Nordic Financial CERT

2024

Generic Threat Landscape Report

Nordic Financial Sector

TLP:CLEAR

December 2023 v. 1.0

- Senior Advisor Threat Intelligence @ NFCERT
- PhD Student @ NTNU

- Background
  - BA in Marketing
  - MA in Counter Terrorism
  - MA in Intelligence
  - 17 years in the Norwegian Army, Five years with intelligence
  - Five years at NFCERT

FREDDY MURSTAD

How to Read the Report

Assessments

- **Percentages**
- Bottom right corner
- Likely versus Unlikely

Statement	NATO Description	NATO
Highly likely	There is very good reason to believe	>90%
Likely	There is reason to believe	60-90%
Even Chance	About as likely as not	40-60%
Unlikely	There is little reason to believe	10-40%
Highly Unlikely	There is very little reason to believe	<10%

NFCERT uses Words of Estimative Probability (WEPs) aka assessment words, as used by NATO

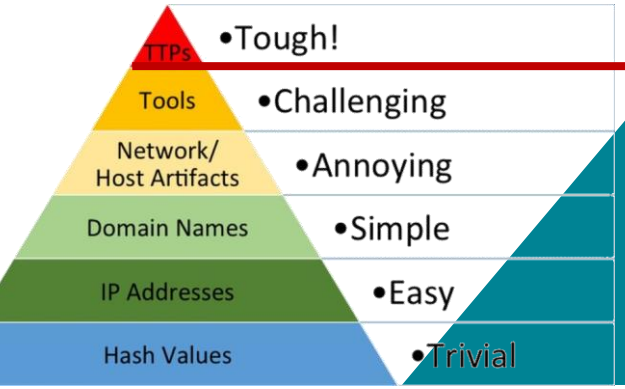
The GTL/CTL Focus

Strategic

Operational

Tactical

Technical



Key Takeaways

General

- Overall, the Nordic threat landscape will **highly likely** remain the same in 2024 compared to GTL 2023, with some moderate variations.
- Break-in groups and ransom, will **highly likely** continue to be a persistent threat to the Nordic financial sector in the coming year.
- The advent of new technology, such as Artificial Intelligence (AI), will **likely** change the threat landscape in the coming year. Exactly how and how much is currently unknown.

Key Takeaways

Organised Crime Group

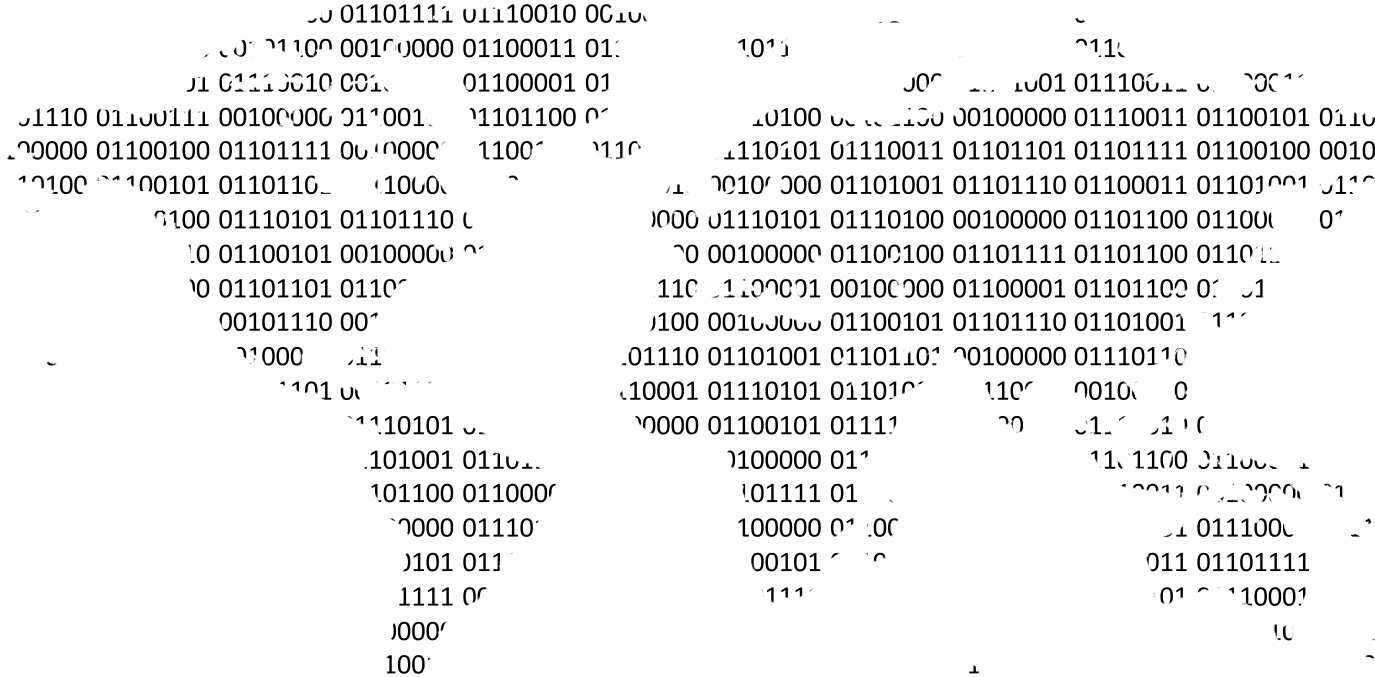
- OCGs are **unlikely** to target a specific critical function. Instead, OCGs will **highly likely** run untargeted campaigns to generate access that will **likely** be sold to other OCGs in the ecosystem.
- Most Initial Access Groups (IAGs) **likely** have the capabilities to penetrate (**IN**) and **even chance** the skills to pivot (**THROUGH**) target systems. They will **likely** hand the access over to pivoting crews.
- Developments in the OCG ecosystems have **likely** introduced new roles, such as data miners, **likely** to improve the identification of valuable data and targets.
- Ransom operators will **highly likely** continue to be a threat in 2024. A ransom incident will **highly likely** involve multiple OCGs, **likely** due to IAGs and affiliates providing ransom groups with access.
- Supply chain attacks will **highly likely** continue in 2024, as the supply chain **likely** remains an attractive target for Nation-States and Organised Crime Groups (OCG).

Key Takeaways

Nation-States

- In the current security climate, a nation-state will **highly unlikely** target a Nordic financial institution directly in the coming year.
- A cyber-attack from a nation-state will **likely** result from collateral damage where the objective is a different target, a target of opportunity or due to a supply chain attack compromising multiple sectors.
- Nordic financial institutions' infrastructure is **likely** viewed as valuable for Nation-States and is **likely** scanned for further operations towards other targets.
- With upcoming elections in 2024, Nation-States will, with an **even chance,** seek information or influence the outcome. It is **unlikely** that the elections in 2024 will impact the Nordic financial sector.
- Cooperation between OCGs and Nation-States will **likely** continue in 2024. There is an **even chance** that a Nation-State APT member could be moonlighting for personal financial gain.

Threat Categories



OCGs and the Evolving Ecosystem

Unchanged focus

- Opportunistic and financial gain
- Relatively short operations
- Maximum ROI, constantly looking for new Modus Operandi

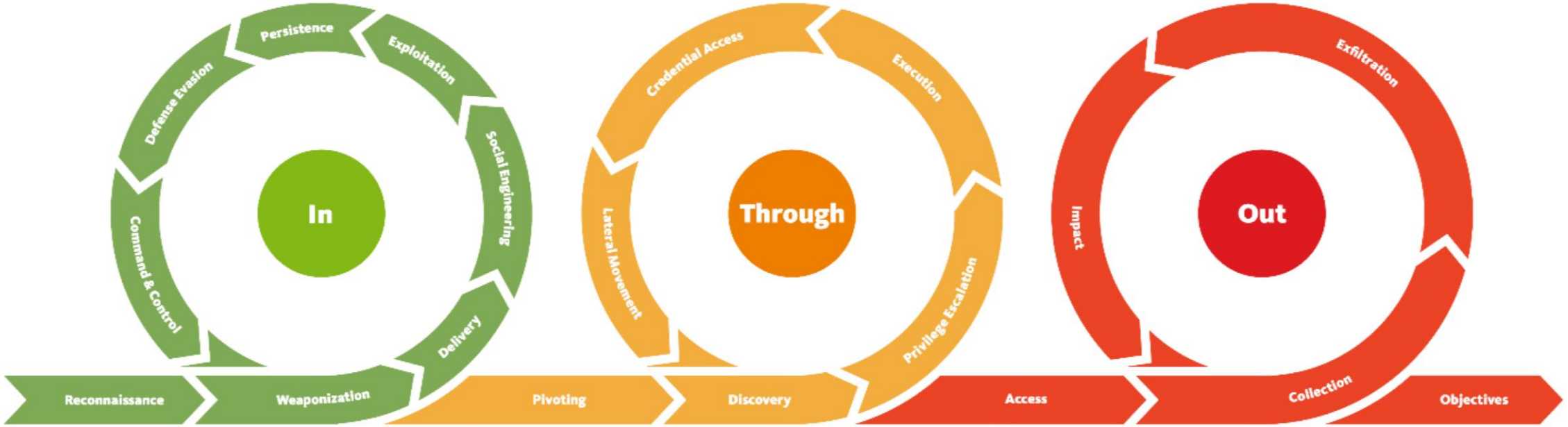
Less fragmented compared to last year

- Specialisation of services
- Lower bar to entry

Complexity remains

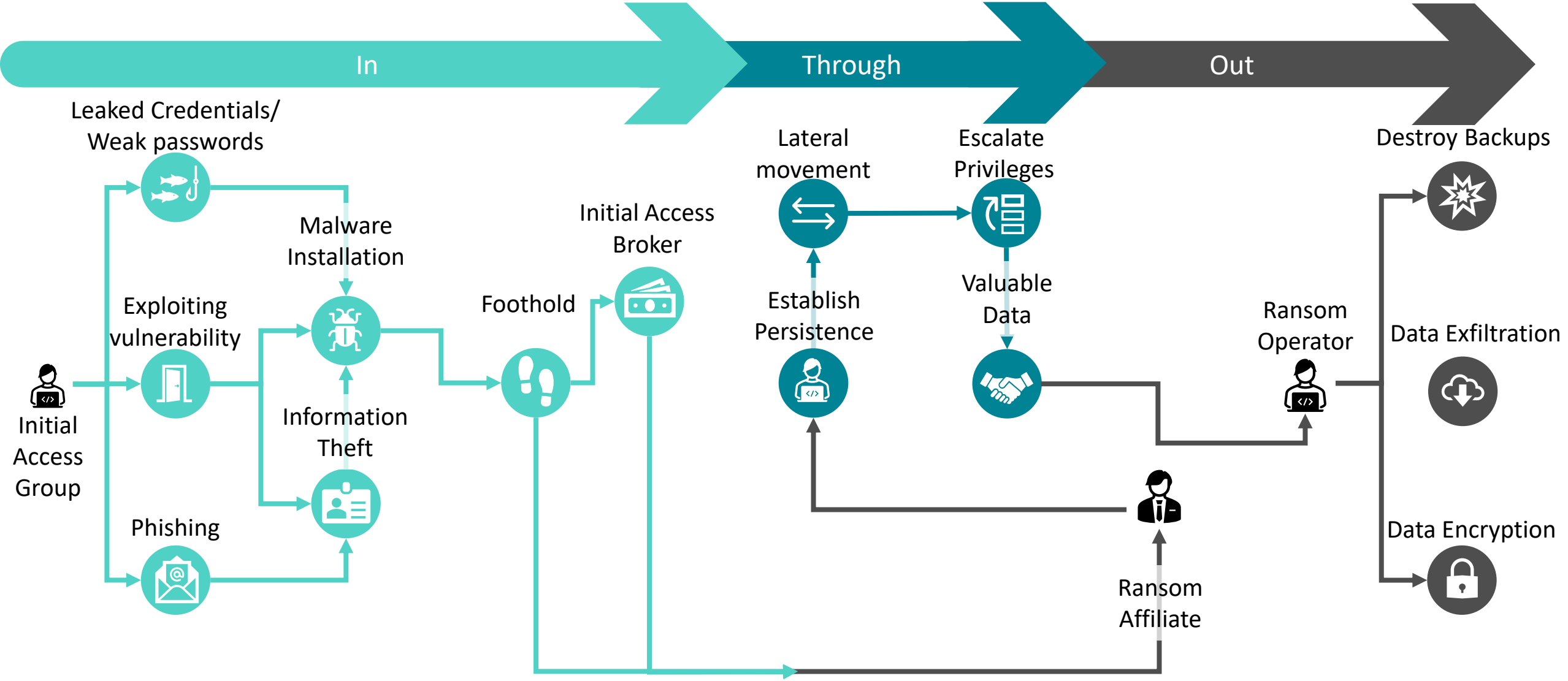
- Several OCGs involved in the same incident
- OCGs vary in capability and intent
- One “as-a-Service” shuts down, new ones pop up

Unified Kill Chain



- IN is where the initial access groups (IAGs) are found. The IAGs specialise in compromising victim networks using phishing campaigns, exploiting vulnerabilities, and using information stealers to gather information about the infected endpoint and network.
- THROUGH is also called “pivoting”, where TAs will try to establish a foothold. The TAs start moving across the victim network to identify the “crown jewels” and work on gaining access to necessary accounts and servers.
- OUT can be viewed as the “actions on objective” of the campaign, where the TAs will try to meet their campaign objectives. The purpose could be monetary gain, stealing data or information, or making data unavailable.

The OCG Ecosystem → Ransom (via affiliate)



OCGs and Ransom

Ransom Activities

- Increase in Ransom incidents world-wide
- No observations of ransom incidents in the financial sector in the Nordics this past year

Top initial access methods:

- Phishing
- Exploiting vulnerabilities in RDP and VPN
- Use of stolen credentials

Ecosystem

- Shift towards less encryption and just exfiltration

Supply Chain

Supply Chain Activities

- Observed multiple notable supply chain attacks, such as MOVEit and 3CX world-wide
- No Nordic financial institutions were seriously affected

Changes

- NFCERT has observed an increased focus by OCGs towards the supply chain and use of zero-days
- NFCERT has observed multiple instances where suspected state-sponsored actors have targeted the victim through its supply chain and gotten access to government infrastructure and others

Nation-States

2023

- Unchanged focus
- Nation States vary in capability and motivation
- The Nordics are not untouched
- Cooperation with OCGs

2024

- Several point towards elections
- Tensions in the geopolitical landscape

Financial Sector

- Dependencies on third parties and other sectors
- Not the most targeted sector

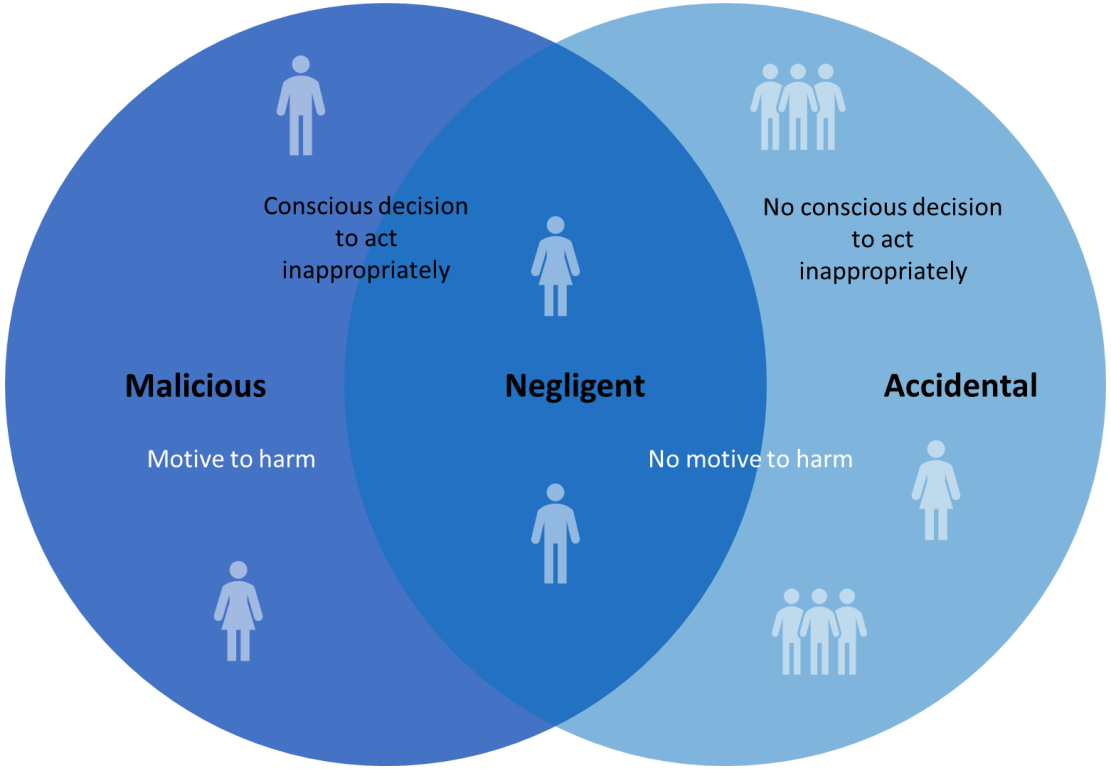
Insiders

Insider Activities

- Observed numerous low-impact and low-severity Insider incidents in 2023 that resulted in the loss of data and/or money
- Most often detected during the final weeks of employment

Changes

- OCGs, ransom operators and Nation-States have attempted to recruit malicious Insiders in 2023
- However, this has not been observed in the Nordics



Hackers

Hackers' capability

- Varying experience and tools
- Lower sophistication

Advancements in large language models (LLM)

- Speculations around lowered threshold for entry-level hackers

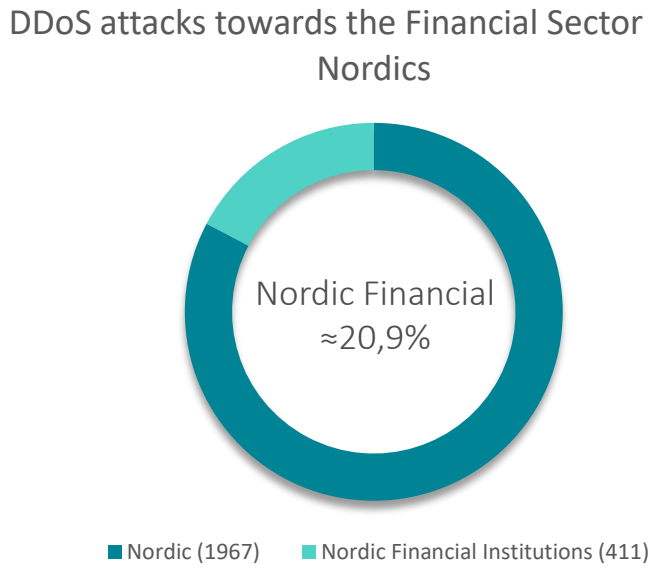
Hacktivists

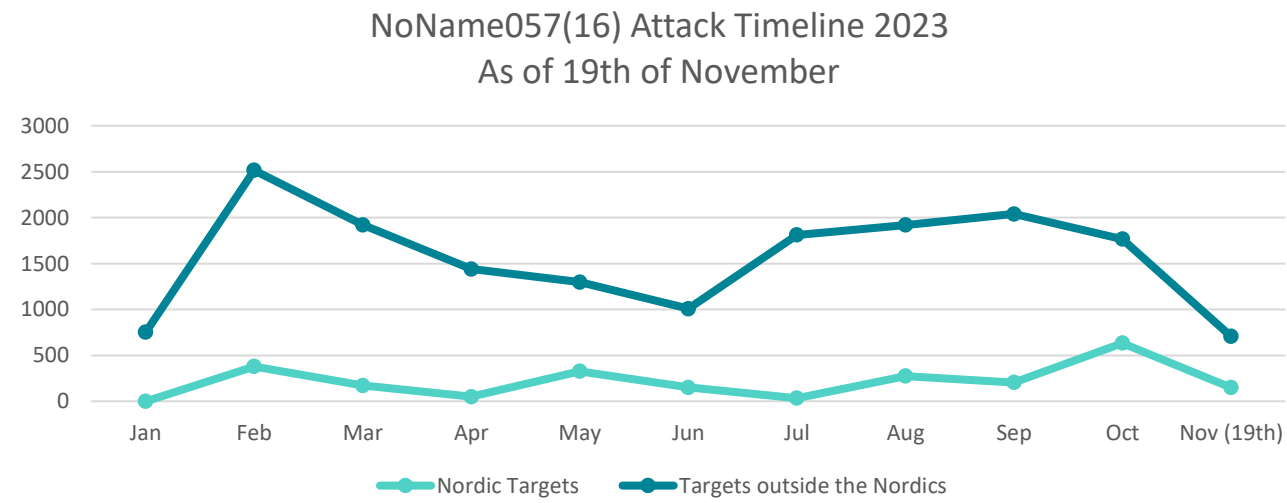
Hacktivists' capabilities and targeting

- Multiple groups
- Varying reasons, equal motivation
- Temporary unavailability

Observations in the Nordics

- All Nordic countries attacked
- No major consequences
- The financial sector is targeted among other sectors





Questions?

We welcome your questions and feedback!

post@nfcert.org
www.nfcert.org