Threat Landscape 2023

Diana Selck-Paulsson

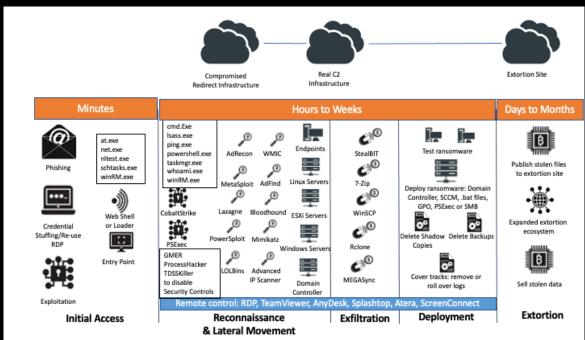# Outline

1. Threat landscape of 2023
2. Ransomware / Cyber-Extortion
3. Hacktivism
4. What do we think this means?
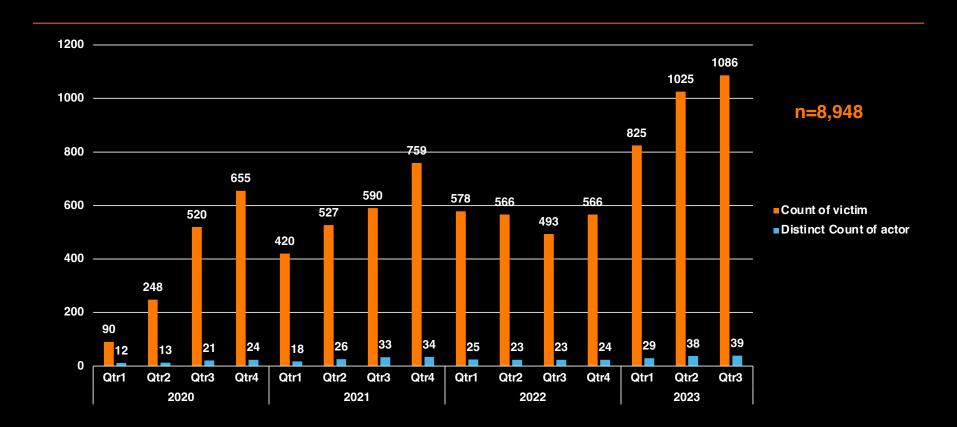
Researching Ransomware / Cy-X
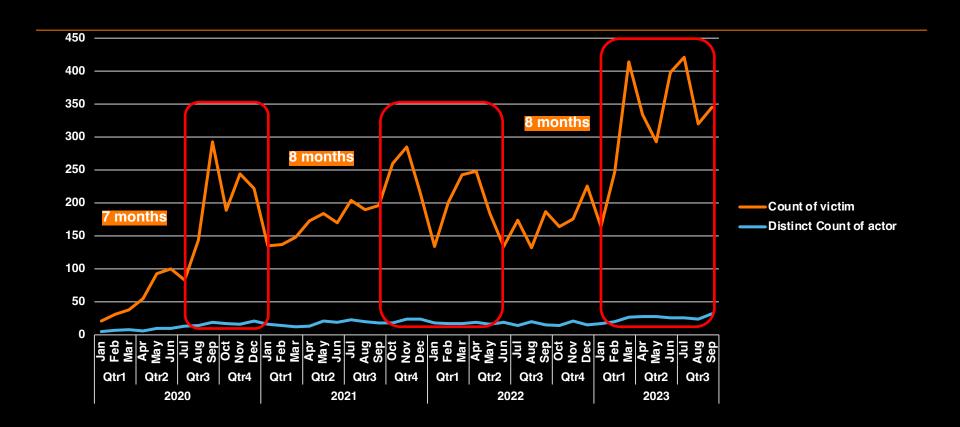
What is the problem ?

Cy-X Threat Landscape

Threats and actors observed
Distinct threats and distinct actors over time

n=8,948

Year	Quarter	Count of victim	Distinct Count of actor
2020	Qtr1	90	12
2020	Qtr2	248	13
2020	Qtr3	520	21
2020	Qtr4	655	24
2021	Qtr1	420	18
2021	Qtr2	527	26
2021	Qtr3	590	33
2021	Qtr4	759	34
2022	Qtr1	578	25
2022	Qtr2	566	23
2022	Qtr3	493	23
2022	Qtr4	566	24
2023	Qtr1	825	29
2023	Qtr2	1025	38
2023	Qtr3	1086	39

Threat Actor Activity

Bar chart "Count of victim" and "Distinct Count of actor" by year:

Year	Count of victim	Distinct Count of actor
2020	1513	33
2021	2296	51
2022	2203	40
2023	2936	50

Top 20 in 2023

Pie chart:

- LockBit3 29%
- Clop 14%
- ALPHV (BlackCat) 11%
- Play 6%
- 8Base 5%
- BianLian 5%
- Royal 4%
- Akira 4%
- Medusa 4%
- Black Basta 3%
- noescape 2%
- BlackByte 2%
- ViceSociety 2%
- losttrust 2%
- Snatch 2%
- Rhysida 2%
- cactus 1%
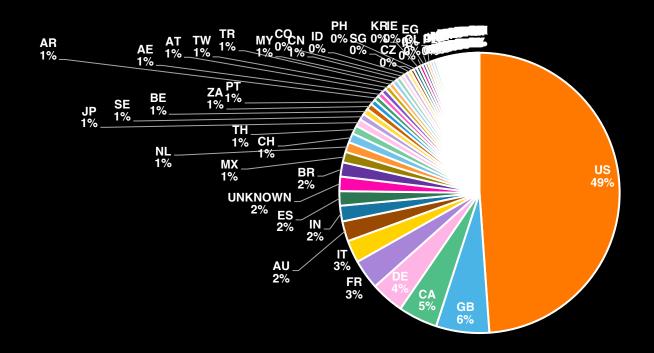- Qilin 1%
- Karakurt 1%
- cloak 1%

Victimology

Cyber Extortion Victims
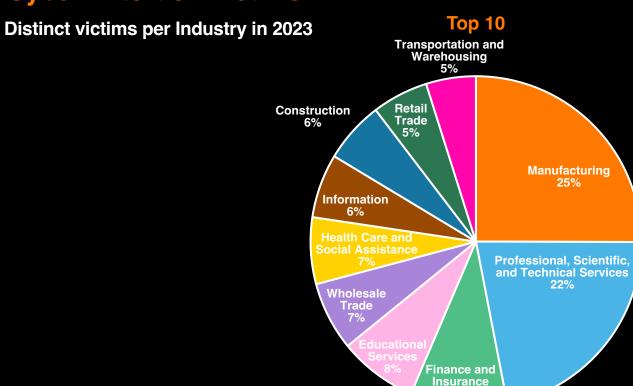
Distinct victims per country in 2023

Cyber Extortion Victims

Distinct victims per country in 2023

Regional shift in the past 24 month

Country	Last 12 Months	Prior 12 Months	Delta %
IN	61	31	97%
Oceania	95	55	73%
Africa	68	40	70%
SEA	110	66	67%
US	1683	1014	66%
Latin America	205	131	56%
CA	162	105	54%
GB	208	137	52%
Other	55	39	41%
Mid East	74	60	23%
East Asia ex CN	79	65	22%
Nordics	47	39	21%
Caribbean region	8	7	14%
Europe	609	566	6%
CN	21	32	-34%

Cyber Extortion Victims

Distinct victims per Industry in 2023

Top 10

- Transportation and Warehousing 5%
- Retail Trade 5%
- Construction 6%
- Information 6%
- Health Care and Social Assistance 7%
- Wholesale Trade 7%
- Educational Services 8%
- Finance and Insurance 9%
- Manufacturing 25%
- Professional, Scientific, and Technical Services 22%

Cy-X / Ransomware - Norway

Threat Actors

- HiveLeaks 5%
- ALPHV (BlackCat) 5%
- DoppelPaymer 5%
- Clop 5%
- Play 5%
- LockBit 2 11%
- Prometheus 16%
- Conti 16%
- REvil 16%
- LockBit 3 16%

Business Size

- Unknown 5%
- Large 5%
- Medium 33%
- Small 57%

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

Top 10 Industry

- Professional, Scientific, and Technical Services 5%
- Mining, Quarrying, and Oil and Gas Extraction 5%
- Finance and Insurance 5%
- Retail Trade 5%
- Construction 9%
- Public Administration 9%
- Manufacturing 33%
- Transportation and Warehousing 19%

What to expect in the Nordics?

Hacktivism
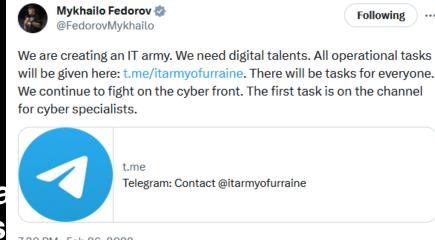
Ukraine war – Hacktivism – the Nordics

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

Mykhailo Fedorov ✔
@FedorovMykhailo

Following ···

We are creating an IT army. We need digital talents. All operational tasks will be given here: t.me/itarmyofurraine. There will be tasks for everyone. We continue to fight on the cyber front. The first task is on the channel for cyber specialists.

t.me
Telegram: Contact @itarmyofurraine
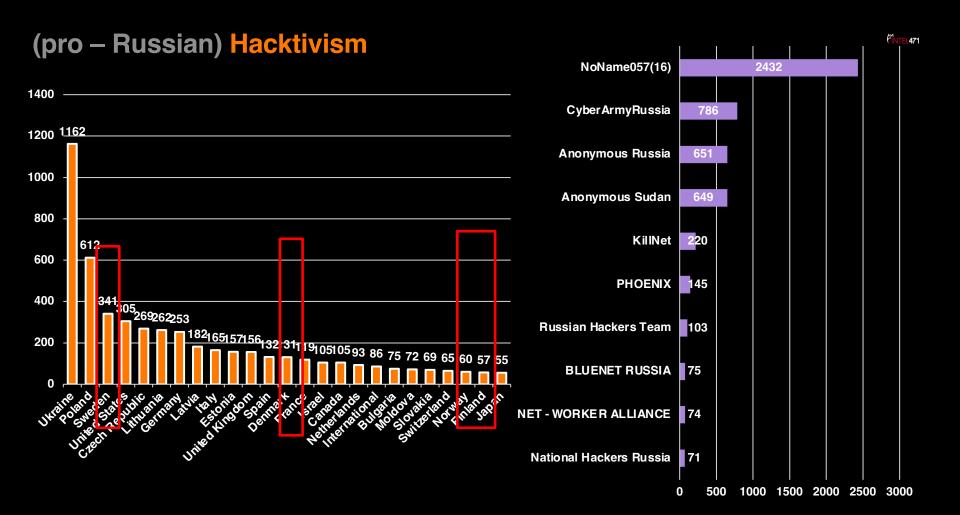
7:38 PM · Feb 26, 2022

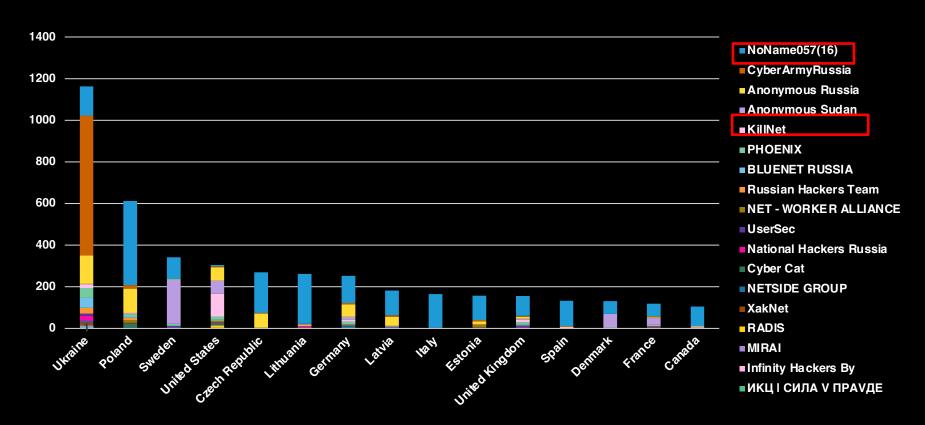**"Ukraine's cyber response pla**
by its Minister of Digital Trans
Albertovych Fedorov – who coordinated one of the
most successful, multifaceted information operations
campaigns ever witnessed in history**."**

(pro – Russian) **Hacktivism**

Who attacks the Nordics & Why

Chart legend:
- NoName057(16)
- CyberArmyRussia
- Anonymous Russia
- Anonymous Sudan
- KillNet
- PHOENIX
- BLUENET RUSSIA
- Russian Hackers Team
- NET - WORKER ALLIANCE
- UserSec
- National Hackers Russia
- Cyber Cat
- NETSIDE GROUP
- XakNet
- RADIS
- MIRAI
- Infinity Hackers By
- ИКЦ | СИЛА V ПРАУДЕ

X-axis: Ukraine, Poland, Sweden, United States, Czech Republic, Lithuania, Germany, Latvia, Italy, Estonia, United Kingdom, Spain, Denmark, France, Canada

Y-axis: 0, 200, 400, 600, 800, 1000, 1200, 1400

Who attacks the Nordics & Why

Legend:
- NoName057(16) - Norway
- CyberArmyRussia - Norway
- Anonymous Sudan - Norway
- Anonymous Russia - Norway

Chart data:
- Nov Qtr4 2022: 2
- Jan Qtr1 2023: 8
- Feb: 2
- Mar: 12, 1
- Jul: 3
- Aug Qtr3: 28
- Sep: 4

Who attacks the Nordics & Why

Anonymous Sudan – Jan 2023

NoName057(16) – Feb 2022

Geopolitical events in 2023 – the Nordics

Physical

Paludans koranafbrændinger i København forløb uden anholdelser

Den dansk-svenske politiker, Rasmus Paludan, brændte fredag tre koraner af forskellige steder i København.

WORLD POLITICS

Right-win... ...n Sweden enrages T... ...a new wrench in... ...d

PUBLISHED TUE, JAN 24 2023... ...M EST | UPDATED TUE, JAN 24 2023... ...M EST

Døgnåben

February & March
Norway forbids Qur'an burning

March
UK forbids Qur'an burning

January   **February**   **March**

Cyber

#OpSweden

January

Anonymous Sudan

Swedish sites are being attacked because of their burning of the Qur'an

84.6K 08:44

January 18

Channel created

Anonymous Sudan
We will attack any country with Cyber attacks against those who oppose Sudan

👁 67.5K 📌 13:20

30/01
Anonymous Sudan attacks Danish institutions

03/02
Anonymous Sudan declares cyberwar on Sweden

February & March
Anonymous Sudan attacks Sweden & Denmark heavily

Geopolitical events in 2023 – the Nordics

Physical

15th of April
Sudan conflict breaks out

Pressmeddelande från Försvarsdepartementet

Tolfte stödpaketet till Ukraina

Publicerad 16 juni 2023

Regeringen har beslutat om ett nytt stödpaket till Ukraina som presenterades på mötet med Ukraine Defence Contact Group i Bryssel 15 juni 2023. Stödet omfattar bidrag till fonder på sammanlagt 230 miljoner kronor och uppdrag till Försvarsmakten om bland annat JAS 39 Gripen och försörjningslösning för donerad krigsmateriel. Det sammanlagda värdet på detta tolfte stödpaket uppgår till cirka 250 miljoner kronor.
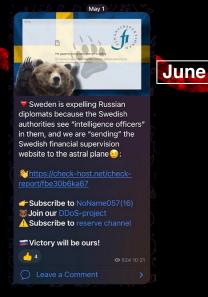
April   May   June

Cyber

February - May
NoName attacks Sweden due aid Ukraine war

May 1

NoName057(16) Eng
4.370 subscribers
Previous Message
‼️ Friends, friends of our friends need peo

🔻 Sweden is expelling Russian diplomats because the Swedish authorities see "intelligence officers" in them, and we are "sending" the Swedish financial supervision website to the astral plane😉:

👋https://check-host.net/check-report/fbe30b6ka67

👉Subscribe to NoName057(16)
🐻Join our DDoS-project
⚠️Subscribe to reserve channel

🇷🇺Victory will be ours!

👍 4   👁 534 10:21

💬 Leave a Comment   >

NoName057(16) Eng
4.370 subscribers
Previous Message
‼️ Friends, friends of our friends need peo

June 18

🔻 Sweden plans to become a nanny for Ukrainians😳

As part of the 12th package of military assistance to Ukraine, Swedish specialists will conduct training for pilots, as well as create service centers for military equipment supplied to the Ukrainian Nazis.

And all this with the money of honest taxpayers😡

We go to Sweden and kill the site of the Swedish port of Helsingborg:

❌https://check-host.net/check-report/104e1db0k84b

28/6
Anonymous Sudan attacks Sweden

NoName057(16) Eng
4.371 subscribers
Previous Message
‼️ Friends, friends of our friends need peo

June 28

Hell is empty. All demons are here

🔻 Swedish police allowed to burn

#OpSweden
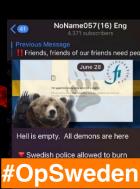
Considering that the Swedish authorities also help Ukrainian terrorists, we could not pass by and killed the website of the financial supervision of Sweden:

❌https://check-host.net/check-report/106e4d37k198

👉Subscribe to NoName057(16)
🐻Join our DDoS-project
⚠️Subscribe to reserve channel

🇷🇺Victory will be ours!

Geopolitical events in 2023 – the Nordics

ARAB NEWS SAUDI ARABIA MIDDLE EAST WORLD BUSINESS MEDIA LIFESTYLE PODCAST

Desecrating the Qur'an a crime in Russia, Putin says in visit to Dagestan

We know that in other countries they treat it differently —

The New York Times

22/7
Danish Refugee Council office in Basra in Iraq is set on fire

...es to Ban Quran ... Muslim Outrage

...horities have struggled to balance free ...anger that security officials say has elevated ...tacks.

29/7
Quran burning in Norway

13/8
Quran burning Sweden

...den torn

Swedish

...rm the Swedish ...aghdad

...s protest

July

August

Physical

#OpSweden

Today

Cyber

Cyber Attacks on Sweden Rises: #OpSweden is Back, This Time With Different Results

Tags: cyber attacks ddos attacks sweden

JULY 6TH 2023

"Whatever affliction befalls you is because of what your own hands have committed."
Qur'an 42:30

August 14

Не удается получить доступ к сайту

We condemn yesterday's idiotic action to burn the Koran in Stockholm😡

The unification of Swedish-Finnish ports - Kvarken Ports - turn off...

https://check-host.net/check-report/1114ee5fke21

Russian version|DDoS project| Reserve channel

Leave a Comment

Who attacks the Nordics & Why – NoName

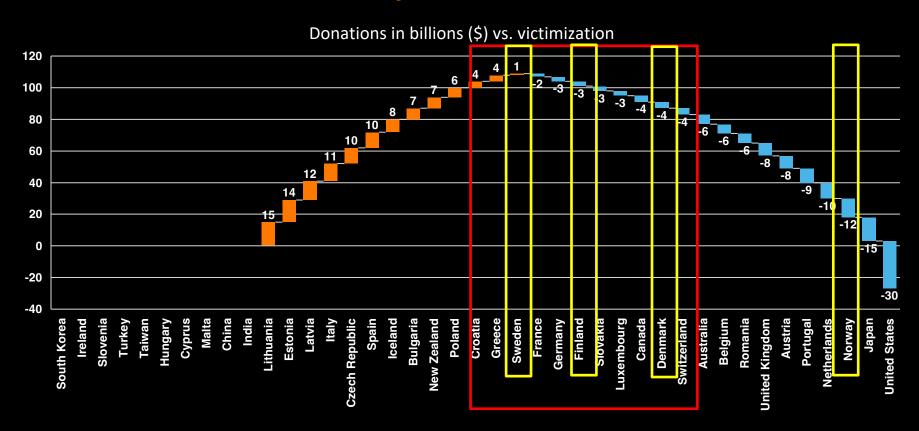| Date	Announcement	Attack Type
02/03/2023	Norway provides military aid to Ukraine	Announcement
02/03/2023	4x DDoS attacks	DDoS
14/03/2023	Norway provides military aid to Ukraine	Announcement
14/03 - 15/03/2023	6x DDoS attacks	DDoS
18/03/2023	Norway provides military aid to Ukraine	Announcement
18/03/2023	3x DDoS attacks	DDoS
13/07/2023	Norway provides military aid to Ukraine	Announcement
13/07/2023	2x DDoS attacks	DDoS
17/08/2023	Norway provides military aid to Ukraine	Announcements
17/08 – 18/08/2023	6x DDoS attacks	DDoS
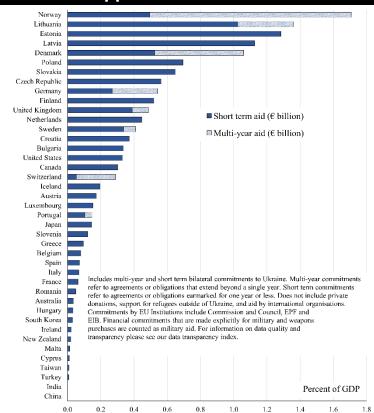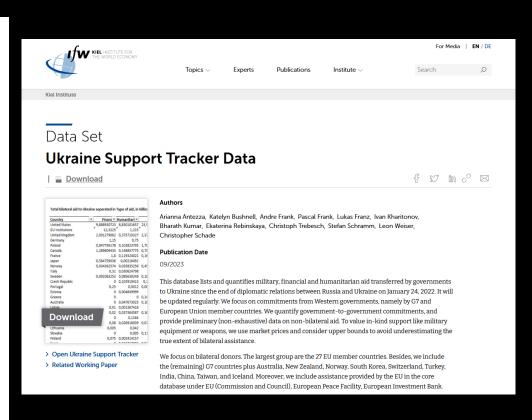
Who attacks the Nordics & Why – NoName057(16)

Ukraine support tracker

What do we think this means?

28

Hacktivism in 2023

- Hacktivism can have very different faces & hacktivist groups are very unpredictable

- We are observing a huge surge
  - Especially true fot the Nordics -> Sweden & Denmark
  - Europe

- We see direct & indirect connection with the Ukraine war + support

- We see a geopolitical entangle of cyber & physical events that are targeting countries & governments

- Its been evolving rapidly, both in form and capability
  - RDoS
  - 100 million requests per second

29

What do we do?

Conclusion

- Come to realize that hacktivism has b

- They organize themselves into 'collec   rces
  - Why don't we?

- We need to be conscious about sever
  - It is THEIR narrative
  - FUD
  - Misinformation campaigns / i   pinion & perception

Thanks

Diana Selck-Paulsson

Lead Security Researcher

Cyberdefense