Nordic Financial CERT

CYBER THREAT LANDSCAPE

for the Nordic Financial Sector 2026

TLP:CLEAR

Introduction by The **General Manager**

On behalf of the NFCERT team, I am honoured to present the 2026 edition of our Cyber Threat Landscape (CTL) report. This report reflects our commitment to strengthening the financial sector's collective resilience and underscores the enduring value of collaboration across our community.

The threat landscape continues to evolve. Geopolitical instability, rapid technological change, and an increasingly complex criminal ecosystem are reshaping the environment in which we operate. At the same time, regulatory expectations are intensifying, and the demands placed on our ability to defend and adapt have never been greater.

The financial sector stands at the centre of these converging dynamics. In such a context, partnership and intelligence sharing are not merely beneficial; they are essential. The role of NFCERT, the CTL, and our broader NFCERT community, vendors, and partners is therefore more critical than ever to sustaining trust and strengthening resilience.

Our purpose remains clear: to support informed decision-making, enhance collective defences, and contribute to a shared understanding of the threats that challenge our sector.

I believe that this report, and the Generic Threat Landscape (GTL) report on which the CTL is built, will serve as a valuable resource, offering insights that inform strategy, guide preparedness, and promote collaboration. Together, we continue to safeguard the integrity and stability of the financial sector in an increasingly uncertain world.

> Our purpose remains clear: to support informed decision-making, enhance collective defences, and contribute to a shared understanding of the threats that challenge our sector.

Morten Drægni
General Manager
Nordic Financial CERT

Contents

NFCERT Threat **landscape overview**

	HIGHER IMPORTANCE		MEDIUM IMPORTANCE	LOW IMPORTANCE
Threat Actors	 Organised Crime Groups An active and evolving ecosystem of threat actors that continuously launch high-volume and opportunistic campaigns.	 Nation-States Geopolitically driven cyber operations for intelligence, critical infrastructure access, and long-term strategic advantages.	 Insiders Malicious insiders may operate for their own reasons or aid criminal or Nation-State actors, driven by coercion or ideology.	 Hackers and Hacktivists Act on ideology or disruption, generating high activity but with minimal impact on Nordic financial stability.
Cross Strategic Threats	 Ransom Operations Remains a major global threat, with increasingly complex extortion tactics and growing indirect risks from third-party dependencies.	 Supply Chain & 3rd Party Heighten threats to financial stability, as criminal and Nation-State actors exploit shared platforms and vendor ecosystems.	 AI Threat actors increasingly exploit AI and LLMs across attack phases, enhancing efficiency, though with no noticeable change in capabilities.	 Post-Quantum Cryptography Threat actors increasingly adopt “harvest now, decrypt later” strategies, stealing encrypted data today for potential future quantum decryption.

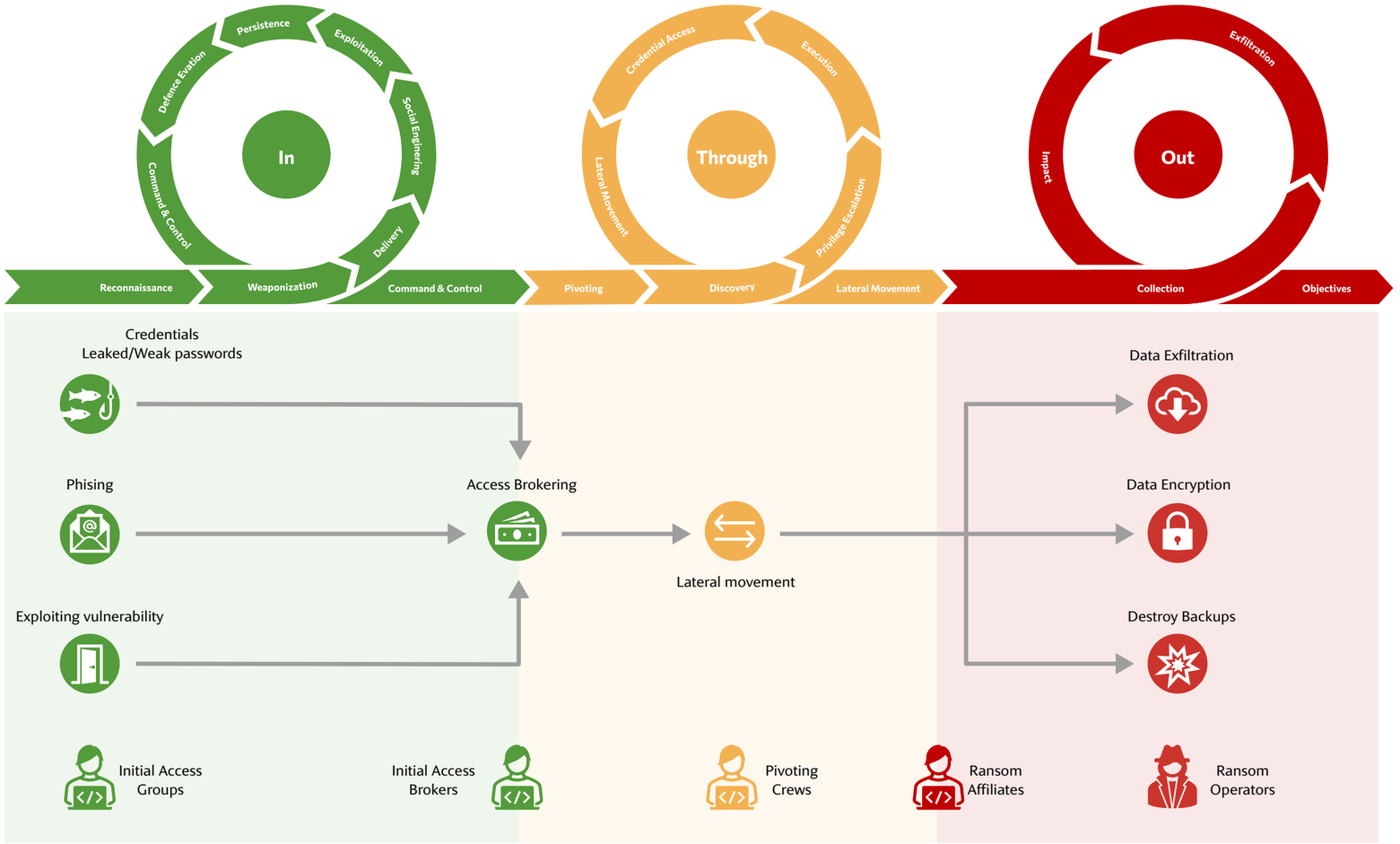
Organised Crime Groups (OCGs) – High-Volume and Opportunistic

OCGs function as profit-driven enterprises embedded in mature underground markets and remain one of the most significant financially motivated threats to the Nordic financial sector in 2026. Their main objective is to generate reliable revenue through credential theft, fraud, extortion and ransomware.

In 2025, activity has increasingly centred on exploiting systemic weaknesses across interconnected ecosystems. These activities are becoming standard components of criminal intrusion playbooks rather than extraordinary tradecraft.

OCGs operate through a highly specialised division of labour. Initial access groups and social engineering crews conduct phishing, vishing, and adversary-in-the-middle campaigns. These campaigns are increasingly enhanced by AI-enabled tooling that improves efficiency and scale, such as automated phishing content, multilingual translations, and voice impersonation. Initial access brokers feed the ecosystem with compromised systems and credentials, creating a scalable supply of ready-made footholds into breached systems. This vibrant ecosystem lowers barriers to entry, accelerates operations, and enables both low-skilled and advanced actors to collaborate efficiently.

The OCG Ecosystem – Ransomware.
Source: NFCERT's Generic Threat Landscape 2026 Report



Strategically, several trends shape the OCG threat landscape in 2025. First, identity-centric operations and infostealer ecosystems continue to increase the scale and speed of credential-driven intrusions, including into cloud-connected environments. Second, specialisation across the criminal value chain has made the ecosystem more resilient to disruption, such as law-enforcement operations or the disbandment of ransom groups. Third, geopolitical instability, including the continued impact of the Russo-Ukrainian war and tensions in the Middle East, contributes to increased collaboration between criminal and state-linked actors. Criminal infrastructure, Ransom-as-a-Service (RaaS) programmes, and access-broker networks are at times reused or leveraged by state-linked actors. These actors seek plausible deniability, complicating attribution and increasing the risk of spillover into European supply chains relied upon by Nordic financial entities.

From a Nordic perspective, OCG activity is primarily observed as high-volume, opportunistic campaigns involving phishing, credential harvesting, and infostealer infections. Supply-chain exposure is expected to remain the primary OCG pathway into the Nordic financial sector: compromise of European suppliers, IT service providers, and shared platforms can create downstream access into the sector.

Given the ecosystem-driven nature of OCG operations, even low-level footholds and accesses can escalate rapidly if resold or reused across criminal networks. Over time, expanding access markets could enable more selective campaigns by capable groups, although opportunistic activity will continue to dominate.

OCG ACTIVITY CAN BE UNDERSTOOD AS OPERATING IN, THROUGH AND OUT OF TARGETED ENVIRONMENTS:

In

Initial access is most commonly achieved by compromising credentials, using infostealers, exposing VPN or remote desktop services, compromising third parties, and exploiting unpatched vulnerabilities or misconfigured cloud services. Identity serves as the primary attack surface.

Through

After gaining initial access, actors will conduct reconnaissance, attempt to escalate privileges, and move laterally across the network using legitimate administrative tools and living-off-the-land techniques to reduce detection. Subsequently, access is assessed for value and sold or bought by various threat actors.

Out

Following these activities, monetisation follows. Access may be resold, data exfiltrated, fraud conducted, or ransomware deployed. Multi-layered extortion models increasingly combine encryption, data theft, and pressure tactics targeting executives, partners, or customers.

Nation-States and Geopolitics

Nation-State sponsored threat actors (TA) operate as instruments of government power. Their objective is long-term strategic advantage, such as intelligence collection, strategic positioning inside critical infrastructure, and political leverage. Their cyber operations follow geopolitical priorities rather than sector-specific motives.

While Nation-State actors as a category are assessed as high importance due to their capabilities and potential systemic impact, their relevance to the Nordic financial sector varies between states. Some actors pose a more direct intelligence or disruptive risk, while others, including partners and allies, are included because their operations can contribute to geopolitical escalation, retaliatory dynamics, or unintended spillover affecting shared financial infrastructure.

In 2025, Russia's war in Ukraine, China's strategic competition with Western states, instability in the Middle East, and North Korea's sanctions pressure drove sustained espionage and supply-chain compromise across Europe. Operations by the United States or Israel against Iranian networks may prompt retaliatory or opportunistic activity affecting Western infrastructure, including financial and payment systems.

Financial institutions were not primary targets, but they are part of the digital infrastructure these actors routinely access. These operations are deliberate and patient. Nation-State TAs exploit supply-chain or third-party vulnerabilities to gain access to critical systems, cloud platforms, identity providers, and widely used software.

Increasingly, Nation-State TAs blend techniques with criminal ecosystems, purchasing access from criminal brokers or blending activity within ransom operations and contractor ecosystems, masking their true intentions inside the organised crime ecosystem. This convergence complicates detection and potentially enables Nation-State campaigns to move through the same suppliers and third-party environments used by Nordic financial institutions.

For the Nordic financial sector, the primary threat from Nation-States is indirect. To the best of our knowledge, there has been no sustained targeting of the Nordic financial sector reported. Still, intrusions into these shared systems and service providers can create systemic disruption, data exposure, or loss of operational integrity.

Executives should therefore focus on the resilience of core financial functions, the integrity of identity and access systems, the concentration of critical suppliers, and the sector's ability to operate under degraded or contested digital conditions.

As geopolitical tensions shift, targeting priorities can change rapidly and without warning. The sector therefore operates in an environment where state-driven cyber activity remains persistent and capable of creating spillover effects into financial operations, even when our sector is not the intended target.

High Importance

Russia
China
North Korea

Medium Importance

USA
Israel
Iran

Russia

Conflict Without Borders

In 2026, Russia's cyber focus remains deeply tied to the war in Ukraine, shaping its operations and global posture. Beyond the battlefield, Russian groups continue probing NATO members, blending espionage and influence to test defences and gather intelligence. Their attention largely centres on government, defence, energy, and other critical infrastructure, while the financial sector is only indirectly exposed, often through suppliers, shared systems, or collateral impact.

Increasingly, Moscow leans on criminal networks, ransomware collectives, and hacktivist personas to mask state involvement, blurring the lines between espionage and crime. Destructive attacks have so far stayed within Ukraine's borders, but regional spillover remains a possibility if tensions rise.

The greatest challenge for finance lies not in direct attack, but in connectivity and common dependencies, the invisible links that tie institutions to wider geopolitical challenges.

China

The Long Game in Cyberspace

China's cyber strategy continues to focus on the long game, deliberate, and deeply integrated into its broader national ambitions. In 2026, its efforts will focus on espionage, intelligence collection, and maintaining digital footholds to ensure strategic advantage over time.

Operating through a state-wide network of governmental, industrial, and academic actors, China blends innovation and stealth. Its teams skillfully exploit vulnerabilities, infiltrate telecom infrastructure, and use sophisticated techniques to impersonate trusted users and move undetected across systems.

In the Nordics, attention centres on governments, research, and high-tech sectors rather than finance. Yet the interconnected nature of global operations means that Nordic financial institutions remain indirectly exposed. Various breaches by Chinese actors demonstrate that distance offers little protection when digital boundaries fade, and influence flows across networks and continents.

North Korea

Strategic Theft in Cyberspace

North Korea's cyber operations in 2026 will continue to merge financial ambition with state strategy. What began as regional covert espionage has evolved into an international revenue engine, funding the regime's weapons development through theft from crypto-currency exchanges.

Alongside financial theft, Pyongyang's focus on intelligence collection is widening, targeting defence, aerospace, diplomatic, and technology sectors across multiple continents. Sophisticated campaigns using "dream job" lures, modular malware, and supply-chain intrusions reveal a methodical pursuit of long-term access.

For the Nordics, direct targeting of financial institutions remains rare. Yet the region sits within a connected web of global operations where collateral exposure is always possible, through shared cloud services, digital suppliers, or foreign subsidiaries. North Korea's blend of espionage and economic exploitation underscores its being a persistent threat, albeit outside most financial institutions' focus area, crypto.

Iran

Echoes of Regional Tensions

In 2026, Iranian cyber operations will continue to mirror the instability of the Middle East. The conflict involving Israel, Hamas, and Iran fuels a steady stream of politically driven cyber activity targeting governments, militaries, and allies across the region. Strategic activities by Western governments will shape the abilities, activities, and capabilities of Iranian threat actors.

Beyond the immediate conflicts, Iran maintains an unclear digital presence, which is believed to focus on espionage and control, i.e., tracking dissidents, monitoring diaspora communities, and gathering intelligence across Europe. These operations often blend surveillance, credential theft, and mobile compromise into persistent, low-visibility campaigns.

Financially motivated activities remain secondary, sometimes overlapping with criminal ventures or moonlighting operators. For the Nordic financial sector, Iran's intent appears limited; however, indirect exposure remains possible through opportunistic attacks or shared infrastructure.

Insider Threats – The Trusted Access Enabler

Malicious insiders remain a low-frequency but high-impact threat to the Nordic financial sector and will continue to act primarily as enablers rather than autonomous disruptors. While most observed incidents in 2025 relate to account misuse and data-handling violations rather than systemic sabotage, insiders increasingly support organised crime groups and nation-state actors seeking trusted access to financial environments.

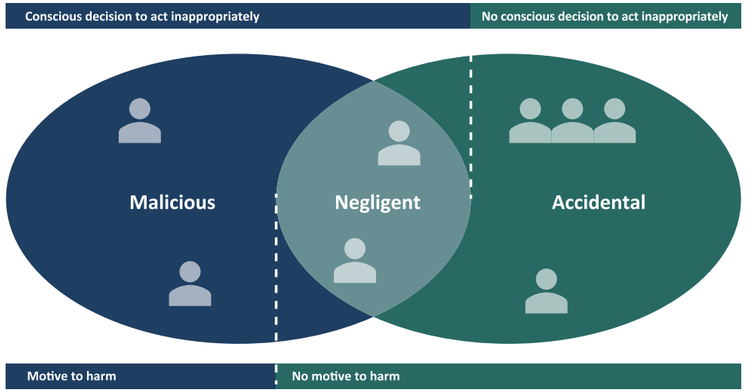
Malicious insiders can operate from any access tier. Privileged users pose the highest potential impact due to administrative rights and system knowledge. Regular employees may provide operational access or sensitive data if recruited, coerced, or ideologically motivated. Third parties, including contractors and vendors, represent the principal insider exposure due to variable governance and cross-organisational access.

In 2025, insider-enabled activity has primarily involved data theft, document staging and compression, unauthorised account access, and facilitation of broader cyber campaigns. Insider-enabled financial misconduct, including improper access to or manipulation of customer data or internal processes, is plausible but expected to be limited in scale. Identity compromise further amplifies exposure, as large-scale credential theft through infostealers blurs the boundary between external intrusion and insider activity.

Malicious insiders are leveraged as facilitators within broader criminal and state-linked ecosystems. It is plausible that cybercriminal groups will attempt targeted recruitment of Nordic financial employees, as observed on underground forums. Nation-State actors are also expected to exploit insider pathways, including through fraudulent hiring schemes and remote employment programmes designed to embed operatives within targeted organisations. Financial stress, grievances, coercion, and ideological alignment remain common motivators.

From a Nordic perspective, confirmed malicious insider cases remain limited, but recruitment attempts have been observed outside of the Nordics, including actors seeking insiders within financial entities to obtain sensitive customer information. The Nordic sector's high-trust environment, reliance on third-party service providers, and extensive remote access models increase structural exposure.

While insider incidents are less frequent than opportunistic external attacks, their potential impact, particularly when involving privileged or third-party access, remains disproportionately high and strategically significant.



Source: NFCERT's Generic Threat Landscape 2026 Report

Definition

An insider is any current or former employee, contractor, partner or third party with authorised access to an organisation's systems, data or facilities. Insiders may be:

Malicious – deliberately misuse access to cause harm or assist external actors.

Negligent – knowingly bypass security rules without intent to harm.

Accidental – unintentionally cause compromise through error or social engineering.

This report focuses specifically on malicious insiders, as they represent the most targeted and strategically relevant insider risk.

Hackers And Hacktivists - Geopolitical Signalling

Hackers is a term often used broadly, but in this report, it refers to lone actors or small groups acting with malicious intent without the structure or resources of organised crime or state-aligned actors. Enabled by widely available attack tools and services, even low-skilled individuals can conduct phishing, account compromise, or basic exploitation at scale. Although such actors remain active in the Nordics, no lone hacker has had a significant direct impact on the Nordic financial sector over the past year, and they are not expected to pose a major strategic threat in 2025.

Hacktivist activity remains a visible but largely disruptive element of the Nordic threat landscape, closely tied to geopolitical events and amplified by media attention. For the Nordic financial sector, impact has generally been limited to short-lived DDoS incidents and nuisance-level disruption rather than lasting compromise or financial damage. They are often synchronised with diplomatic developments or security policy decisions to maximise symbolic effect.

Two main clusters operate against Nordic interests: one aligned with pro-Russian narratives, particularly active since the invasion of Ukraine, and one aligned with pro-Palestinian and pro-Islamic causes. Over the past year, activity affecting Nordic financial institutions has primarily been linked to the former, with minimal impact from the latter. A notable development is opportunistic probing of internet-exposed operational technology (OT) services during geopolitical spikes. Although such cases remain rare, increasing use of automated scanning and denial of service (DoS) tools lowers the threshold for visibility-driven attacks against exposed systems.

1. Target Selection (In):
Administrators identify politically symbolic or strategically visible web services, often linked to government policy, defence support or financial infrastructure.

2. Target Distribution (In):
Selected targets are distributed via Telegram and dedicated platforms to a volunteer network using the DDoSia toolkit.

3. Attack Execution (Through):
Participants generate coordinated traffic towards the designated service, typically using automated scripts designed for rapid mobilisation rather than technical sophistication.

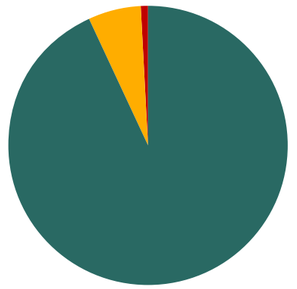
4. Service Disruption (Out):
The targeted website or online service experiences temporary degradation or outage until traffic subsides or mitigation measures take effect.

5. Amplification & Narrative (Out):
The group publishes screenshots, uptime-check links or performance graphs as proof-of-impact, framing the disruption within a broader geopolitical narrative.

Source: "An Analysis of NoName057(16)" by SocRadar and the Unified Killchain Framework

Registered DDOS attacks – 2025

21 290
Total attacks



Hacktivism

Hacktivism refers to cyber operations conducted by individuals or collectives to advance political, ideological, social or religious causes. Activities are typically overt and visibility-driven, aiming to generate attention, signal support or undermine confidence rather than to achieve sustained covert access or financial gain.

What is DDoS?

A Distributed Denial-of-Service (DDoS) attack is a malicious attempt to disrupt the normal availability of a targeted server, network or online service by overwhelming it with traffic from multiple sources, thereby degrading or temporarily blocking access for legitimate users.

Future Cross Strategic Threats

Ransom Operations

The ransom ecosystem continues to evolve as a sophisticated criminal enterprise. In 2026, its resilience will continue to be powered by lucrative Ransom-as-a-Service models, specialist roles, and an ability to rebound quickly from law-enforcement disruption.

Most intrusions still begin with stolen credentials, compromised endpoints, or phishing campaigns that exploit human trust. Once inside, attackers use one of two pathways: exfiltrating critical data and threatening to publish it for ransom, or exfiltrating the data, encrypting it, and then demanding a ransom to provide the decryption key, shifting the impact from operational shutdowns to reputational and possibly regulatory consequences.

Across the Nordics, small and medium-sized organisations remain frequent victims. In the coming year, this may include service providers supporting the financial sector. For financial institutions, the greater threat lies in indirect exposure through vendors and shared platforms, where a single compromise can reverberate across networks.

Supply-Chain Attacks and Third-Party Breaches

The deep reliance on third-party vendors, Software-as-a-Service (SaaS) providers, and open-source components continues to create hidden pathways for intrusion. The interconnected nature of modern finance ensures that one weak link can expose many. This is why supply-chain compromises and third-party data breaches remain one of the most significant challenges facing the financial sector in 2026.

Criminal groups now specialise in exploiting these dependencies, using them for scalable access or selling entry points to others in thriving underground markets. Nation-state actors follow a similar playbook, blending espionage with stealth by infiltrating trusted vendors or co-opting criminal infrastructure.

Even minor vulnerabilities in public code repositories can cascade through entire ecosystems, turning routine updates into potential breaches. Attacks rarely begin with a direct strike on financial institutions; instead, they ripple outward from upstream breaches affecting service providers and shared technology platforms.

Large Language Models (LLMs) and AI

In 2026. LLMs and AI will further transform the cyber threat landscape. Threat actors use LLMs to accelerate vulnerability discovery, phishing, and automation across attacks. OCGs rely on commercial models, while Nation-States deploy advanced systems.

Beyond technical use, AI-driven deepfakes, mis- and disinformation amplify deception and uncertainties, eroding public trust and posing growing challenges to resilience and reputation.

Post-Quantum Cryptography (PQC)

The rise of quantum computing is already influencing how adversaries operate. Future breakthroughs could unlock today's encrypted data; they are stealing information now to decrypt later.

Nation-states and criminals exploit delays in quantum-safe encryption, leveraging legacy vulnerabilities across connected systems. The issue lies in gradual protection erosion, making post-quantum resilience a long, uneven test of preparedness and digital ecosystem trust.

NFCERT and CTL – Foundation And Background

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

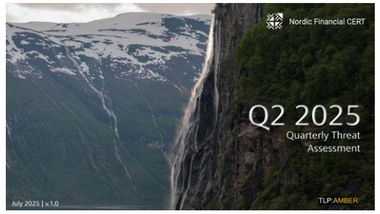
The purpose of Nordic Financial CERT is to strengthen the Nordic financial industry's resilience to cyber-attacks by enabling Nordic financial entities to respond rapidly and efficiently to cybersecurity threats and financial crime prevention. NFCERT is a collaborative community that enables members to work together to address cyber-attacks and crime, share information, and respond 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) 2026 report, published on December 1st, 2025, with 140+ pages and 400+ references. The GTL report is available to all members of the Nordic Financial CERT.

The CTL report features insights from incidents, reports, and other knowledge gained from various internal and external sources. This includes NFCERT forums such as the Threat Intelligence Committee (TIC), Cyber Defence, and Financial Crime Prevention (FCP). Our reports also build on knowledge from vendors, partners, other sector CERTs across the Nordics, and security communities like FS-ISAC and Curated Intelligence.

In addition, some of the contributions to this report come from all the Nordic National Cyber Security Centres (NCSCs) and from some Defence and Police Intelligence Services. 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 specifically address the Nordic financial sector.



The following publications may be used as further reading

- **NFCERT community** – Reported cases and incidents, as well as intelligence reporting from the community
- **The Finnish Security Intelligence Service (Suojelupoliisi, SUPO)** – Yearbook
- **The Finnish Transport and Communications Agency (TRAFICOM) i.e. NCSC-FI** – Cyber Weather reports
- **SAMSIK DD (former CFCS-DK)** – The Cyber Threat Against Denmark and "Nationalt Risikobillede 2025"
- **Swedish Security Service (Säkerhetspolisen, SÄPO)** – Yearbook
- **The Swedish Bankers' Association (Svenska Bank-föreningen)** – Hotbildsbedömning för Sveriges banker 2025
- **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
- **Nordic Sektor CERTs** – Various Nordics Sector-Focused Reports
- **Vendor reports** – Various reports

Nordic Financial CERT

post@nfcert.org
www.nfcert.org

Design: BRANDstasjonen 2026