Orange
Cyberdefense

Hej.

I am Diana.

Lead Security Researcher in the Security Research Center team.

You can find me on Twitter: @DianaSelck & LinkedIn: Diana Selck-Paulsson

orange™

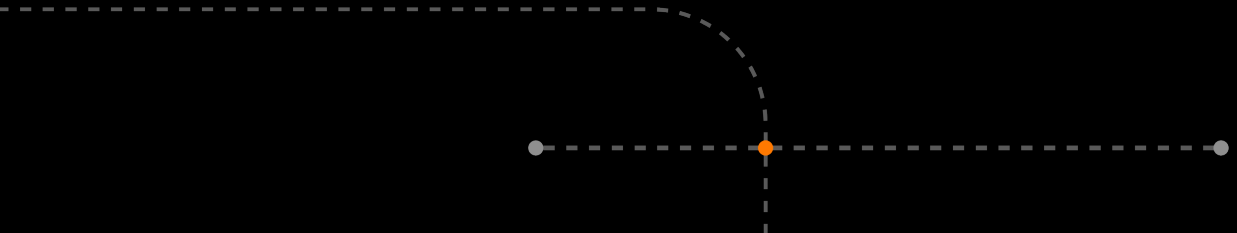
Outline

1. **Researching Cy-X / Ransomware**
2. **Threat landscape of 2022**
   - Cy-X
     - Threat actors & ecosystem
     - Impact: global & local
   - Ukraine war
   - The case of Sweden
3. **Disrupting Cy-X as a form of crime**

Cy-X is a form of computer crime in which the security of a corporate digital asset (Confidentiality, Integrity or Availability) is compromised and exploited in a threat of some form to extort a payment.

Orange
Cyberdefense

Researching Cy-X / Ransomware



orange™

OCD's research capabilities

Methodology:

- We collect A LOT of data
- From our operational teams
  - CERT
  - CSIRT
  - The Global Cybercrime Fighting Unit
- External partnership for research
  - Intel471

Research questions:

What do we learn from the darkweb leaks?

Who are the victims?

Who is impacted the most?

How has the Ukraine war shaped the Cy-X ecosystem?

What do we think this all means?

Researching Cy-X

- **Quantitative data set**
- Scraping darkweb sites

  - Real time view on Cy-X leaks
  - Manual enrichment process to understand victimology

- **Qualitative Research**
- Neutralization techniques (crime theory)

  - Over 200 content pieces (negotiation chats, press releases)
  - Blog post series

Blog

It might be wrong, but there was a good reason: Neutralization through an appeal to higher loyalties

5 April 2023

Cybersecurity | Cyber-Extortion (Cy-X) | Cybercrime

Blog

Levelling the field: the 'condemning the condemners' neutralization technique

8 February 2023

Cyber-Extortion (Cy-X) | Cybercrime | Research

Blog

Noble vigilantes and victim-blaming: neutralization in cyber extortion by 'denying the victim'

15 December 2022

Cyber-Extortion (Cy-X) | Cybercrime | Research

Blog

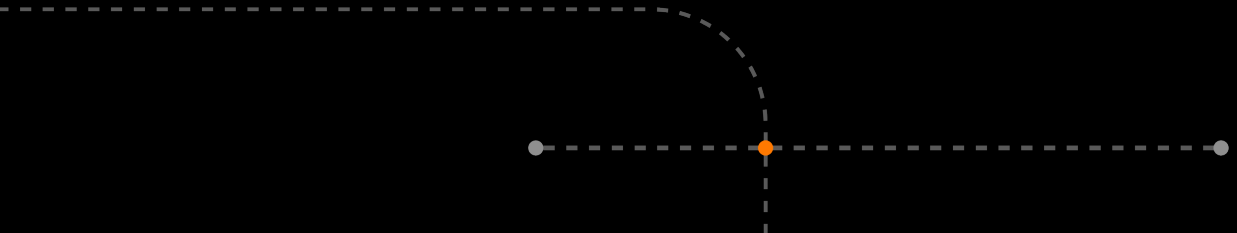
Reframing ransomware as a 'service' for the victim: the denial of injury neutralization technique

11 October 2022

Cyber-Extortion (Cy-X) | Cybercrime | Research

Orange
Cyberdefense

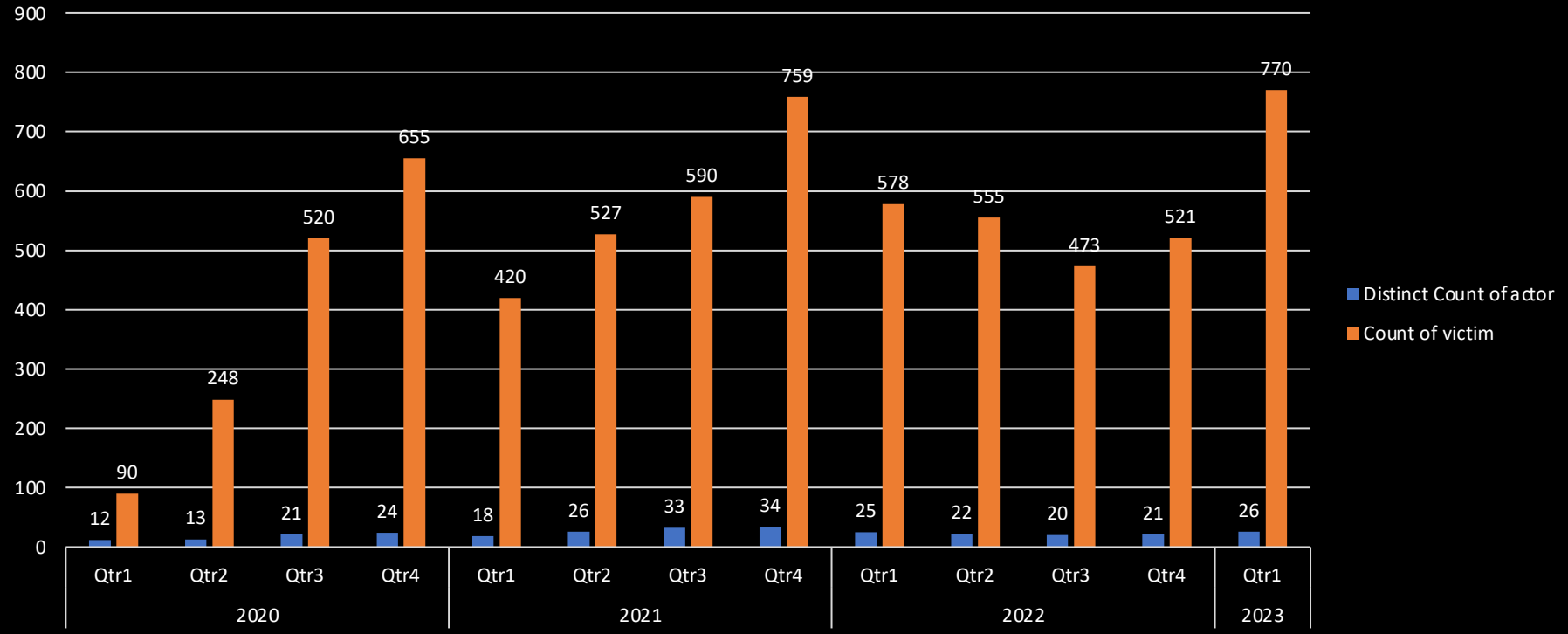
Threat landscape of 2022



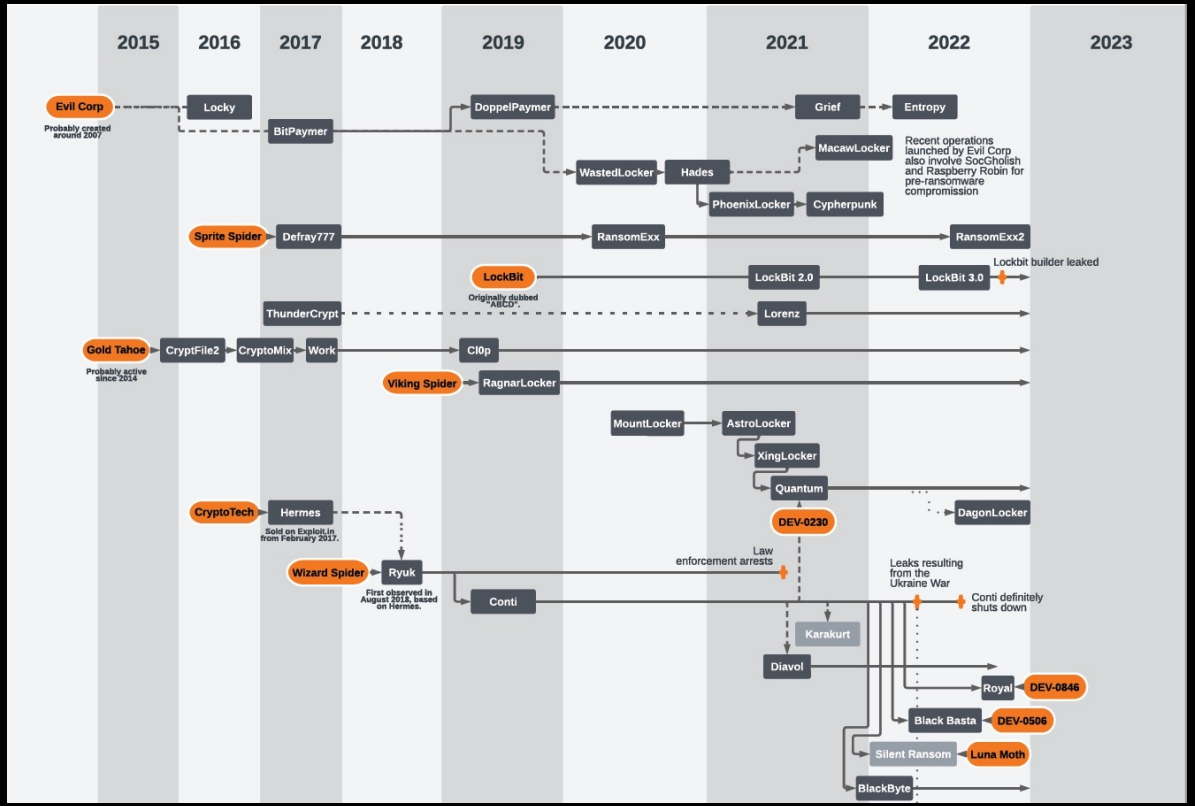
orange™

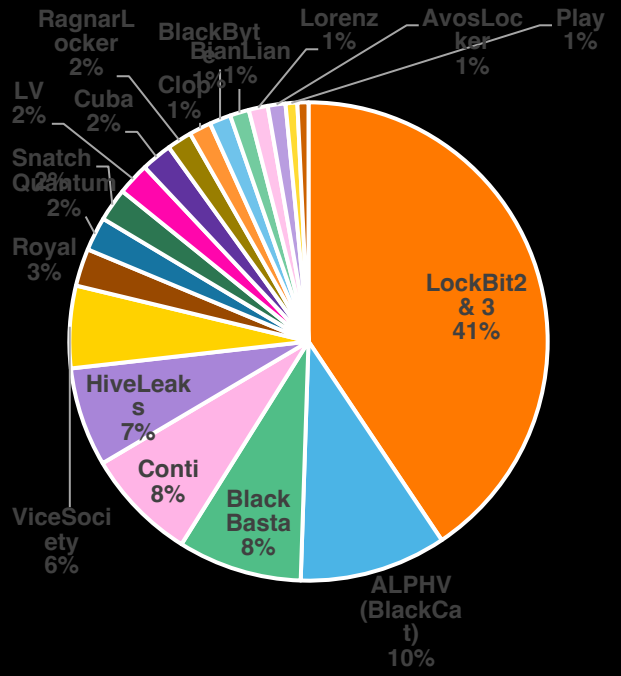
Threats and actors observed

Distinct threats and distinct actors over time



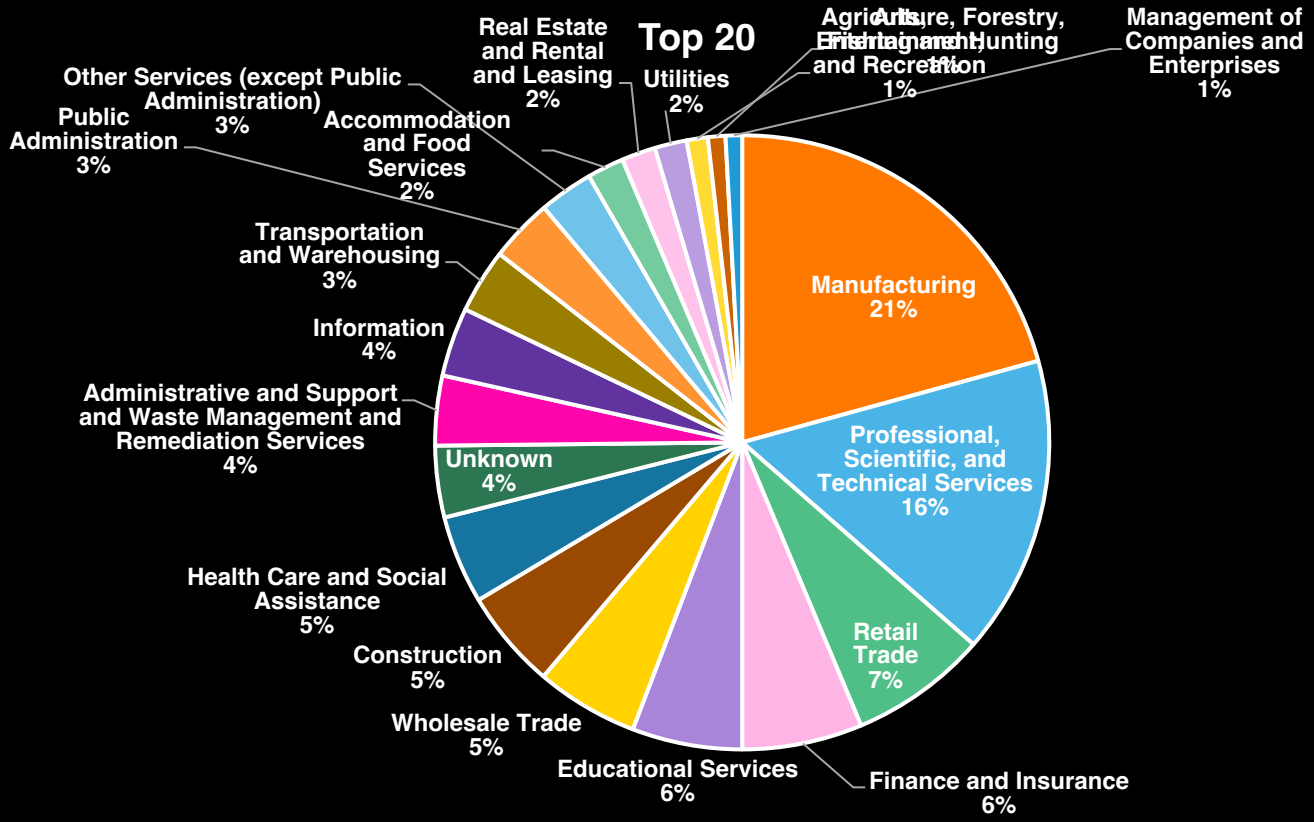
Threat Actor Activity





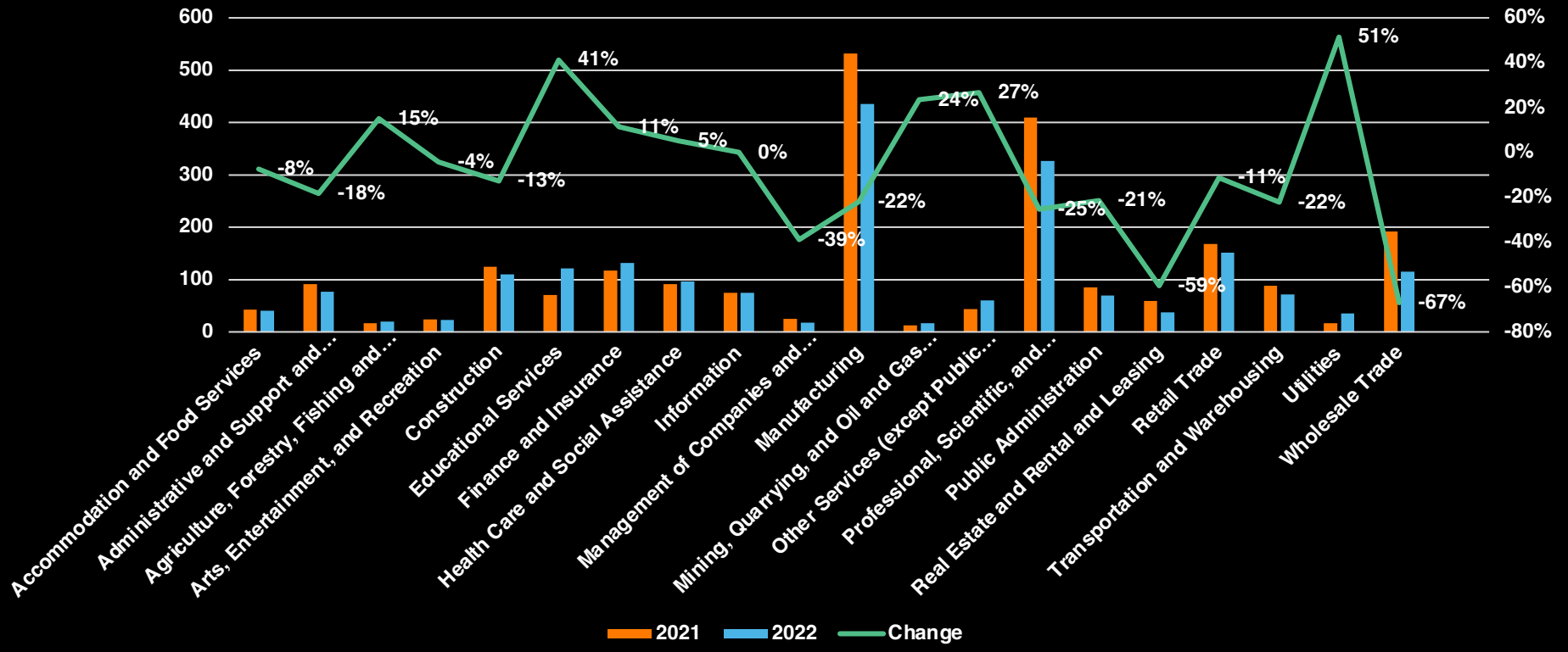
Cyber Extortion Victims

Distinct victims per Industry in 2022



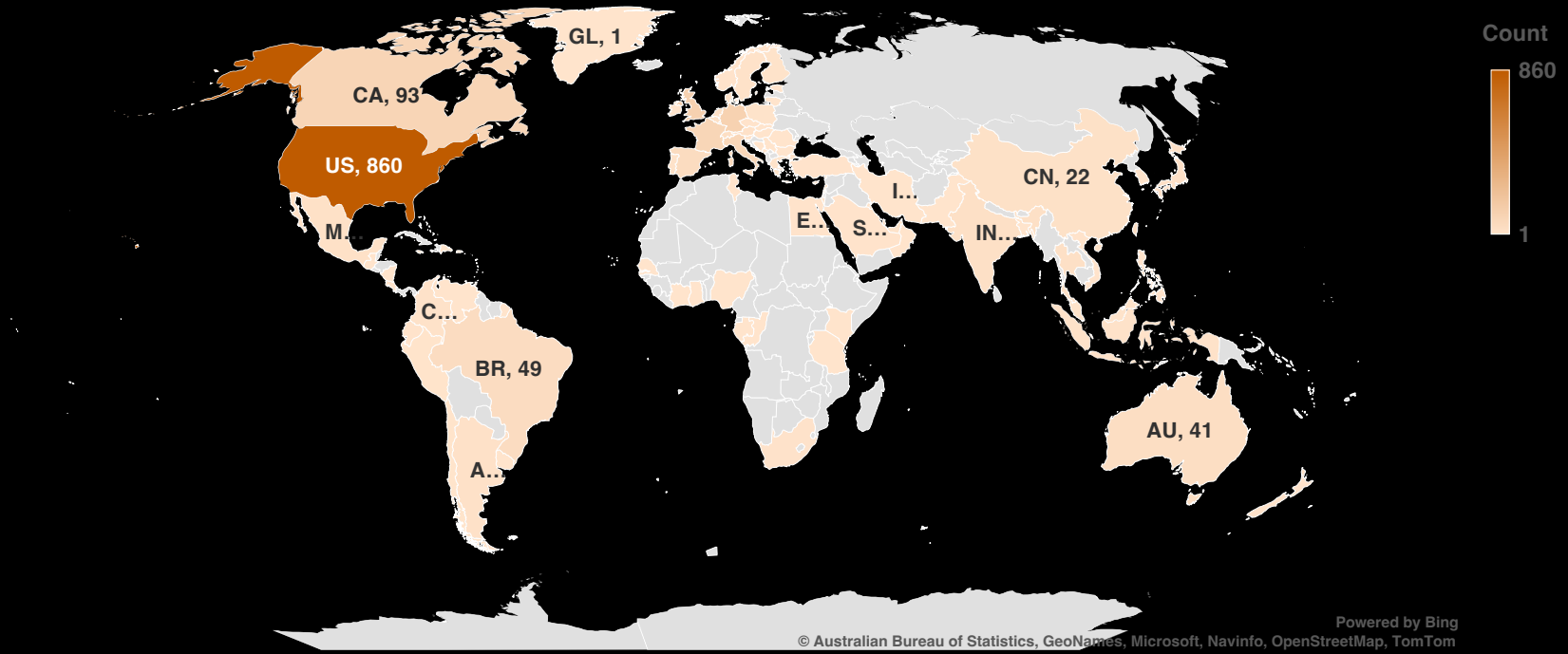
Cyber Extortion Victims

Changes between 2021 and 2022



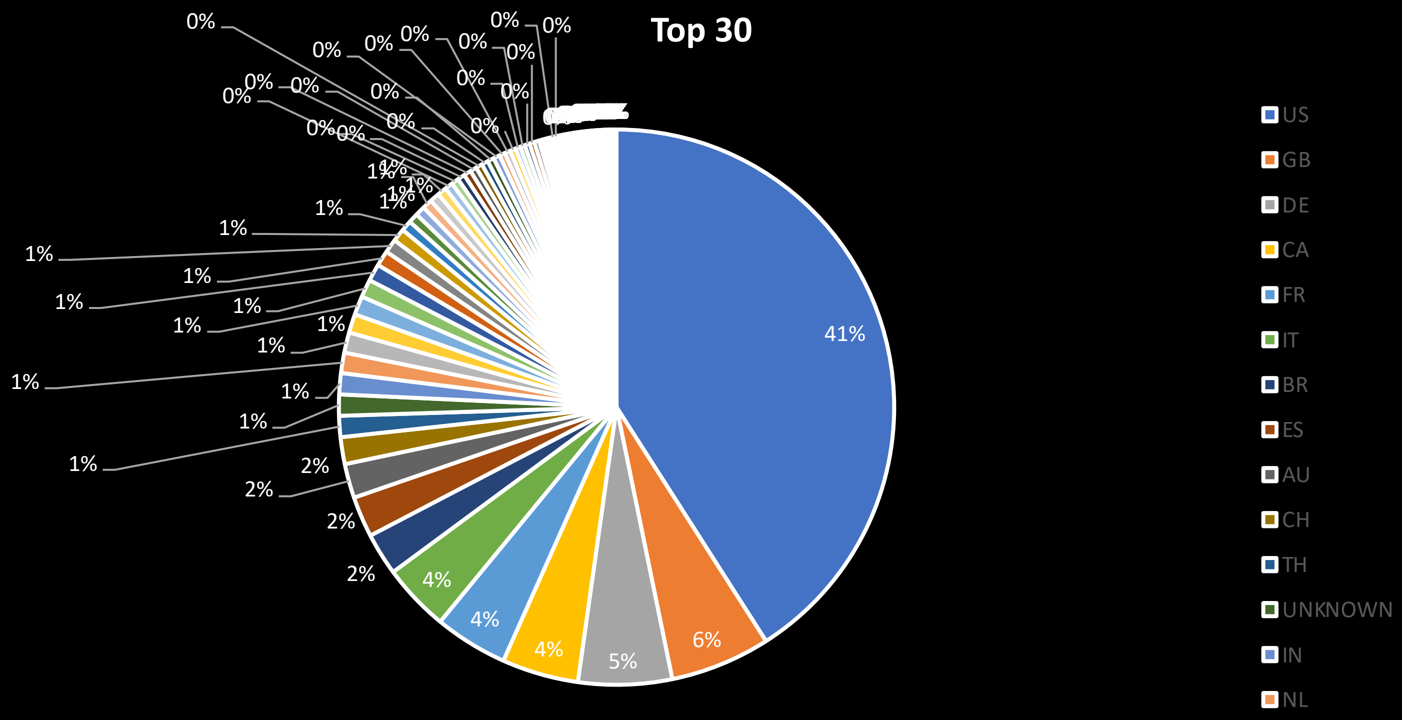
Cyber Extortion Victims

Distinct victims per country in 2022

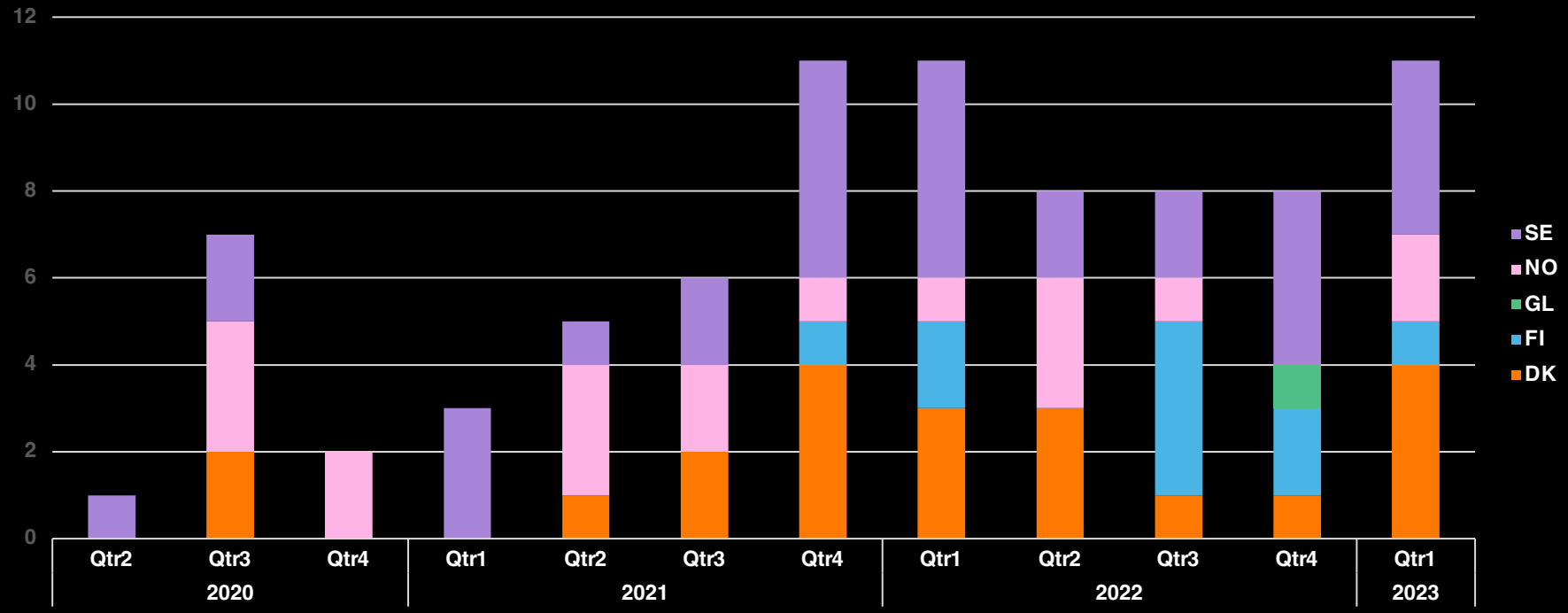


Cyber Extortion Victims

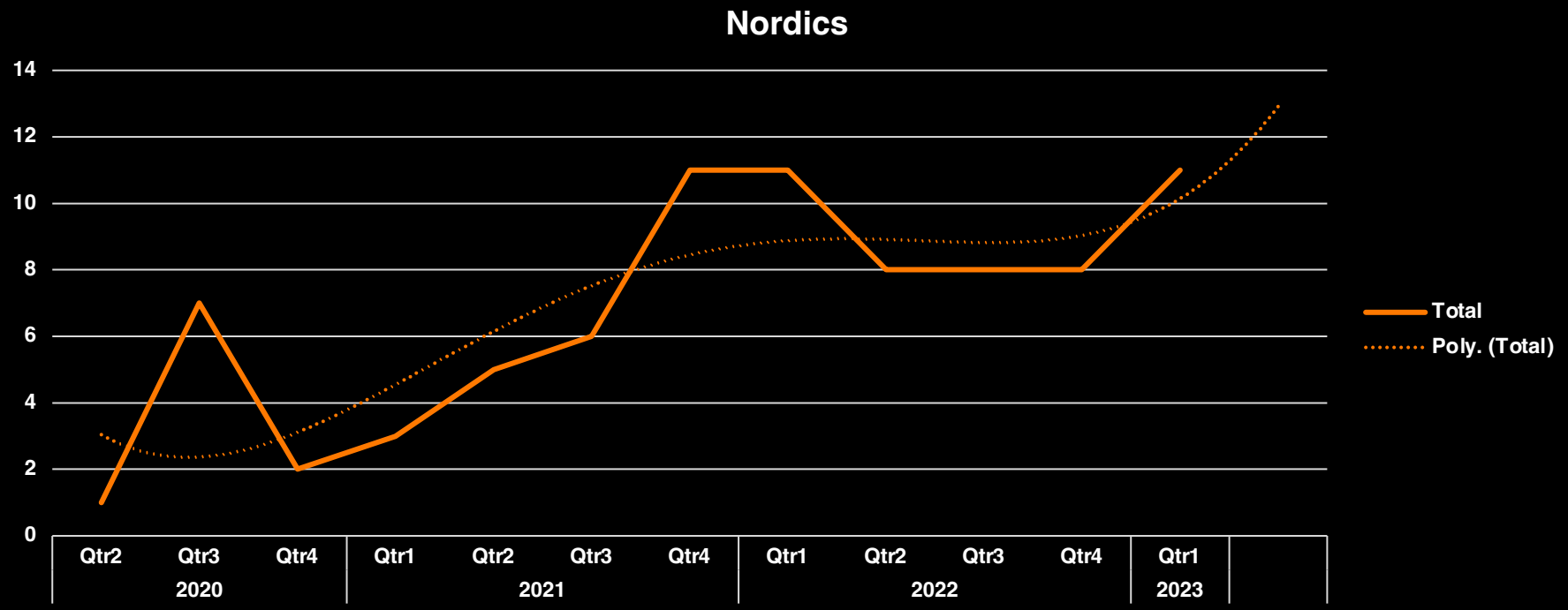
Distinct victims in countries in 2022



Cy-X victim geography – the Nordics

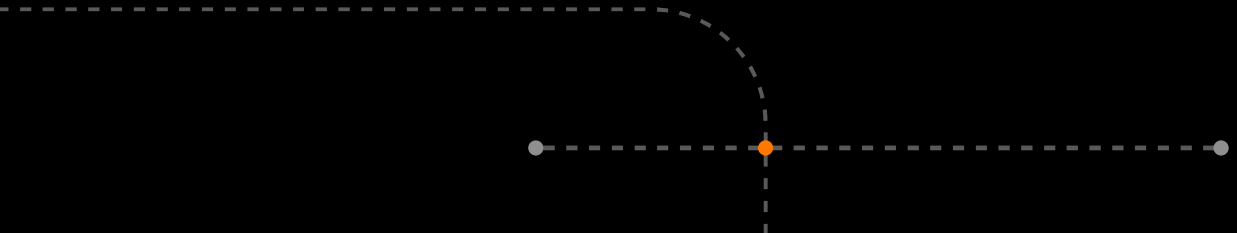


Cy-X victim geography – the Nordics



Orange
Cyberdefense

Ukraine war



orange™

Did the Ukraine war impact the criminal ecosystem of Cy-X?

NATO PARLIAMENTARY ASSEMBLY
ASSEMBLEE PARLEMENTAIRE DE L'OTAN

HOME NEWS MEMBERSHIP ABOUT US WORK E-LIBRARY CONTACT

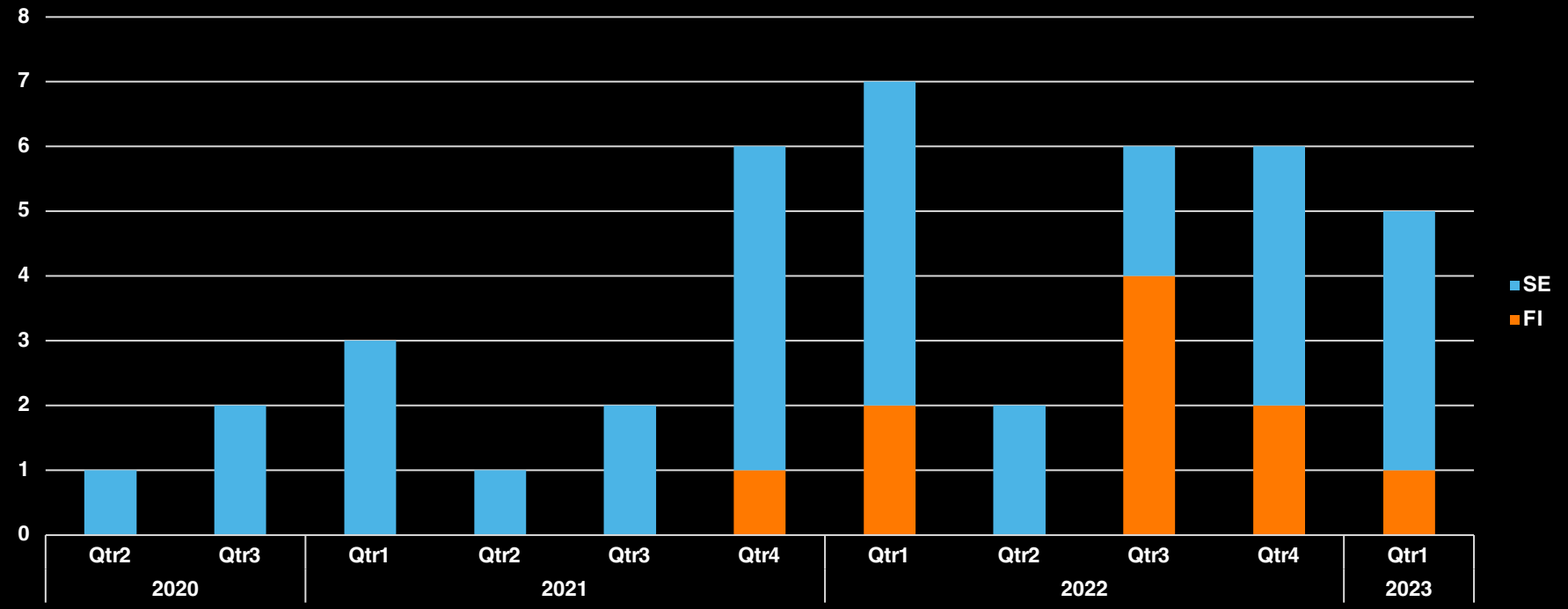
Finland & Sweden Accession

RATIFICATION OF FINLAND AND SWEDEN'S ACCESSION TO NATO

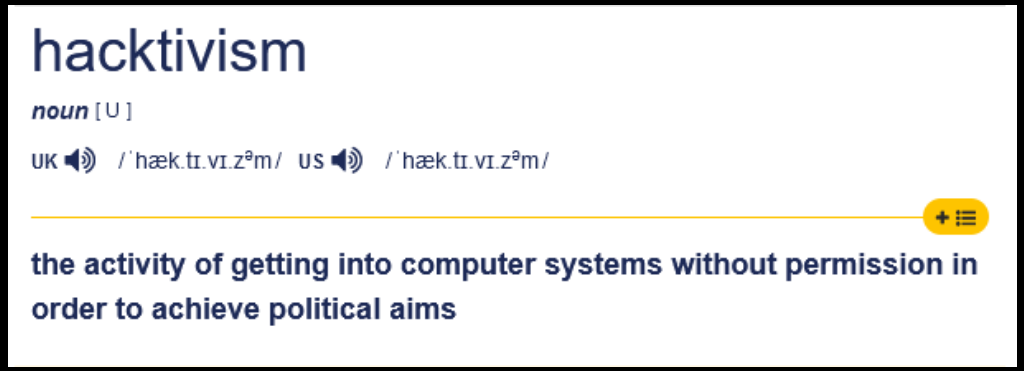
After thorough debates across their whole societies and with large parliamentary majorities supporting the decision, Finland and Sweden simultaneously handed their official letters of application to join NATO over to NATO Secretary General Jens Stoltenberg on 18 May 2022. NATO Heads of State and Government extended an invitation to Finland and Sweden to join the Alliance at the Madrid Summit on 29 June 2022. The accession protocols for both countries were signed on 5 July 2022 after completion of accession talks. The protocols must now be ratified by all Allies, according to their national procedures.

As of 4 April 2023, Finland becomes the 31st member of NATO and the NATO PA.

Ukraine war & Cy-X



Ukraine war – hacktivism – the Nordics



hacktivism

noun [U]

UK /ˈhæk.tɪ.vɪ.zᵊm/ US /ˈhæk.tɪ.vɪ.zᵊm/

the activity of getting into computer systems without permission in order to achieve political aims

"Ukraine's cyber response plan was carefully crafted by its Minister of Digital Transformation – Mykhailo Albertovych Fedorov – who coordinated one of the most successful, multifaceted information operations campaigns ever witnessed in history."

https://www.darkowl.com/blog-content/one-year-later-a-look-back-at-the-ukraine-conflict-and-its-impact-on-the-global-criminal-digital-ecosystem/

Meanwhile in Sweden ….

The Guardian

Sweden

Burning of Qur'an in Stockholm funded by journalist with Kremlin ties

Permit for demonstration at which anti-Islam provocateur burned Muslim holy book was paid for by far-right journalist linked to Moscow-backed media

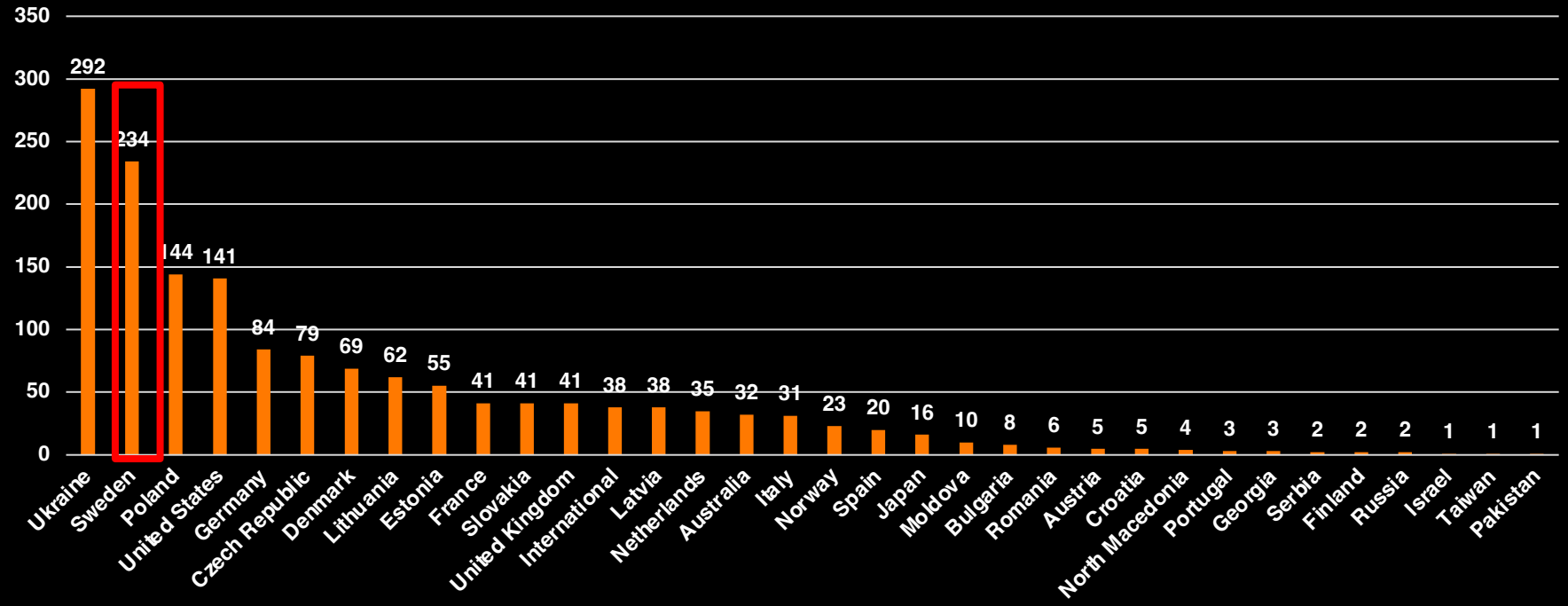
Jennifer Rankin

Fri 27 Jan 2023 17.54 GMT

Rasmus Paludan (left) at an event in Denmark in 2022 at which he burned the Qur'an. Photograph: Muhammet Ikbal Arslan/Getty Images

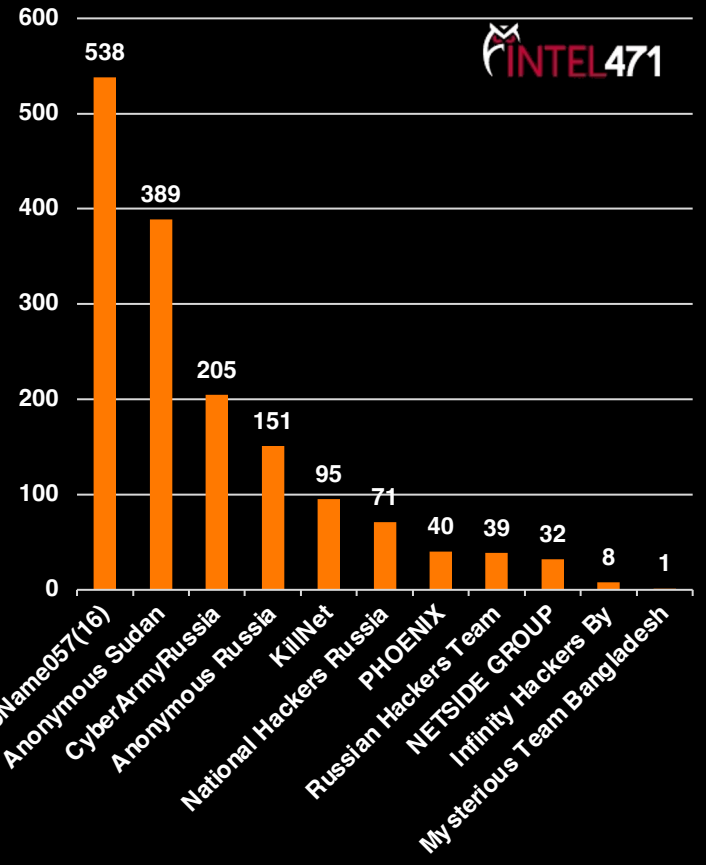
https://www.theguardian.com/world/2023/jan/27/burning-of-quran-in-stockholm-funded-by-journalist-with-kremlin-ties-sweden-nato-russia

Ukraine war & Hacktivism - 2023



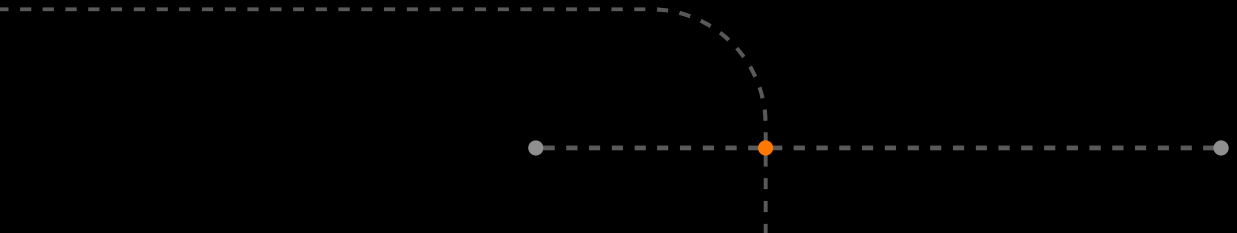
Ukraine war & Hacktivism - 2023

- Timeline
- 18th of January Anonymous Sudan created telegram channel with the message
- "We will attack any country with Cyber attacks against those who oppose Sudan.“
- 21st of January 2023 - right-winged Rasmus Paludan burns Qur’an near Turkey's embassy in Stockholm.
- 23rd of January 2023 starts DDOS-ing Swedish sites: government sites, universities, banks, airport etc.
- Feb – March: Sweden and Denmark are under DDOS attack
- 19th of February 2023, the pro-Russia hacktivist group Killnet announced on its Telegram channel that Anonymous Sudan had officially become a member of the Killnet collective
- Since then, they have been targeting other countries opposing Islam (in their opinion)



Orange
Cyberdefense

Disrupting Cy-X / Cybercrime



orange™

Orange
Cyberdefense

Under the theme of **DISRUPT AND DISMANTLE THREAT ACTORS**, it looks at the following points:

STRATEGIC OBJECTIVE 2.1: INTEGRATE FEDERAL DISRUPTION ACTIVITIES

STRATEGIC OBJECTIVE 2.2: ENHANCE PUBLIC -PRIVATE OPERATIONAL COLLABORATION TO DISRUPT ADVERSARIES

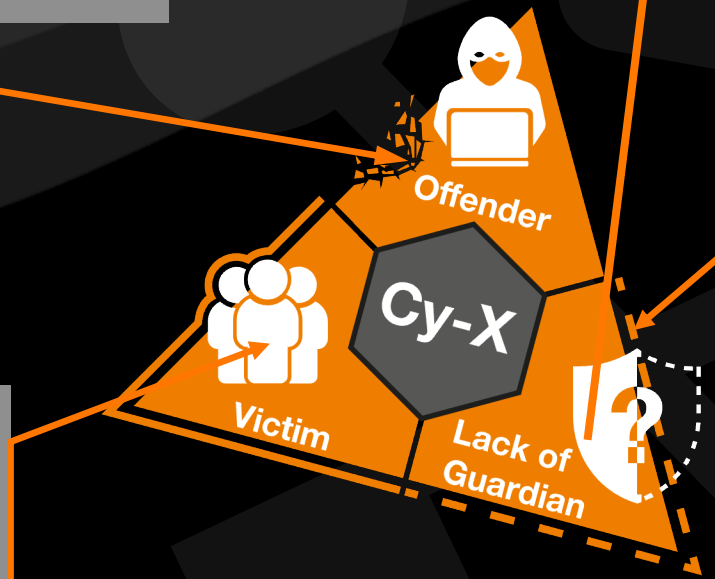
STRATEGIC OBJECTIVE 2.3: INCREASE THE S PEED AND SCALE OF INTELLIGENCE S HARING AND VICTIM NOTIFICATION

STRATEGIC OBJECTIVE 2.4: PREVENT ABUSE OF U.S.-BASED INFRASTRUCTURE

STRATEGIC OBJECTIVE 2.5: COUNTER CYBERCRIME, DEFEAT RANSOMWARE

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

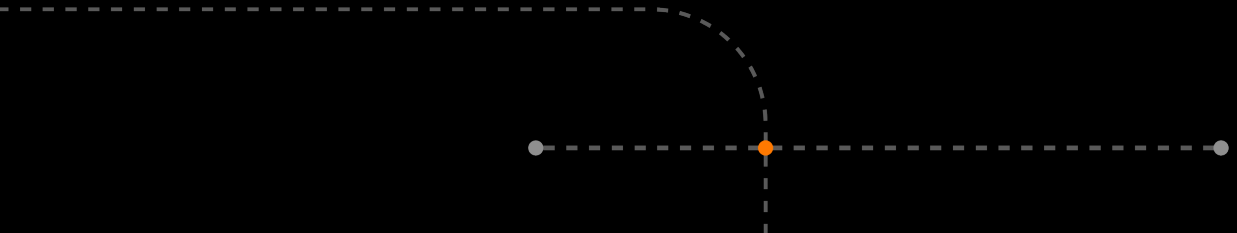
Get suitable guardians in place:
- Technical controls
- 'Social' guardians – government, individuals, teams and groups



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

Conclusion



orange™

Take aways

- We saw an 8% decrease in Cy-X
- We do believe the Ukraine war disrupted the criminal ecosystem of Cy-X temporarily (in 2022)
- We suspect higher volumes of victims moving into 2023 (unfortunately!)
  - We will continue seeing a regional shift
    - Southeast Asia
    - South & Central America
    - Nordics (more impacted by Cy-X, hacktivism & process of NATO membership)
    - Middle East
    - Africa
- We will see pro-Russian groups lashing out more towards other Nations due to Ukraine's resilience
  - Destruction & Disruption
- We need to continue working on RAT!