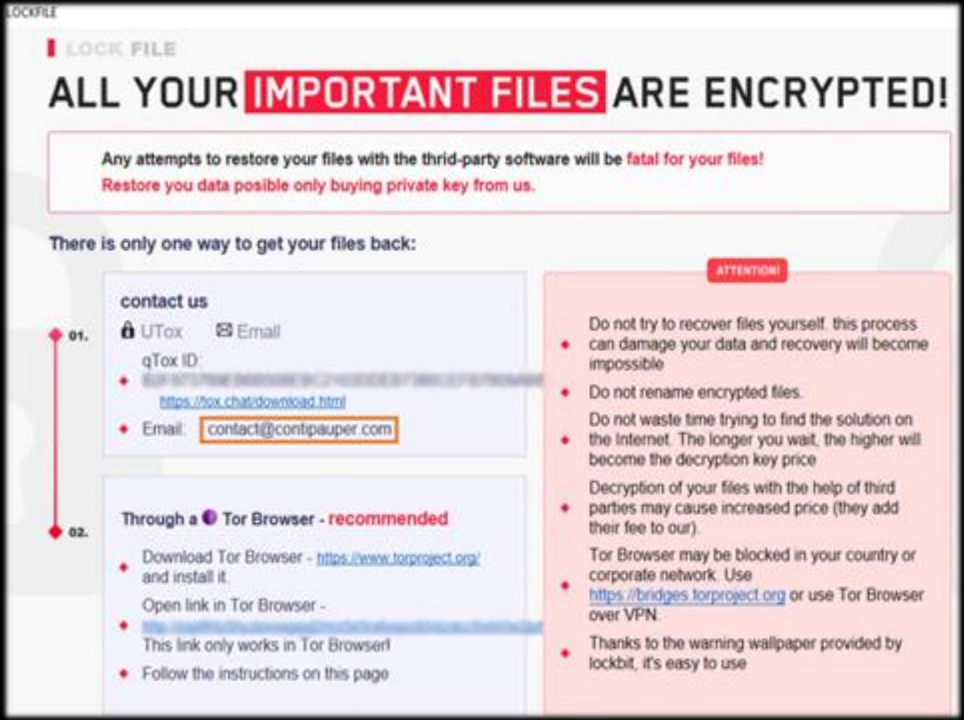
Loss of data confidentiality for files, infrastructure, and User accounts.

## Who is involved:

Incident has not been identified yet!

orange™ Cyberdefense

# Ransomware Deployment 9-10th May



LOCKFILE

LOCK FILE

ALL YOUR IMPORTANT FILES ARE ENCRYPTED!

Any attempts to restore your files with the thrid-party software will be fatal for your files!
Restore you data posible only buying private key from us.

There is only one way to get your files back:

01.

contact us

UTox   Email

qTox ID:

- [redacted]
  https://tox.chat/download.html
- Email: contact@contipauper.com

02.

Through a Tor Browser - recommended

- Download Tor Browser - https://www.torproject.org/ and install it.
- Open link in Tor Browser - [redacted] This link only works in Tor Browser!
- Follow the instructions on this page

ATTENTION!

- Do not try to recover files yourself. this process can damage your data and recovery will become impossible
- Do not rename encrypted files.
- Do not waste time trying to find the solution on the Internet. The longer you wait, the higher will become the decryption key price
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our).
- Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org or use Tor Browser over VPN.
- Thanks to the warning wallpaper provided by lockbit, it's easy to use

orange Cyberdefense

# War story - Summary

## Situation:

Local IT began restoring and, together with local resources and together with local resources, launched an investigation.

## Immediate Risk:

Release of data including proprietary, confidential and personal information. Reputational damage. Unknow to Local IT

Lessons Learned:

- Insufficient Incident Preparation and Planning
- Insufficient Documentation
- No Methodology
- Destroyed evidence through too quick recovery

# Case Study

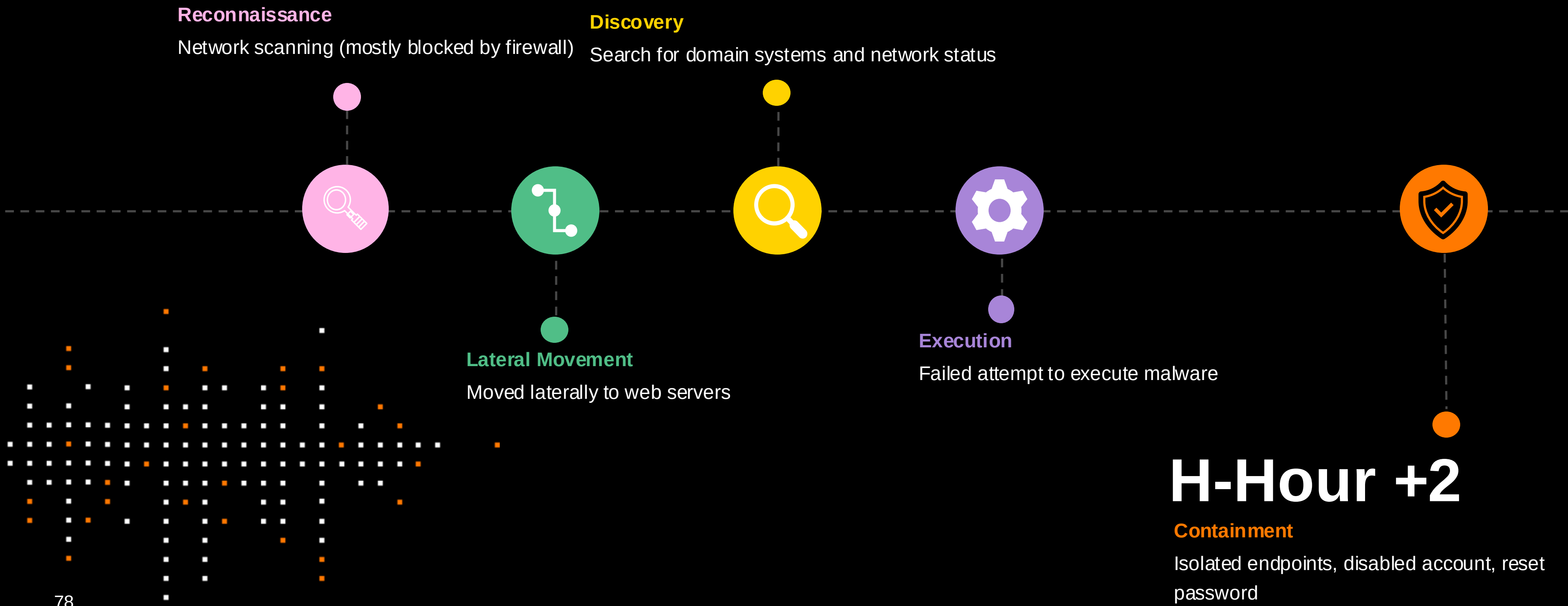
## Undisclosed Client

- 4 emergency cases in the last 15 months
- Been on a journey and have learnt the hard way
- Grown their security team from 1-man band, to several security professionals, from CISO down
- Last IR engagement contained prior to calling our CSIRT – details on the next few slides…

# Attack timeline

Cyberdefense

# June 2024...



**Reconnaissance**

Network scanning (mostly blocked by firewall)

**Lateral Movement**

Moved laterally to web servers

**Discovery**

Search for domain systems and network status

**Execution**

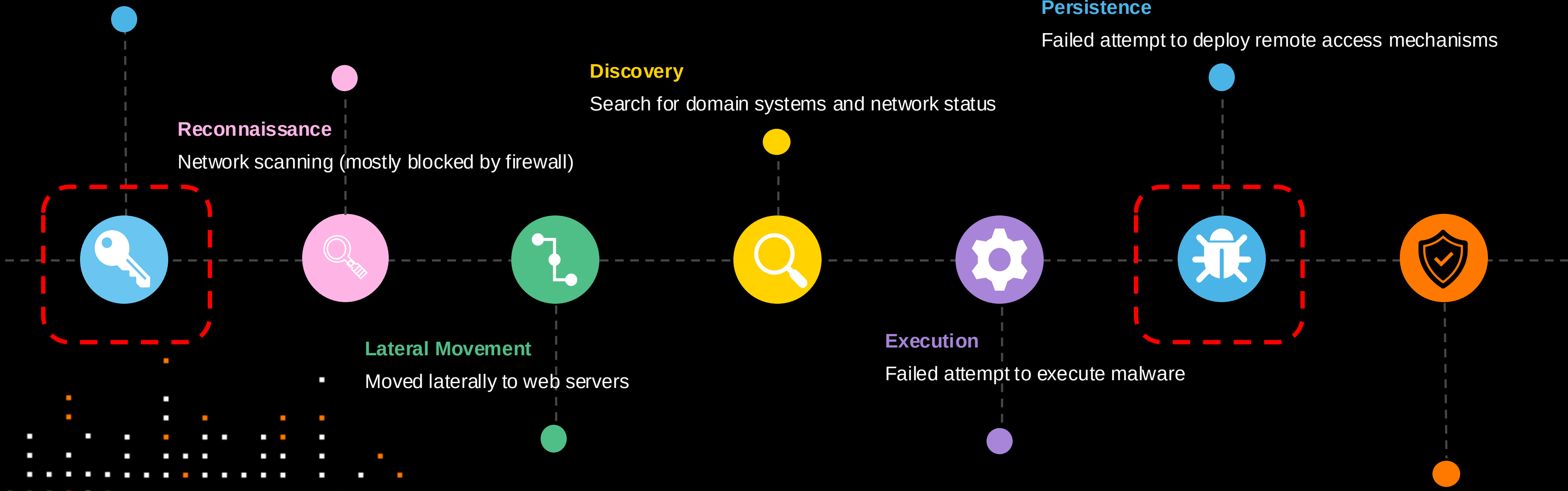
Failed attempt to execute malware

## H-Hour +2

**Containment**

Isolated endpoints, disabled account, reset password

# June 2024…



**Exploit of VPN Vulnerability**

Exploit enabled attacker to access valid credentials of privileged account

**Reconnaissance**

Network scanning (mostly blocked by firewall)

**Lateral Movement**

Moved laterally to web servers

**Discovery**

Search for domain systems and network status

**Execution**

Failed attempt to execute malware

**Persistence**

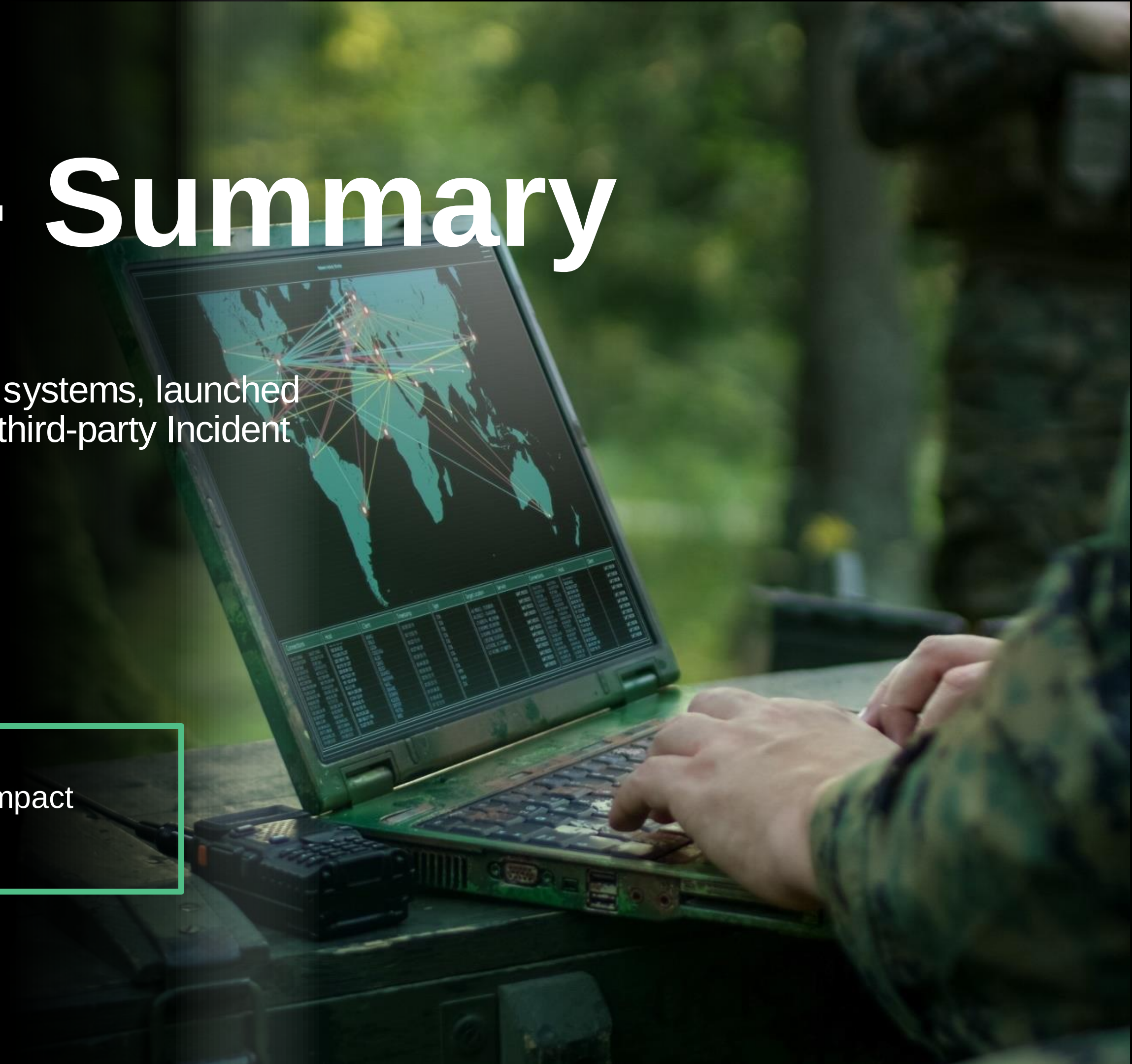
Failed attempt to deploy remote access mechanisms

## H-Hour +2

**Containment**

Isolated endpoints, disabled account, reset password

# War story - Summary



## Situation:

Local IT began quick isolation of affected systems, launched a formal investigation and called on their third-party Incident Response Team within hours.

## Immediate Risk:

Potential lateral movement.

Lessons Learned:

- Swift actions taken by a mature team limited the impact
- Improved Documentation
- Clear Methodology in place

# Key Aspects of Incident Response

## Understanding Risk:

External vs Internal Threat Actors. Risk strategies: Mitigate, Avoid, Transfer, Accept.

## Knowing the Phases of Incident Response (IR Life Cycle):

Preparation, Identification, Containment, Eradication, Recovery.

## Being aware of Stakeholders:

Management, IT, Legal, HR, PR, third-parties, law enforcement, clients/customers.

## Knowing your Documents:

Incident Response Plan, Play Books.

## Disaster Recovery:

Recovery Objectives. CSIRT vs Cyber Insurance…

# Be Brilliant at the Basics

4 P’s (there are many more!)

## Phishing

- MFA is not enough – you need Conditional Access Policies and/or Passkeys (“Phishing-Resistant MFA”)
- Are you aware of the current TTPs attackers are using to penetrate email security controls and deliver bait to your uses?
- And what will be next? Are you (and your users) keeping track of the ever-evolving threat landscape?

## Patching

- You can’t patch what you don’t know about. How confident are you with your network visibility?
- When was your last Black Box penetration test?

## Ports

- Which access points do you have directly exposed to the internet?

## Passwords

- Audit your company’s passwords before the attackers do
- What is the oldest password on your domain? Go and find out!
- Your passwords are part of your identity – don’t treat them like a string of text

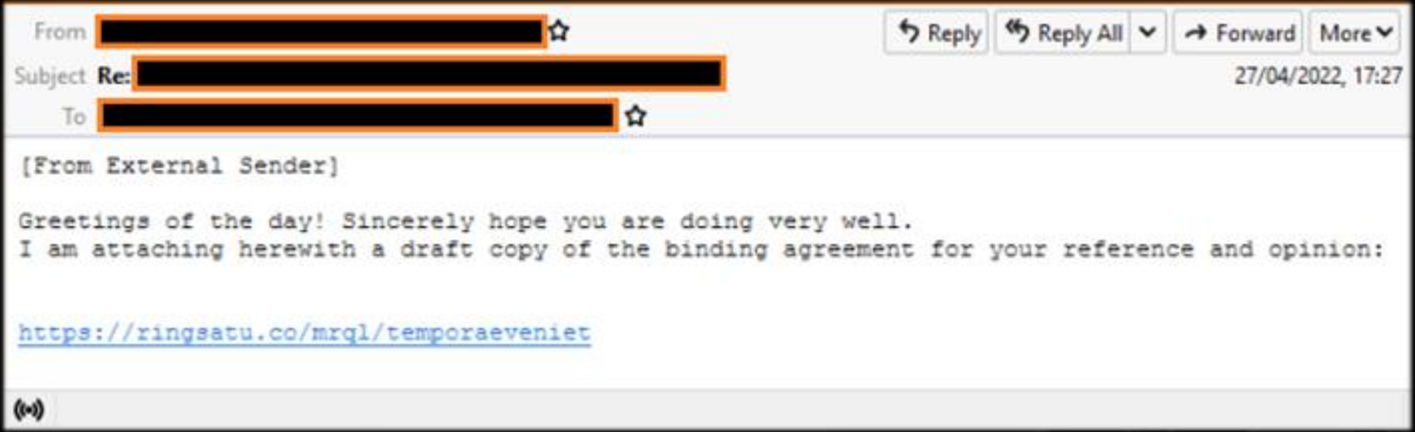
orange™ Cyberdefense

YEAH.....
THAT'S NOT GOING TO HAPPEN
quickmeme.com

# Business Email Compromise

Would you click on this?

Sent from a colleague in reply to another email.



From [redacted] ☆

Subject Re: [redacted]

To [redacted] ☆

27/04/2022, 17:27

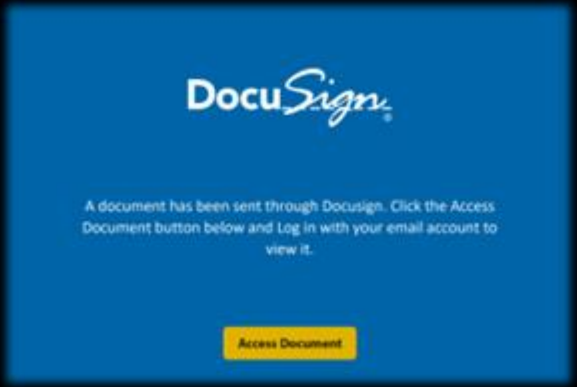
```
[From External Sender]

Greetings of the day! Sincerely hope you are doing very well.
I am attaching herewith a draft copy of the binding agreement for your reference and opinion:


https://ringsatu.co/mrql/temporaeveniet
```

orange™ Cyberdefense

# Business Email Compromise

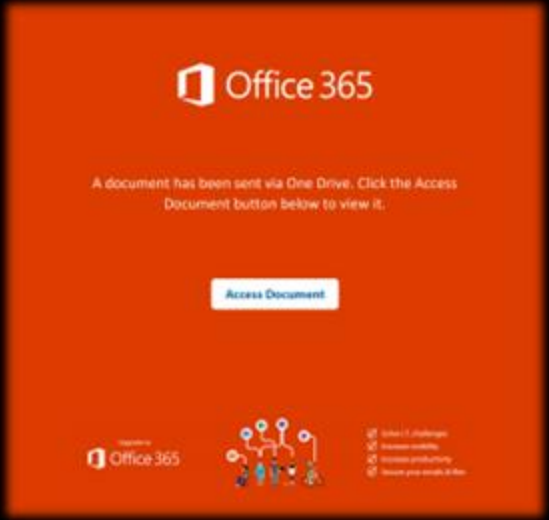
Would you click on these?

Received from SharePoint. “John has shared a file with you”.



DocuSign

A document has been sent through Docusign. Click the Access Document button below and Log in with your email account to view it.



Office 365

A document has been sent via One Drive. Click the Access Document button below to view it.

orange™ Cyberdefense

# Business Email Compromise

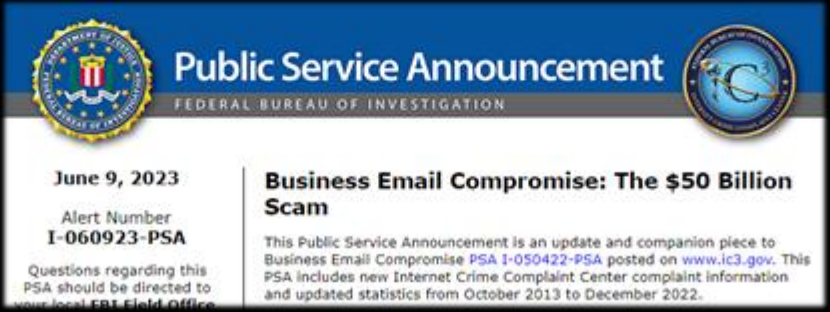
Data Security, Vulnerability Management, Email security

## WhatsApp used in BEC scam to pilfer $6.4M

Simon Hendery April 21, 2023

# FBI Business Email Compromise Statistics

|  |  |
|---|---|
| Between October 2013 and December 2022 |  |
| Domestic and international incidents: | 277,918 |
| Domestic and international exposed dollar loss: | $ 50,871,249,501 |
| Between June 2016 and December 2021 |  |
| Domestic and international incidents: | 241,206 |
| Domestic and international exposed dollar loss: | $ 43,312,749,946 |



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

June 9, 2023

Alert Number
I-060923-PSA

Questions regarding this PSA should be directed to your local FBI Field Office

**Business Email Compromise: The $50 Billion Scam**

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA I-050422-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to December 2022.

# Preparation is crucial to damage limitation of an incident

# Cybersecurity is no longer a check-box exercise!

orange™

orange™

Cyberdefense

Building a safer digital society.

orange Cyberdefense

# Maintain Operational Resilience

Bo Drejer, GRC Manager, Orange Cyberdefense Denmark

Mats Lindblad, GRC Manager, Orange Cyberdefense Sweden

Bernstorff Slot 3. October 2024

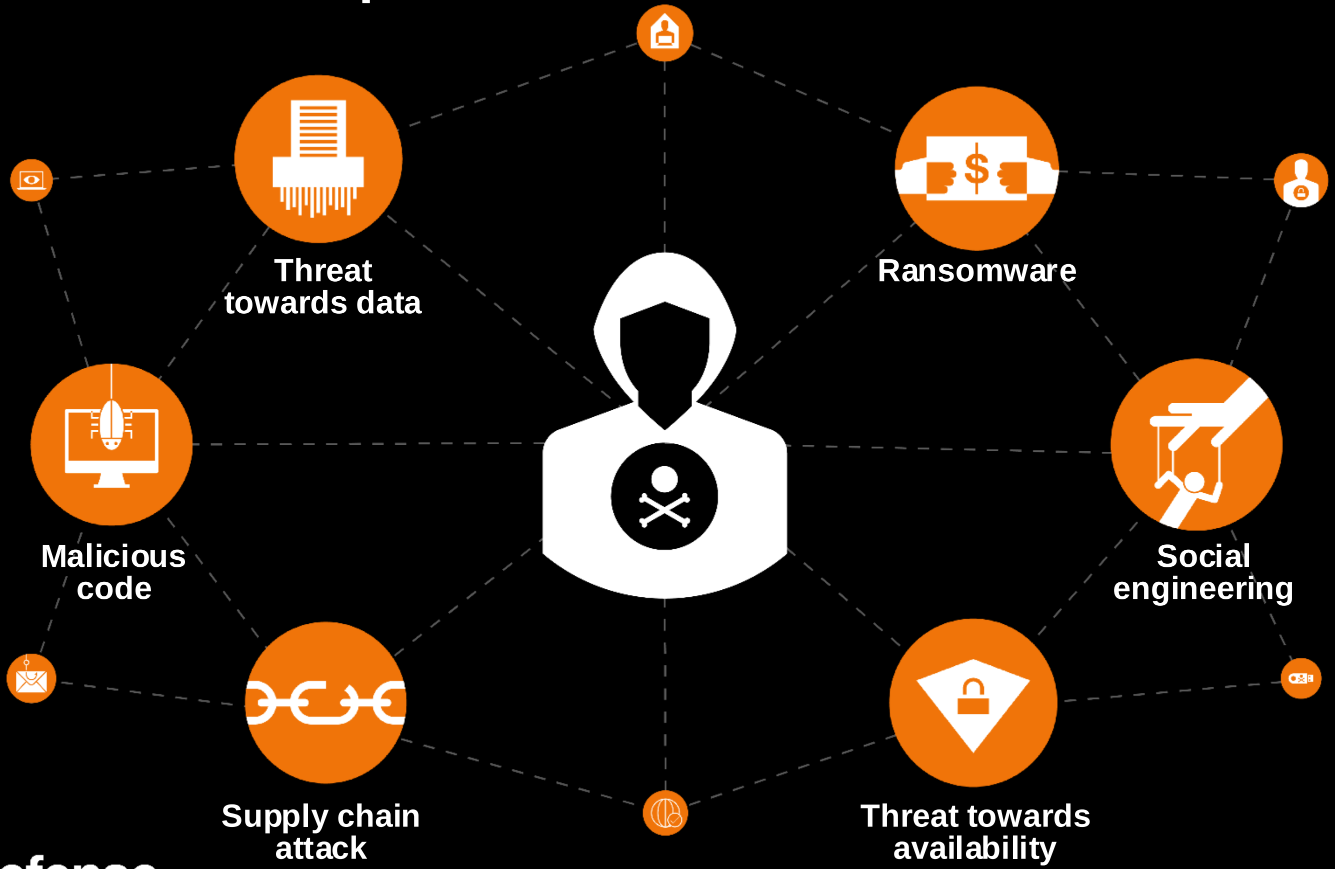
# Resilience

# What is this?

# Resilience definition

”The ability to recognise risks & changes
in an environment and adjust to them”

# Threat Landscape.



Threat towards data

Ransomware

Malicious code

Social engineering

Supply chain attack

Threat towards availability

orange™ Cyberdefense

# The swans

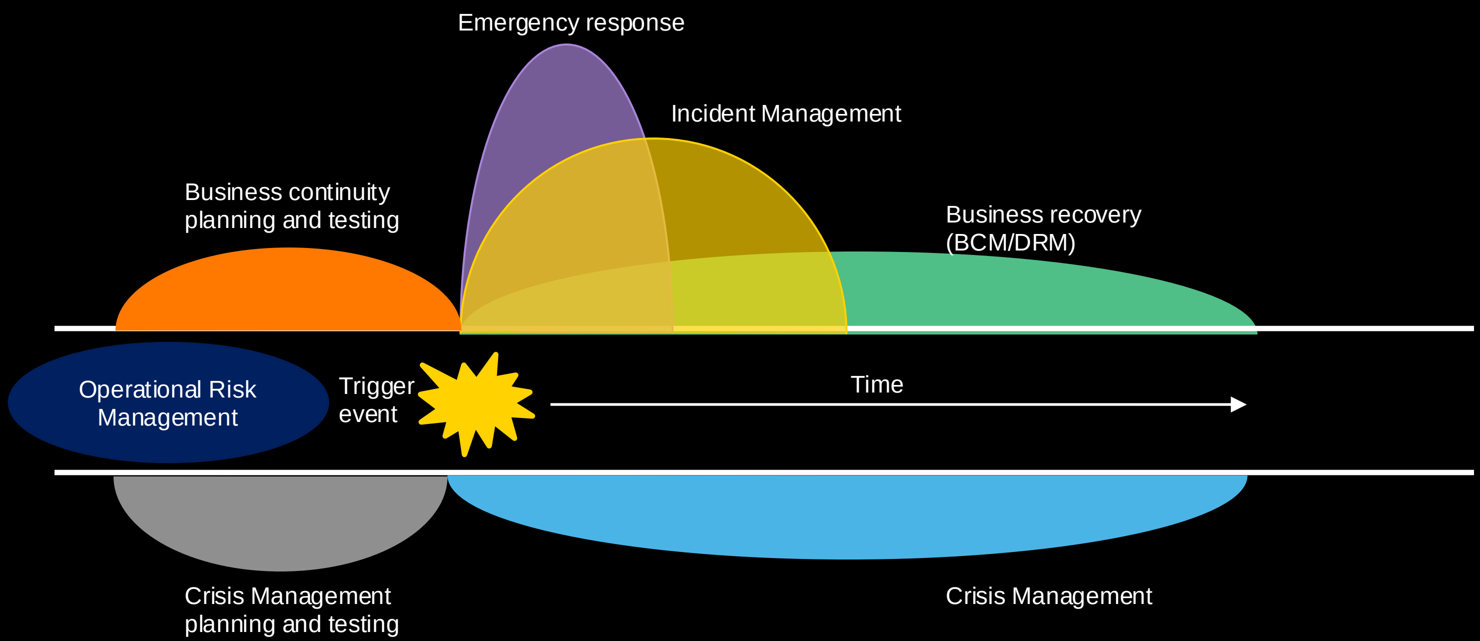
Unknown unknowns

Known unknowns

Known knowns

Source: Dr Deborah Pretty

# General Perspective - Resilience


Emergency response
Incident Management
Business continuity planning and testing
Business recovery (BCM/DRM)
Operational Risk Management
Trigger event
Time
Crisis Management planning and testing
Crisis Management

Strategic

Tactictal

Operational

# 3 P’s

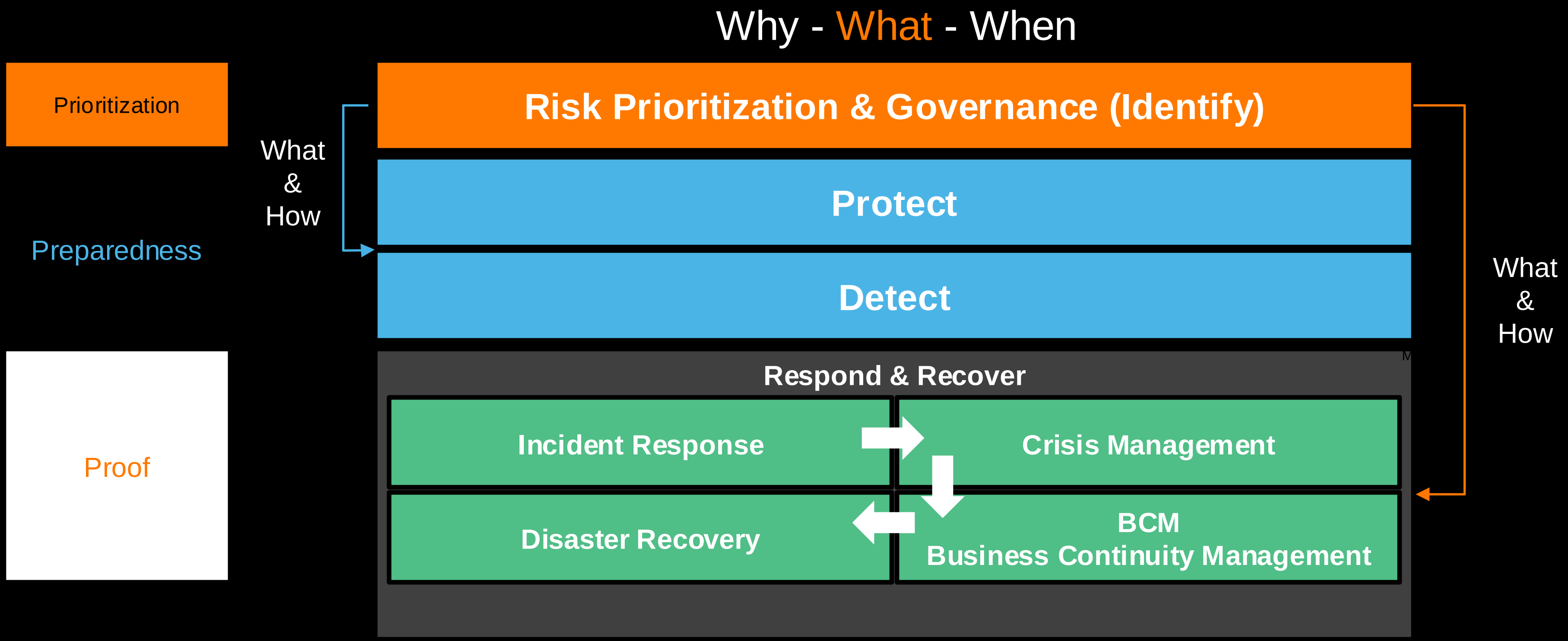
# Prioritization

# Preparedness

# Proof

# GRC - optimizing and operationalizing risk mitigation & investments

## Significant part of organizational resilience



Why - What - When

Prioritization

Preparedness

Proof

What & How

Risk Prioritization & Governance (Identify)

Protect

Detect

Respond & Recover

Incident Response

Crisis Management

Disaster Recovery

BCM
Business Continuity Management

What & How

# NIS2: Predictability Of Significant European Supply Chains

Accountability!

Know Your Risk

Protect Adequately

Ability To React On Incident

Ability To Recover

# Security by Design

## Legislation & Directives

Ulrik Ledertoug
CTO

> NIS2 er noget alle bør have på dagsordenen – og prioritere højt nu. I må ikke gå i stå, men skal fortsætte med implementeringen på trods af udsættelsen, så I kan blive compliant hurtigst muligt. Hvis I ikke er startet endnu, så kom i gang. Det er især vigtigt, hvis man har kunder eller samarbejdspartnere i andre EU-lande, hvor den nationale implemen-tering ikke er forsinket.

# Security by Design

## Legislation & Directives

Bo Drejer
GRC Manager

> Første skridt hen imod NIS2-compliance er at få lavet en risiko-vurdering, som giver overblik. Det er en vigtig og værdifuld forudsætning for, at man kan foretage den nødven-dige optimering af ressourcer og prioritering af indsatsområder, hvilket er fundamentet for, at man kan arbejde målrettet med at styrke den operationelle cybersikkerhed.

# …ensuring increased business resilience is now a board-level matter, too.

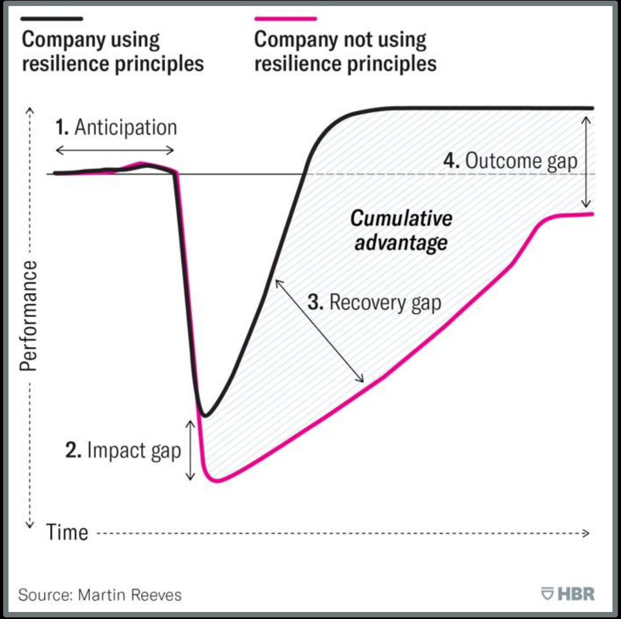
## The benefits of resilience

Anticipate threats faster

Better resistance to the initial shock

Rebound more quickly

Benefit from increased fitness post shock

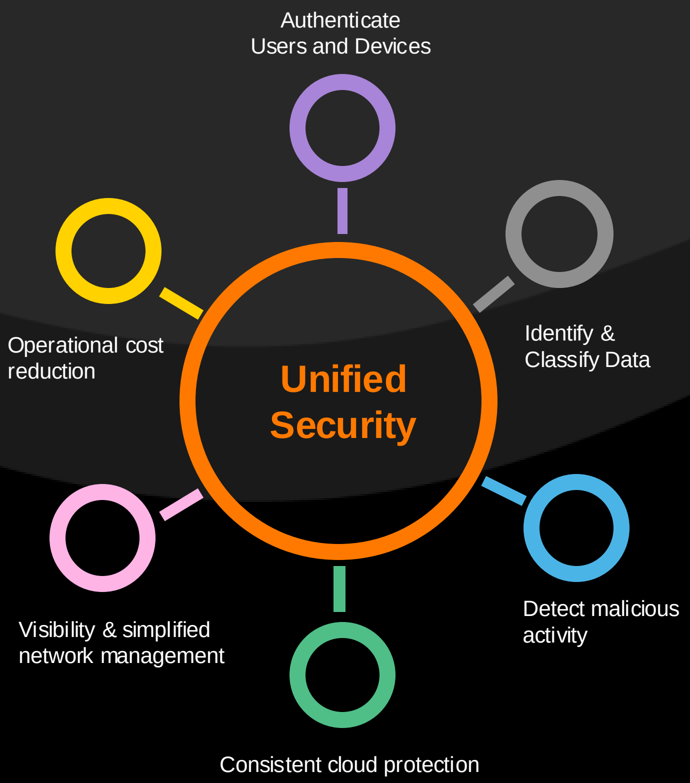


Source: Martin Reeves

Source: A Guide to Building a More Resilient Business, Harvard Business Review.

# Changing The Game

With Holistic Architecture


Authenticate Users and Devices
Identify & Classify Data
Detect malicious activity
Consistent cloud protection
Visibility & simplified network management
Operational cost reduction
Unified Security

**Business driven security policies sets the scene**

Business driven risk management defines access

**Taking offset in identity visibility**

Individuals, Devices, Solutions

**Dynamic access control based upon**

Type, Status, Verification, Location, Criticality, etc.

Business driven central control and visibility!

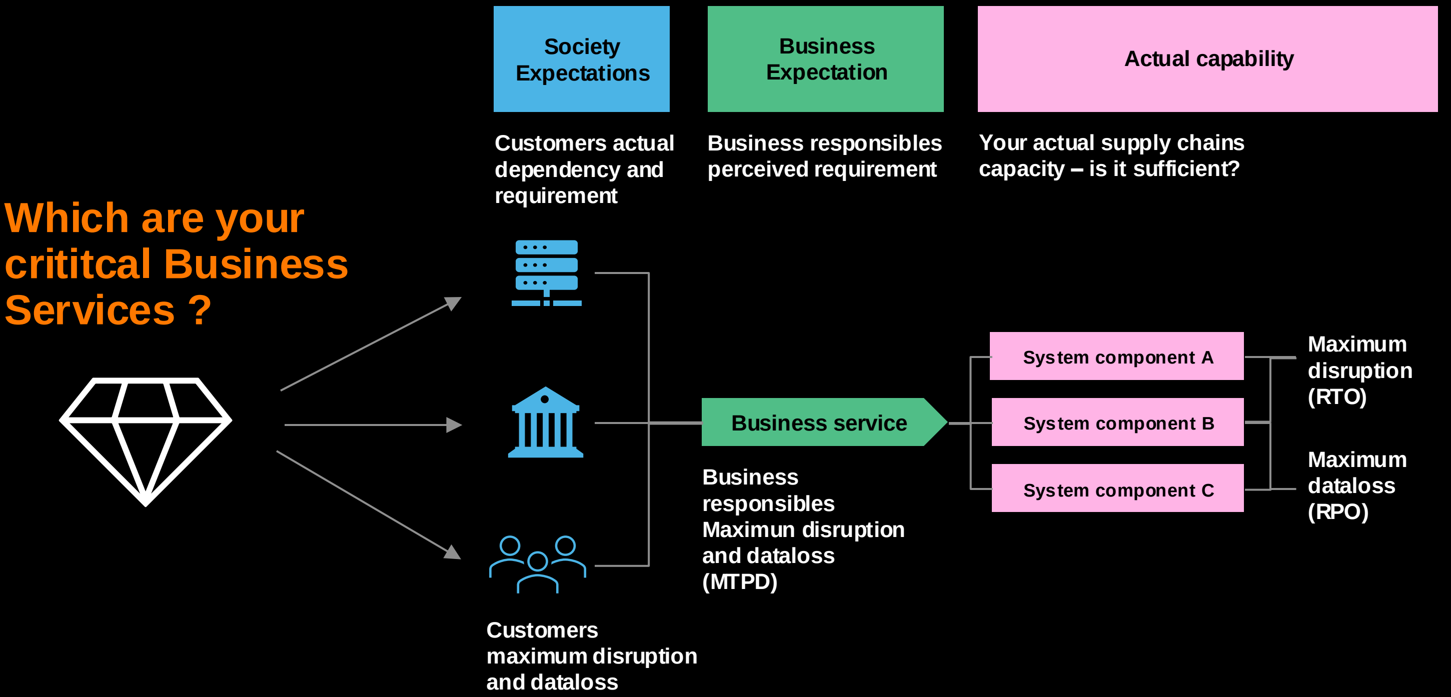
# Important Questions

- Are our (critical) business risks adressed sufficiently?
- Visibility of who and what has accesss to what?
- Visibility of what is implemented and if it is done correctly?
- Do I have enough ressources for timely implementation?
- Are we sufficiently efficient on detecting and blocking attacks in a timely fashion?
- Is Crisis Management, Business Continuity, Disater Recovery adeqautely tested

Transparent prioritization, reporting and execution based upon business risk!

# Risk Prioritisation & Governance

## Which business functions are most critical?



Which are your crititcal Business Services ?

Society Expectations

Customers actual dependency and requirement

Business Expectation

Business responsibles perceived requirement

Actual capability

Your actual supply chains capacity – is it sufficient?

Business service

Business responsibles Maximun disruption and dataloss (MTPD)

System component A

System component B

System component C

Maximum disruption (RTO)

Maximum dataloss (RPO)

Customers maximum disruption and dataloss

# Real world example

## Strengthening of operational capability: Prioritization, Protection and Recovery

- Technically mature customer
- Performed Top-Down BIA
- Production and distribution of most importance
- 90% of production & distribution depended on it-infrastructure

→ 4 months later they had trained and could document recovery of IT-infrastructure within 24 hours

orange Cyberdefense

# Resilience anticipation – learnings matter!

Tacoma Bridge

# GRC

**Contact**

Bo Drejer, GRC Manager
bo.drejer@orangecyberdefense.com
+45  2148 0381

orange™ Cyberdefense

orange™

Cyberdefense

We build a safer digital society.