Nordic Financial CERT
By members, for members

2025

Cyber Threat Landscape

for the Nordic Financial Sector

TLP:CLEAR

Introduction by The General Manager

This is the second edition of our public Cyber Threat Landscape (CTL) report, designed to provide a clear, high-level understanding of Nordic financial entities' current cyber threat environment. With the EU Digital Operational Resilience Act (DORA) now in effect from January, this report can help inform financial institution employees who need to have a high-level non-technical understanding of the current cyber threat to their institution and the sector. DORA reinforces the need for resilience, preparedness, and coordinated responses to cyber threats, making intelligence-sharing and collaboration even more critical.

Another goal for this report is to promote open sharing on cyber threats and incidents and to give the industry a public and relevant cyber threat picture anchored on a solid, well-documented basis.

Cyber resilience cannot be built in isolation; it relies on trusted partnerships and timely intelligence. Our reports are the result of close collaboration with our members, with contributions from Nordic government entities and TIBER Cyber Teams (TCTs). The reports are examples of how sharing and collaboration produce results greater than the sum of their parts. They also show the value of having a common, authoritative understanding of the cyber threat across the financial sector – including public/private.

Major geopolitical events, including wars in Ukraine and the Middle East, rising tensions in the Taiwan Strait, and a looming global trade war, have shaped the threat landscape so far in 2025. These factors directly influence the Nordic financial sector's cyber threat landscape. Threat actors, including Nation-States, cybercriminal organisations, and Hacktivist groups, are adapting their tactics, and financial institutions must stay ahead of these evolving threats.

We hope this report contributes to your understanding of the threat landscape towards the Nordic financial sector. Please let us know if you have comments, questions, or suggestions for improvement.

> "The cyber threat level facing the Nordic financial sector remains high but stable."
>
> *NFCERT's Generic Threat Landscape 2025 Report*

Morten Tandle
General Manager
Nordic Financial CERT

Contents

Forecast 2025

HIGHER IMPORTANCE

MEDIUM IMPORTANCE

Organised Crime Groups

Collaborative efforts

Organised Crime Groups (OCGs) continue to be the primary and most significant cyber threat to the Nordic financial sector. Their ability to develop new and improved ways for initial access makes this category as relevant as ever. NFCERT is confident that OCG's focus on breaching systems and extorting money from the victims will continue throughout 2025.

Nation-States

Cyber activity as means to an end

Although active in the Nordics, Nation-States have not affected the finance sector this past year. Nation-States will attempt to use their cyber capabilities to further their foreign interests. They have historically attempted to influence elections through cyber activity, but a significant impact on the Nordic financial industry is unlikely. Geopolitical events will remain the primary driver behind most Nation-State-sponsored cyber operations in 2025.

Supply Chain & Third Party

A Looming Threat

The Nordic financial sector is at risk due to its extensive and complex supply chain, as past infiltration attempts targeting third-party software and supply chains demonstrated. OCGs will continue to try leveraging trusted relationships with vendors, while Nation-State actors remain prepared to use supply-chain compromises for initial access in cyber espionage campaigns. Although unlikely to target the financial sector directly, these activities may still produce second- or third-order impacts.

DRIVERS FOR CHANGE - GEOPOLITICS

Hacktivism

Event-driven targeting

Hacktivism, through DDoS attacks, has become a part of the baseline for the Nordic financial industry, and this is expected to remain unchanged throughout 2025. Hacktivists will continue to target entities in the Nordics, with event-driven target selection. Effective countermeasures will keep attacks at low levels of impact.

Artificial intelligence (AI)

The New Kid on the Block

Artificial Intelligence (AI) is rapidly changing the way cybercriminals and security professionals operate. While AI-powered tools help strengthen defences, they are also misused by attackers to enhance their tactics. So far, AI has not fundamentally changed the threat landscape of cyber threats. However, understanding both the threats and benefits of AI is essential for making informed decisions about cybersecurity going forward.

Understanding Cyber Threats – The Who And The Why

The Nordic financial sector faces a complex cyber threat landscape that continues to evolve, where multiple actors operate with different motivations and levels of sophistication.

There are a multitude of different threat actors (TAs) and threat categories active in the Nordic threat landscape. The primary threat categories to the financial sector come from Organised Crime Groups (OCGs), Nation-State actors, Malicious Insiders, Hackers, and Hacktivists.

OCGs are still the most active threat. They are financially driven and have become more organised and specialised over the years. They use scalable “as-a-service” models, such as RaaS (ransom-as-a-service), allowing them to target multiple industries and countries simultaneously. Their attacks are opportunistic, highly adaptable, and focused on maximising profit.

Nation-State TAs represent a more strategic and well-resourced cyber threat. These actors engage in prolonged and sophisticated cyber operations aimed at espionage, disruption, and influence campaigns. Their activities are often driven by geopolitical interests, seeking to gain a competitive advantage through cyber-enabled intelligence gathering or direct interference.

Malicious Insiders pose a particularly difficult challenge, as they may already have authorised access to critical systems. These individuals may be motivated by financial gain,ideological beliefs, coercion, or personal grievances. Their actions can lead to espionage, fraud, sabotage, or cyberattacks. Both OCGs and Nation-State actors have been known to exploit Insiders to facilitate cyber operations.

Hackers, while varying in skill level and intent, do not pose a significant threat to the financial sector. Many act independently, testing their abilities or engaging in cybercrime on a smaller scale without long-term objectives. Their impact is often limited compared to more organised and resourced cybercriminal groups.

Hacktivists (Hackers + activists) can cause reputational damage and operational disruptions. However, they are not considered a major threat to systemic financial functions. Hacktivists focus on political or ideological causes, and their attacks are often highly visible and disruptive, further empowered by media attention. Still, Hacktivists have not had any lasting impact on the financial stability of the Nordic region.

	Likely to pose a significant threat	**Unlikely** to pose a significant threat
OCGs	●	
Nation-States	●	
Insiders	●	
Malicious Hackers and Hacktivists		●

Source: NFCERT’s Generic Threat Landscape 2025 Report

Organised Crime Groups (OCGs) – The Profit Chasers

OCGs function like highly efficient businesses, using sophisticated cyber operations to maximise financial gain. Their objective is to breach as many systems as possible, and their methods are constantly evolving, making them a persistent and adaptable threat to the financial sector.

OCGs use deceptive tactics such as phishing emails to trick employees into revealing sensitive information, exploiting security weaknesses in software, or purchasing access to already compromised networks. Once inside a system, OCGs work to establish long-term access, silently extracting valuable data or deploying ransomware to lock critical systems, forcing organisations to pay large sums to regain control.

The capabilities and resources of OCGs vary widely. Like legitimate businesses, they reinvest their profits to purchase malware, infrastructure, and illicit services from other cybercriminal groups, constantly refining their tactics. The most advanced OCGs collaborate with other cybercriminal groups to expand their reach and effectiveness.

The evolving international political landscape, including the Russo-Ukrainian war, tensions in the Middle East and Asia, and looming trade wars, have a direct impact on cybercriminal activities. Nation-States increasingly use OCGs, Insiders, and other criminal groups as proxies to carry out attacks, giving them plausible deniability while benefiting from the highly active cybercriminal ecosystem.

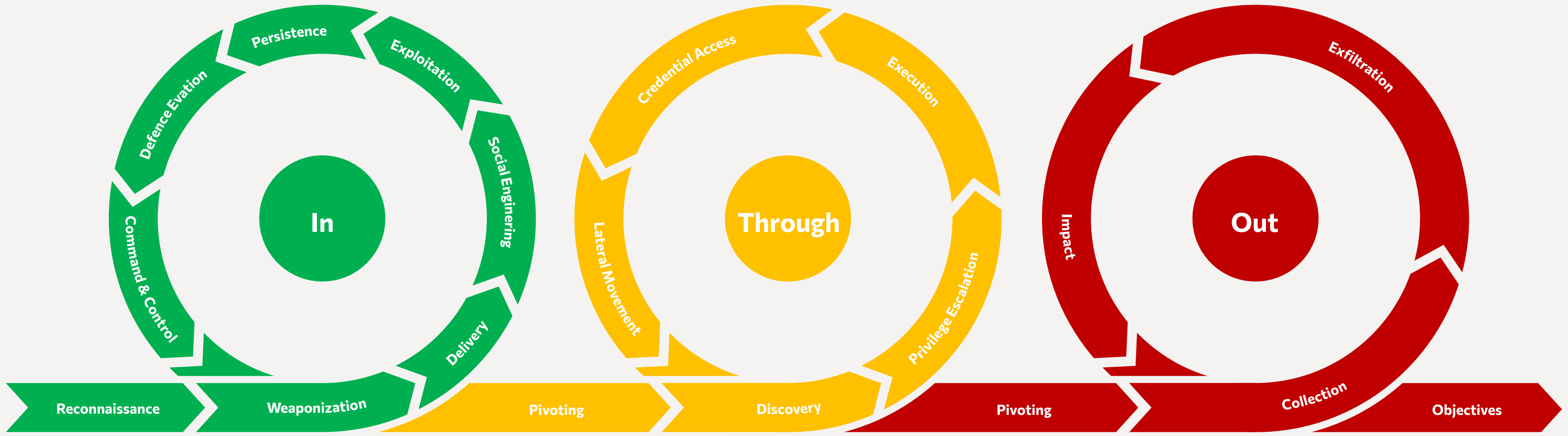


Figure 1 - https://www.unifiedkillchain.com

AI is also playing an increasing role. OCGs use AI to automate and improve phishing campaigns, identify new vulnerabilities, and evade detection. The rise of unrestricted Large Language Models (LLMs) has provided cybercriminals with powerful tools to generate more plausible content, launch more convincing phishing attacks, and even create simple malware. These AI-driven tools are readily available on underground markets, making cyber threats more sophisticated and difficult to counter.

The financial sector remains a prime target for OCGs, which constantly adapt to exploit new vulnerabilities. Understanding these threats is essential for organisations to strengthen their cybersecurity defences, mitigate risks, and prepare for an evolving cyber landscape where financial gain continues to drive cybercriminal activity.

Cybercriminal groups collaborate to target financial entities, and their attacks can be mapped into a structured process: breaking into systems (IN), moving through a network undetected (THROUGH), and carrying out their final objective (OUT). Understanding this process is key to strengthening cybersecurity defences.

First, attackers gain access **(in)** by exploiting weak points such as phishing emails, stolen passwords, or unpatched software. Some groups specialise in gaining entry and then selling access to others. With cybercrime tools now widely available for purchase, even less-experienced criminals can launch sophisticated attacks.

Once inside, attackers move **through** the system, searching for valuable data or control over critical operations. They disguise their activity to avoid detection, making it difficult to stop them before they reach their objective. The final stage **(out)** involves stealing sensitive data, deploying ransomware, or disrupting operations.

Ransom attacks remain one of the most serious cyber threats to the financial sector, with attacks becoming more sophisticated and coordinated. In the Nordic financial sector, cybercriminals attempt breaches regularly, constantly scanning for weaknesses. Many of these attacks are opportunistic, targeting multiple industries across different countries, but financial entities remain a key focus due to the potential for high payouts.

Nation-States are also leveraging cybercriminals to conduct attacks on their behalf. This blurs the line between traditional cybercrime and state-sponsored operations, making it harder to trace attacks and defend against them. Governments use these partnerships to achieve strategic goals while maintaining deniability.

Financial entities must adopt a proactive cybersecurity strategy to stay ahead of these threats. A strong defence requires intelligence-driven security, real-time monitoring, and the ability to detect and respond to threats quickly. Cyber resilience is not just about preventing attacks; it is about ensuring business continuity in an increasingly hostile digital environment.

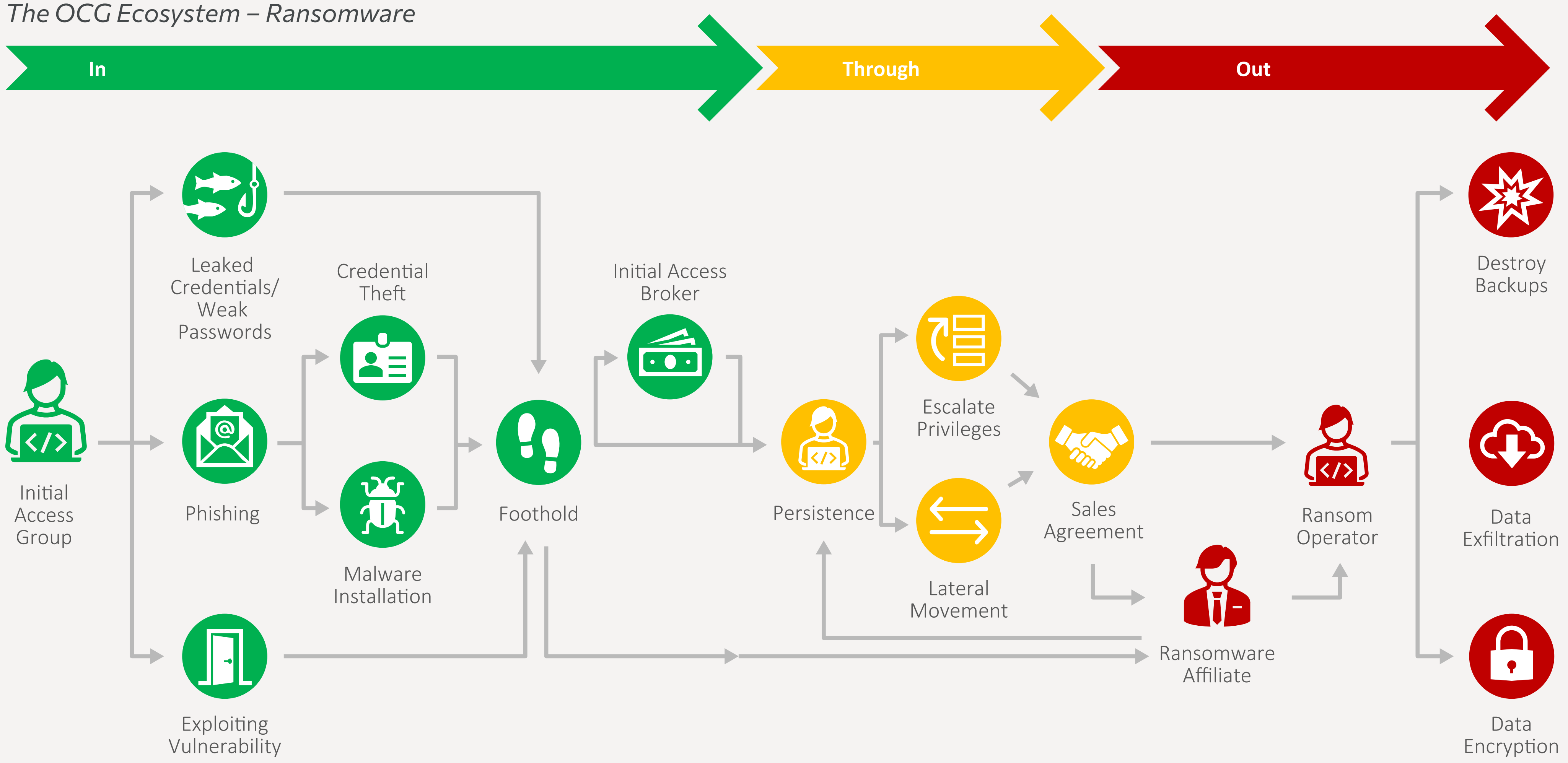
Ransom

Ransom is a type of extortion where cybercriminals steal a victim's data, and attackers threaten to leak, sell, or misuse stolen data unless their demands are met. These attacks often target sensitive personal, financial, or corporate information, pressuring victims into paying to avoid reputational or legal consequences.

Ransomware (Ransom + Software)

Ransomware is a specific type of ransom incident where cybercriminals use ransom software, hence the name, to encrypt a victim's data, making it inaccessible until a ransom is paid. This software-based attack locks critical files or systems, pressuring victims to pay for decryption and regain access to their data.

The OCG Ecosystem – Ransomware



Source: NFCERT's Generic Threat Landscape 2025 Report

Supply Chain & Third-Party Attacks – The Weak Link of The Chain

Cybercriminals are increasingly targeting supply chains as a direct path and third parties as an indirect path to their intended targets. Financial entities rely on a complex network of suppliers, making supply-chain and third-party security a growing global concern.

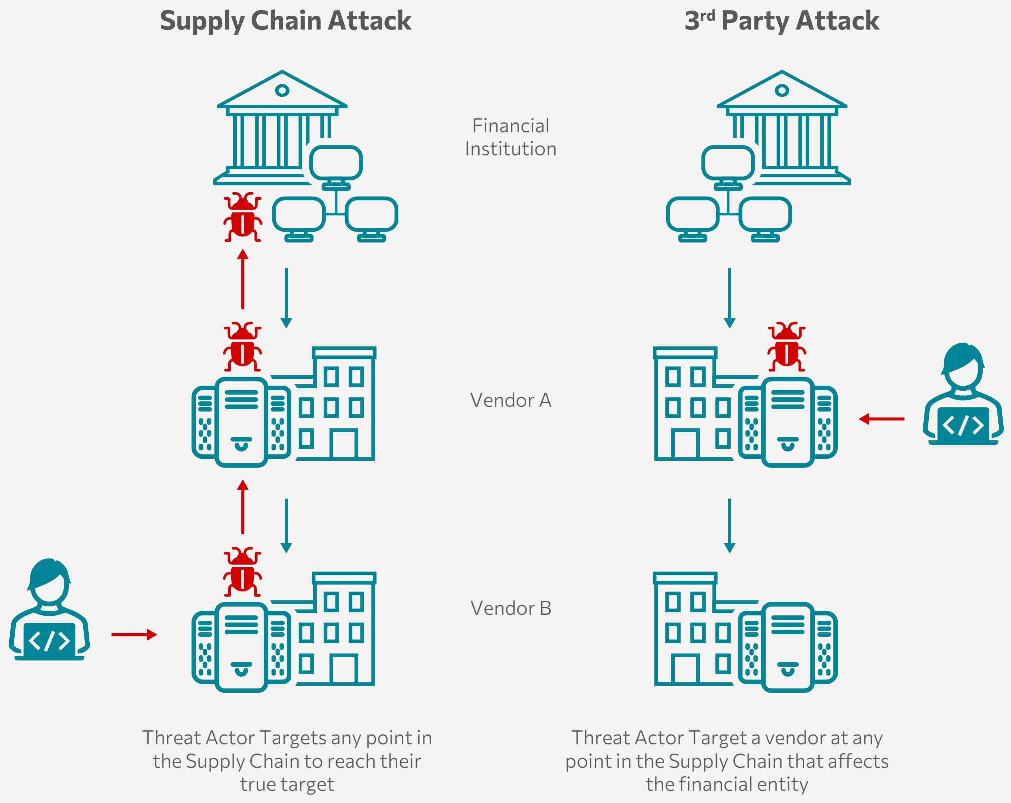
Recent cyberattacks on major global technology providers like Microsoft, Okta, Snowflake, and TietoEvry show the vulnerability of supply chains. These attacks have allowed Threat Actors to infiltrate organisations and government systems worldwide.

While major supply-chain attacks have not directly impacted the Nordic financial sector, there is an increasing likelihood that criminals and state-backed Hackers will attempt to exploit weaknesses in the supply chain. Financial entities may suffer data breaches, service disruptions, or cyber espionage if suppliers are compromised.

Cybercriminal groups and Nation-State actors have increasingly focused on supply-chain attacks, leveraging vulnerabilities in widely used software and services. While the Nordic financial sector has so far avoided major disruptions from these incidents, the increasing frequency of supply-chain attacks highlights the need for enhanced security measures.

Strengthening supply-chain security requires continuous monitoring, rigorous vendor assessments, and proactive risk management to prevent financial entities from becoming the next target.

Regulations such as DORA and NIS2 emphasise the importance of securing these third-party relationships to prevent disruptions and data breaches.


Supply Chain Attack
3rd Party Attack
Financial Institution
Vendor A
Vendor B
Threat Actor Targets any point in the Supply Chain to reach their true target
Threat Actor Target a vendor at any point in the Supply Chain that affects the financial entity

Source: NFCERT's Generic Threat Landscape 2025 Report

Supply Chain Attack

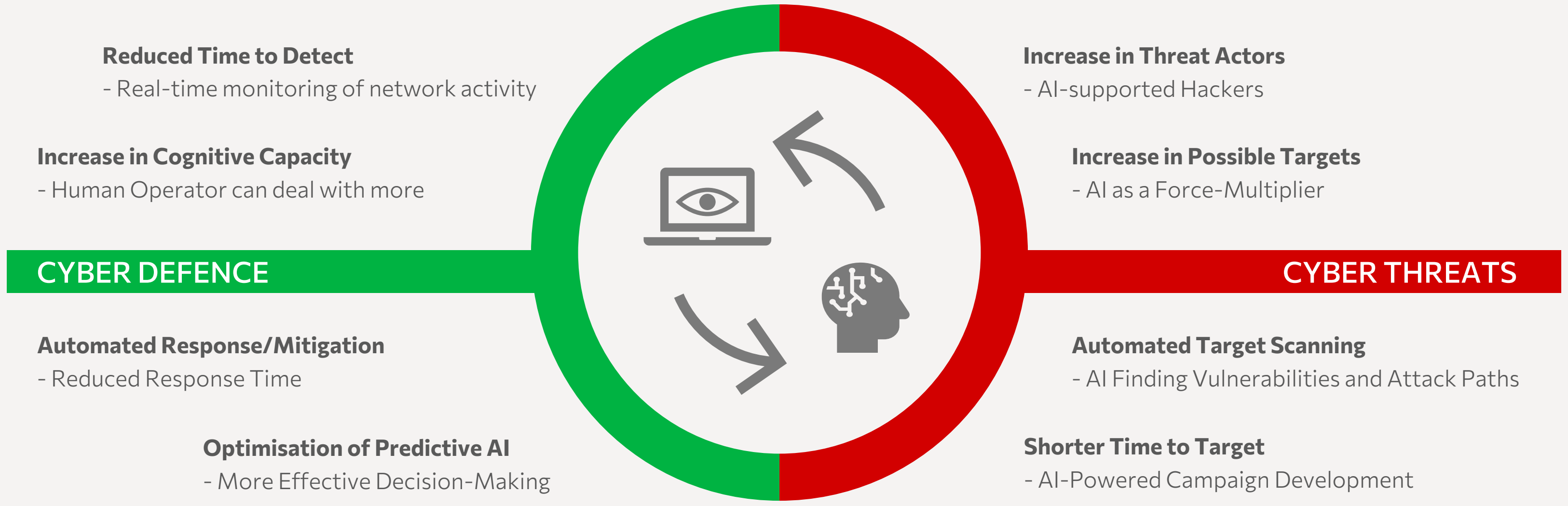
A supply-chain attack occurs when a threat actor compromises your supplier as a means to infiltrate your organisation, often bypassing traditional security controls. This is especially dangerous when attackers exploit trusted software or service providers that financial entities depend on to operate critical systems and manage sensitive data.

3rd Party Breach

A third-party breach is when a threat actor attacks a vendor, and you are inadvertently part of the compromise. These attacks can occur at any point in the supplier network, making detection and mitigation particularly challenging.

Artificial Intelligence – The New Kid on The Block

The rapid development of Artificial Intelligence (AI) and Large Language Models (LLMs) has led cybercriminals to explore their use for malicious purposes. While these technologies are still evolving, threat actors are testing AI to improve the speed and effectiveness of their campaigns. However, AI is a tool, not a magic solution. Attackers and defenders use AI, but it does not currently replace human expertise.



Reduced Time to Detect
- Real-time monitoring of network activity

Increase in Cognitive Capacity
- Human Operator can deal with more

CYBER DEFENCE

Automated Response/Mitigation
- Reduced Response Time

Optimisation of Predictive AI
- More Effective Decision-Making

Increase in Threat Actors
- AI-supported Hackers

Increase in Possible Targets
- AI as a Force-Multiplier

CYBER THREATS

Automated Target Scanning
- AI Finding Vulnerabilities and Attack Paths

Shorter Time to Target
- AI-Powered Campaign Development

Source: NFCERT's Generic Threat Landscape 2025 Report

TAs use LLMs to generate realistic phishing content, create fake websites, develop malware, and automate parts of their attacks. AI tools also enable them to produce deepfake videos, images, and voices to enhance deception in social engineering schemes. Nation-State actors, including those from Russia, China, North Korea, and Iran, are actively experimenting with LLMs to refine their cyber tactics.

Despite these efforts, AI has not significantly increased the success rate of cyberattacks. While LLMs can assist in coding malware or developing botnets, they still require skilled human operators to execute attacks. Attackers use AI to enhance their speed and efficiency rather than fully automating cybercrime.

So far, AI has not fundamentally changed the landscape of cyber threats, but as the technology evolves, its impact on cybersecurity will continue to grow.

At the same time, AI is becoming a crucial tool for cybersecurity defence. Law enforcement and security teams are integrating AI into threat detection, monitoring, and response efforts. AI-powered security systems can automate real-time threat detection, accelerate response times, and improve overall resilience against cyber threats.

While defenders are working to stay ahead of cybercriminals in this evolving landscape, the long-term impact of AI on cybersecurity remains an ongoing discussion. The focus is on using AI to enhance defences while being mindful of the risks associated with over-reliance on automation.

Artificial Intelligence (AI)

AI can be thought of as computer systems and machines that reason, learn, and can perform tasks that typically require human intelligence, such as recognising patterns, making decisions, and automating processes.

Large Language Models (LLMs)

LLMs are a subset of AI, and there are many LLMs, such as ChatGPT, Grok, Gemini, Perplexity, etc. LLMs are large deep-learning models pre-trained on vast amounts of data to recognise, translate, predict, or generate text. They are useful for digesting, summarising, and creating content across many industries, including cyber.

Nation-States – Cyber Attacks Serving Foreign Interests

Cyber activities by **Nation-State** actors, i.e. government-backed hacking groups, are expected to be consistent with each Nation's stated geopolitical ambitions, with operations and focus primarily outside the Nordic finance sector. Nation-State actors' focus and activity levels could shift with little to no warning due to alterations in the current geopolitical landscape.

2024, has been marked by global elections and conflicts across multiple regions, shaping the cyber threat landscape. Nation-State actors have largely focused their efforts outside the Nordic financial sector. However, a foreign state allegedly targeted one financial entity with offices abroad. This incident highlights that the financial sector is not immune to cyber threats, as Nation-States use cyber operations to gather intelligence, disrupt critical systems, and create uncertainty. In 2024, Nation-State groups continued using criminal tactics and outsourcing operations to private entities. Nation-State actors were also exploiting employees as Insider threats, often recruiting through digital platforms.

In 2025, elections will be held in multiple Nordic countries, with parliament elections in Norway and local elections in Denmark. Although Nation-State-sponsored cyber activity has historically been tied to elections, it has not significantly impacted the Nordic financial industry. Geopolitical events could trigger sanctions and other diplomatic events, which could increase cyber espionage and influence campaigns. Even if Nation-State actors do not directly target Nordic financial entities, they actively go after industries connected to finance, such as cloud and internet providers and the energy sector. A cyberattack on one of these related sectors could create indirect risks for reduced financial stability. The level of geopolitical tension in 2025 will play a key role in shaping the cyber threat landscape.

The most relevant Nation-State actors are covered in detail on the following page.

Who's Targeting the Nordics?

According to Nordic secret services, Russian and Chinese cyber groups have long targeted Nordic entities for espionage, mapping future cyberattack targets, stealing data, and gaining policy insights. While the primary focus has been government and defense, finance remains indirectly at risk.

Why This Matters

The Nordic financial sector is not a primary target today, but its dependencies on other industries make it vulnerable. As geopolitical tensions evolve, staying informed is key to managing cyber risks in 2025 and beyond.

Russia

A Continuous Cyber Threat

Russia continues to prove a significant cyber threat globally, where the usage of cyber activities is an intrinsic element of the Russian doctrine. Although Moscow's usage of cyber activities has been focused on Ukraine since 2022, Russia has slowly expanded its scope with cyber activities outside Ukraine. The war has caused a break with the West, and the NATO expansion in the Nordics reinforces the focus on the High North as the political and geographical buffer against NATO.

Russian Advanced Persistent Threats (APTs) increasingly leverage commodity malware and appear to have outsourced some cyberespionage operations to Organised Crime Groups or used their Malware-as-a-Service. Russia has adapted as organisations modernise their systems and transition to cloud-based infrastructure. Russian APTs have moved beyond their traditional means of initial access, such as exploiting software vulnerabilities in an on-premises network and instead target the cloud services themselves

China

The Most Active And Persistent

Western Intelligence agencies continue to perceive China as the most active and persistent cyber threat, with the highest number of Advanced Persistent Threat (APT) groups. China's holistic approach to cyber continues and their actions emphasise the absence of a hard line between the public and private sectors as a deliberate strategy to strengthen Beijing's economic and political power. Recent cyber operations show a high risk appetite.

No activity towards the Nordic financial industry has been observed.

China's cyber capabilities are reportedly more extensive than those of every other major Nation-State combined. Their APTs engaged in malicious cyber activities to pursue national interests by infiltrating critical infrastructure networks and cloud services.

North Korea

Driven By Economic And Technological Motives

North Korea constitutes a cyber threat most often driven by economic motives. Their offensive cyber program has matured and become sophisticated and agile, able to target the financial and Information Technology sectors to conduct software supply attacks. North Korea has cooperated with cybercriminals, such as the Play Ransom group.

North Korean APTs primarily leverage spear phishing and phishing for initial access. They have sometimes used supply-chain compromises and trojanised software installers. A noteworthy trend has been North Korean Threat Actors' (TAs) adaptation and abuse of popular cloud Services.

North Korean APTs use several approaches in their cyber operations, including but not limited to generating malware, exploiting zero-days, and leveraging North Korean Insider' access to enable cyber intrusions.

Iran

A Reactive Cyber Threat

Iran's willingness to conduct cyber operations has continued in 2024. Although assessed as opportunistic in the attacks towards Israeli targets, Teheran's use of cyber activities has primarily been reactive. Beyond cyber activities related to regional objectives, Iranian Nation-State TAs have sought financial gain in some of their cyber operations. Ransomware attacks attributed to Iran were designed to appear financially motivated but were predominantly destructive.

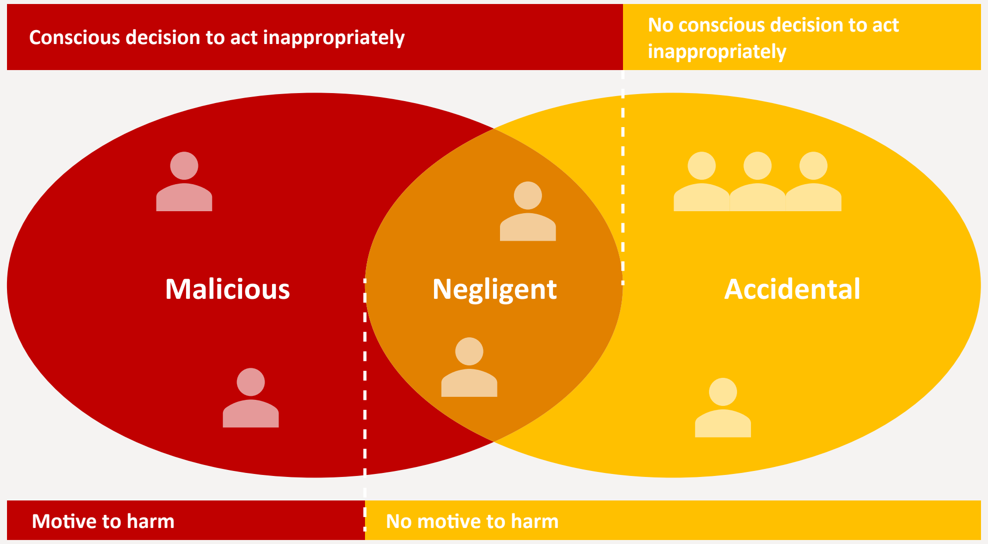
The Nordics is not a region of particular interest to Iranian APTs. However, reporting from Nordic security services indicates that Iran's focus could change if individuals already targeted by Iran travel to, or are located in, the Nordics or if the Nordic countries' policies are perceived as hostile towards the regime. For example, Iran has been active against Iranian diaspora in the Nordics in 2024.

Insider Threats – The Human Piece of The Puzzle

Malicious Insiders can pose a significant threat to financial entities, as individuals with access to critical systems and information can exploit their position for malicious purposes. While some Insiders unintentionally create security risks through negligence or mistakes, the most serious threat comes from **malicious** Insiders, i.e. those who intentionally misuse their access for personal gain or external influence.

Malicious Insiders deliberately steal, manipulate, or destroy data, intellectual property, and/or financial assets. They may also provide system access to external cybercriminals or foreign entities. Unlike accidental security breaches, these individuals have the knowledge, motivation, and opportunity to cause significant damage. Financial entities are particularly vulnerable because Insiders understand internal security measures and can bypass controls designed to prevent external threats.

Criminal groups and foreign intelligence agencies also attempt to recruit Insiders by offering financial incentives, job opportunities, or through coercion. In some cases, Insiders actively seek to sell their access to external threat actors.


Conscious decision to act inappropriately
No conscious decision to act inappropriately
Malicious
Negligent
Accidental
Motive to harm
No motive to harm

Source: NFCERT's Generic Threat Landscape 2025 Report

The Nordic financial sector has experienced a rise in Insider-related incidents, though most have been low-impact cases resulting in data or financial loss. While there is no confirmed evidence of Organised Crime Groups, ransomware operators, or Nation-States directly recruiting Insiders in the Nordic financial sector, there have been attempts to gather sensitive information through professional networking platforms.

Malicious Insiders' motivations vary but often fall under one of four motivations (MICE): greed or financial set-back (Money), ideological misalignment and differences in opinion on topics of interest (Ideology), forced by a third party (Coercion), or workplace conflict, personal grievances or loss of trust in management (Ego).

Addressing Insider threats requires financial entities to strengthen monitoring and access controls, implement early warning systems, and foster a workplace culture that encourages reporting suspicious behaviour. As the financial landscape evolves, organisations must remain vigilant against external cyber threats and those from within.

Malicious Insiders remain a threat to Nordic financial entities due to their ability to bypass internal controls. Sophisticated Threat Actors and Nation-States continuously attempt to recruit Insiders to facilitate breaches. If Nation-States target the Nordic financial sector, it will be for espionage rather than destructive attacks.

Insider Threats

An Insider is any current or former employee, partner or contractor, including third parties, that has or used to have access to the organisation's digital assets, including personnel, facilities, information, equipment, networks, and systems, and may intentionally or unintentionally abuse this knowledge or access.

In our reporting, we focus on malicious Insiders, who may pose a more significant threat than negligent and accidental Insiders. For more, see the "threat activities by Insiders" section in the NFCERT 2025 GTL Report.

Malicious Insiders exploit their access to bypass security controls, often using simple techniques like data staging and exfiltration via removable media, email, or cloud storage.

Hackers And Hacktivists – Attacks with A Cause

Hackers is a term often used for all types of malicious cyber actors. However, in this report, they are individuals who hack with malicious intent and have a wide range of experience and tools. Although individual malicious hackers have been operating in the Nordics, there has not been any Hacker able to successfully impact the financial sector in the Nordics in 2024. Lone Hackers are not expected to pose a significant threat towards the Nordic financial industry in 2025. However, they might have intentions to attack or partake in an attack.

Hacktivists' activity has been a key characteristic of the cyber threat landscape in the Nordic financial sector in 2024. Although high in volume, there has been limited impact. The sheer volume of incidents and, perhaps even more so, the heightened media attention has contributed to the attention and unfounded fear surrounding these DDoS attacks. However, despite the media's attention and some DDoS attacks that have caused downtime in the Nordic financial sector, Hacktivists have predominantly failed to achieve any significant impact on the stability of financial services.

Cyber activities by Hacktivist groups towards the Nordic financial sector have been exclusively DDoS attacks. There have been other claims, such as alleged data leaks, but these claims have been disproved. In most instances from the past two years, Hacktivists' DDoS attacks towards the Nordic financial sector have been reported as mere nuisances without significant operational impact.

In 2024, NFCERT has tracked 46 different Hacktivist groups known to target the Nordics, doubling since 2023. However, the observed activities in 2024 showed a 52% decline compared to 2023. I.e., although the number of groups has risen, the number of serious attacks has declined.

The different Hacktivist groups operating in the Nordics can generally be divided into two clusters: one cluster supports a pro-Russian narrative, and the other cluster supports a pro-Palestinian and pro-Islamic narrative. There have also been multiple Hacktivist attacks not attributed to any Hacktivist group in 2024.

1. Reconnaissance
Identifying and selecting the target webservice. Supporters and sponsors may also suggest targets.

2. Target distribution
Designate and distribute the target to followers.

3. Attack
Overwhelming amount of network traffic generated towards the targeted webservice.

4. Impact
The targeted webservice is rendered unavailable for the duration of the attack or until mitigation is in place.

5. Propaganda
The hacktivist group post evidence of a successful attack through a screenshot of the unavailable service and/or a link to a website checking availability

Based on Blueprint for attacks used by pro-Russian activists in Centre For Cyber Security Denmark, "The Cyber Threat Against Denmark, May 2023".

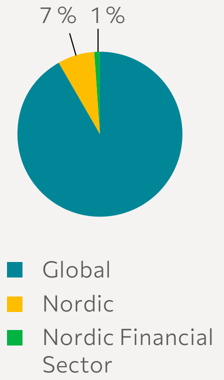
11

Groups active towards entities in the Nordics in 2024 registered

Registered DDoS Attacks – 2024

25 927

Attacks total



Hacktivism

Hacktivists, a combination of Hackers and activists, are individuals or groups motivated by political agendas and convey their political message using various types of cyber attacks, such as Distributed Denial of Service (DDoS) attacks.

What is DDoS?

A Distributed Denial-of-Service (DDoS) attack is a malicious action that disrupts the normal flow of traffic to a targeted server, network, or service by overwhelming the target or the surrounding infrastructure with a flood of traffic.

The Report – Foundation And Background

Nordic Financial CERT is a nonprofit organisation governed and paid for by its members in the Nordic financial industry. It aims to be the central sharing hub, connecting all the local stakeholders in the Nordic countries, including law enforcement, CERTs and others.

The purpose of Nordic Financial CERT is to strengthen the Nordic financial industry's resilience to cyber-attacks by enabling Nordic financial institutions to respond rapidly and efficiently to cybersecurity threats and online crime. As a collaborative initiative, it allows members to work together when handling cyber-attacks and crime, sharing information and responding to threats in a coordinated manner.

This report is one of the outcomes of such collaboration.
The report you are holding summarises our Generic Threat Landscape (GTL) 2025 report published on December 1st, 2024, with 137 pages and 418 references. The GTL report is available to all members of the Nordic Financial CERT. The report features insight from the NFCERT's incidents, reports, and other knowledge gained from NFCERT forums, such as the Threat Intelligence Committee (TIC), Cyber Defence, and Anti-Fraud.

The report also builds on knowledge from members, vendors, partners, other sector CERTs across the Nordics, and security communities like FS-ISAC.

In addition, some of the contributions to this report are from government entities in the Nordics (National Cyber Security Centres (NCSC) and Defence and Police Intelligence). The information is verified, analysed, and evaluated by the NFCERT's Threat Analysis Cell (TAC) before being refined into this report.

Openly available publications and assessments from government sources align with our understanding of the cyber threat landscape. However, NFCERT has scoped and extended the analysis to address the Nordic financial sector specifically.

The following publications may be used as further reading

- **The Finnish Security Intelligence Service** (Suojelupoliisi, SUPO) – Yearbook
- **The Finnish Transport and Communications Agency** (TRAFICOM) i.e. NCSC-FI – Cyber Weather reports
- **Centre For Cyber Security (CFCS-DK)** – The Cyber Threat Against Denmark and The Cyber Threat Against the Financial Sector in Denmark
- **Swedish Security Service** (Säkerhetspolisen, SÄPO) – Yearbook
- **The Swedish Bankers' Association (Svenska Bankföreningen)** – Hotbildsbedömning för Sveriges banker
- **The Norwegian National Security Authority (Nasjonal Sikkerhetsmyndighet, NSM)** – Risiko
- **Norwegian Intelligence Service** (Forsvarets Etterretningstjeneste, NIS) – FOKUS
- **Norwegian Police Security Service (Politiets Sikkerhetstjeneste, PST)** – Nasjonal Trusselvurdering
- **Sector-focused reports** – Various reports from SektorCERT (DK), Helse CERT (NO), TeleCERT (NO and DK)
- **Microsoft** – Various reports, such as the Microsoft Digital Defense Report
- **Google** – Various reports, such as "cybersecurity forecast"

Nordic Financial CERT

post@nfcert.org
www.nfcert.org

Design: BRANDstasjonen 2025