Threat Landscape 2023

Diana Selck-Paulsson

orange™ Cyberdefense

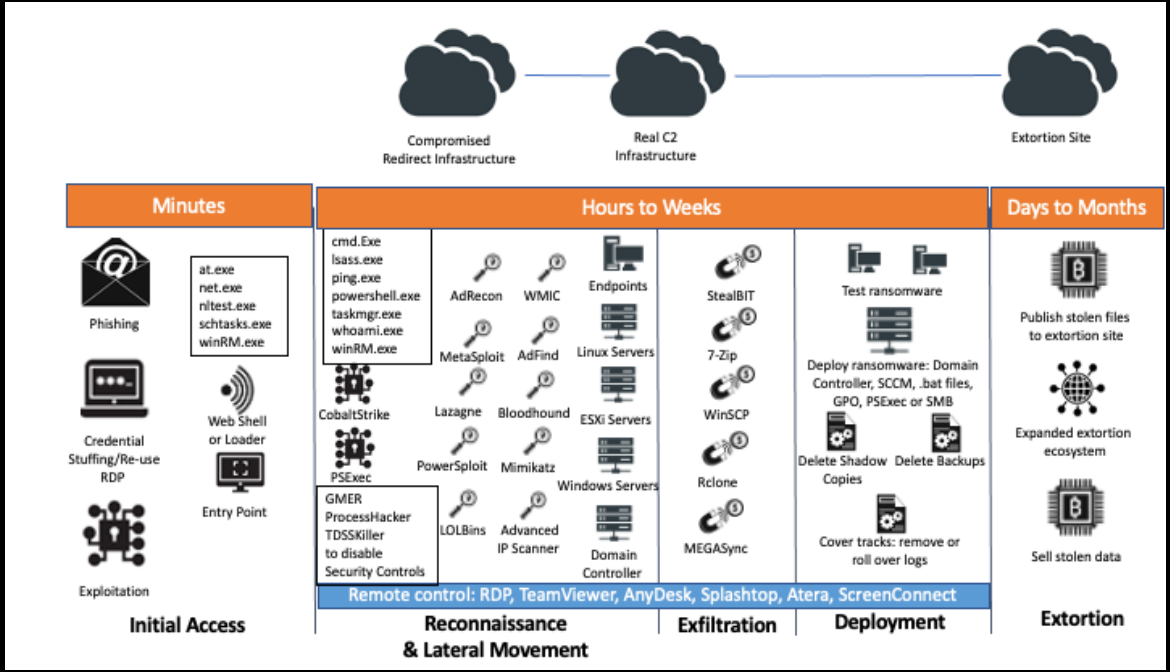
Outline

1. Threat landscape of 2023
2. Ransomware / Cyber-Extortion

Researching Ransomware / Cy-X

What is the problem ?

Maze Ransomware



Compromised Redirect Infrastructure

Real C2 Infrastructure

Extortion Site

Minutes

Hours to Weeks

Days to Months

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

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

CobaltStrike

PSExec

GMER
ProcessHacker
TDSSKiller
to disable
Security Controls

AdRecon

WMIC

Endpoints

MetaSploit

AdFind

Linux Servers

Lazagne

Bloodhound

ESXi Servers

PowerSploit

Mimikatz

Windows Servers

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

Publish stolen files to extortion site

Expanded extortion ecosystem

Sell stolen data

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

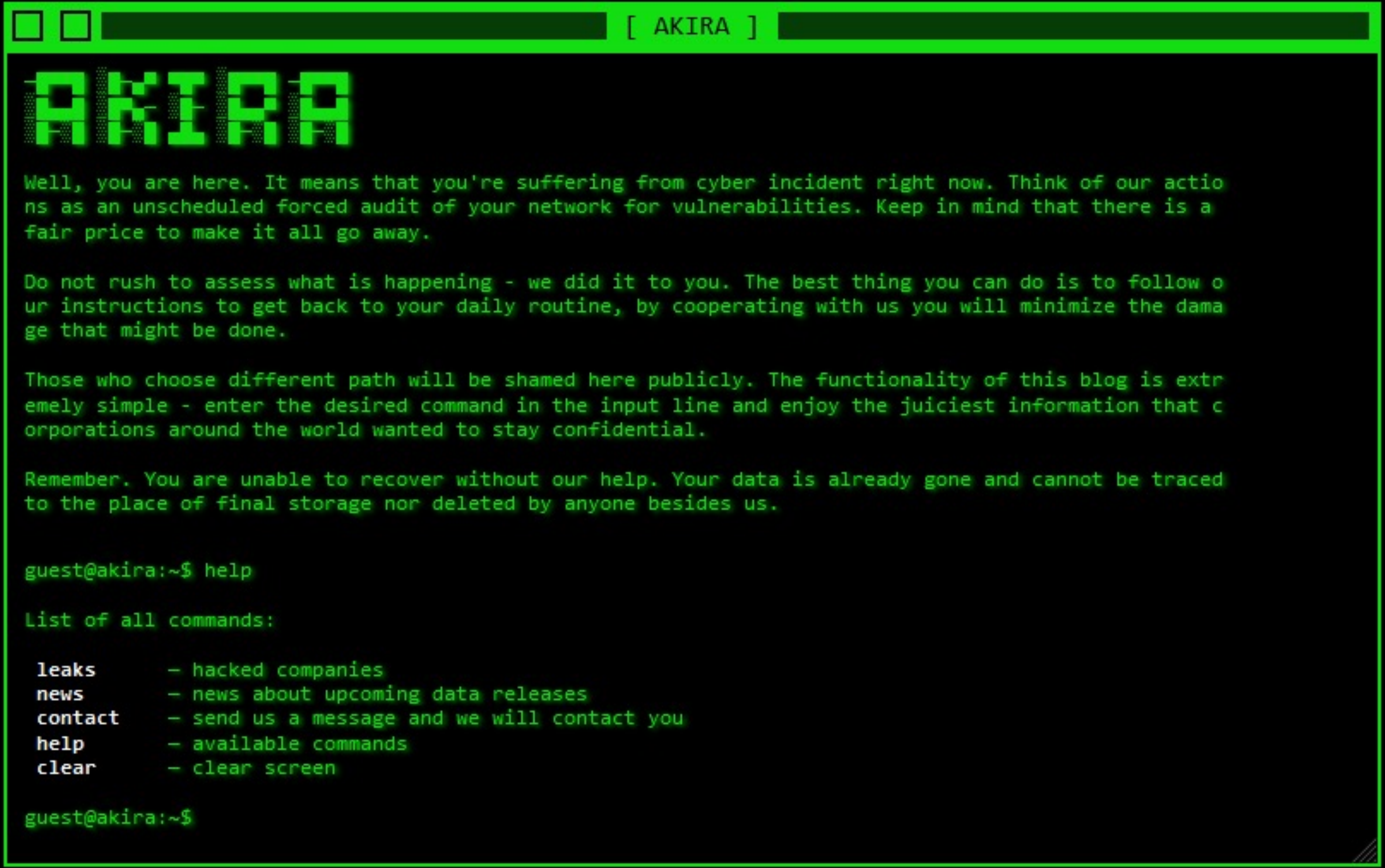
Reconnaissance & Lateral Movement

Exfiltration

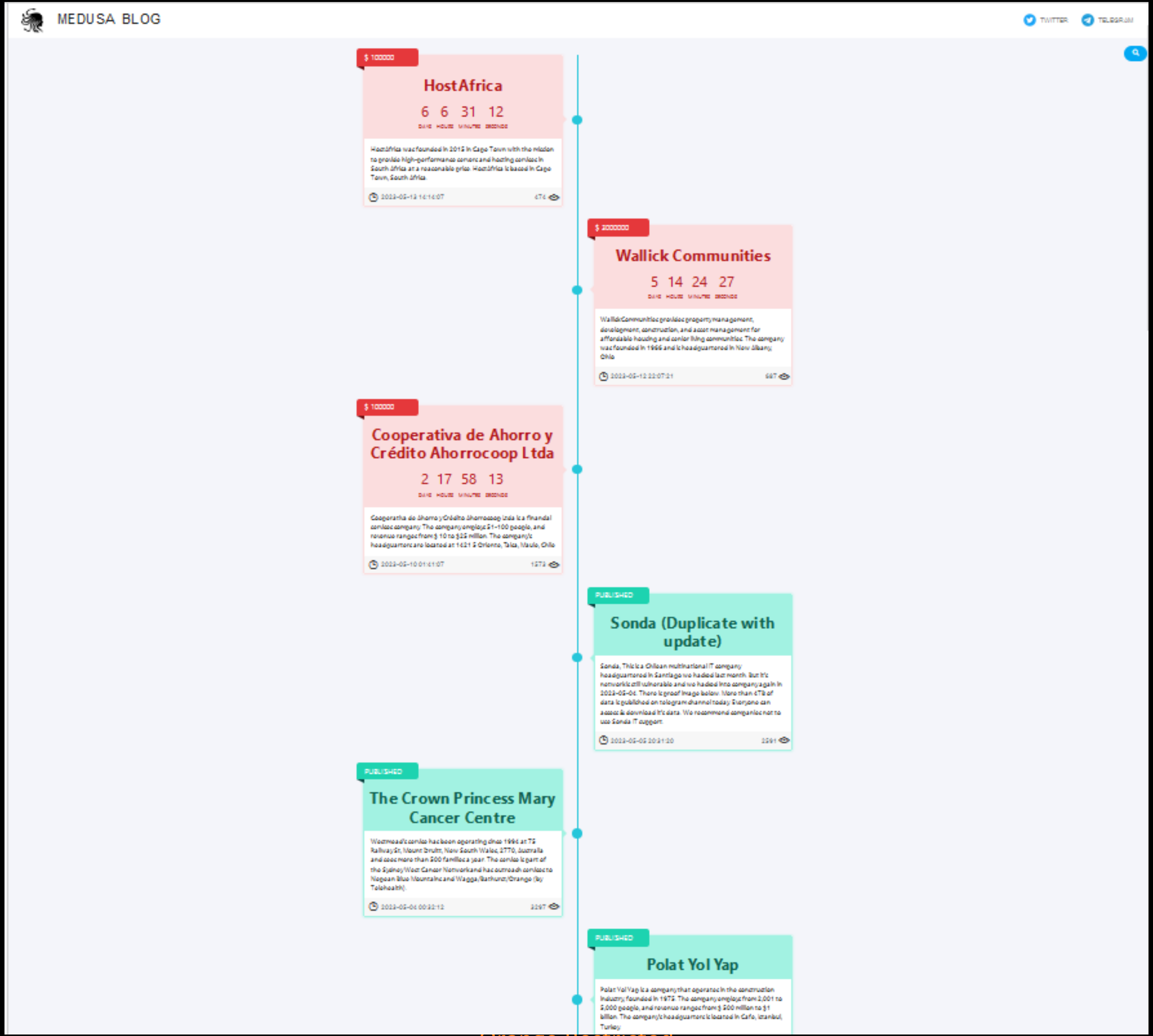
Deployment

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



```
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:~$
```



MEDUSA BLOG

TWITTER TELEGRAM

$ 100000

HostAfrica

6 6 31 12
DAYS HOURS MINUTES SECONDS

HostAfrica was founded in 2015 in Cape Town with the mission to provide high-performance servers and hosting services in South Africa at a reasonable price. HostAfrica is based in Cape Town, South Africa.

2023-05-13 14:14:07 474

$ 2000000

Wallick Communities

5 14 24 27
DAYS HOURS MINUTES SECONDS

Wallick Communities provides property management, development, construction, and asset management for affordable housing and senior living communities. The company was founded in 1966 and is headquartered in New Albany, Ohio

2023-05-12 22:07:21 687

$ 100000

Cooperativa de Ahorro y Crédito Ahorrocoop Ltda

2 17 58 13
DAYS HOURS MINUTES SECONDS

Cooperativa de Ahorro y Crédito Ahorrocoop Ltda is a financial services company. The company employs 51-100 people, and revenue ranges from $ 10 to $25 million. The company's headquarters are located at 1621 5 Oriente, Talca, Maule, Chile

2023-05-10 01:41:07 1573

PUBLISHED

Sonda (Duplicate with update)

Sonda, This is a Chilean multinational IT company headquartered in Santiago we hacked last month. But it's networks still vulnerable and we hacked into company again in 2023-05-04. There is proof image below. More than 4TB of data is published on telegram channel today. Everyone can access & download it's data. We recommend companies not to use Sonda IT support.

2023-05-05 20:31:30 2591

PUBLISHED

The Crown Princess Mary Cancer Centre

Westmead's service has been operating since 1994 at 75 Railway St, Mount Druitt, New South Wales, 2770, Australia and sees more than 500 families a year. The service is part of the Sydney West Cancer Network and has outreach services to Nepean Blue Mountains and Wagga/Bathurst/Orange (by Telehealth).

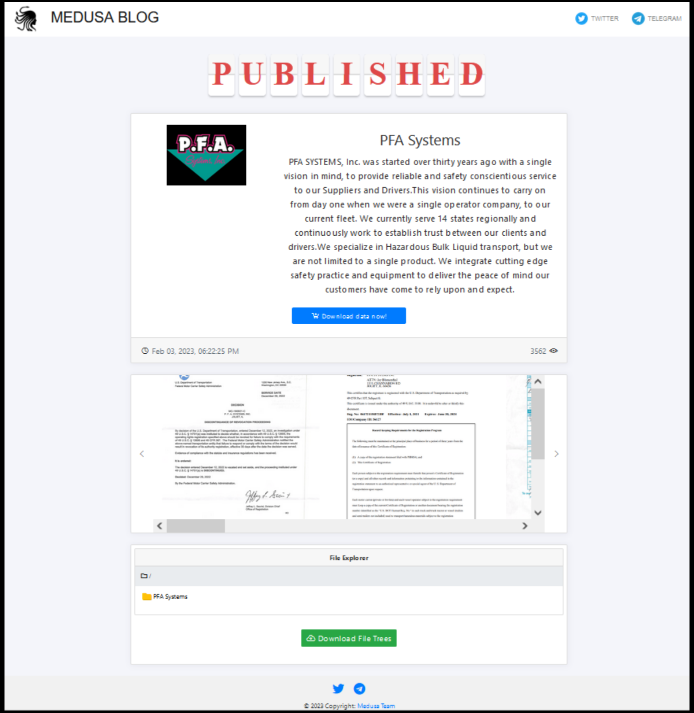
2023-05-04 00:32:12 3297

PUBLISHED

Polat Yol Yap

Polat Yol Yap is a company that operates in the construction industry, founded in 1975. The company employs from 2,001 to 5,000 people, and revenue ranges from $ 500 million to $1 billion. The company's headquarters is located in Cafe, Istanbul, Turkey

What happens when your company is posted on a Cy-X leaksite?



MEDUSA BLOG

PUBLISHED

PFA Systems

PFA SYSTEMS, Inc. was started over thirty years ago with a single vision in mind, to provide reliable and safety conscientious service to our Suppliers and Drivers.This vision continues to carry on from day one when we were a single operator company, to our current fleet. We currently serve 14 states regionally and continuously work to establish trust between our clients and drivers.We specialize in Hazardous Bulk Liquid transport, but we are not limited to a single product. We integrate cutting edge safety practice and equipment to deliver the peace of mind our customers have come to rely upon and expect.

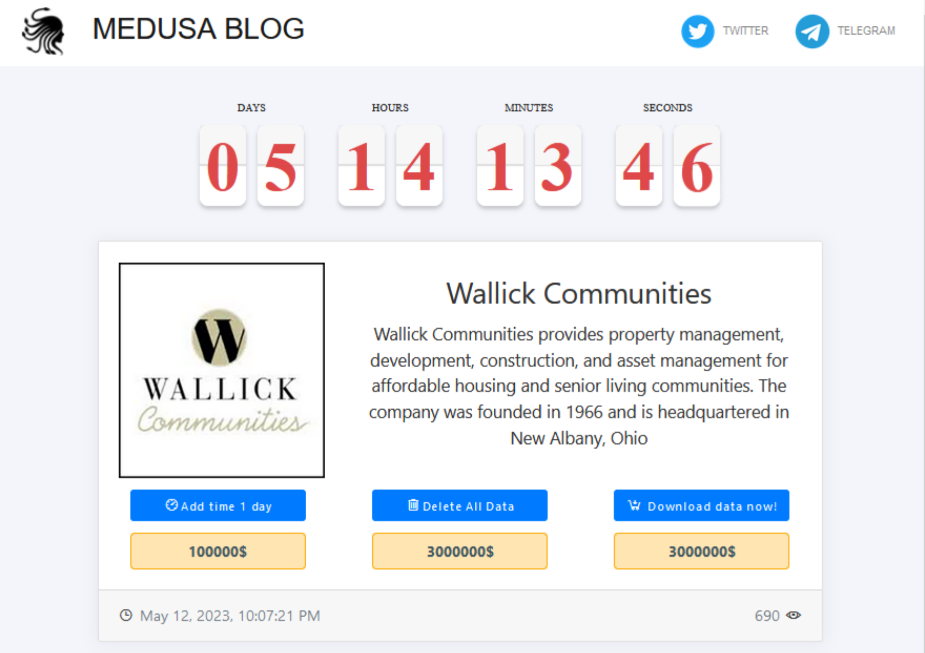
Feb 03, 2023, 06:22:25 PM — 3562

File Explorer

/

PFA Systems

© 2023 Copyright: Medusa Team



MEDUSA BLOG

DAYS	HOURS	MINUTES	SECONDS
05	14	13	46

Wallick Communities

Wallick Communities provides property management, development, construction, and asset management for affordable housing and senior living communities. The company was founded in 1966 and is headquartered in New Albany, Ohio

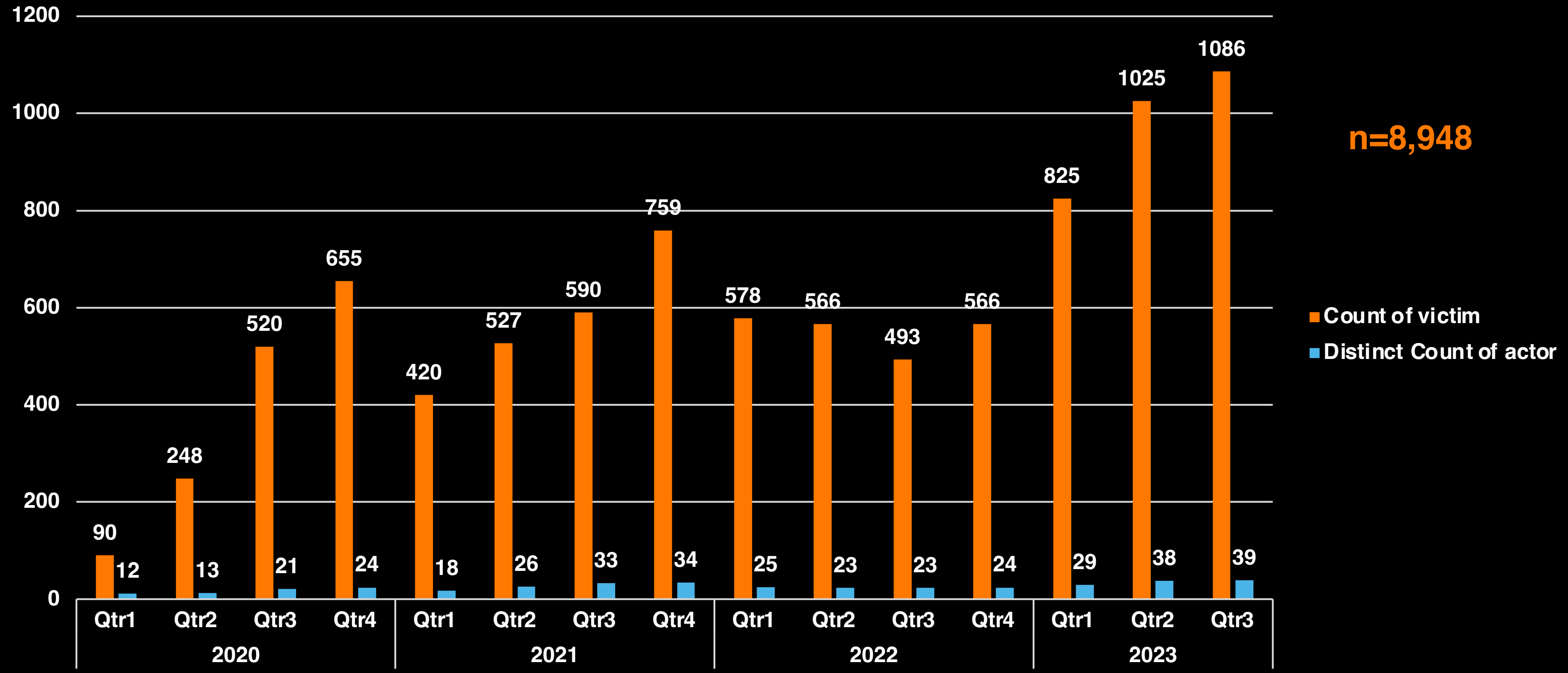
Add time 1 day	Delete All Data	Download data now!
100000$	3000000$	3000000$

May 12, 2023, 10:07:21 PM — 690

Cy-X Threat Landscape

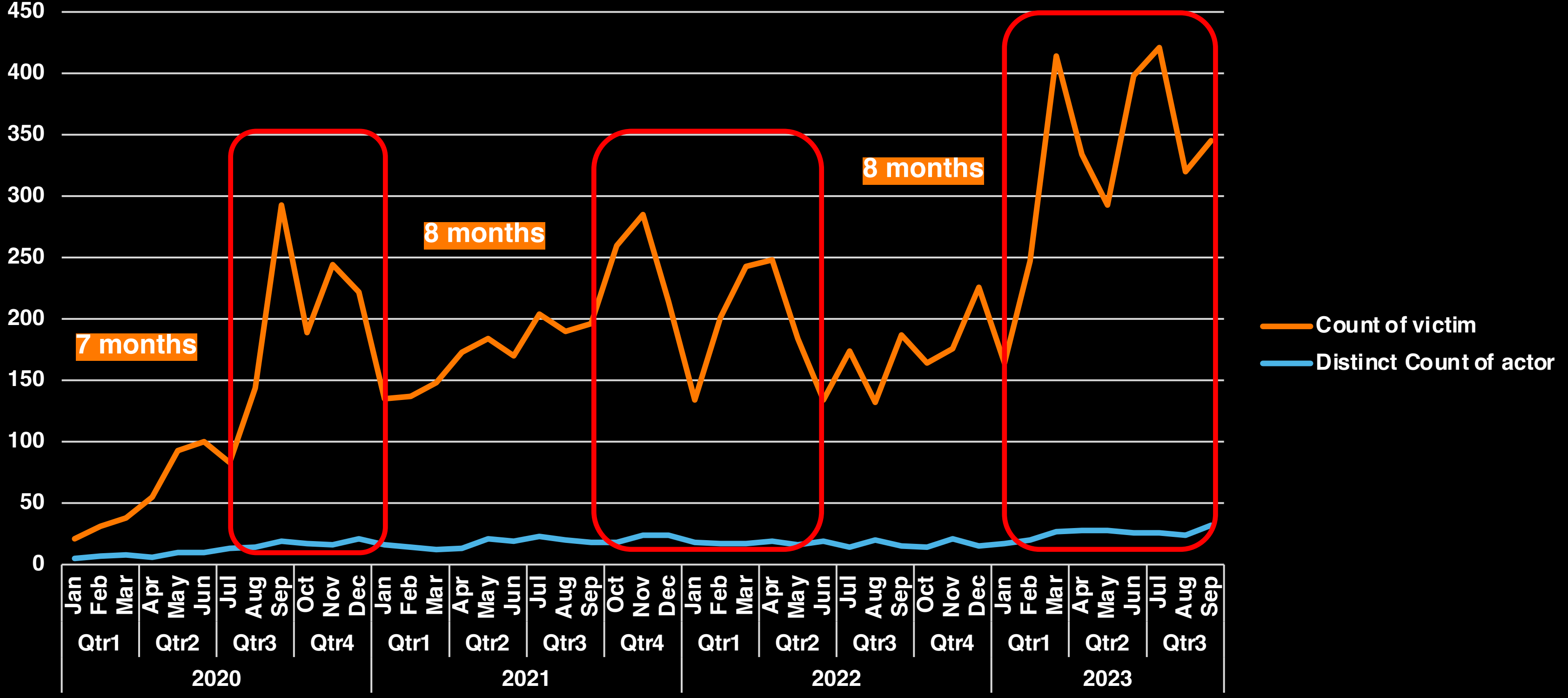
Threats and actors observed

Distinct threats and distinct actors over time

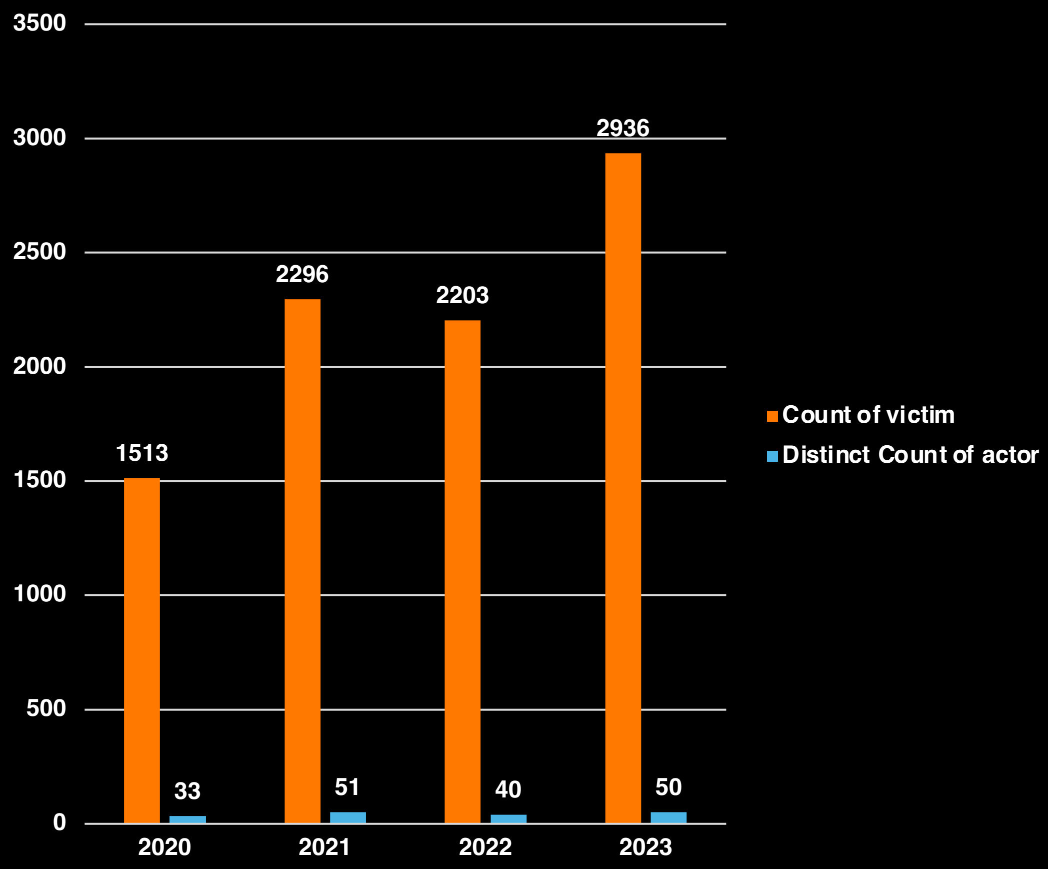


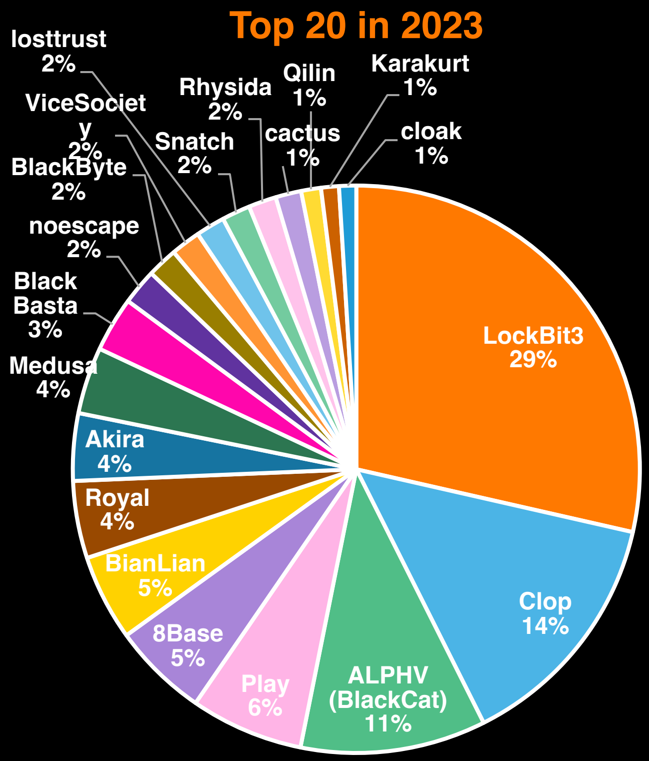
Threats and actors observed

Distinct threats and distinct actors over time



Threat Actor Activity

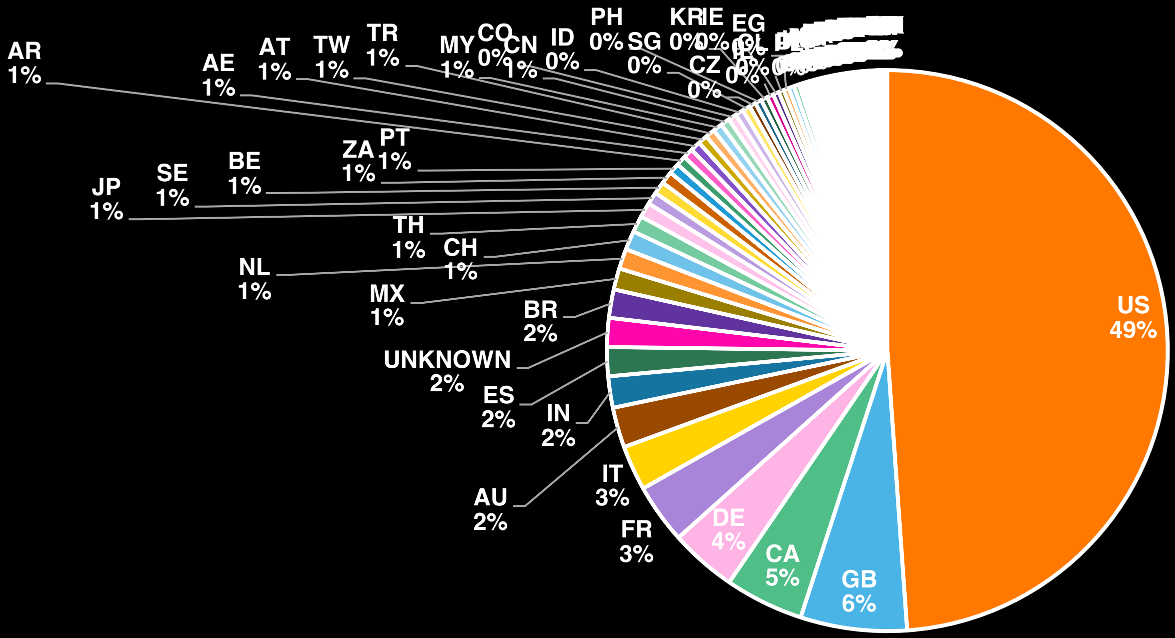



Top 20 in 2023

Victimology

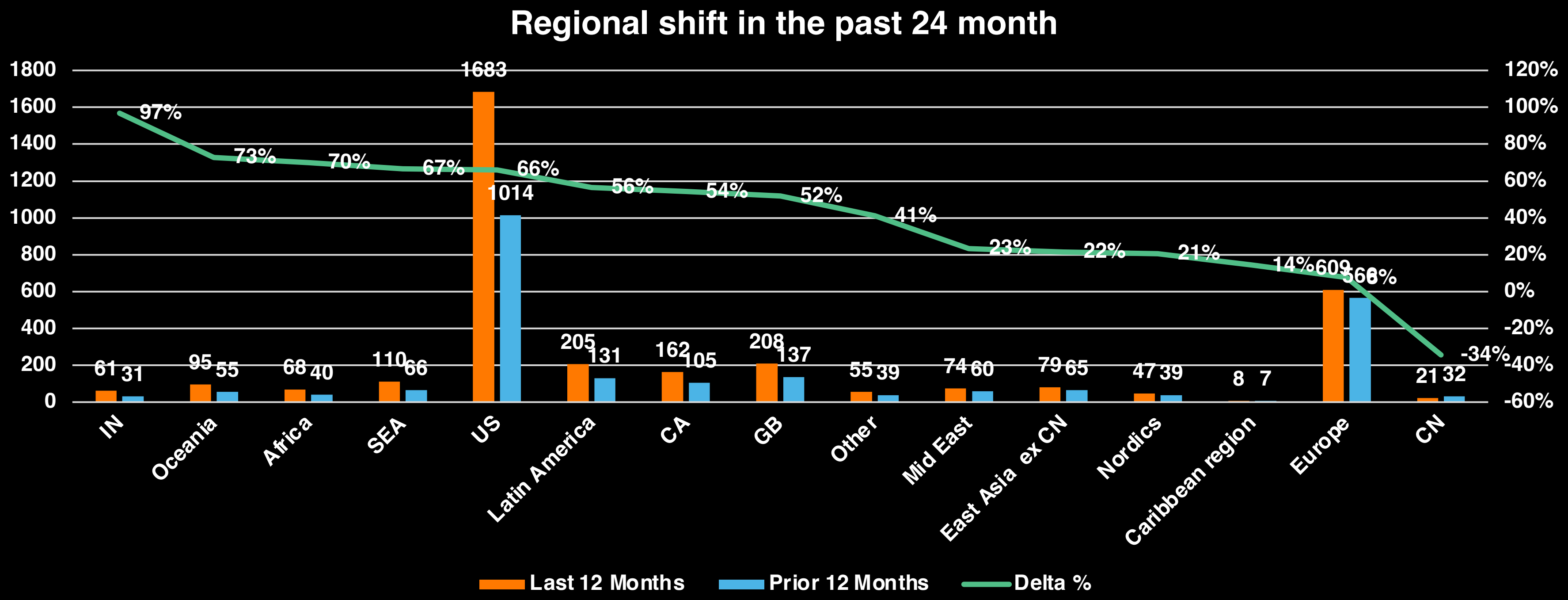
Cyber Extortion Victims

Distinct victims per country in 2023

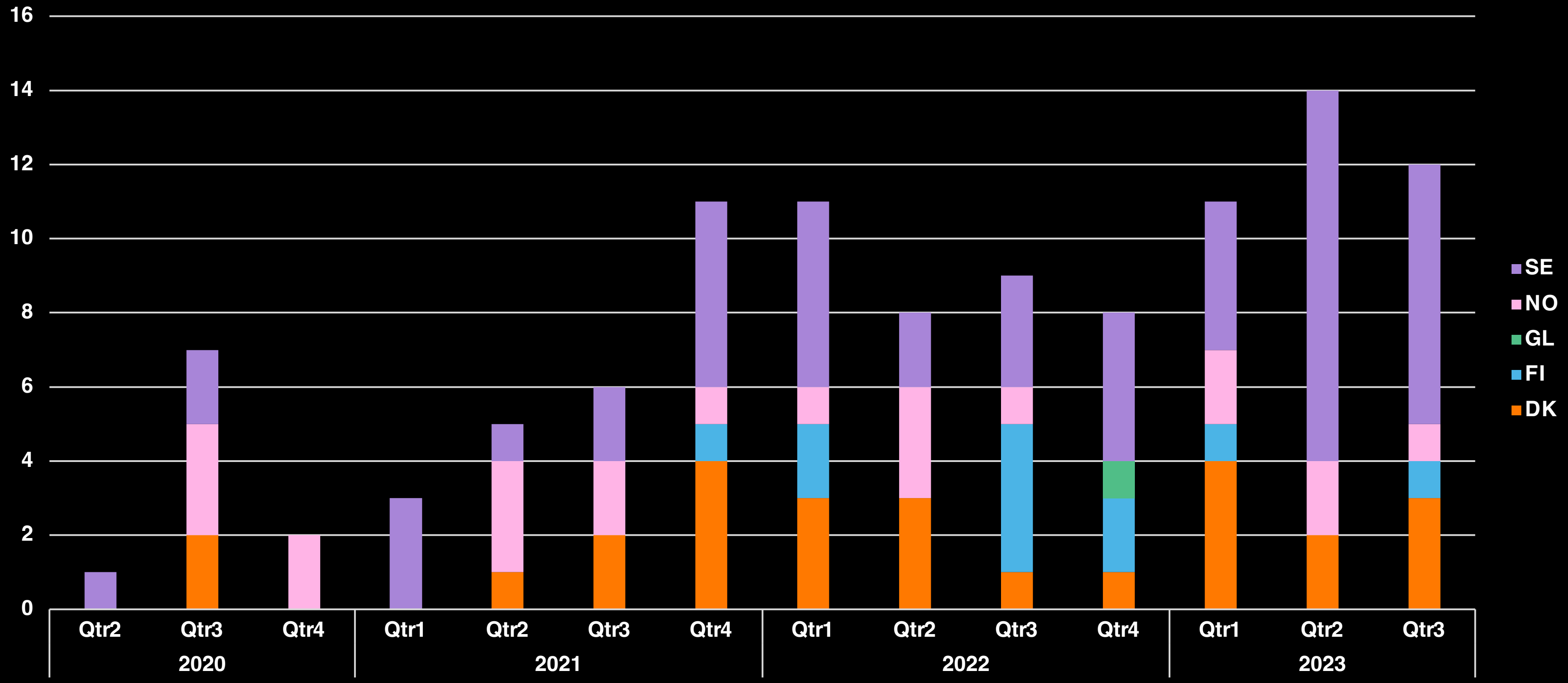


Cyber Extortion Victims

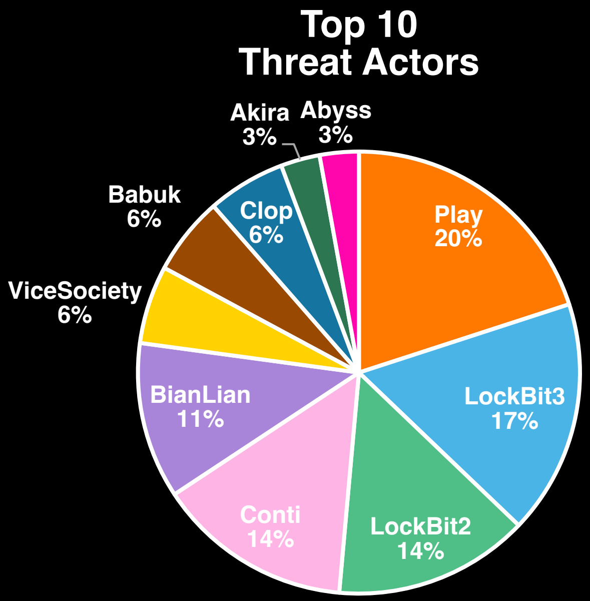
Distinct victims per country in 2023



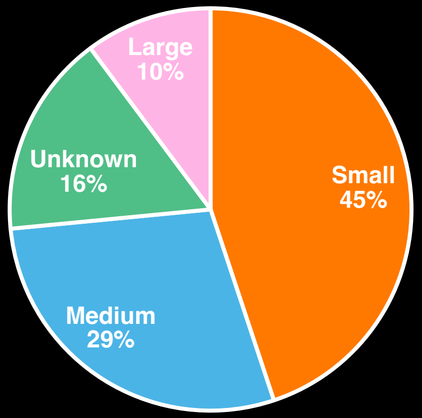
Impact to the Nordic countries



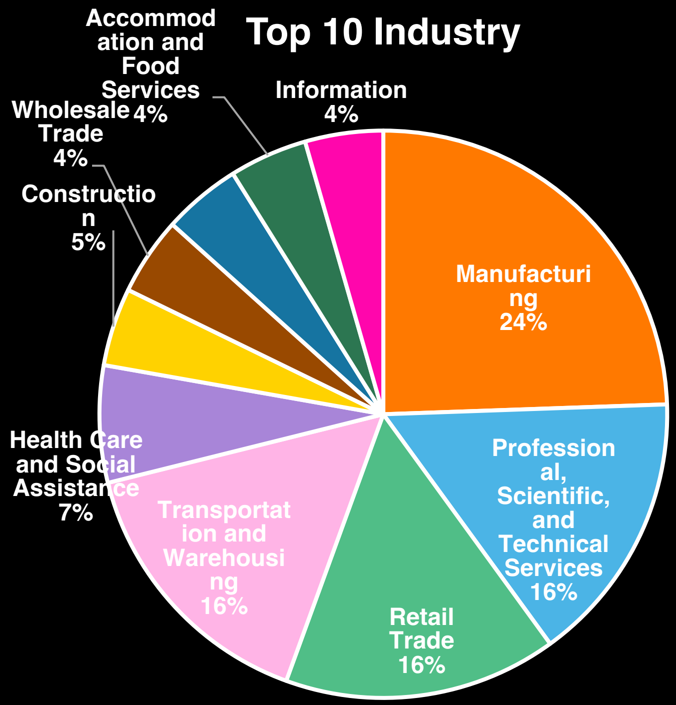
Cy-X / Ransomware - Sweden



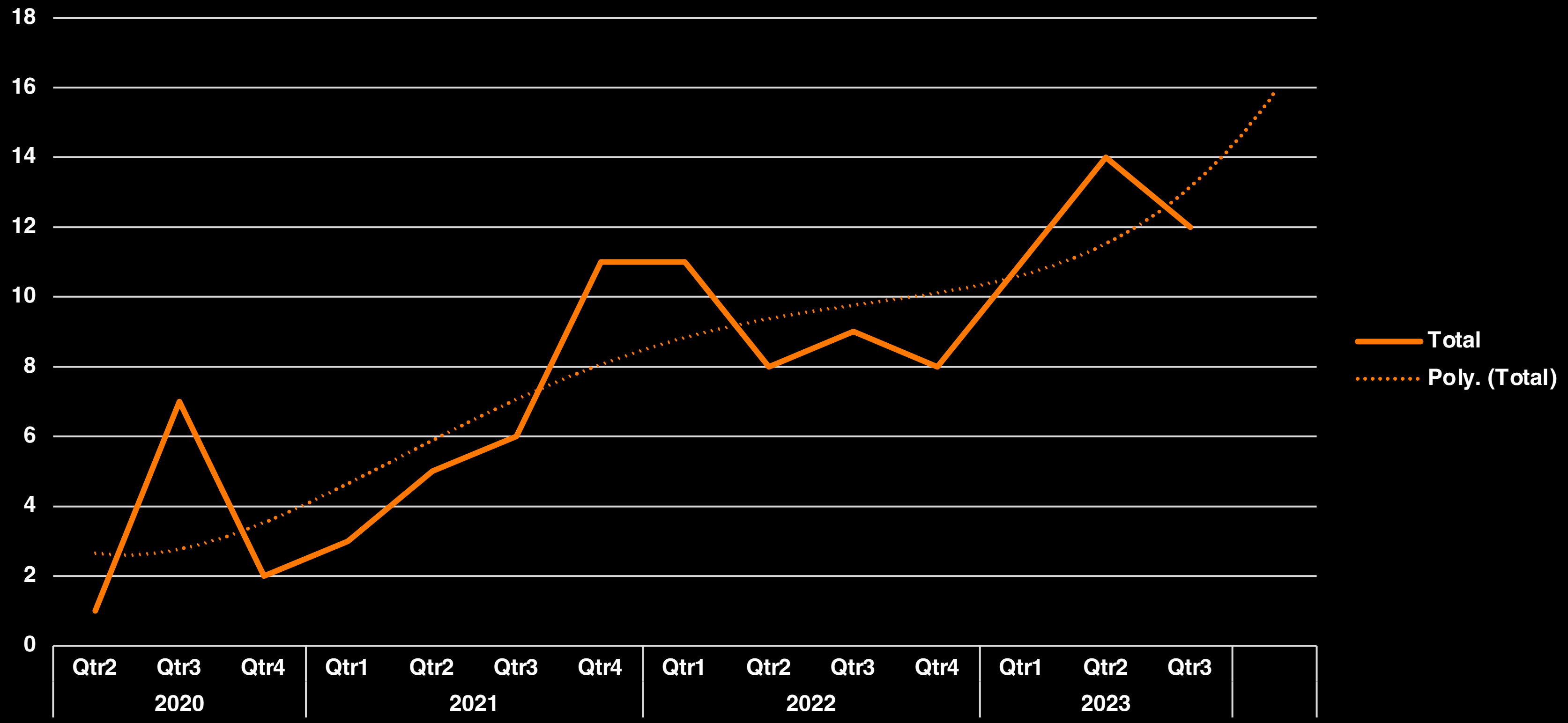
Business Size



Business Size	Employee Count
Small	1-49
Medium	50-249
Large	250+

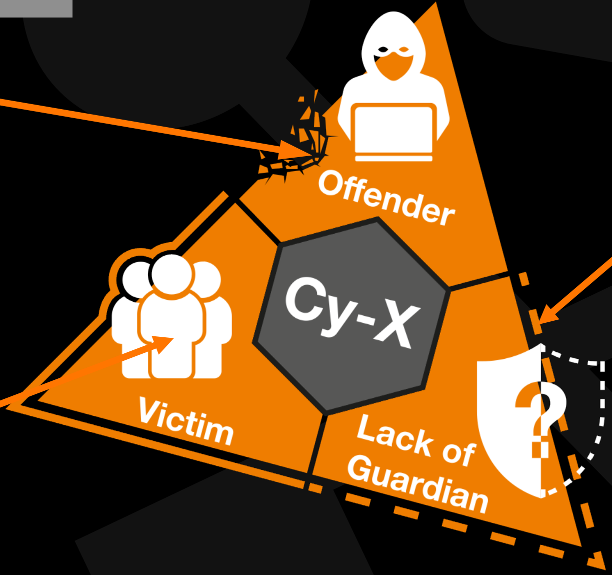


What to expect in the Nordics?



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:

- **Visibility**. A large attack surface
- **Vulnerability**. Poor cybersecurity practices
- **Inertia**: ‘Data’ is easy to access and exfiltrate
- **Value**: The value of the data to the victim
- **Access**: The amount of time and space allowed to the attacker

Thanks

Diana Selck-Paulsson

Lead Security Researcher

orange™ Cyberdefense