Nordic Financial CERT
By members, for members

2024

Cyber Threat Landscape

for the Nordic Financial Sector

TLP:CLEAR

Summary

We proudly present our first open **Cyber Threat Landscape report** for the Nordic Financial Sector. This report is a companion to our closed Generic Threat Landscape (GTL) 2024 report, which covers the threats thoroughly for cyber professionals.

The financial sector provides critical services which our Nordic societies cannot function without. The Nordic Financial CERT's (NFCERT) vision is a cyber-robust financial sector. A key part of our contribution is sharing threat intelligence and knowledge about the cyber threat landscape, as exemplified by this and other reports. With this report, we want to promote open sharing on cyber threats and incidents and give the industry a public and relevant cyber threat picture anchored on a solid, well-documented basis.

The report and knowledge base are the product of a collaborative community effort with our members and the Nordic TIBER Cyber Teams (TCTs) at the centre, with contributions from Nordic government entities. We work together to pool our collective knowledge because the total shared picture is better than the parts each of us has.

The overall cyber threat to the financial sector is high, and the threat level is relatively stable compared to last year. We expect the threat to stay high in the coming year. The most serious and imminent threat comes from the criminal groups who run ransom(ware) operations. Their continued success in our societies makes them a formidable, persistent, and capable threat to the financial sector.

A more visible threat in the Nordic financial sector is the influence operations/Hacktivists, which use denial-of-service attacks to spread fear and gain attention for their cause.

There are also threats from Nation-States and Insiders, which must be considered.

We hope you find this report useful. Please let us know if you have comments, questions, or suggestions for improvement.

We are listening.

Morten Tandle
General Manager
Nordic Financial CERT

Contents

Forecast 2024

Organised Crime Groups

Continued professionalisation

Organised crime groups (OCGs) remain the most significant threat to the Nordic financial industry. The increased specialisation and professionalisation is expected to continue in 2024. The adaptiveness and trend of directly extorting money from the victims will continue if the method is deemed effective.

Nation-States

Events sparking global interests

Nation-States will continue to conduct cyber activities congruent with their domestic and foreign objectives. In 2024, multiple elections are scheduled worldwide, including in the Nordics. As Nation-States historically have followed elections closely, 2024 is expected to be no exception. However, the influence of Nation-States on elections is not expected to directly affect the cyber threat landscape for the Nordic financial industry.

Supply Chain

Increased focus on the supply chain

The Nordic financial sector's supply chain is extensive and complex. Over the past years, threat actors (TAs) have attempted to infiltrate supply chains through third-party software and vendors with varying success. Incidents like Okta and MOVEit illustrate that some TAs can bypass the defensive systems of their targets virtually undetected by infiltrating the source codes or the update mechanisms of a software or service.

In 2024, NFCERT expects an increased focus on "popular" third parties that may provide multiple opportunities for TAs to profit from multiple affected companies. Both OCGs and Nation-States are expected to exploit zero-day vulnerabilities related to these common third parties in the coming year.

HIGHER IMPORTANCE

Hacktivism

Continued disturbance

Hacktivism is expected to continue being part of the Nordic financial threat landscape. However, the trend shows that the attacks on the Nordic financial industry are often ineffective. The Nordic financial sector must be prepared for Hacktivist attacks that may have an operational impact, though the sector is expected to remain largely unaffected.

Artificial intelligence (AI)

Improved, professionalised, and scaled phishing

There are numerous assumptions about the potential impact Large Language Models (LLMs) and AI will have on the threat landscape. NFCERT believes AI's malicious use is still limited but expects developments in malicious usage in 2024. The developments are expected to enhance social engineering techniques, adapt to Nordic languages, and lower the threshold for actors to build and automate campaigns.

MEDIUM IMPORTANCE

Threats Towards the Nordic Financial Sector – A Summary

The cyber threat landscape in the Nordic financial sector is a complex ecosystem where threat actors collaborate and operate in each other’s domains.

Cybersecurity is a continuous effort, not a one-time victory. Understanding the threats’ motivations and tactics is vital for establishing effective countermeasures and comprehending the actual risks from the threat landscape. By understanding the threats and taking proactive measures, Nordic financial institutions can stay ahead of the curve and protect their valuable assets.

The threat actors are divided into five main threat categories: Organised Crime Groups (OCGs), Nation-State actors, Insiders, Hackers, and Hacktivists. **Organised Crime Groups** (OCGs) emerge as the most concerning threat. Driven by profit, they employ sophisticated tools and tactics like orchestrating ransom attacks, phishing scams, and malware deployments to steal money and data. Their adaptability and collaboration with other OCGs and Nation-States necessitate constant monitoring and robust defensive measures.

Nation-State actors play their part in the threat landscape. Backed by vast resources and advanced capabilities, their activities range from espionage and intellectual property theft to disrupting critical infrastructure for the government’s strategic objectives. Though direct attacks are less likely, Nordic financial institutions remain valuable targets as collateral damage or stepping-stones to other objectives.

While less prominent, other actors deserve attention. **Insiders** – employees with access to sensitive information – can become unwitting pawns in cyberattacks motivated by financial gain, personal beliefs, or coercion. Implementing strong security measures and employee monitoring is essential to mitigate this threat.

Although not the most significant threat, individual **Hackers** are often driven by curiosity, revenge, or recognition. They can still cause disruption but rarely pose a significant threat.

Hacktivists launch cyberattacks to promote a political or personal cause or conviction. However, their impact on financial stability is usually minimal. Regardless, their disruptive potential should not be dismissed.

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

Threat Actor’s Toolbox – The Cyber Jargon

Ransom

Ransomware is a software that denies access to files, computers, or devices by encrypting the content until a ransom is paid. In 2023, some threat actors started stealing data without encrypting it. This trend is pure extortion, as it does not contain any ransom software.

OCGs often use ransomware, but it has also been utilised by Nation-State actors seeking monetary gain outside office hours (moonlighting). Collaboration among different threat actors in ransom operations and the number of incidents are expected to rise in 2024.

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.

Following the invasion of Ukraine in February 2022, various activist groups have initiated DDoS attacks against the Nordic financial sector. Despite the media attention garnered by these attacks, they have predominantly failed to achieve their intended impact on the financial sector. However, there have been DDoS attacks that have caused prolonged downtime outside the financial sector.

Zero-Day

A zero-day vulnerability is a hitherto unknown vulnerability or software flaw. The term “zero-day” refers to the number of days a software vendor has known about the exploit.

Nation-States and some OCGs are known to exploit zero-day vulnerabilities. In 2023, there are reported several instances where zero-days in the supply chain have been exploited. The general trend of increasingly exploiting zero-days is expected to continue in 2024 by Nation-States and OCG.

AI and LLM

Large Language Models (LLMs) comprehend and generate text based on input data. Malicious LLMs, such as WormGPT and FraudGPT, are designed to generate malicious content and are being advertised on underground markets.

With the recent advancements in artificial intelligence (AI) and LLMs, there are speculations about whether the threshold for entry-level Hackers has been lowered. There are also speculations whether it is a force multiplier for the attackers. However, upcoming iterations of LLMs are expected to be limited to what is already possible but could become an integrated part of the cybercrime business model.

Wipers

Wipers disrupt systems by deleting files, typically not for profit. They are more commonly used by Nation-State actors and Hacktivists rather than OCGs.

Prior to the Ukraine invasion, exclusive Wiper malware was relatively scarce. However, the prevalence surged with the onset of the invasion. This shift signifies Nation-States’ willingness to incorporate Wipers into their arsenal to complement military manoeuvres.

Organized Crime Groups (OCGs) – The Profit Chasers

OCGs often run widespread and opportunistic cyberattack campaigns to compromise as many systems as possible for financial gain. They commonly use techniques such as mass phishing emails, exploit system vulnerabilities, or purchase access to already compromised systems, all fuelled by one goal: profit.

OCGs reach their objectives through various illegal activities, including ransomware attacks, selling stolen data, and other forms of cyber extortion. They are adept at staying under the radar, often using legitimate tools already present in victims' systems to avoid detection.

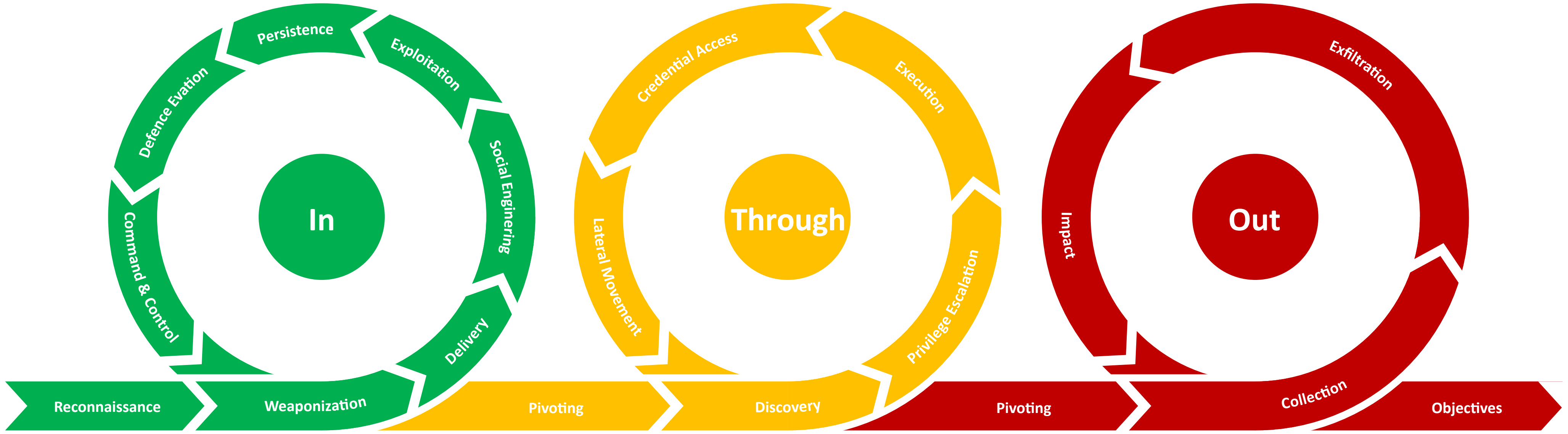


Figure 1 - https://www.unifiedkillchain.com/

The presence of security weaknesses such as outdated and unpatched software, the absence of phishing-resistant Multi-Factor Authentication (MFA), and potential human error susceptibility to phishing often provide opportunities for OCGs to launch attacks. They are also quick to exploit global events for themed cyberattacks. OCGs operate with a business-like approach, reinvesting their profits into more sophisticated tools and services, such as buying and exploiting undisclosed vulnerabilities (zero-day). They continually refine their tactics and collaborate to enhance their capabilities.

Additionally, OCGs are increasingly intertwined with geopolitical conflicts, with some Nation-States using OCGs as proxies to conduct cyber operations, obscuring the former's involvement and complicating attribution efforts.

With technological advancements, OCGs are also exploring using Artificial Intelligence (AI) to automate attacks, develop more sophisticated malware, and enhance social engineering tactics. The rise of AI-driven tools like Malicious Large Language Models (LLMs) is a testament to this trend, signalling potential changes in the cyber threat landscape.

It is anticipated that OCGs will continue to exploit technological advances, like AI, to enhance attacks.

Overall, OCGs will continue evolving, leveraging both new technologies and geopolitical issues, presenting ongoing challenges for cybersecurity defences. OCGs have evolved into sophisticated networks, often orchestrating collaborative attacks that span various stages, from initial infiltration and pivoting through networks to final objectives, where they move data out of the victim networks.

These criminals utilise a 'service-based' approach, where specific skills like data mining or access brokering are offered within the cybercrime ecosystem. This specialisation allows even less experienced threat actors to participate in complex cyber operations.

In 2023, the Nordic region saw a rise in such cyber threats, although financial institutions have managed to avoid successful attacks. The trend suggests that collaborative efforts among OCGs will likely continue.

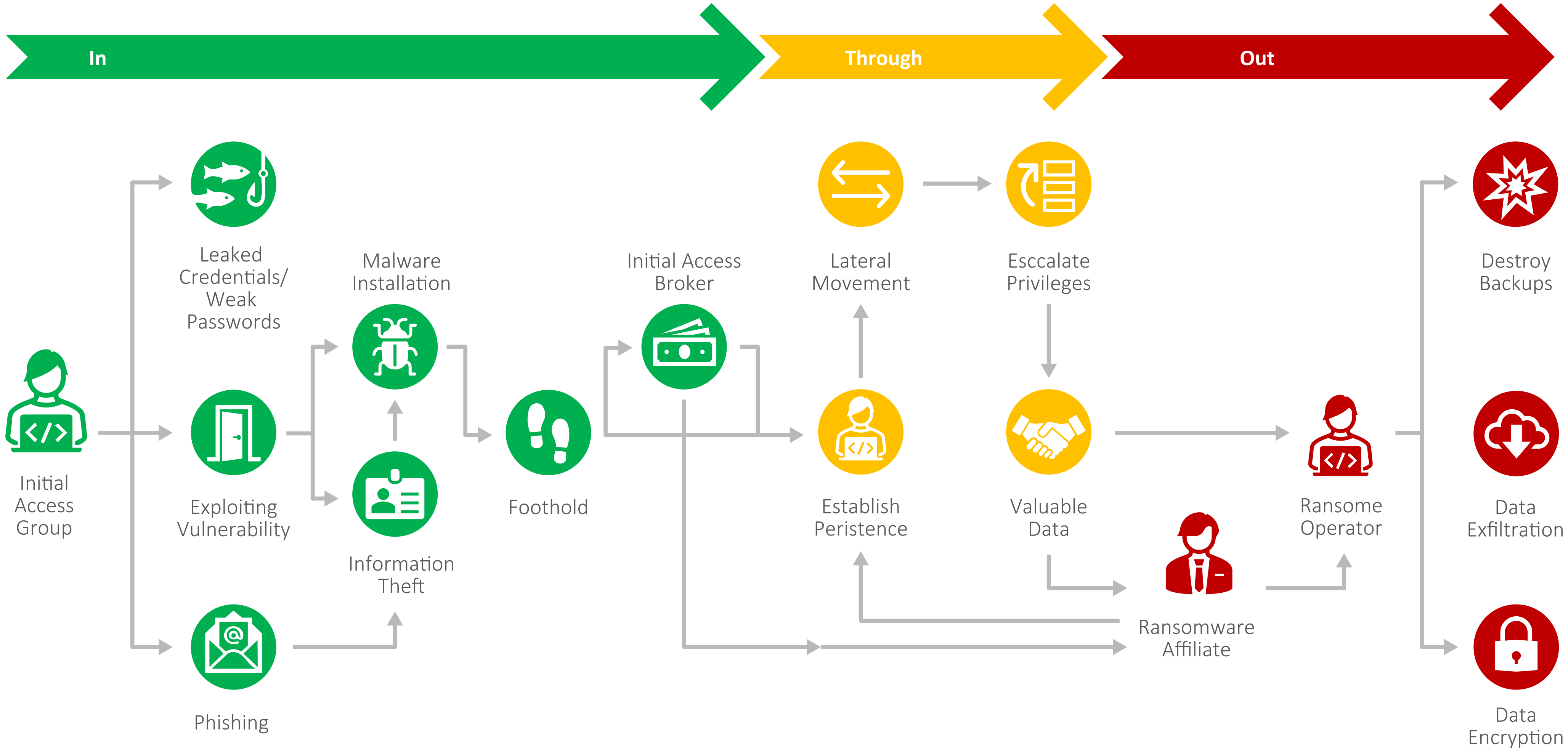
Ransom attacks have evolved in the past year. Criminals increasingly opt to simply steal data without using ransomware to encrypt it and demand payment to prevent its release. This approach differs from traditional ransomware attacks, where attackers encrypt data and demand payment for decryption keys. Even if a ransom is paid, attackers might demand additional payments to prevent data leaks. Notably, the Nordic region saw an uptick in ransomware incidents in 2023, echoing global trends.

Initial Access Groups (IAG) gain access to victim networks through deceptive phishing emails, exploit security weaknesses, or use stolen login information. The IAGs may sell the access through Initial Access Brokers (IABs) or maintain a presence within the network. As the OCGs navigate through the network, they target valuable data or systems and collaborate with ransom groups. If successful, they can either encrypt the data, threaten to publish it unless a ransom is paid, or steal it outright and extort money in exchange for not releasing it.

The process from initial breach to exerting control varies in time. However, there is a trend towards faster execution, sometimes within hours. Financial institutions are prime targets, with criminals seeking extensive control over their systems, mainly focusing on administrative functions that enable widespread data encryption.

Strategically, this means that organisations must be vigilant and prepared for both traditional and evolving cyber threats. Collaboration among different cybercrime groups makes defending against attacks more complex, necessitating a comprehensive cybersecurity approach that includes robust defence and rapid incident response capabilities.

The OCG Ecosystem – Ransomware



Nation-States – When Governments Attack

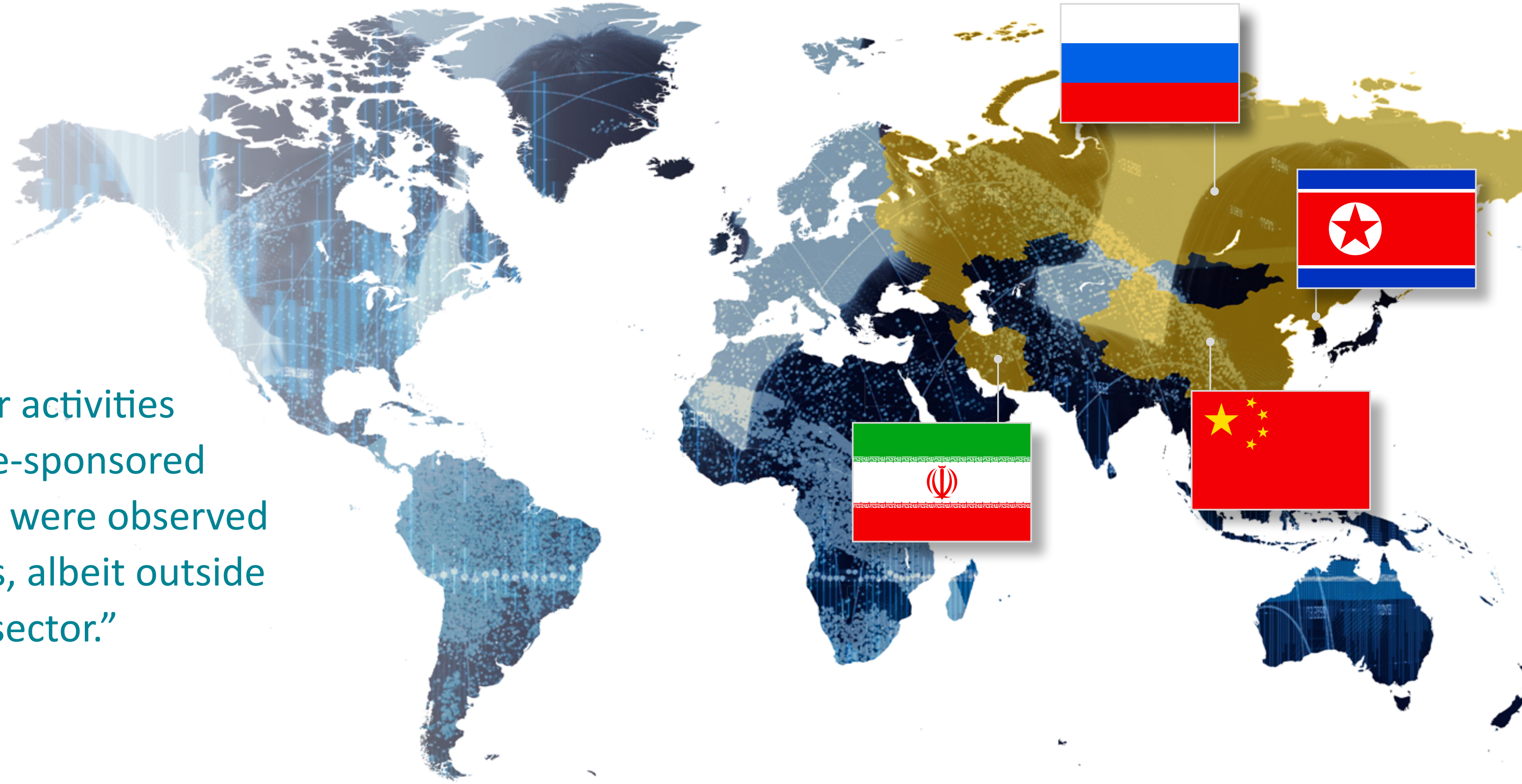
Nation-State actors conduct cyber operations congruent with their political and strategic ambitions. Their cyber activity is often related to intelligence gathering, but they also circumvent sanctions by conducting cyber activities for financial gains.

In 2023, Nation-State sponsored groups continued to play their part in the global cyber threat landscape, and their activities have been in line with their strategic ambitions and consistent with previous assessments by NFCERT.

Nordic organisations have experienced cyberattacks attributed to Nation-States. Although none of the attacks have been towards the Nordic financial sector, they serve as a reminder of foreign interest in the Nordics. The attacks in the Nordics have ranged from opportunistic to targeted and as a way to hit a primary target in a third country. For example, Russia and China have used infrastructure in the Nordics to conduct cyber operations against other countries. Reports indicate that Nation-State actors have collaborated with OCGs in suspected ransomware attacks, suggesting that the former is pursuing financial gain.

War in Ukraine, China's assertiveness as an economic and military power, and the Israel-Hamas war have generated tensions impacting the cyber domain. A continuance of these tensions is expected to continue in 2024.

> "In 2023, cyber activities linked to state-sponsored threat groups were observed in the Nordics, albeit outside the financial sector."



In 2024, several elections are scheduled, which are expected to be of interest to Nation-States due to current and impending sanctions. The effects of pivotal events such as elections vary but may extend to cyberspace, including cyber espionage and disruptive or influence operations. Iceland and Finland will hold presidential elections, adding significance to the latter due to Finland's NATO accession. However, the upcoming elections are not expected to impact the Nordic financial industry directly. Looking ahead to 2024, Nation-States will continue to conduct cyber operations aligned with their Nation's ambitions and continue their moonlighting operations.

The most relevant Nation-State actors are often referred to as the "big four" and are covered on the following page.

Russia

An Expanded Scope

Russia's war with Ukraine showcases its use of cyberattacks as an intrinsic element of modern conflict, altering European security perspectives. While Ukraine remained its main priority in 2023, Russia's cyber activities extended to other nations. The Kremlin use cyber activities to further national and foreign aspirations, with a growing willingness to use cyber operations in recent years. However, the war in Ukraine has shown that Russia has limited capabilities to engage in new operations. Russian Advanced Persistent Threats (APTs) adhere to the principle "once a target, always a target", reusing gathered information to regain access.

Although the financial sector in the Nordics is not Russia's top priority, they conduct cyber espionage in the Nordics. Expulsions of Russian diplomats prompt Russia to rely on cyberspace for intelligence gathering, leading to an expected rise in cyber espionage activity.

China

A Potent Cyber Threat

China is a significant cyber threat due to its capabilities and numerous APTs. China's cyber strategy is integral to its long-term objectives, including economic growth, technological advancement, and domestic and regional control. Chinese cyberattacks have emphasised stealth, supply chain and software vulnerabilities. Blurred lines between state-sponsored actors, private companies, and criminal organisations are among China's strengths.

The Nordics are targeted for intelligence gathering, particularly related to technology and political affairs. The activity reflects the Chinese ambitions in the High North as part of the Belt and Road initiative to connect China and the West. Despite not focusing on financial institutions, China is known to exploit vulnerabilities in software suppliers, which could indirectly affect the financial sector.

North Korea

Targeting Finance

North Korea views cyber operations as an "all-purpose sword" serving three priorities: intelligence collection on perceived enemies, enhancing military capabilities and acquiring funds to support the regime and its nuclear weapon program. Imposed sanctions have led to financial theft globally, explicitly focusing on Decentralised Finance (DeFi) services like crypto and blockchain platforms. The focus is expected to remain in 2024 and might stem from issues with stealing and laundering traditional currency after the Bangladesh heist in 2016.

In 2023, North Korean actors were suspected of conducting the first cascading software supply chain attack. According to Microsoft, North Korean APTs have targeted defence companies in the Nordics. Despite the focus on financial institutions, there have been no reported cyberattacks by North Korea in the Nordic financial sector in 2023.

Iran

Increased Sophistication

In 2023, Iran demonstrated a growing experience and willingness to conduct cyber operations with wipers. The use of cyber activities is expected to be aligned with Teheran's geopolitical and regional ambitions, economic imperatives, and perceived threats to the regime's stability. Iranian APTs engage in cyber espionage, influence operations and ransomware attacks. However, uncertainties persist regarding Iranian cyber capabilities, as other nations have emulated Iran using their tools and infrastructure. Iran is also known to cooperate in cyber activities with other Nation-States.

In 2023, an Iranian APT has been tied to a cyberattack in the Nordics, moonlighting for personal financial gain. Iran has also been linked to intelligence activities in the Nordics towards its diaspora and opposition. However, Iran is not expected to pose a cyber threat to the Nordic financial sector in 2024.

Insider Threats – The Hidden Dangers Within

The **Insider** phenomenon is often an underestimated cyber threat. Insiders encompass a broad spectrum of individuals — current or former employees, partners, contractors, and even third parties. With their privileged access to an organisation's digital assets and intimate knowledge about processes and procedures, these individuals can inadvertently or deliberately misuse this access and understanding.

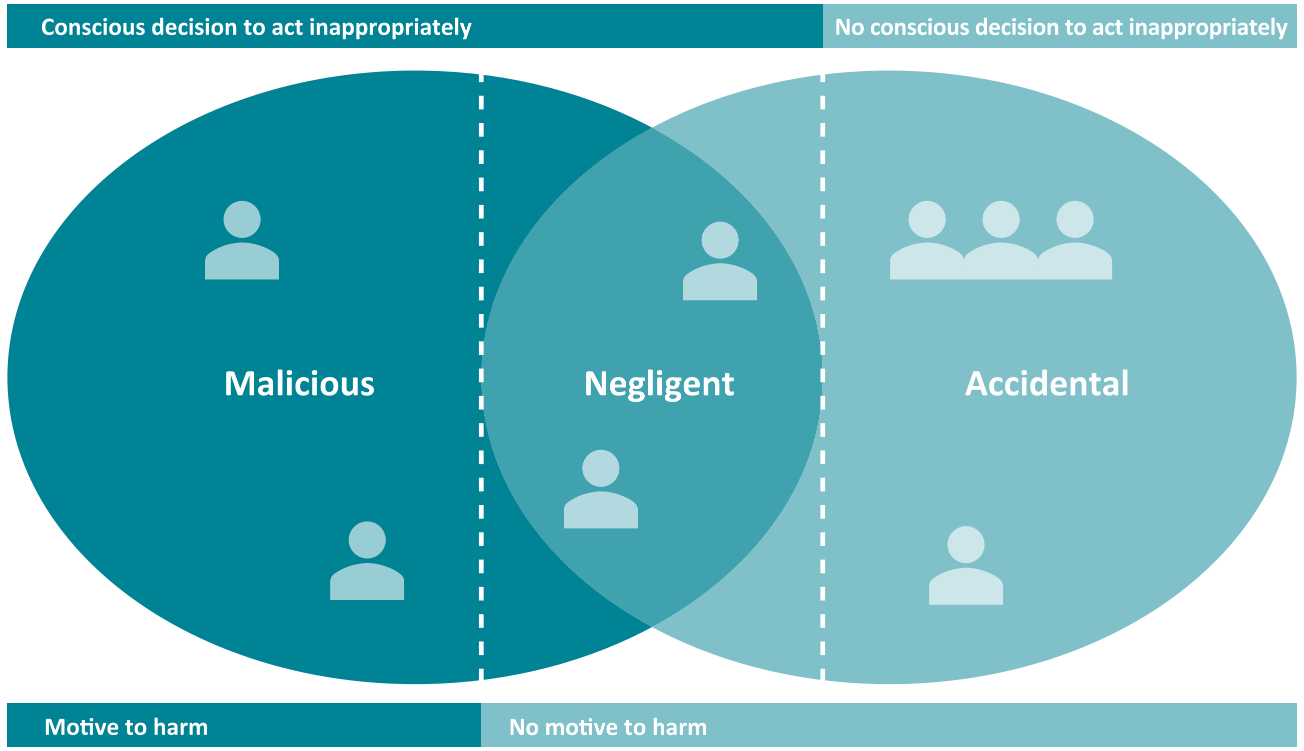
Malicious Insiders intentionally inflict harm on their organisations, driven by motives such as money, ideology, coercion, or ego. They may steal sensitive data or intellectual property or facilitate unauthorised system access. In contrast, without malicious intent, negligent Insiders engage in risky behaviours that may inadvertently expose their organisations to threats. Though not aimed at causing harm, these actions can significantly compromise organisational security. Accidental insiders, lacking malicious intent and awareness of the risks, engage in unsafe practices purely out of ignorance, posing another threat.

The impact of Insider threats extends beyond their intentions. Their in-depth knowledge and access enable them to circumvent security measures that can lead to substantial financial losses and prolonged recovery times.

The Insider threat is not limited to individual actions. OCGs and Nation-States exploit Insiders to further their agendas, ranging from espionage to influence operations. The recruitment of Insiders can occur through various means, including online advertisements, direct solicitations, or even deceptive employment offers.

As the landscape evolves, the threat posed by Insiders, whether part of a Nation-State's strategy, an OCG's plan, or a Hacker's scheme, remains a critical concern for financial institutions. This concern underscores the need for robust security measures and vigilant threat monitoring.

The Nordic region has witnessed numerous Insider incidents, albeit of low impact and severity, highlighting the real and present danger these threats pose.


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

Hackers and Hacktivists – Headline Grabbing Activities

Hackers are, in this report, individuals with malicious intent and varying experience and tools. In 2023, no individual Hacker has successfully impacted the financial industry in the Nordics. There have been speculations about Hackers' use of Large Language Models (LLMs) in attacks. However, the LLMs cannot yet automate the malware process entirely but could simplify the process for those with prior knowledge. Lone Hackers are not expected to pose a significant threat towards the Nordic financial industry in 2024, although they might have intentions to attack or partake in an attack.

Hacktivists engage in malicious cyber activities to advocate for a specific cause. The motivation varies from political or social views to cultural or religious beliefs, national pride, revenge or ideology. In 2023, several Hacktivist groups were active against the Nordics, including the financial sector. Although the financial sector in the Nordics accounted for approximately 17% of all DDoS attacks observed by NFCERT towards the Nordics in 2023, most attacks went unnoticed. Despite the media attention garnered by these attacks, they have predominantly failed to achieve prolonged downtime for websites belonging to the Nordic financial sector. This emphasises the assessment that while Hacktivists have demonstrated interest, they have lacked the capability to impact financial stability significantly. The likelihood of an attack has been dependent on a Nation's stance on issues like Russia or controversies like the burning of the Holy Quran. Given the surge of Hacktivists in the past two years, the Nordic financial sector is expected to continue to observe DDoS attacks in 2024.

Hactivists in numbers – 2023

19 557	2 378	411	23
DDoS attacks registered	DDoS attacks towards the Nordic Countries registered	DDoS attacks towards the Nordic Financial Sector registered	Groups active towards the Nordics in 2023 registered

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 toa website checking availability of websites.

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

Supply Chain Attacks – A Looming Threat

The Nordic financial sector relies on a vast network of suppliers that provide essential services and software. Recent trends have shown that OCGs are increasingly targeting these supply chains.

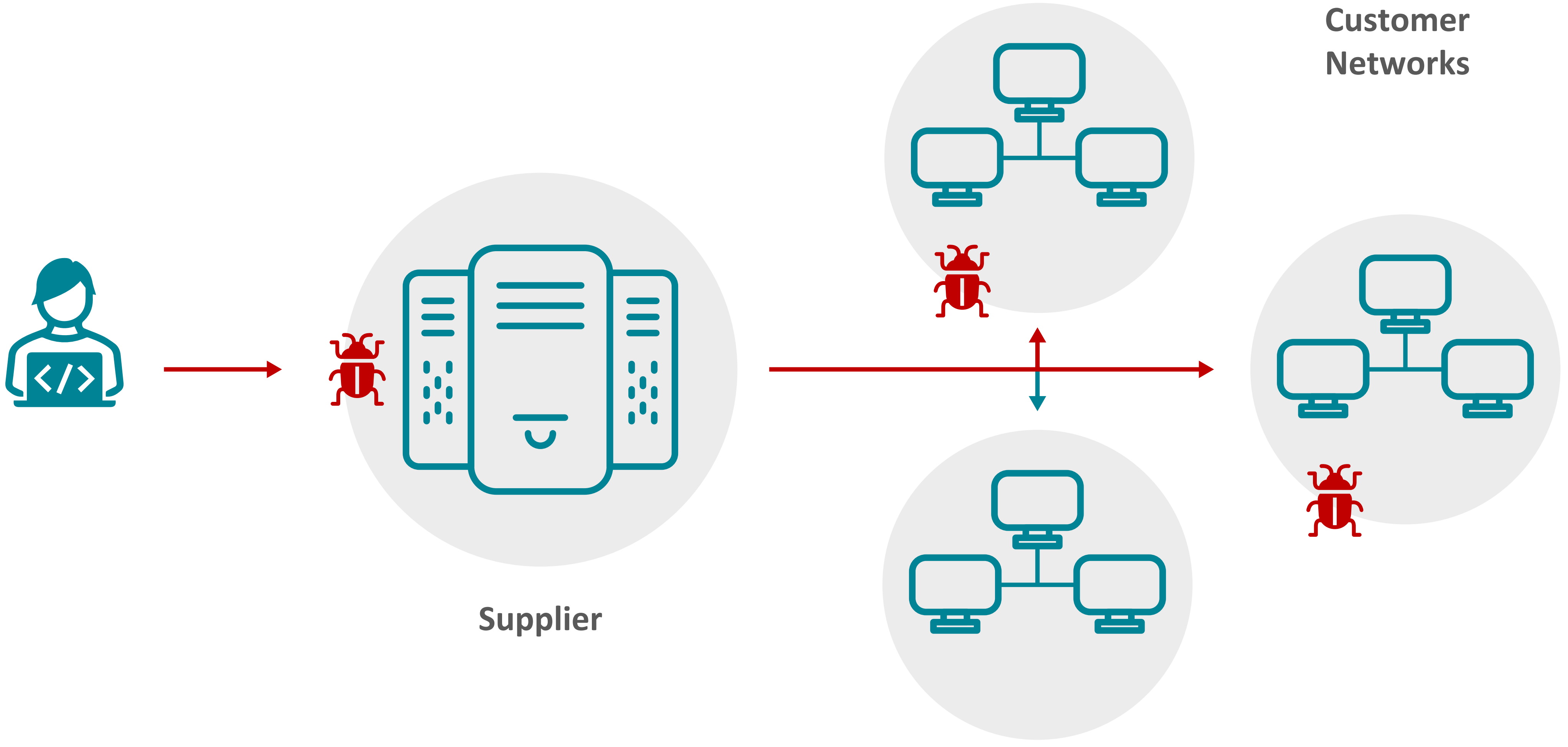
By exploiting third-party systems, like software updates or vendor services, attackers can access multiple organisations simultaneously. High-profile incidents like SolarWinds and MOVEit have demonstrated that even well-defended organisations can be vulnerable through their supply chain connections.

In 2023, there was a noticeable increase in supply chain attacks globally, with OCGs and Nation-State actors exploiting these channels to infiltrate targets stealthily. One significant method has been through managed file transfer (MFT) systems, which handle sensitive data and have been compromised to access a range of confidential information.

While the Nordic financial sector has been relatively unscathed by global incidents, it has not been entirely immune. An attack exploiting a Citrix vulnerability did lead to some level of compromise. However, it was contained and handled without further escalation.

Going forward, OCGs and Nation-States are expected to continue to search for and exploit vulnerabilities within the financial sector's supply chain, highlighting the ongoing need for robust cybersecurity measures.

The figure below is a general overview of a supply chain attack. In this attack, the supplier's systems are compromised, which allows the threat actor to infiltrate other victim networks by choice.



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) 2024 report published December 1st, 2023, with 136 pages and 539 references. The GTL report is available to all members of the Nordic Financial CERT. The report features insight from the NFCERT's reports throughout the year, NFCERT Threat Intelligence Committee (TIC), members, vendors, partners, CERTs like the Norwegian HelseCERT, 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, Defence and Police Intelligence). The information is verified, analysed and evaluated by the NFCERT's cyber intelligence professionals 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 cover the Nordics and specifically addressed the Nordic financial sector.

The following publications may be used as further reading.

- **The Finnish Security Intelligence Service (Suojelupoliisi, SUPO)** – Yearbook
- **The Finnish Transport and Communications Agency (TRAFICOM)** – Cyber Weather reports
- **Centre For Cyber Security (CFCS)** – The Cyber Threat Against Denmark and The Cyber Threat Against the Financial Sector in Denmark
- **Swedish Security Service (Säkerhetspolisen, SAPO)** – Yearbook
- **The Swedish Bankers' Association (Svenska Bankföreningen)** – Hotbildsbedömning för Sveriges banker
- **The Norwegian National Security Authority (Nasjonal Sikkerhetsmyndighet, NSM)** – Nasjonalt Digitalt Risikobilde and Risiko
- **Norwegian Intelligence Service (Forsvarets Etterretningstjeneste, NIS)** – FOKUS
- **Norwegian Police Security Service (Politiets Sikkerhetstjeneste, PST)** – Nasjonal Trusselvurdering
- **Microsoft** – Various reports, such as the Microsoft Digital Defense Report

Nordic Financial CERT

Q1 2023
Quarterly Threat Assessment

Nordic Financial CERT

By members, for members

April 2023 v.1.0

Q1 2023
TLP:AMBER

IMAGE: Jordan Holiday (Pixabay)

Q2 2023
TLP:AMBER

Nordic Financial CERT

Quarterly Threat Assessment

Q2 2023 | Nordic Financial CERT

By members, for members June 2023

Quarterly Threat Assessment

Q3 2023 | Nordic Financial CERT

By members, for members

Q3 2023

Nordic Financial CERT

Q4 2023
Quarterly Threat Assessment

December 2023 | v.1.0

TLP:AMBER

Together, we strengthen the Nordic financial industry's resilience to cyber-attacks.

We welcome your questions and feedback
post@nfcert.org
www.nfcert.org