Hotlandskapet

Cy-X / Ransomware
Hacktivism

Peter Larsson

CTO Orange Cyberdefense Sverige

Agenda

- Orange Cyberdefense – vilka är vi?
- Hotlandskapet – Sverige och Norden
    - Hacktivism
    - Ransomware/Cy-X
- Hot – Hur ska vi agera?

Trevligt att träffas!

Vi är en ledande leverantör av cybersäkerhetstjänster.
Vi har en global styrka, som vi nyttjar i kombination med vår lokala närvaro.

Säkra det digitala samhället

Över 400
Cybersäkerhetsexperter
fördelade på 7 kontor
i Sverige
+2500 anställda i världen

+8,700
kunder
i världen,
bidrar till vårt intelligensstyrda fundament

1
fokus
Cyber
säkerhet

Leader in European Managed Security Services Providers.

FORRESTER®

500+
källor matas kontinuerligt in i vår dataalake med information om cyberhot

Leader European Managed Security Services.

IDC

24/7/365
kontinuerlig övervakning
SOC
Malmö
Stockholm

Erkänd leverantör i flera rapporter
Managed Detection and Response, Incident Response and Digital Forensics, OT Security, Threat Intelligence & Managed Security Services

Gartner

Forskning om cybersäkerhet och förståelse om hoten – en del av vårt DNA

Våra cybersäkerhetsexperter, forskare och analytiker övervakar de senaste hoten och sårbarheterna, så att våra kunder kan känna till hoten i förväg och fokusera sitt arbete där det gör mest nytta.

250+

experter fokuserade på R&D och hotforskning.

20%

av våra pentestares tid läggs på forskning

50

dagar i förväg kan våra underrättelser finnas innan de dyker upp i andra källor.

80+

Publicerade rapporter och framträdanden på säkerhetskonferenser förra året.

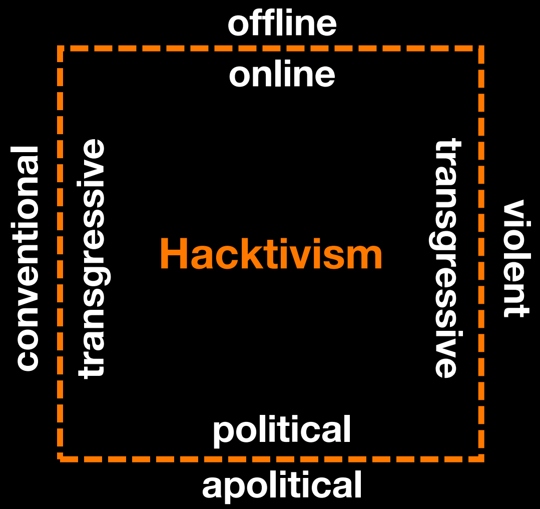
2.500

unika hot indikatorer okända för andra i vår hotdatabas.

30

CVEs tilldelade oss av MITRE.

1 Hacktivism



offline

online

conventional

transgressive

Hacktivism

transgressive

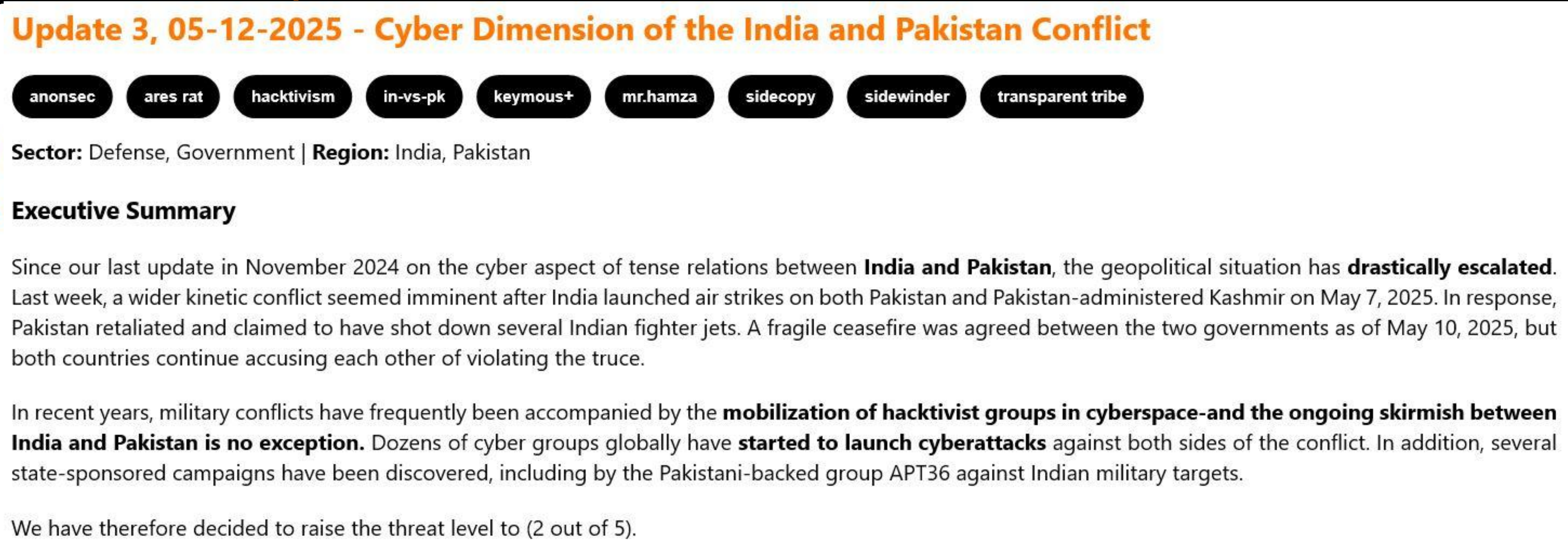
violent

political

apolitical

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

Hacktivism | Pågående geopolitiska konflikter



Update 3, 05-12-2025 - Cyber Dimension of the India and Pakistan Conflict

anonsec | ares rat | hacktivism | in-vs-pk | keymous+ | mr.hamza | sidecopy | sidewinder | transparent tribe

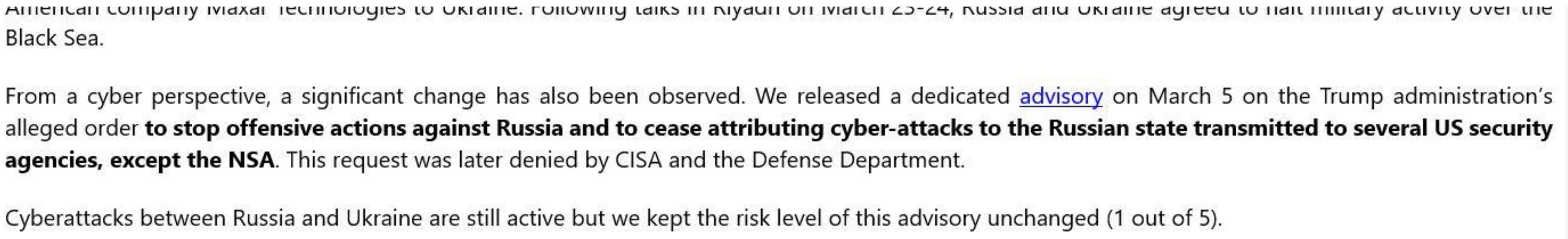
Sector: Defense, Government | **Region:** India, Pakistan

Executive Summary

Since our last update in November 2024 on the cyber aspect of tense relations between **India and Pakistan**, the geopolitical situation has **drastically escalated**. Last week, a wider kinetic conflict seemed imminent after India launched air strikes on both Pakistan and Pakistan-administered Kashmir on May 7, 2025. In response, Pakistan retaliated and claimed to have shot down several Indian fighter jets. A fragile ceasefire was agreed between the two governments as of May 10, 2025, but both countries continue accusing each other of violating the truce.

In recent years, military conflicts have frequently been accompanied by the **mobilization of hacktivist groups in cyberspace-and the ongoing skirmish between India and Pakistan is no exception.** Dozens of cyber groups globally have **started to launch cyberattacks** against both sides of the conflict. In addition, several state-sponsored campaigns have been discovered, including by the Pakistani-backed group APT36 against Indian military targets.

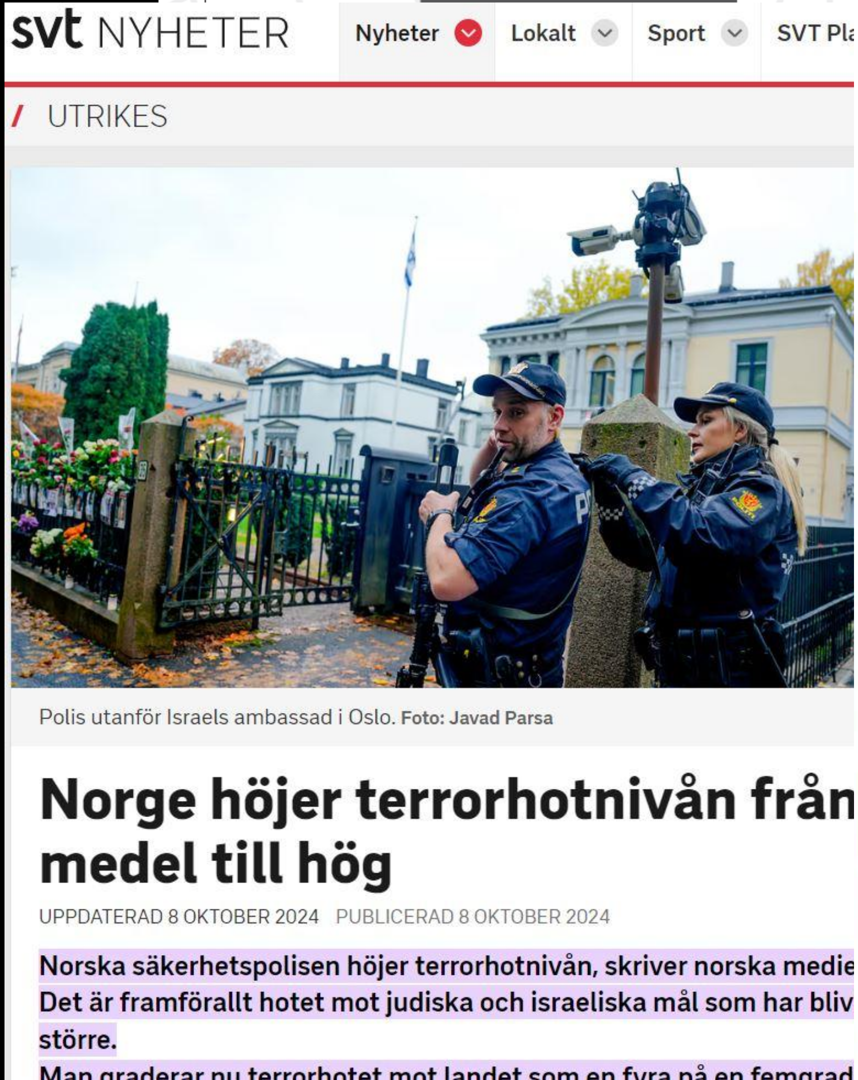
We have therefore decided to raise the threat level to (2 out of 5).



American company Maxar Technologies to Ukraine. Following talks in Riyadh on March 23-24, Russia and Ukraine agreed to halt military activity over the Black Sea.

From a cyber perspective, a significant change has also been observed. We released a dedicated advisory on March 5 on the Trump administration's alleged order **to stop offensive actions against Russia and to cease attributing cyber-attacks to the Russian state transmitted to several US security agencies, except the NSA**. This request was later denied by CISA and the Defense Department.

Cyberattacks between Russia and Ukraine are still active but we kept the risk level of this advisory unchanged (1 out of 5).



/ UTRIKES

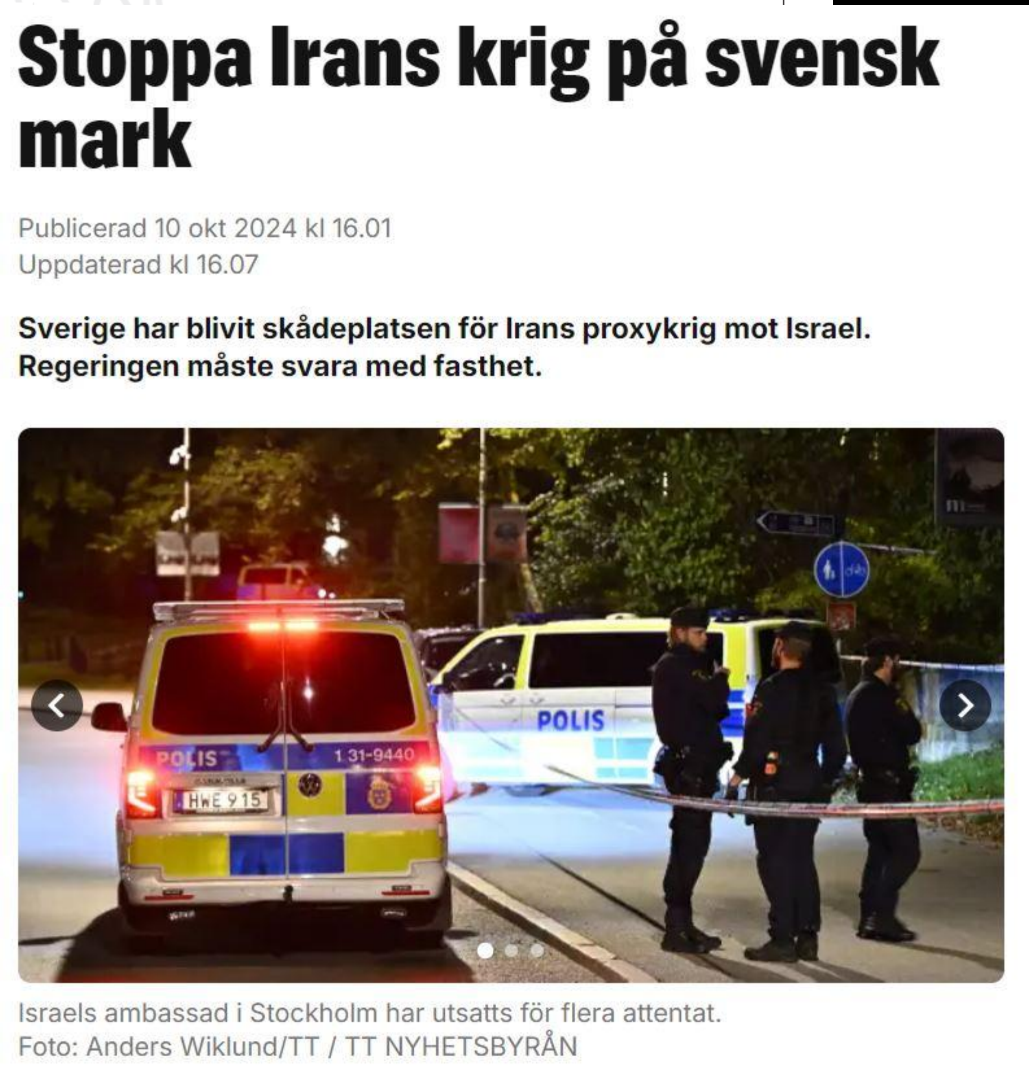
Polis utanför Israels ambassad i Oslo. **Foto: Javad Parsa**

Norge höjer terrorhotnivån från medel till hög

UPPDATERAD 8 OKTOBER 2024 PUBLICERAD 8 OKTOBER 2024

Norska säkerhetspolisen höjer terrorhotnivån, skriver norska medie Det är framförallt hotet mot judiska och israeliska mål som har bliv större.

Man graderar nu terrorhotet mot landet som en fyra på en femgrad

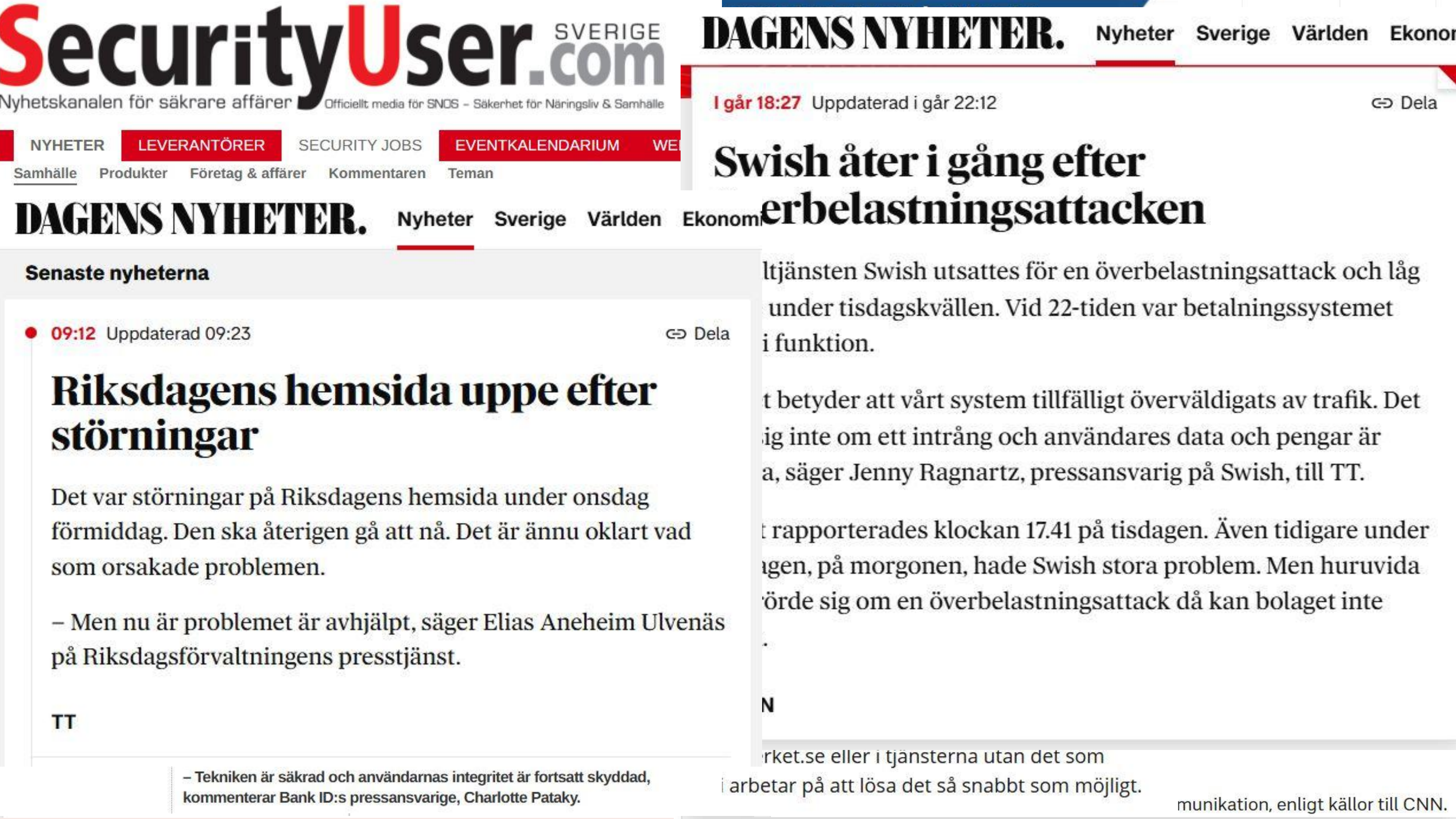


Stoppa Irans krig på svensk mark

Publicerad 10 okt 2024 kl 16.01
Uppdaterad kl 16.07

Sverige har blivit skådeplatsen för Irans proxykrig mot Israel. Regeringen måste svara med fasthet.

Israels ambassad i Stockholm har utsatts för flera attentat.
Foto: Anders Wiklund/TT / TT NYHETSBYRÅN



SecurityUser.com SVERIGE

Nyhetskanalen för säkrare affärer

Officiellt media för SNOS – Säkerhet för Näringsliv & Samhälle

NYHETER LEVERANTÖRER SECURITY JOBS EVENTKALENDARIUM WE

Samhälle Produkter Företag & affärer Kommentaren Teman

DAGENS NYHETER. Nyheter Sverige Världen Ekonom

I går 18:27 Uppdaterad i går 22:12 Dela

Swish åter i gång efter erbelastningsattacken

ltjänsten Swish utsattes för en överbelastningsattack och låg under tisdagskvällen. Vid 22-tiden var betalningssystemet i funktion.

t betyder att vårt system tillfälligt överväldigats av trafik. Det ig inte om ett intrång och användares data och pengar är a, säger Jenny Ragnartz, pressansvarig på Swish, till TT.

t rapporterades klockan 17.41 på tisdagen. Även tidigare under ıgen, på morgonen, hade Swish stora problem. Men huruvida örde sig om en överbelastningsattack då kan bolaget inte

N

DAGENS NYHETER. Nyheter Sverige Världen Ekonom

Senaste nyheterna

● 09:12 Uppdaterad 09:23 Dela

Riksdagens hemsida uppe efter störningar

Det var störningar på Riksdagens hemsida under onsdag förmiddag. Den ska återigen gå att nå. Det är ännu oklart vad som orsakade problemen.

– Men nu är problemet är avhjälpt, säger Elias Aneheim Ulvenäs på Riksdagsförvaltningens presstjänst.

TT

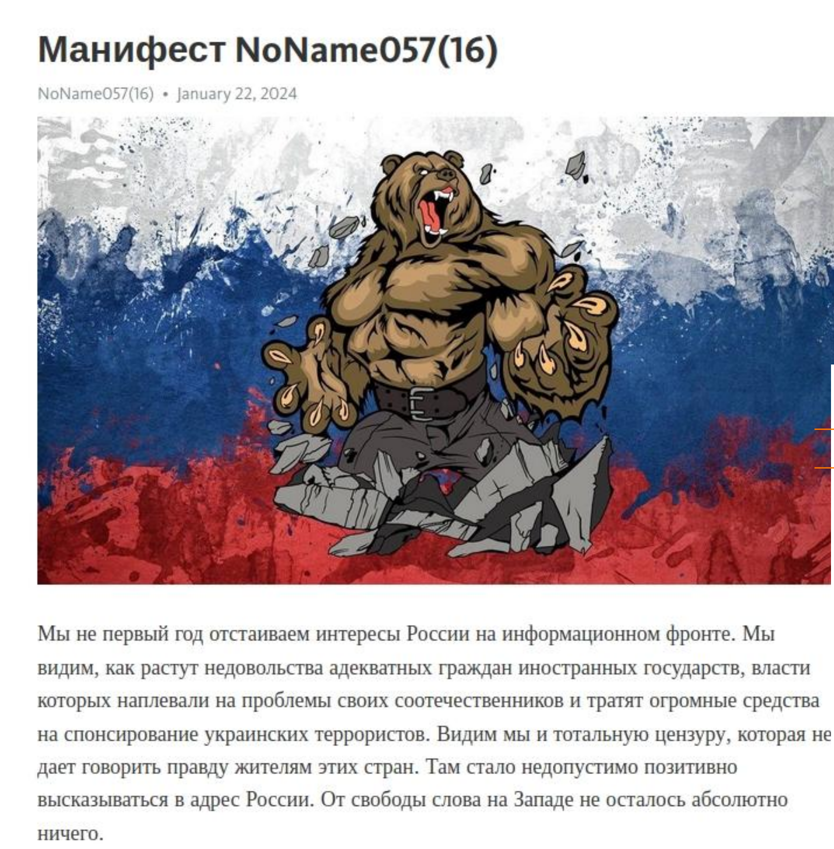
– Tekniken är säkrad och användarnas integritet är fortsatt skyddad, kommenterar Bank ID:s pressansvarige, Charlotte Pataky.

rket.se eller i tjänsterna utan det som

i arbetar på att lösa det så snabbt som möjligt.

munikation, enligt källor till CNN.

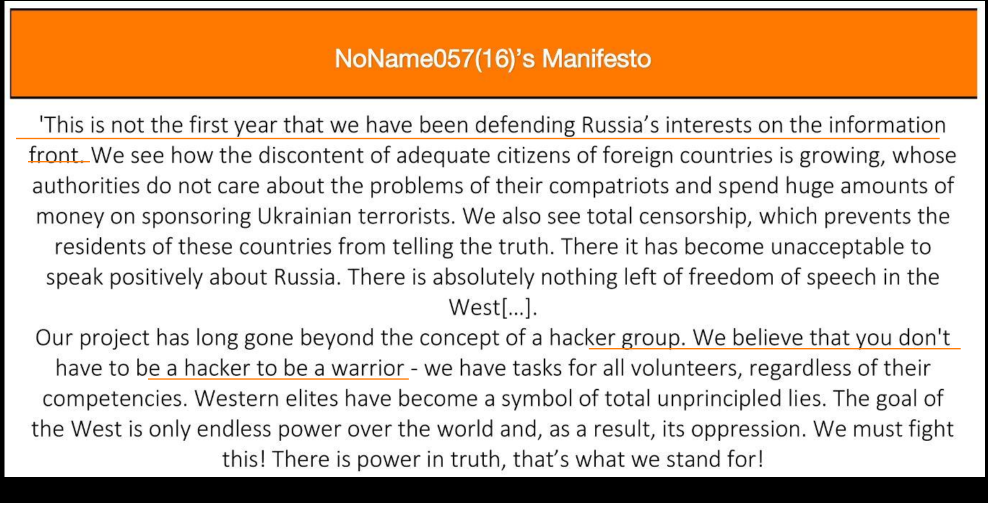
NoName057(16) - Manifesto



Манифест NoName057(16)

NoName057(16) • January 22, 2024

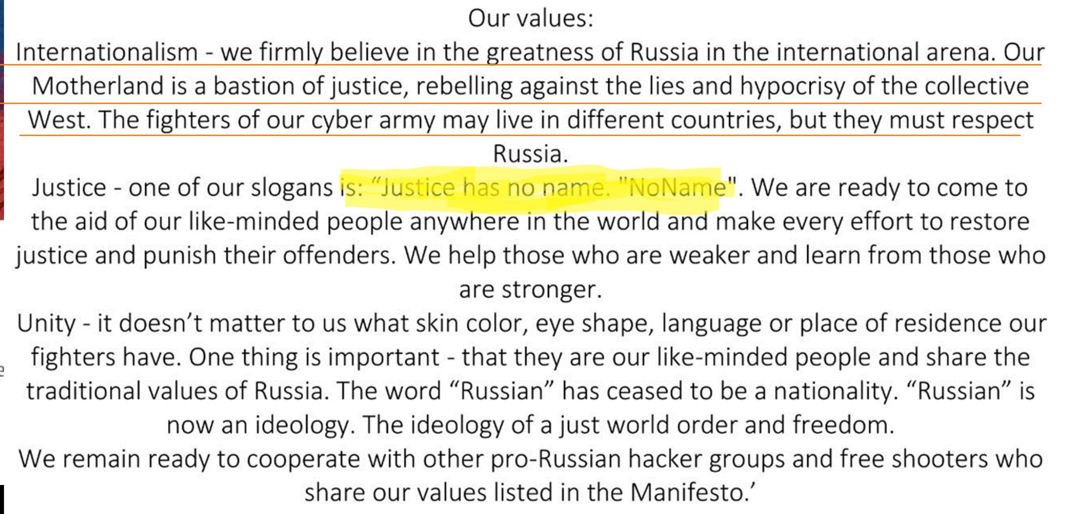
Мы не первый год отстаиваем интересы России на информационном фронте. Мы видим, как растут недовольства адекватных граждан иностранных государств, власти которых наплевали на проблемы своих соотечественников и тратят огромные средства на спонсирование украинских террористов. Видим мы и тотальную цензуру, 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.



NoName057(16)'s Manifesto

'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.'

2 Forskning Ransomware / Cy-X

Cy-X | Terminologi

Ransomware

Mjukvarufamilj - många olika
Verktyg - vem är ansvarig
Smalare fokus: tekniskt

VS.

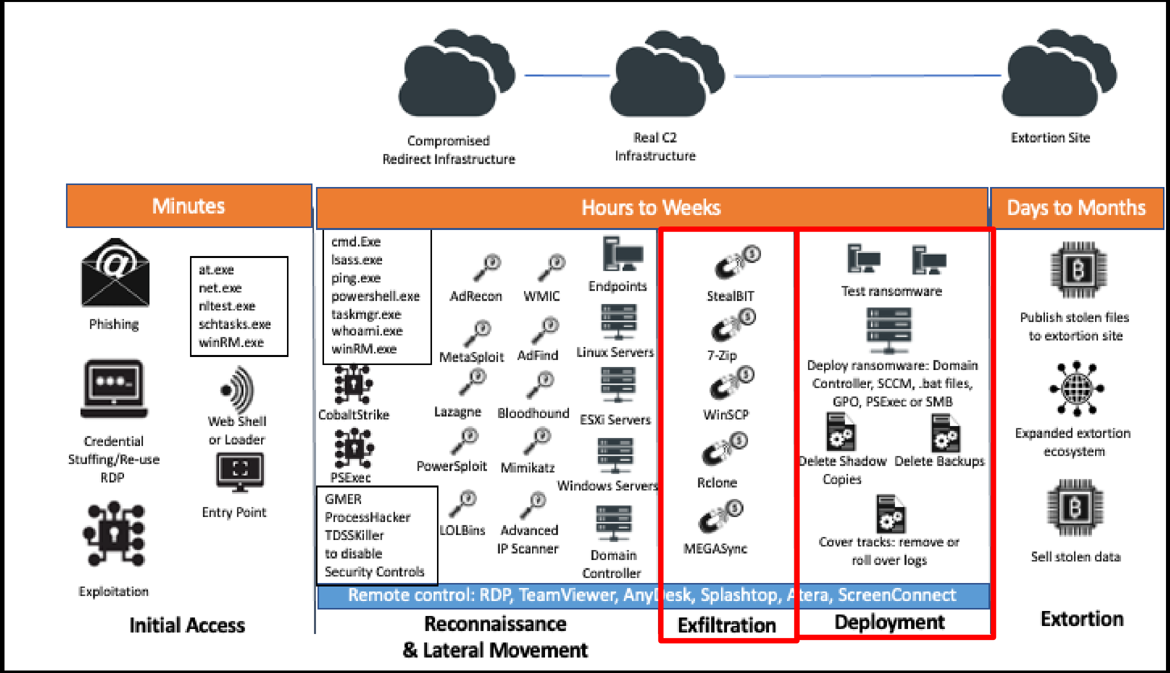
Cyber extortion

Kriminell handling
Juridisk definition - brottsoffer
Bredare fokus: människor och organisationer

"Hack & leak" attacker

Vad är problemet ?

Maze Ransomware



Compromised Redirect Infrastructure

Real C2 Infrastructure

Extortion Site

Minutes

Phishing

at.exe
net.exe
nltest.exe
schtasks.exe
winRM.exe

Credential Stuffing/Re-use RDP

Web Shell or Loader

Entry Point

Exploitation

Initial Access

Hours to Weeks

cmd.Exe
lsass.exe
ping.exe
powershell.exe
taskmgr.exe
whoami.exe
winRM.exe

AdRecon

WMIC

Endpoints

MetaSploit

AdFind

Linux Servers

CobaltStrike

Lazagne

Bloodhound

ESXi Servers

PSExec

PowerSploit

Mimikatz

Windows Servers

GMER
ProcessHacker
TDSSKiller
to disable
Security Controls

LOLBins

Advanced IP Scanner

Domain Controller

StealBIT

7-Zip

WinSCP

Rclone

MEGASync

Test ransomware

Deploy ransomware: Domain Controller, SCCM, .bat files, GPO, PSExec or SMB

Delete Shadow Copies

Delete Backups

Cover tracks: remove or roll over logs

Remote control: RDP, TeamViewer, AnyDesk, Splashtop, Atera, ScreenConnect

Reconnaissance & Lateral Movement

Exfiltration

Deployment

Days to Months

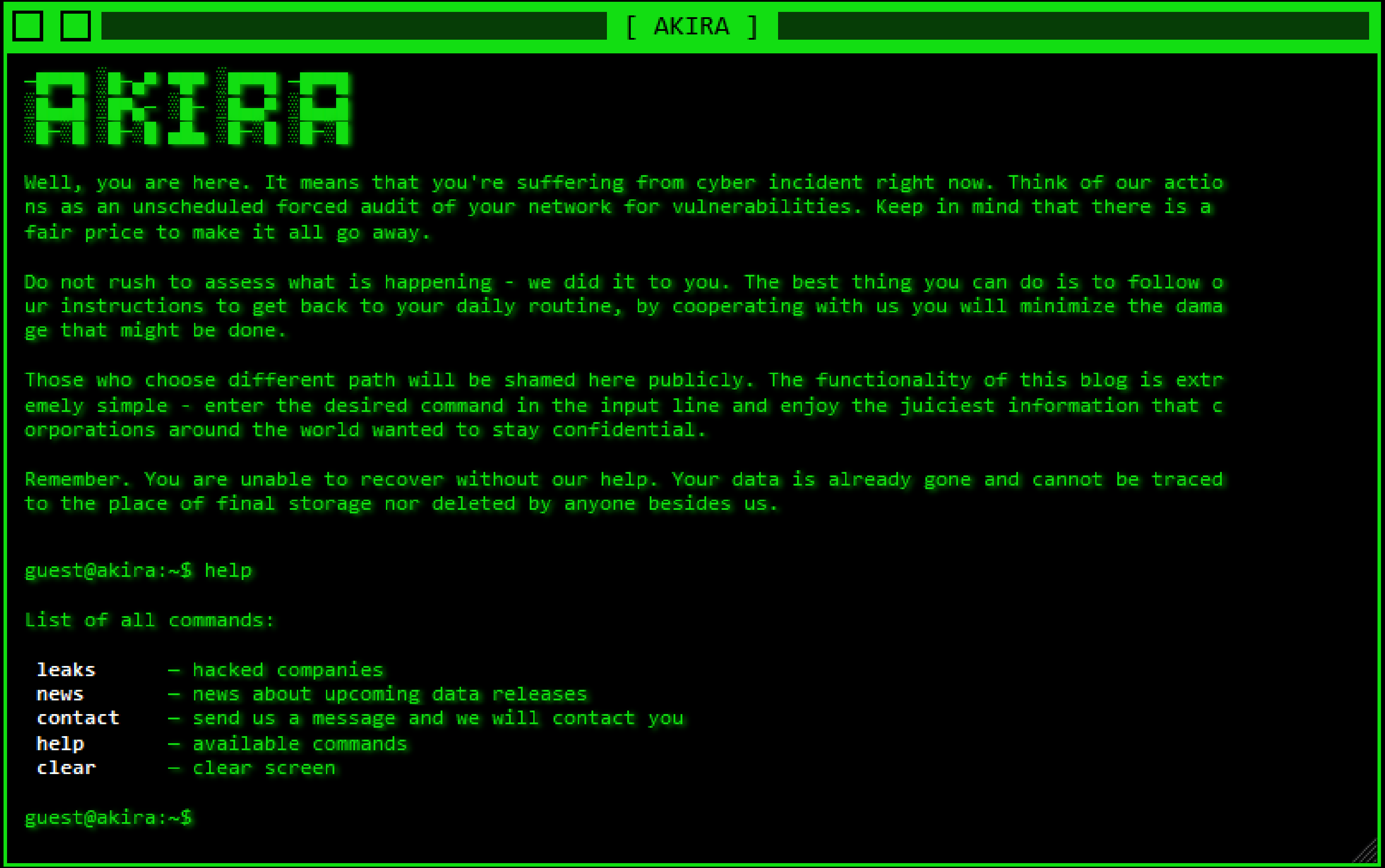
Publish stolen files to extortion site

Expanded extortion ecosystem

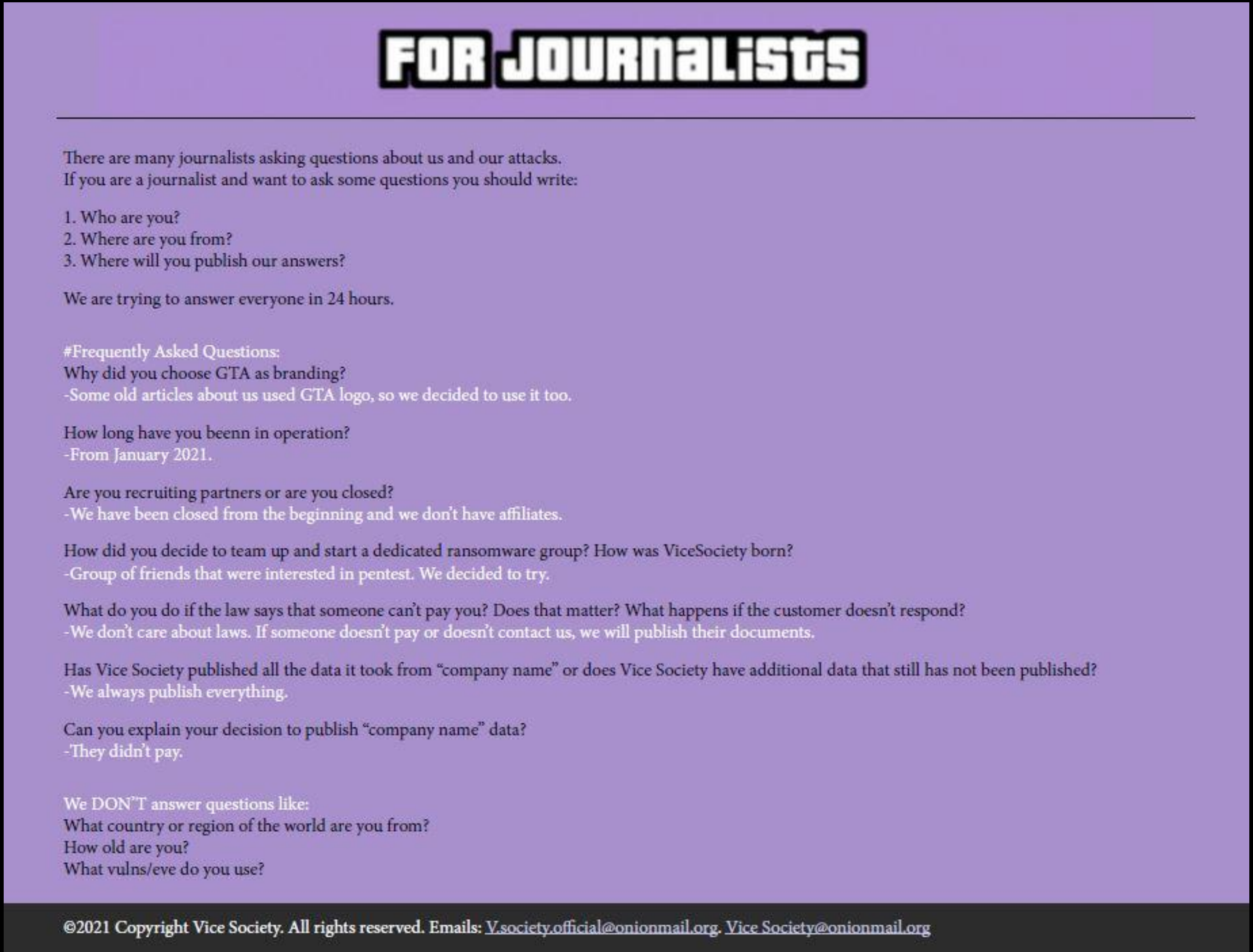
Sell stolen data

Extortion

https://www.cyfirma.com/blogs/maze-ransomware-group-declared-successful-exploits-of-many-organizations-and-released-massive-data-on-public-site-in-one-day/
https://twitter.com/uuallan/status/1441936468729946114



```
AKIRA

Well, you are here. It means that you're suffering from cyber incident right now. Think of our actio
ns as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a
fair price to make it all go away.

Do not rush to assess what is happening - we did it to you. The best thing you can do is to follow o
ur instructions to get back to your daily routine, by cooperating with us you will minimize the dama
ge that might be done.

Those who choose different path will be shamed here publicly. The functionality of this blog is extr
emely simple - enter the desired command in the input line and enjoy the juiciest information that c
orporations around the world wanted to stay confidential.

Remember. You are unable to recover without our help. Your data is already gone and cannot be traced
to the place of final storage nor deleted by anyone besides us.


guest@akira:~$ help

List of all commands:

 leaks       — hacked companies
 news        — news about upcoming data releases
 contact     — send us a message and we will contact you
 help        — available commands
 clear       — clear screen

guest@akira:~$
```



FOR JOURNALISTS

There are many journalists asking questions about us and our attacks.
If you are a journalist and want to ask some questions you should write:

1. Who are you?
2. Where are you from?
3. Where will you publish our answers?

We are trying to answer everyone in 24 hours.

#Frequently Asked Questions:
Why did you choose GTA as branding?
-Some old articles about us used GTA logo, so we decided to use it too.

How long have you beenn in operation?
-From January 2021.

Are you recruiting partners or are you closed?
-We have been closed from the beginning and we don't have affiliates.

How did you decide to team up and start a dedicated ransomware group? How was ViceSociety born?
-Group of friends that were interested in pentest. We decided to try.

What do you do if the law says that someone can't pay you? Does that matter? What happens if the customer doesn't respond?
-We don't care about laws. If someone doesn't pay or doesn't contact us, we will publish their documents.

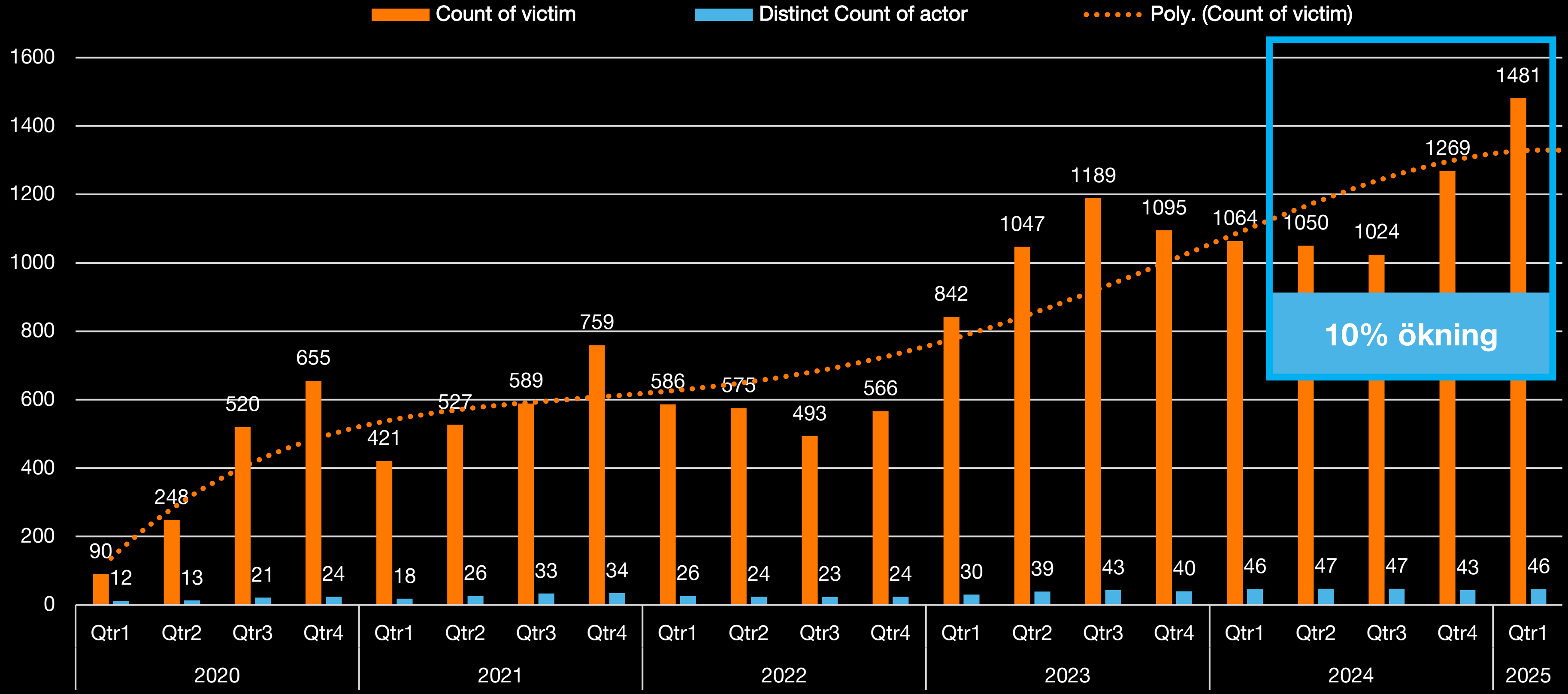
Has Vice Society published all the data it took from "company name" or does Vice Society have additional data that still has not been published?
-We always publish everything.

Can you explain your decision to publish "company name" data?
-They didn't pay.

We DON'T answer questions like:
What country or region of the world are you from?
How old are you?
What vulns/eve do you use?

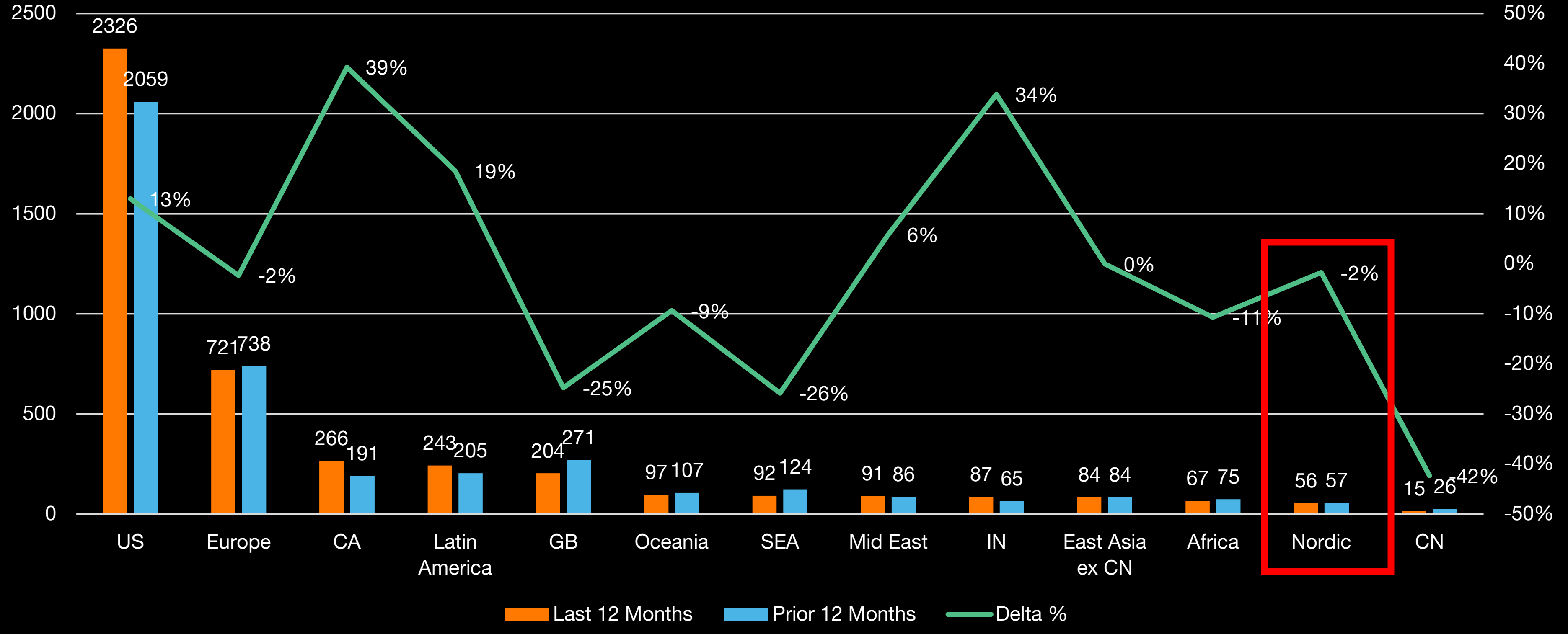
Cy-X över tid

Antal offer och hotaktörer observerade över tid

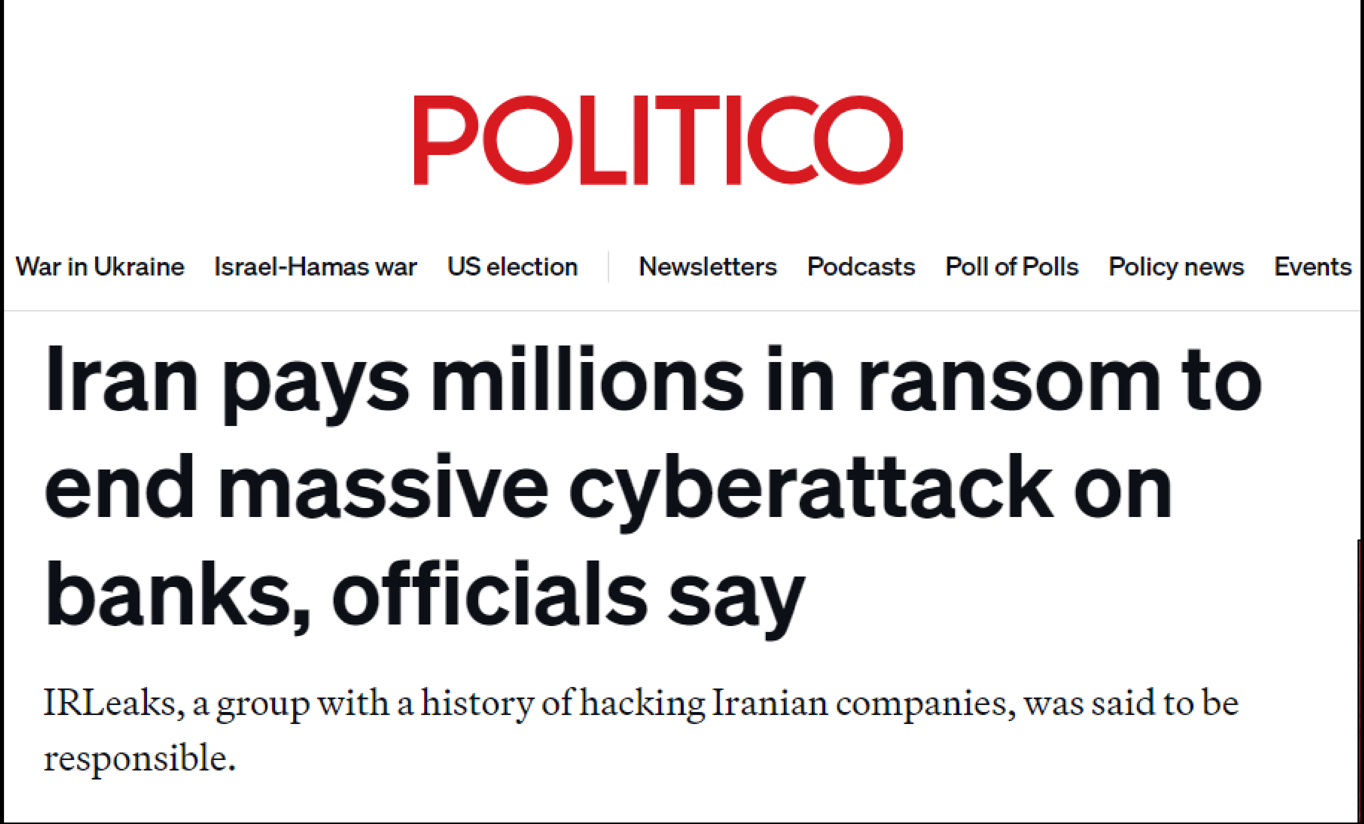


Antal offer per region - förändring

Regional uppdelning: jämförelse mellan de två senaste 12 mån perioderna



Vilka attackeras inte?

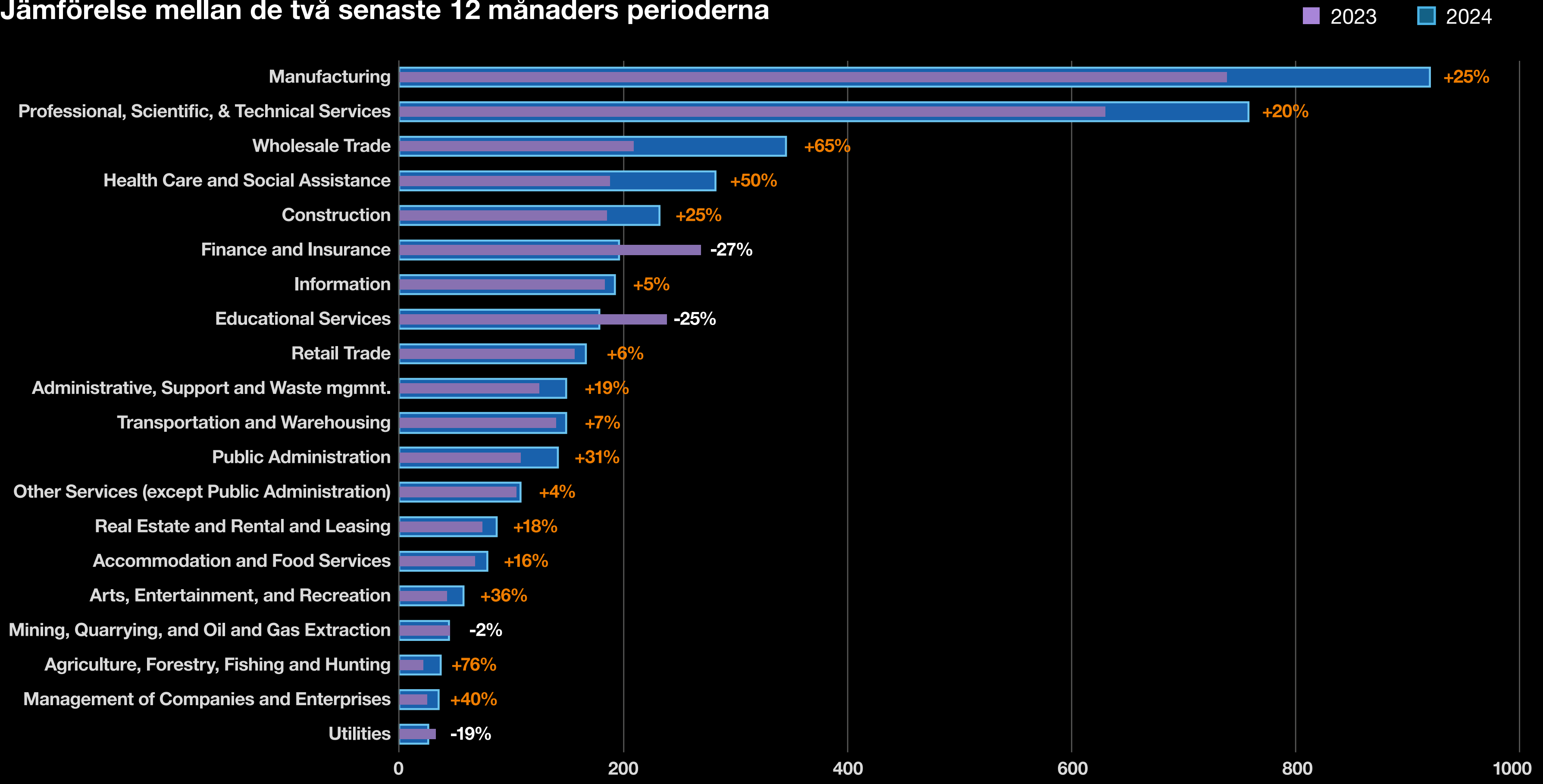


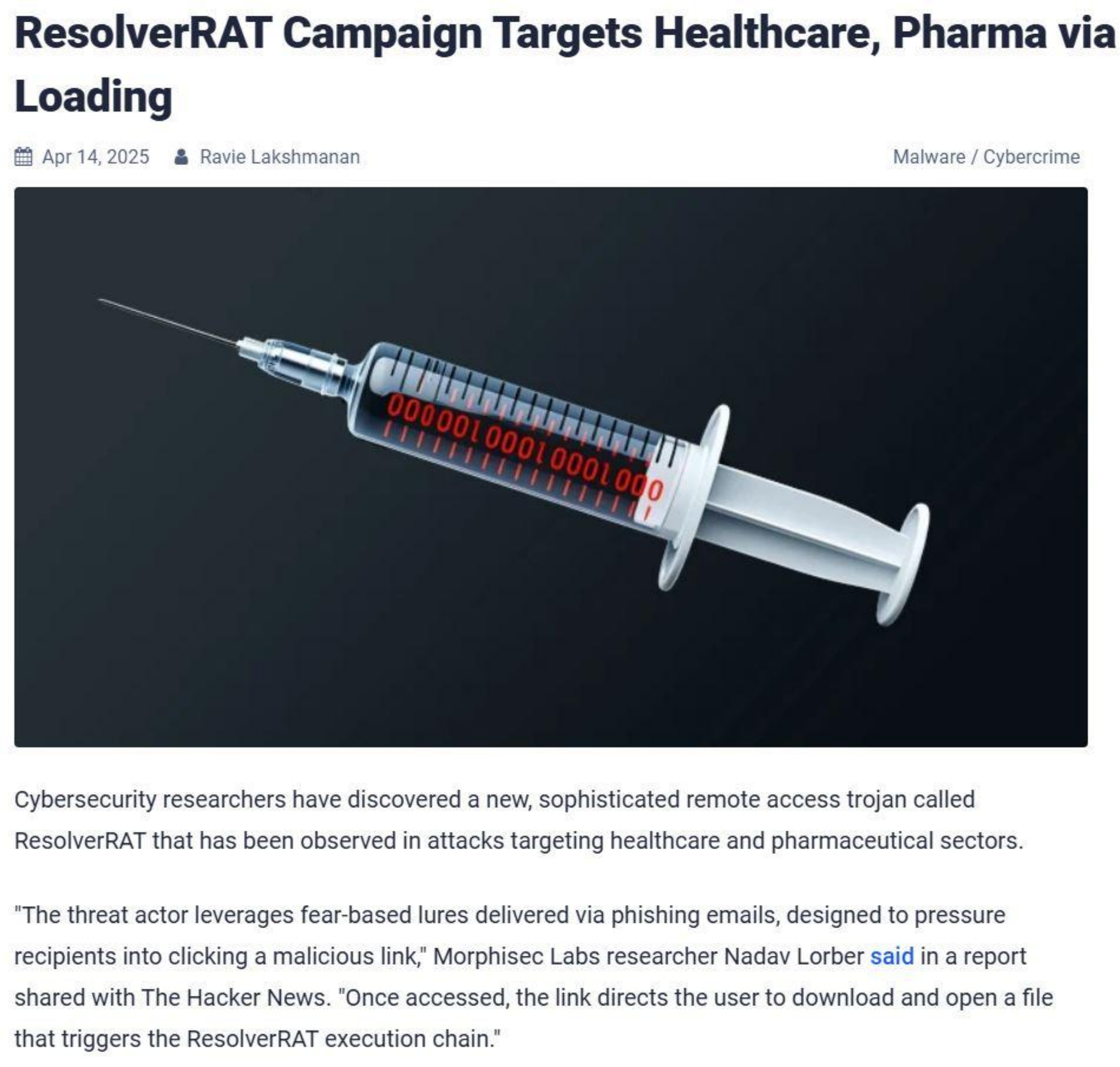
Iran pays millions in ransom to end massive cyberattack on banks, officials say

IRLeaks, a group with a history of hacking Iranian companies, was said to be responsible.

Cy-X: Antal offer per näringsgren - Förändring

Jämförelse mellan de två senaste 12 månaders perioderna





ResolverRAT Campaign Targets Healthcare, Pharma via Loading

Apr 14, 2025 Ravie Lakshmanan Malware / Cybercrime

Cybersecurity researchers have discovered a new, sophisticated remote access trojan called ResolverRAT that has been observed in attacks targeting healthcare and pharmaceutical sectors.

"The threat actor leverages fear-based lures delivered via phishing emails, designed to pressure recipients into clicking a malicious link," Morphisec Labs researcher Nadav Lorber said in a report shared with The Hacker News. "Once accessed, the link directs the user to download and open a file that triggers the ResolverRAT execution chain."

t EU healthcare orgs

February 20, 2025 03:00 AM 0

dents and teachers use paper and pen to record

ed.

ker has been spotted in

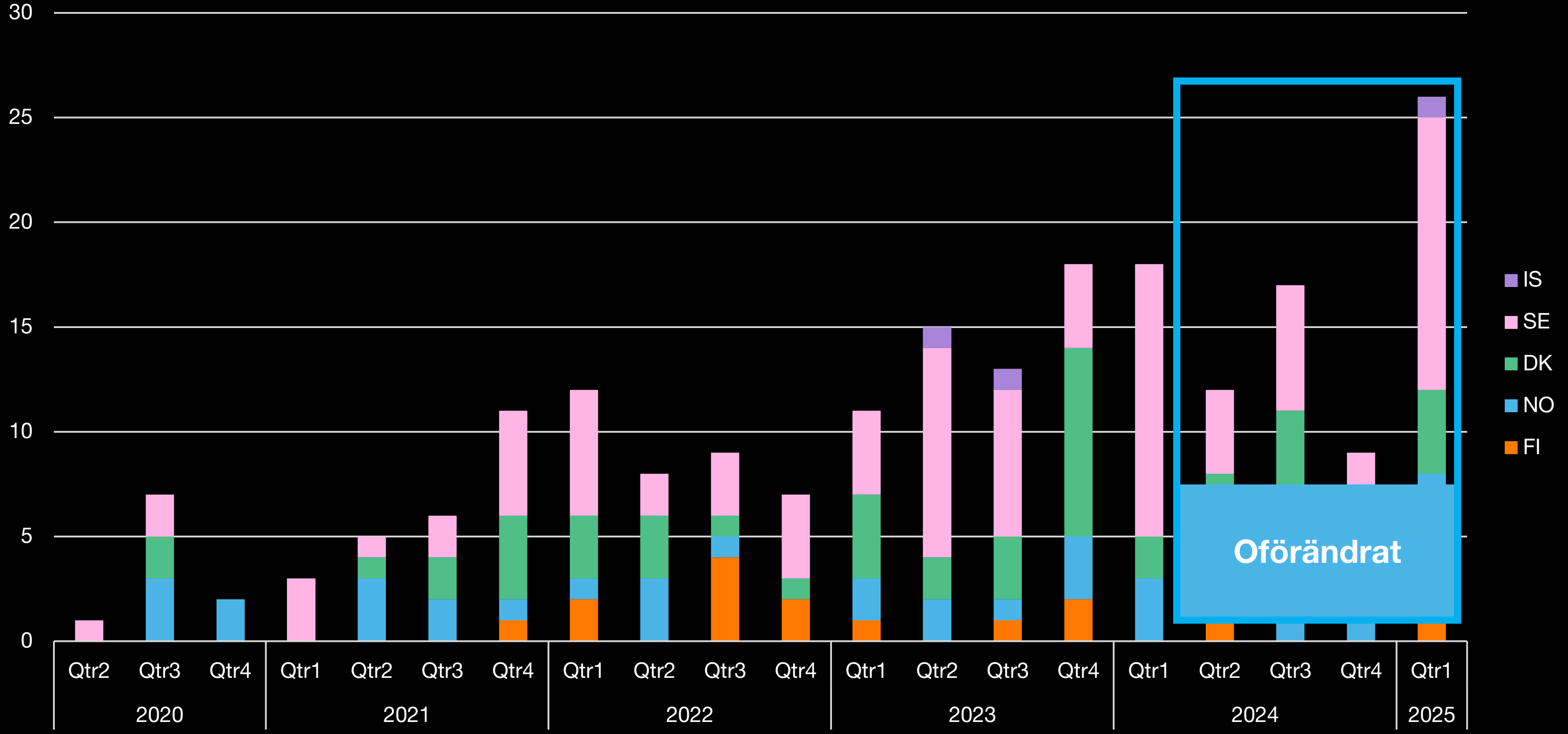
ONSDAG 19 FEBRUARI

ning Event

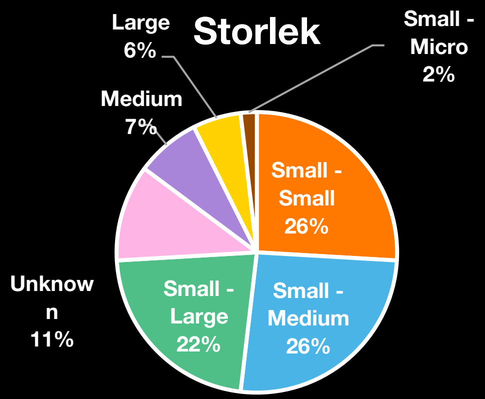
UARI

n,

Profil : Norden

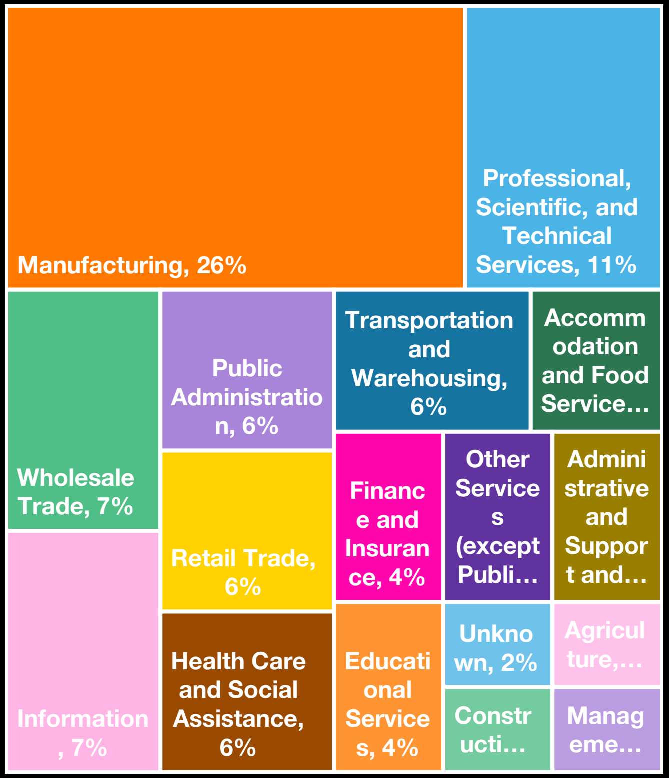


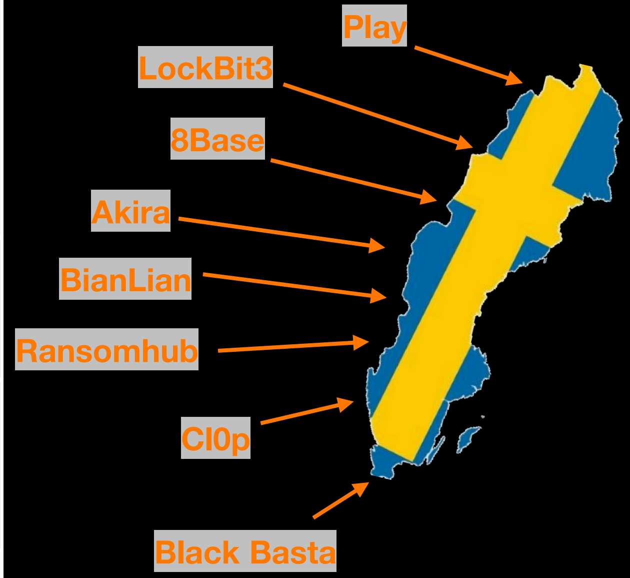
Sveriges hotprofil

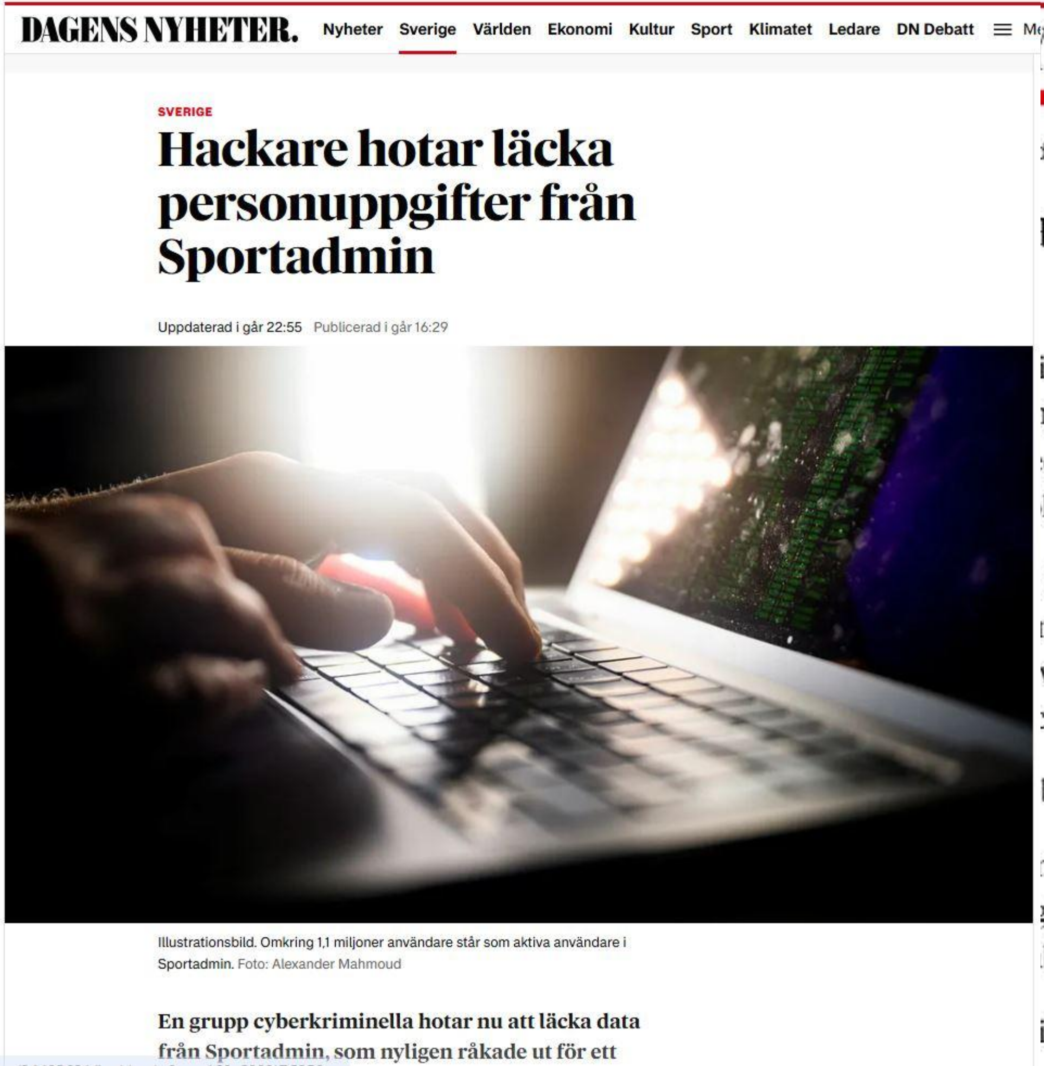


Employee Count	Orange Cyberdefense classification
1 - 9	Small - Micro
10 - 49	Small - Small
50 - 249	Small - Medium
250 - 999	Small - Large
1,000 – 9,999	Medium
10,000+	Large

Näringsgrenar 2023 - 2024







DAGENS NYHETER. Nyheter Sverige Världen Ekonomi Kultur Sport Klimatet Ledare DN Debatt Me

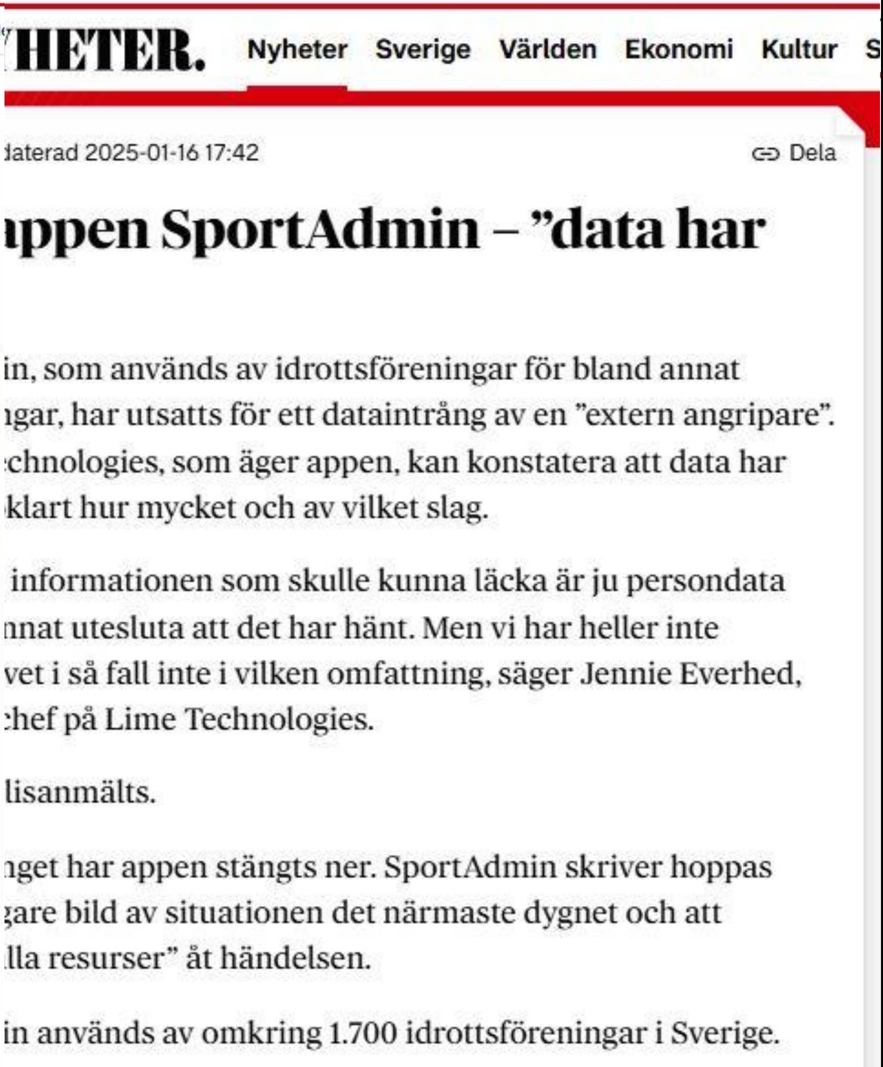
SVERIGE

Hackare hotar läcka personuppgifter från Sportadmin

Uppdaterad i går 22:55 Publicerad i går 16:29

Illustrationsbild. Omkring 1,1 miljoner användare står som aktiva användare i Sportadmin. Foto: Alexander Mahmoud

En grupp cyberkriminella hotar nu att läcka data från Sportadmin, som nyligen råkade ut för ett



YHETER. Nyheter Sverige Världen Ekonomi Kultur S

ɪdaterad 2025-01-16 17:42 Dela

ɪppen SportAdmin – ”data har

in, som används av idrottsföreningar för bland annat
ıgar, har utsatts för ett dataintrång av en ”extern angripare”.
:chnologies, som äger appen, kan konstatera att data har
ıklart hur mycket och av vilket slag.

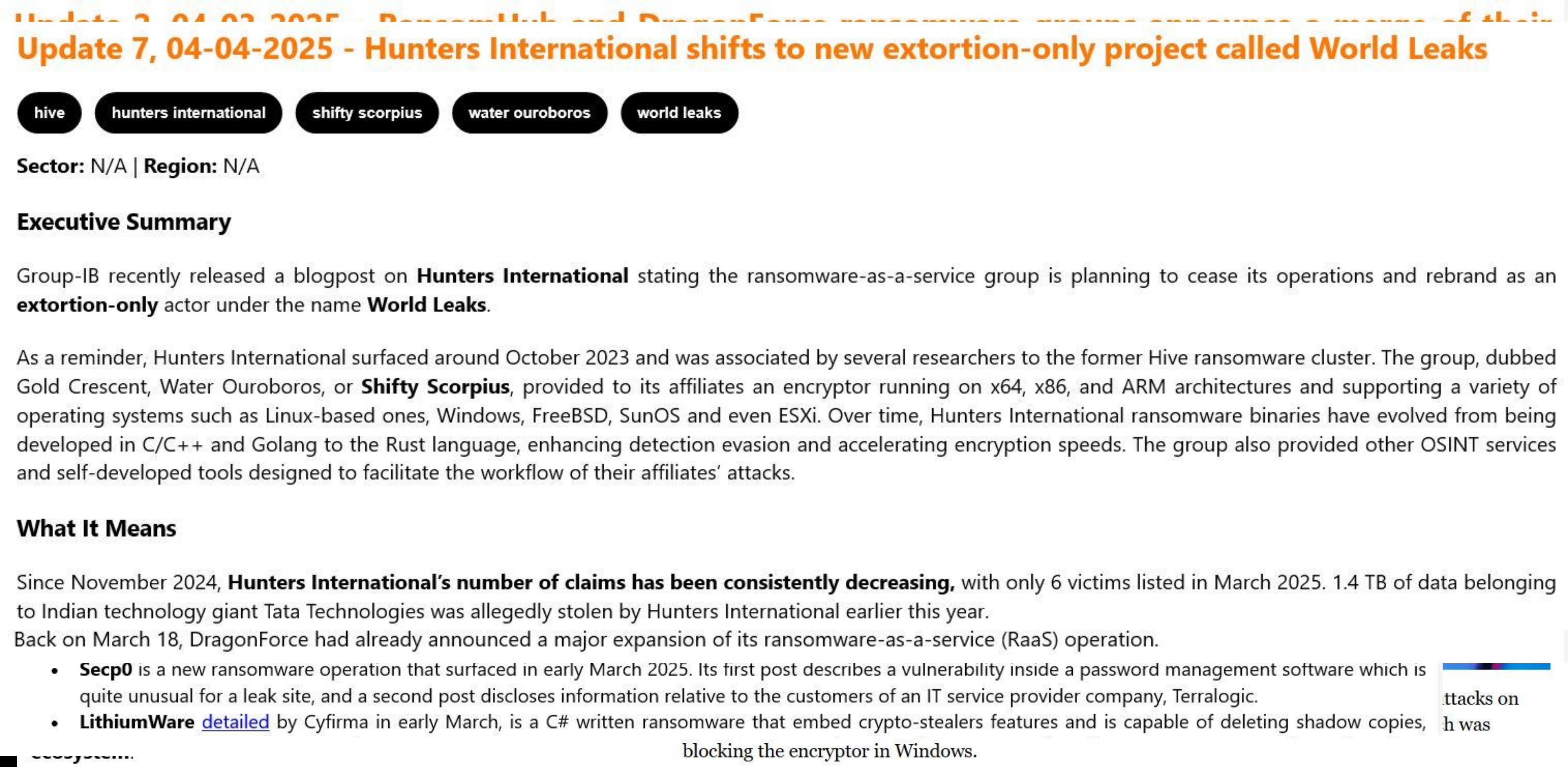
informationen som skulle kunna läcka är ju persondata
ınnat utesluta att det har hänt. Men vi har heller inte
vet i så fall inte i vilken omfattning, säger Jennie Everhed,
:hef på Lime Technologies.

lisanmälts.

ıget har appen stängts ner. SportAdmin skriver hoppas
ȝare bild av situationen det närmaste dygnet och att
lla resurser” åt händelsen.

in används av omkring 1.700 idrottsföreningar i Sverige.

Cy-X Hotlandskapet - ständig förändring



Update 7, 04-04-2025 - Hunters International shifts to new extortion-only project called World Leaks

Sector: N/A | **Region:** N/A

Executive Summary

Group-IB recently released a blogpost on **Hunters International** stating the ransomware-as-a-service group is planning to cease its operations and rebrand as an **extortion-only** actor under the name **World Leaks**.

As a reminder, Hunters International surfaced around October 2023 and was associated by several researchers to the former Hive ransomware cluster. The group, dubbed Gold Crescent, Water Ouroboros, or **Shifty Scorpius**, provided to its affiliates an encryptor running on x64, x86, and ARM architectures and supporting a variety of operating systems such as Linux-based ones, Windows, FreeBSD, SunOS and even ESXi. Over time, Hunters International ransomware binaries have evolved from being developed in C/C++ and Golang to the Rust language, enhancing detection evasion and accelerating encryption speeds. The group also provided other OSINT services and self-developed tools designed to facilitate the workflow of their affiliates' attacks.

What It Means

Since November 2024, **Hunters International's number of claims has been consistently decreasing,** with only 6 victims listed in March 2025. 1.4 TB of data belonging to Indian technology giant Tata Technologies was allegedly stolen by Hunters International earlier this year.

Back on March 18, DragonForce had already announced a major expansion of its ransomware-as-a-service (RaaS) operation.

- **Secp0** is a new ransomware operation that surfaced in early March 2025. Its first post describes a vulnerability inside a password management software which is quite unusual for a leak site, and a second post discloses information relative to the customers of an IT service provider company, Terralogic.
- **LithiumWare** detailed by Cyfirma in early March, is a C# written ransomware that embed crypto-stealers features and is capable of deleting shadow copies,

ttacks on

h was

ecosystem.

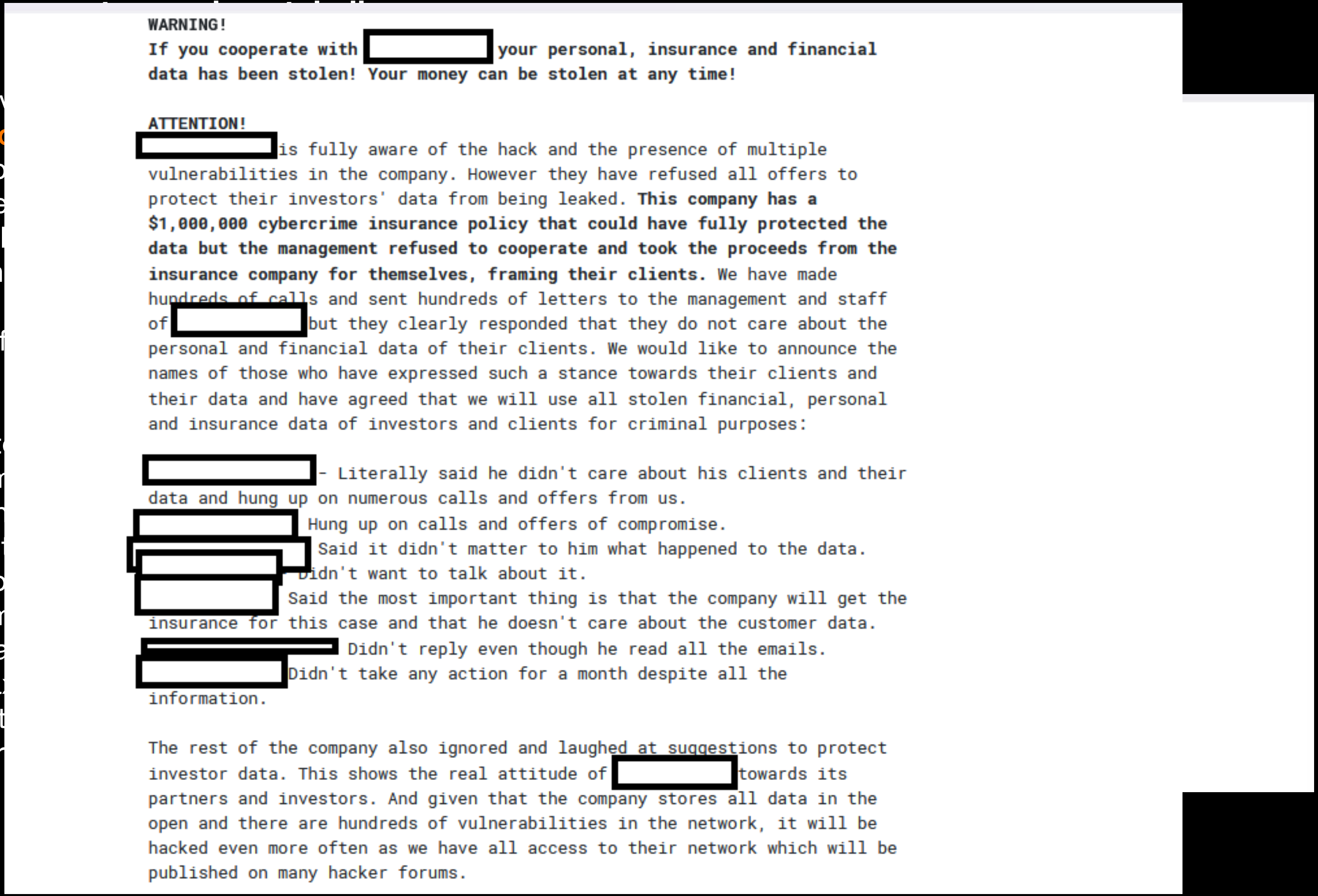
blocking the encryptor in Windows.

Skadliga rykten

“Offentligt trakasserande“

Utöver de trender vi har beskriv
skett en märkbar förändring i t
hotaktörer på den mörka webb
mer aggressiva, med angripare
trakasserande taktik. Detta ink
individer inom drabbade organ
egen "privata" kommunikation
publicera länkar till offrens prof
medieprofiler.

I vår Cy-Xplorer-rapport diskut
fenomenet som kallas "revictim
stulna information delas mellan
vilket förstärker skadan. Detta
maximerar inte bara den psyko
offren utan öppnar också fler m
intäktsgenerering. Vi kommer a
denna trend där hotaktörer ma
för sin egen vinning, genom att
så mycket värde som möjligt fr



WARNING!
If you cooperate with [redacted] your personal, insurance and financial data has been stolen! Your money can be stolen at any time!

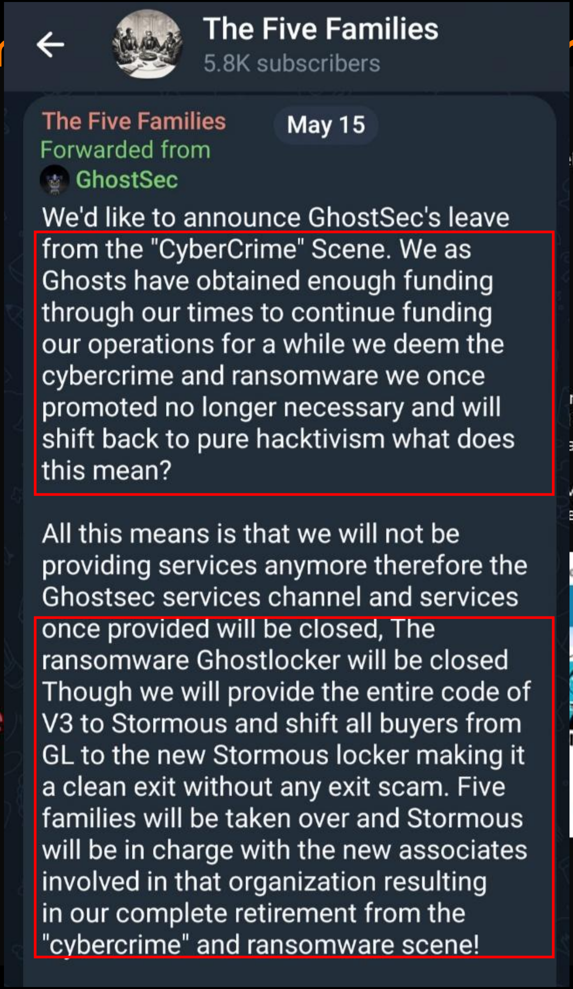
ATTENTION!
[redacted] is fully aware of the hack and the presence of multiple vulnerabilities in the company. However they have refused all offers to protect their investors' data from being leaked. **This company has a $1,000,000 cybercrime insurance policy that could have fully protected the data but the management refused to cooperate and took the proceeds from the insurance company for themselves, framing their clients.** We have made hundreds of calls and sent hundreds of letters to the management and staff of [redacted] but they clearly responded that they do not care about the personal and financial data of their clients. We would like to announce the names of those who have expressed such a stance towards their clients and their data and have agreed that we will use all stolen financial, personal and insurance data of investors and clients for criminal purposes:

[redacted] - Literally said he didn't care about his clients and their data and hung up on numerous calls and offers from us.
[redacted] Hung up on calls and offers of compromise.
[redacted] Said it didn't matter to him what happened to the data.
[redacted] Didn't want to talk about it.
[redacted] Said the most important thing is that the company will get the insurance for this case and that he doesn't care about the customer data.
[redacted] Didn't reply even though he read all the emails.
[redacted] Didn't take any action for a month despite all the information.

The rest of the company also ignored and laughed at suggestions to protect investor data. This shows the real attitude of [redacted] towards its partners and investors. And given that the company stores all data in the open and there are hundreds of vulnerabilities in the network, it will be hacked even more often as we have all access to their network which will be published on many hacker forums.

Hacktivism nware & vice versa

-
-
-
-
- Hacke



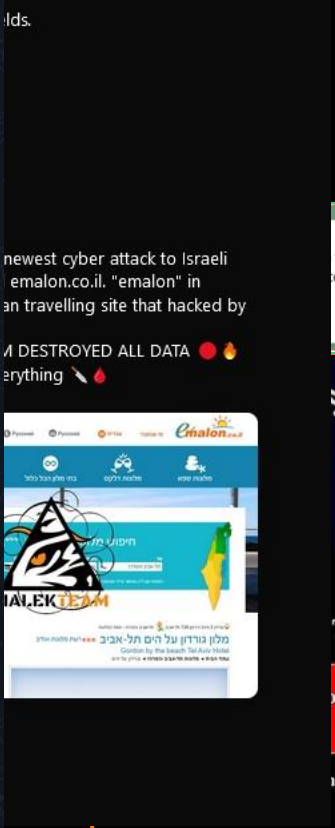
The Five Families
5.8K subscribers

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!



lds.

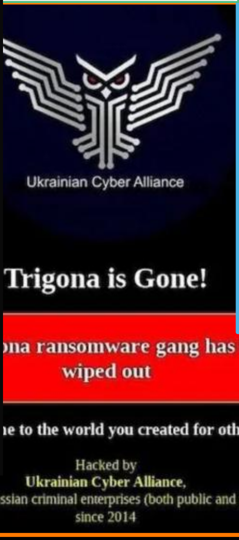
newest cyber attack to Israeli
emalon.co.il. "emalon" in
an travelling site that hacked by

M DESTROYED ALL DATA 🔴🔥
erything 🔪🩸

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

the following countries: Iran,
countries. Message

👁 112 📌 7:20 AM

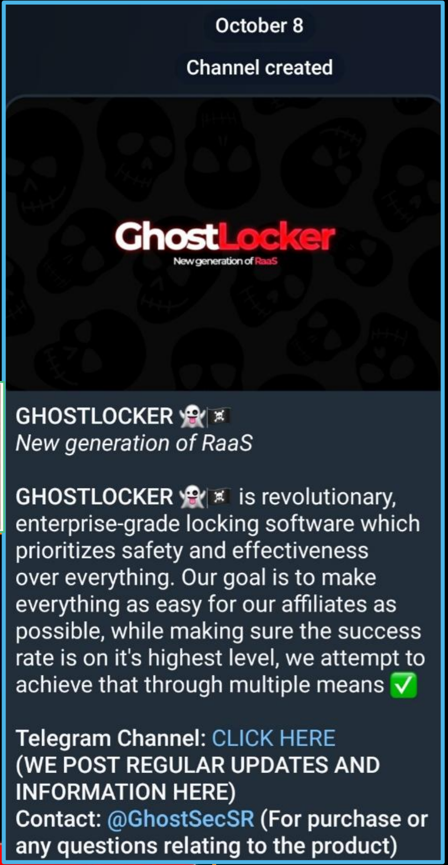


Trigona is Gone!

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

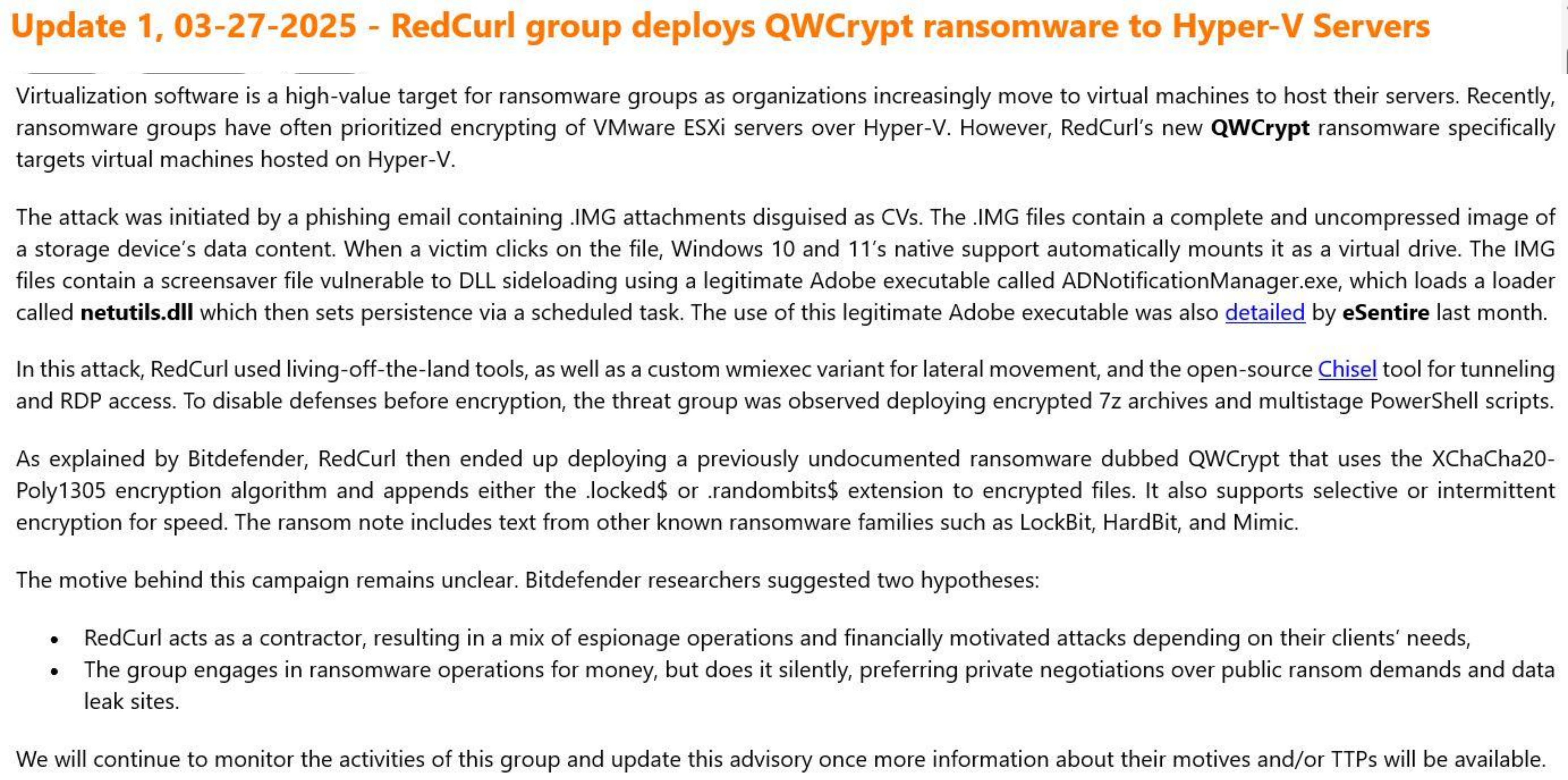
Channel created

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)

Hacktivism crossover to ransomware & vice



Update 1, 03-27-2025 - RedCurl group deploys QWCrypt ransomware to Hyper-V Servers

Virtualization software is a high-value target for ransomware groups as organizations increasingly move to virtual machines to host their servers. Recently, ransomware groups have often prioritized encrypting of VMware ESXi servers over Hyper-V. However, RedCurl's new **QWCrypt** ransomware specifically targets virtual machines hosted on Hyper-V.

The attack was initiated by a phishing email containing .IMG attachments disguised as CVs. The .IMG files contain a complete and uncompressed image of a storage device's data content. When a victim clicks on the file, Windows 10 and 11's native support automatically mounts it as a virtual drive. The IMG files contain a screensaver file vulnerable to DLL sideloading using a legitimate Adobe executable called ADNotificationManager.exe, which loads a loader called **netutils.dll** which then sets persistence via a scheduled task. The use of this legitimate Adobe executable was also detailed by **eSentire** last month.

In this attack, RedCurl used living-off-the-land tools, as well as a custom wmiexec variant for lateral movement, and the open-source Chisel tool for tunneling and RDP access. To disable defenses before encryption, the threat group was observed deploying encrypted 7z archives and multistage PowerShell scripts.

As explained by Bitdefender, RedCurl then ended up deploying a previously undocumented ransomware dubbed QWCrypt that uses the XChaCha20-Poly1305 encryption algorithm and appends either the .locked$ or .randombits$ extension to encrypted files. It also supports selective or intermittent encryption for speed. The ransom note includes text from other known ransomware families such as LockBit, HardBit, and Mimic.

The motive behind this campaign remains unclear. Bitdefender researchers suggested two hypotheses:

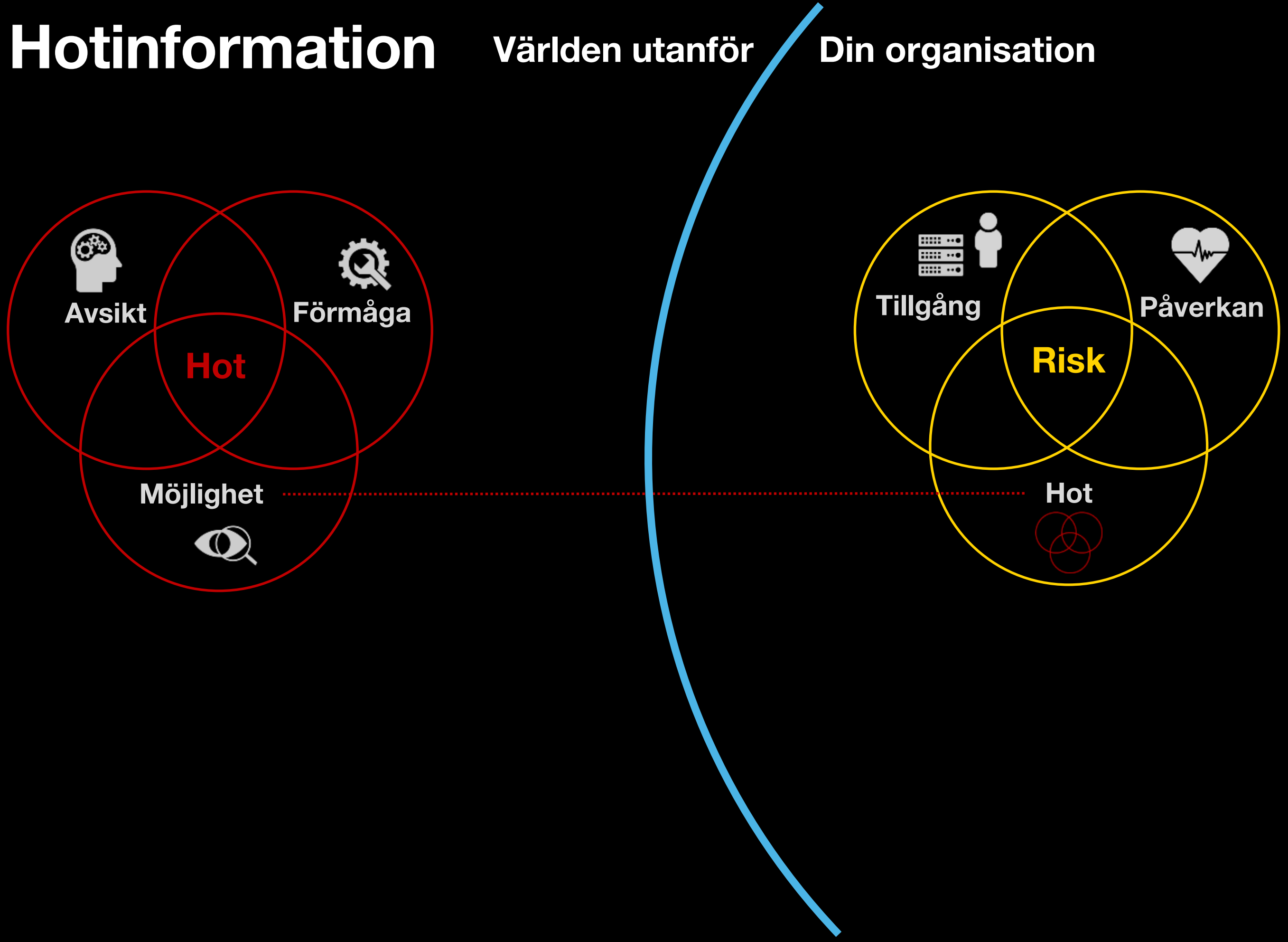
- RedCurl acts as a contractor, resulting in a mix of espionage operations and financially motivated attacks depending on their clients' needs,
- The group engages in ransomware operations for money, but does it silently, preferring private negotiations over public ransom demands and data leak sites.

We will continue to monitor the activities of this group and update this advisory once more information about their motives and/or TTPs will be available.

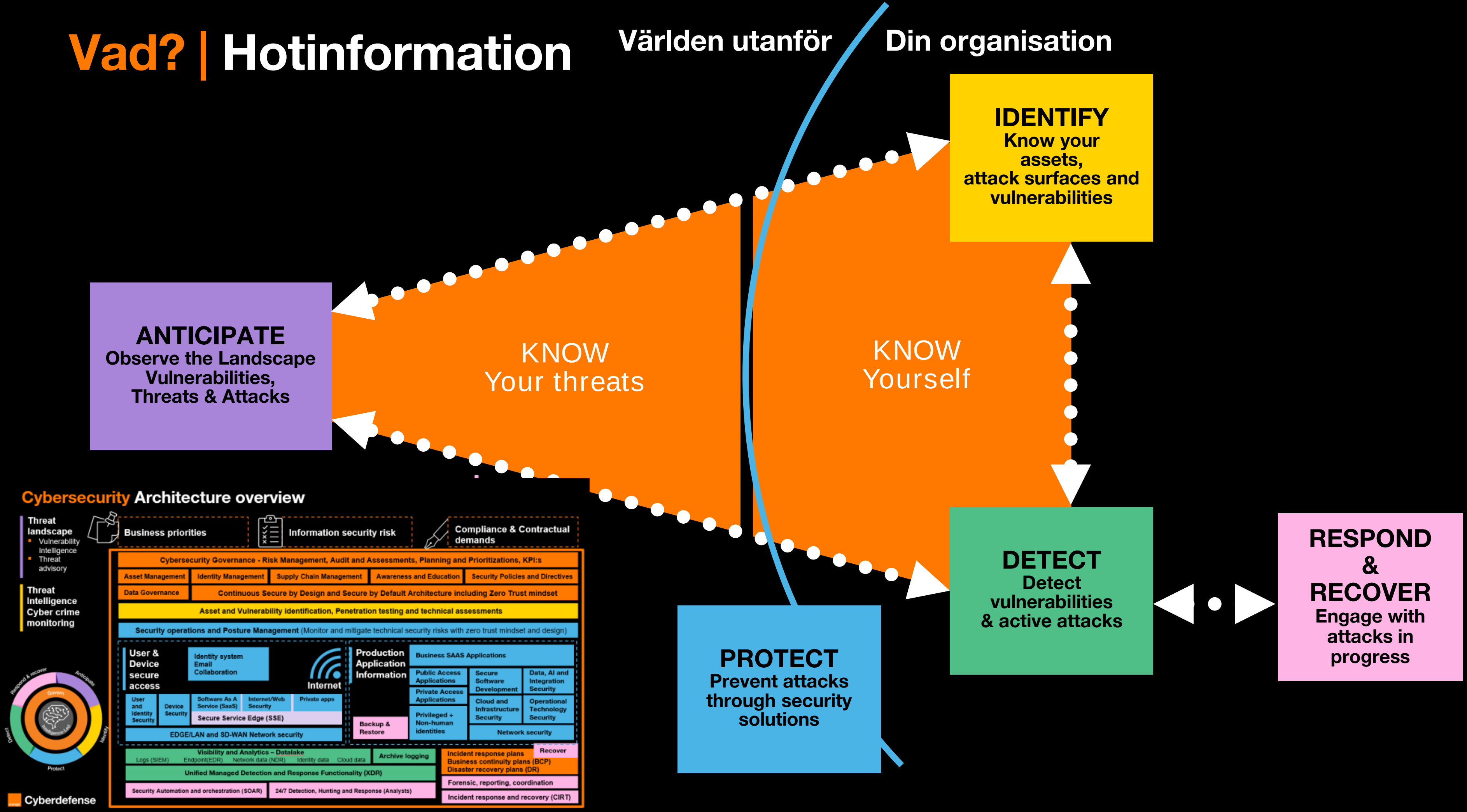
Slutord

Varför fokuserar vi på hot?
Vad kan du göra?

Vad? | Hotinformation



Vad? | Hotinformation



Världen utanför

Din organisation

ANTICIPATE
Observe the Landscape
Vulnerabilities,
Threats & Attacks

KNOW
Your threats

KNOW
Yourself

IDENTIFY
Know your
assets,
attack surfaces and
vulnerabilities

DETECT
Detect
vulnerabilities
& active attacks

**RESPOND
&
RECOVER**
Engage with
attacks in
progress

PROTECT
Prevent attacks
through security
solutions

Cybersecurity Architecture overview

Threat landscape
- Vulnerability Intelligence
- Threat advisory

Threat Intelligence
Cyber crime monitoring

Business priorities

Information security risk

Compliance & Contractual demands

Cybersecurity Governance - Risk Management, Audit and Assessments, Planning and Prioritizations, KPI:s

Asset Management | Identity Management | Supply Chain Management | Awareness and Education | Security Policies and Directives

Data Governance | Continuous Secure by Design and Secure by Default Architecture including Zero Trust mindset

Asset and Vulnerability identification, Penetration testing and technical assessments

Security operations and Posture Management (Monitor and mitigate technical security risks with zero trust mindset and design)

User & Device secure access

Identity system
Email
Collaboration

Internet

User and Identity Security | Device Security | Software As A Service (SaaS) | Internet/Web Security | Private apps

Secure Service Edge (SSE)

EDGE/LAN and SD-WAN Network security

Production Application Information

Business SAAS Applications

Public Access Applications | Secure Software Development | Data, AI and Integration Security

Private Access Applications | Cloud and Infrastructure Security | Operational Technology Security

Backup & Restore | Privileged + Non-human identities | Network security

Visibility and Analytics – Datalake
Logs (SIEM) Endpoint(EDR) Network data (NDR) Identity data Cloud data

Archive logging

Unified Managed Detection and Response Functionality (XDR)

Security Automation and orchestration (SOAR) | 24/7 Detection, Hunting and Response (Analysts)

Recover

Incident response plans
Business continuity plans (BCP)
Disaster recovery plans (DR)

Forensic, reporting, coordination

Incident response and recovery (CIRT)

Cyberdefense

Goda nyheter!

De rekommenderade grundläggande åtgärderna är fortfarande desamma, TTP:erna har inte förändrats i grunden

1

Utnyttjade sårbarheter

Ha en strategi för patchhantering och sårbarhetshantering

2

Stulna identiteter

Ha en strategi för identitets- och åtkomsthantering med multifaktorautentisering

3

Påverkad backup

Ha en strategi för affärskontinuitet och dataåterställning

4

Lång påverkan på affären

Ha en strategi och en plan för hantering av incidenter och cyberkriser orange™

orange™

Cyberdefense

Building a safer digital society.