STRATEGIC REPORT TLP:CLEAR

Cyber threats impacting the financial sector in 2024 - focus on the main actors

Livia Tibirna, Coline Chavane and TDR team, February 2025

sekoia

Table of Contents

Introduction

This report provides an overview of the main actors involved in malicious campaigns impacting the financial sector in 2024. It follows up on a previous Sekoia report focusing on the emerging trends in the financial cyber threat landscape.

This report will dive into cybercrime actors and state-sponsored intrusion sets tracked and documented by Sekoia. As this report is a synthesis of latest 2024 campaigns targeting financial entities, further information on the intrusion sets at the origin of the attacks and mentioned below can be found on the Sekoia.io platform, including a history of their past operations and descriptions of their tactics, techniques and procedures. If additional information is requested on a specific threat actor, please contact us at tdr@sekoia.io.

Key Takeaways

> **Initial Access Brokers** (IABs) play a critical role in the cybercrime activities impacting the financial sector, enabling large-scale, **multi-layered attacks** by monetising unauthorised network access.

> **Ransomware and extortion actors** pose a major threat to the financial sector, conducting consistent campaigns that leverage advanced malware, exploit vulnerabilities, disrupt operations, and cause major financial and reputational damage.

> Prolific **Trojan operators** deploy **increasingly sophisticated banking malware** in targeted campaigns, exploiting desktop and mobile vulnerabilities, including biometric data theft, to compromise financial institutions globally.

> The large adoption of the **Phishing-as-a-Service** model for Adversary-in-the-Middle (AiTM) campaigns **democratises advanced phishing capabilities** and fuels high-volume, targeted attacks on financial institutions.

> State-sponsored threat actors are also targeting the financial sector for various motivations, ranging from **making financial gain** to **covert cyber espionage operations and destabilisation**.

> Historical APTs targeting the sector are attributed to North-Korea, which use cyber operations against lucrative targets to **bypass international economic sanctions** and **finance its ballistic missile and nuclear weapons programs**.

> APTs attributed to Iran and China also targeted the sector and cooperated with cybercrime operators to **improve the cost-benefit tradeoff** of strategic cyber operations and **cover the tracks of state-sponsored operations**.

> State-sponsored threat actors sometimes pursue both financial gain and intelligence gathering. This dual motive is partly driven by some governments **outsourcing** segments of their cyber operations to **private entities**. These profit-driven private actors have been observed exploiting accesses used for strategic operations for their own benefit afterwards.

An overview of the cybercrime actors impacting the financial sector

Discussing the lucrative **cybercrime actors** specifically targeting the financial sector is challenging due to their **opportunistic** nature and ability to rapidly adapt to evolving opportunities for expanding the attack surface. The continuous expansion of the **Malware-as-a-Service** (MaaS) and, more broadly, the **Cybercrime-as-a-Service** (CaaS) ecosystems, further blurs the lines between distinct intrusion sets, making the attribution of cybercrime campaigns to specific groups or individuals increasingly difficult. This **fragmentation specific to** the cybercriminal ecosystem also complicates efforts to analyse and cluster specific actors.

In this section, we will provide a breakdown of the **most prevalent actors** in the cybercrime landscape that were observed conducting campaigns impacting the financial sector.

Initial Access Brokers (IABs)

The **Initial Access Brokers** (IABs) are individuals or groups that specialise in gaining **unauthorised access** into networks and systems, often through phishing attacks, exploitation of vulnerabilities, or compromising Remote Desktop Protocols (RDP). They commonly **sell access** on cybercrime forums and marketplaces to other malicious actors, often to the highest bidder. In other instances, access brokers are consolidated intrusion sets closely collaborating with a limited number of actors. These interactions highlight increasingly complex correlations among attackers, enabling numerous intrusion sets to bypass the initial access phase to focus on monetising the further steps of their operations.

Example of an IAB selling unauthorised initial access to an unnamed financial organisation. Source: Threat actor's post on the XSS cybercrime forum

The **impact** of IABs extends beyond the immediate consequences of a breach. They act as **key enablers of large-scale cybercrime campaigns** by facilitating access to critical systems. The proliferation of initial accesses sold by IABs on different platforms significantly reduced the entry barrier for subsequent compromises, leading to **increasing volume and diversity of attacks**, often involving coordinated, **multi-layered campaigns**.

Some of the most well-documented IABs that are known for targeting financial institutions in their campaigns are **TA577**, **TA569**, **TA570**, **Hive0145**, Prophet Spider (*aka* UNC961 *aka* Gold Melody), among others. Intrusions conducted by those IAB actors over the past few years commonly ended up with **ransomware deployment**. Yet, there is increasing evidence of state-sponsored actors closely cooperating with other IABs or even acting as IABs (*e.g.* the Iran-nexus APT33, as detailed later in this report).

So, the emergence of IABs led to the **commoditisation of cybercrime**, with access to financial assets becoming a transactional good that can be sold to multiple actors. As financial institutions store vast amounts of sensitive data and operate critical infrastructure, such attacks can finally lead to **disruptions**, **reputational damage**, and substantial **financial losses**. Moreover, the interconnected nature of the financial ecosystem amplifies the **risks of supply chain compromises**.

TA577

Motivation:
- Lucrative

Victimology:
- Opportunistic

Infection vectors:
- Phishing, spearphishing
- Valid accounts

Tools & Malware:
- EvilProxy
- DarkGate
- IcedID
- Latrodectus
- PikaBot
- SquirrelWaffle
- SystemBC
- Qakbot
- SmokeLoader
- Ursnif

For further insights into the TA577 intrusion set, please check the dedicated page on the Sekoia CTI platform

Ransomware and extortion actors

Ransomware and extortion-related intrusion sets represent a significant and persistent threat to the financial sector. As we outlined in the first part of our financial cyber threat landscape, dated November 2023, the **financial industry** was identified as **one of the most impacted by ransomware** campaigns in recent years.

Financial institutions, including banks, insurance providers, and payment processors, represent **attractive targets** due to several factors. Their widespread presence, critical operational functions, reliance on third-party supply chain vendors, and access to sensitive data make them lucrative for attackers. Disruptions in this sector not only causes operational downtime but also risks significant reputational damage and financial loss.

During 2024, numerous ransomware groups such as **RansomHub**, **Scattered Spider**, **Qilin** (*aka* Agenda), **LockBit**, and **Meow**, publicly claimed financial entities as victims. These intrusion sets most often conducted **lucrative**, **opportunistic** campaigns. Yet, in isolated cases, ransomware intrusion sets can conduct campaigns of economic sabotage, or else affiliates of Ransomware-as-a-Service (RaaS) operations can prove to be members of state-sponsored groups.

The ransomware campaigns conducted by major threat groups in 2024 against the financial sector and other industries are relatively advanced, with an **increasing incidence** of attacks **exploiting zero-day vulnerabilities**, **supply chain** attacks, and **double extortion** tactics. One notable example is the exploitation of at least two zero-day vulnerabilities in file transfer software developed by Cleo. First identified in December 2024, this campaign was claimed by **TA505**, a well-established intrusion set known to deploy the Cl0p ransomware, that engaged in post-exploitation activity. TA505 is a major ransomware and extortion actor that repeatedly conducted massive vulnerability exploitation campaigns, including supply chain attacks, affecting **a wide range of sectors worldwide**.

RansomHub

Motivation:
- Lucrative

Victimology:
- Mostly opportunistic

Infection vectors:
- Phishing, spearphishing
- Vulnerability exploitation (CVE-2020-1472)
- Valid accounts
- Password-spraying

Tools & Malware:
- RansomHub (custom malware)
- EDRKillShifter (custom malware)
- PuTTY, Rclone, WinSCP (for exfiltration)

For further insights into the RansomHub intrusion set, please check the dedicated page on the Sekoia CTI platform.

One notable example of highly prolific ransomware actors in 2024 is **RansomHub**, a RaaS and extortion group first observed in February 2024. Since its emergence, it quickly became **one of the most active and impactful** intrusion sets in the ransomware threat landscape. Its rise was likely fuelled by the takedown of LockBit and the scam exit of the BlackCat operation shortly beforehand.

RansomHub develops and distributes its own **custom ransomware**, which is also utilised by other advanced intrusion, including CosmicBeetle, Scattered Spider, and Evil Corp. RansomHub stands out for its diverse evasion techniques, particularly its **capabilities to bypass EDR systems**. This includes the deployment of a custom malware known as **EDRKillShifter**, designed to disable or manipulate EDR solutions and increase the success rate of its campaigns. Based on Trend Micro data, the **financial sector represented 8,6% of RansomHub's victims** between July 2023 and September 2024.

Another prominent intrusion set reported **deploying several ransomware** strains is **Scattered Spider**, active since at least May 2022. The intrusion set's campaigns leveraging ransomware such as **RansomHub**, **BlackCat** and **Qilin** impacted a wide range of industries over time, including the financial sector. Notably, EclecticIQ reported on a **long-term Scattered Spider campaign** targeting cloud infrastructures within the **insurance and financial** sectors up to Q2 2024.

One of most notable techniques leveraged by Scattered Spider is **targeted phishing**. Starting from mid-September 2024, Sekoia analysts identified a **new website template** used by the intrusion set to create phishing pages impersonating specific organisations. These phishing pages mimic the Okta login portal and are hosted in the AS 39287 (ABSTRACT, FI). They use almost empty HTML pages, loading JavaScript and a fake authentication page.

Part of this infrastructure targets **financial assets**, such as the **Revolut banking platform**. Examples include domains like okta-revolut[.]com and revolut-okta[.]com, that **target Revolut employees**. This is persistent with Reliaquest's observations, reporting that **20–25% of domains** impersonated by Scattered Spider in the second half of 2024 **targeted the finance and insurance sectors**, while 25–30% impersonated cryptocurrency platforms, collectively representing **50–55% of their activity**.

Scattered Spider

Motivation:

- Lucrative

Victimology:

- Mostly opportunistic

Infection vectors:

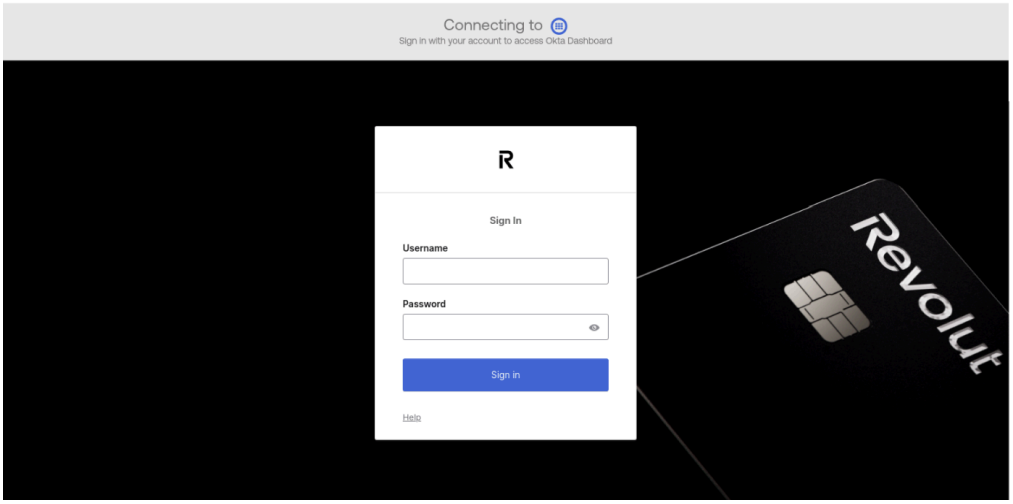
- Phishing, including smishing and voice phishing, targeted AiTM phishing pages
- Valid Accounts
- SIM swapping

Tools & Malware:

- Phishing kits: EIGHTBAIT aka 0ktapus, and two other unnamed kits
- Ransomware: RansomHub, BlackCat, Qilin
- Exfiltration: 7zip, AirByte, Azure Storage Explorer, Backblaze, DropBox, File.io, Filedropper.com, FileZilla, Gofile, Mega, Paste.ee, Rclone, Storj, Temp.sh, WinRar, WinSCP

For further insights into the Scattered Spider intrusion set, please check the dedicated page on the Sekoia CTI platform.

Typosquatted domain and phishing page targeting Revolut employees, highly likely attributed to Scattered Spider



Prolific Trojan operators

Malware targeting banking assets, notably desktop and mobile banking trojans, are one of the **longest-standing threats** faced by the financial sector. The malicious codes used, along with the groups deploying them, are increasingly sophisticated and, above all, continue to **expand their scope** of operations.

Solar Spider is one such advanced intrusion set distributing a **custom JavaScript Remote Access Trojan** (RAT) known as **JSOutProx**. The malware is continuously **updated** to expand its capabilities and **broaden its scope of use**, with a new version deployed to an extended list of targets starting in early 2024.

Unlike many cybercriminal actors whose activities are largely opportunistic, such as ransomware or infostealer operators, **Solar Spider engages in targeted campaigns**. According to open-source reports dating back to 2019, the intrusion set's targeting consists mainly of financial entities. While Solar Spider operations initially focused on small and medium-sized businesses within the Asia-Pacific (APAC) region, they expanded **their campaigns into the Middle East and North Africa** (MENA) region, significantly amplifying their cybercriminal activities.

In 2024, analysis by Resecurity indicated with moderate confidence that JSOutProx may have been **developed by actor(s) from China** or those affiliated with it.

Solar Spider

Motivation:
- Lucrative

Victimology:
- Starting from early 2024: financial institutions in the Middle East
- Historically: financial organisations in the Philippines, Laos, Singapore, Malaysia, India — and lately, Saudi Arabia, along with government organisations in India and Taiwan

Infection vectors:
- Phishing

Tools & Malware:
- JsOutProx

For further insights into the Solar Spider intrusion set, please check the dedicated page on the Sekoia CTI platform.

GoldFactory is another advanced intrusion set actively targeting financial institutions to deliver custom mobile malware since mid-2023. GoldFactory develops and deploys a range of highly **sophisticated banking Trojans**, including **GoldPickaxe**, **GoldKefu**, **GoldDigger**, and **GoldDiggerPlus**.

While the GoldFactory victims over 2023 and 2024 were mainly located in the APAC region, Group-IB analysts assess that GoldFactory's geography of operations may **extend beyond the initially targeted countries,** which were Vietnam and Thailand.

GoldFactory

Motivation:
- Lucrative

Victimology:
- Banking applications in APAC countries like Vietnam and Thailand

Infection vectors:
- Manipulation of Apple devices through Mobile Device Management (MDM)
- Leverage of the Apple's TestFlight platform to distribute fake cryptocurrency applications

Tools & Malware:
- GoldPickaxe, GoldKefu, GoldDigger and GoldDiggerPlus malware

For further insights into the GoldFactory intrusion set, please check the dedicated page on the Sekoia CTI platform.

One of the main intrusion set's deployed malware is **GoldPickaxe**, an advanced mobile Trojan which includes versions for iOS and Android. GoldPickaxe's purpose is to **gather personal information** from victims, along with **biometric data such as facial recognition**. The stolen data is leveraged to create **deepfakes** in order to autonomously access the victim's banking application.

The GoldFactory malware is notable for being the **first iOS Trojan harvesting facial recognition data** used for unauthorized access to bank accounts. This development is closely related to adoption of facial authentication as a security measure for money transfers applied in the target countries.

As of February 2024, Group-IB has not identified any instances of these malware being sold on cybercrime forums and marketplaces. Therefore, it is challenging to determine whether the above-mentioned banking malware could be adopted for wider distribution within the cybercriminal ecosystem.

GoldFactory is reported being almost certainly composed of **Chinese-speaking members**, along with local cybercriminals from the targeted countries such as Vietnam and Thailand. Moreover, the group includes distinct development and operational teams, each focusing on specific regions. These findings align with the **expansion of the Chinese-speaking cybercriminal ecosystem** observed over the past five years, possibly extending their targeting from China to other regions.

It is worth noting that while the Trojan operators mentioned above are reportedly expanding their target regions beyond APAC, traditional Banking Trojans are now rarely, if ever, used against Western entities. These Trojans primarily relied on web injection techniques to manipulate data in web browsers, particularly on banking websites. However, modern browsers become increasingly secure, progressively incorporating features to prevent such attacks.

Furthermore, the widespread adoption of two-factor authentication (2FA) makes it difficult to exploit stolen credentials obtained through basic phishing pages. Enhanced processes, tools, and security measures have likely rendered these attacks less effective for organisations. As for individuals, most bank transfers now take place via mobile applications, which are generally secure enough to prevent such threats.

Phishing-as-a-Service: an increasingly specialised cybercriminal ecosystem

Based on Sekoia data, the **most prevalent phishing-related threats** as of early 2025 include **Tycoon 2FA**, **NakedPages**, **Sneaky 2FA**, **Storm-1167** and **Evilginx**. This aligns with recent observations from ANY.RUN which also highlights **Mamba 2FA**. At least three of these (Tycoon, Mamba, Sneaky) represent major **Adversary-in-the-Middle** (AiTM) phishing kits distributed under the **Phishing-as-a-Service** (PhaaS) model, while Evilginx is an open-source AiTM kit available on GitHub. The PhaaS model allows phishing kit developers to provide pre-built phishing tools and infrastructure to other operators, notably pertaining to the cybercriminal lucrative ecosystem.

The adoption of the PhaaS model typically **amplifies the threat** by offering ready-to-use, scalable phishing kits, thereby lowering the barrier to entry for cybercriminals. This typically results in a higher volume of attacks and poses attribution challenges. Furthermore, PhaaS frameworks are often **highly customisable**, enabling **targeted campaigns** that frequently focus on specific industries, including financial institutions.

> Unlike typical phishing attacks, **AiTM campaigns** are meant to **intercept live authentication sessions** between users and legitimate websites, including credentials but also session cookies, to **bypass multi-factor authentication** (MFA) methods for large-scale credential theft.
>
> Therefore, the AiTM phishing kits represent a **significant threat to financial institutions**, which rely heavily on MFA for securing employees and clients accounts. Moreover, financial organisations and the finance departments of other businesses are prime targets for AiTM phishing attacks as they provide access to high-value assets, allowing attackers to perform fraudulent transactions or access restricted financial information.

Tycoon 2FA phishing kit

Storm-1747 is an intrusion set that develops and operates the Tycoon 2FA phishing kit since at least mid-2023. The phishing kit has since been sold and distributed in the wild under the PhaaS model. As of early 2025, Tycoon is the most widespread phishing kit, based on Sekoia telemetry.

The phishing kit leverages the AiTM technique, using an attacker-controlled reverse proxy server to host the phishing webpage, intercept victims' inputs, relay them to the legitimate service, and prompt the MFA request. Once the user completes the MFA challenge and authentication is successful, the server captures session cookies, enabling attackers to hijack the session and bypass MFA, even if credentials are later updated. By successfully mimicking login pages, Tycoon makes it more difficult for end-users to identify phishing attempts, increasing the likelihood of successful attacks.

Sneaky 2FA phishing kit

Sneaky 2FA is one of the latest notable newcomers to the PhaaS ecosystem, operating as an AiTM phishing kit and distributed in the wild since at least October 2024. As of December 2024, Sneaky 2FA phishing pages were hosted on compromised infrastructure, including hijacked WordPress websites and other attacker-controlled domains.

Sneaky 2FA is sold to other cybercriminal actors via Telegram channels by a persona known as "Sneaky Log" (also referred to as Sneaky Support). Sekoia analysts assess with high confidence that the Sneaky developer adapted portions of code from the W3LL OV6 phishing kit, previously documented by Group-IB. This highlights the continuous interconnectivity within the Cybercrime-as-a-Service ecosystem, where code sharing and repurposing among cybercriminals enable rapid innovation and expansion of malicious capabilities.

An overview of APTs targeting the financial sector

This section focuses on a second category of threat actors targeting the financial sector, which are the state-sponsored Advanced Persistent Threats (APTs). These are malicious clusters operated, contracted or financed by a state's intelligence service to support its strategic objectives. These groups can be made up of military units, state bureaus, but also private companies' employees, and civilians recruited from universities or hacker communities.

Conventionally, the primary motivation of APT groups is intelligence gathering. Accessing data from financial institutions can serve for individual surveillance purposes, but also for exercising political pressure on another country.

However, given the critical role of financial services for populations and their inherent access to massive money flows, the **principal objective of state-sponsored operations targeting this sector is either lucrative or disruptive**. This particularity of APTs operations targeting the financial sector will be further developed in this section.

Motivations behind state-sponsored campaigns targeting the financial sector

State-sponsored threat actors' operations are motivated by **strategic objectives**. Due to the ability of a state to invest massively in cyber capabilities to achieve a specific political goal, state-sponsored operations are characterised by their **high-level of sophistication** and their **precise targeting**.

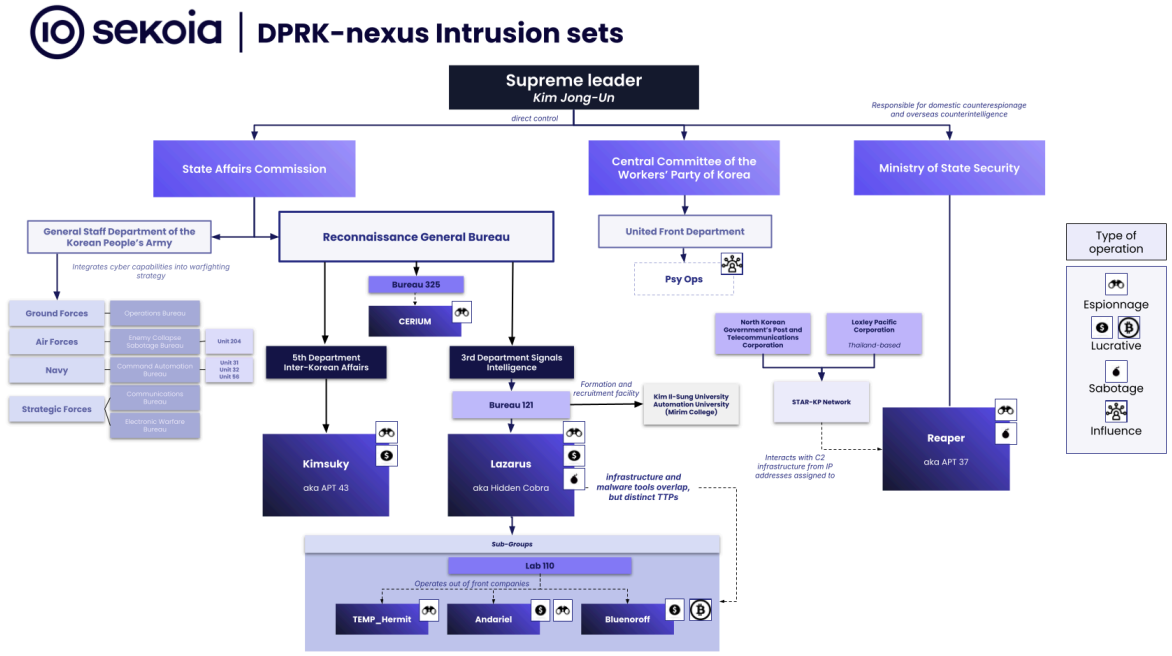
As far as the financial sector is concerned, there are a number of strategic objectives for conducting cyber operations. First, state-sponsored actors can be tasked with generating **financial gain** to bypass international sanctions or to fund strategic plans. These motivations are found in particular in campaigns conducted by **North Korean APTs**, which target **financial entities as well as cryptocurrencies**, and by **Iranian APTs**, which focus mainly on **financial entities in the Middle East**. To a lesser extent, when state-sponsored operations are outsourced to private companies, civilian employees can use the access gained for the operation to make profit and complete their revenue. This was especially observed for **APTs attributed to China**, such as APT41.

Second, state-sponsored cyber operations can serve **espionage purposes**, such as gaining information about individuals or about a targeted entity (a company, a country). This was especially the case for APTs attributed to **Iran** targeting Israeli entities and to **China** in South East Asia targeting neighboring countries ahead of negotiations for commercial policies in the region. Finally, cyber operations attributed to a state can target financial entities for disruptive purposes such as APTs related to **Russia**, which targeted Ukrainian banks to destabilise the country in the context of the war.

North Korean APTs historically targeting the financial sector

Historically, **North Korean intrusion sets** are the most active in targeting financial entities. They mostly focused on luring individuals to access networks of strategic entities and conducting supply chain attacks, including banks. They also largely target decentralised finance (DeFi) and cryptocurrencies.

North Korea has leveraged cyber operations for strategic purposes since at least 2004, including **cyberespionage**, **lucrative** campaigns, **destructive** and **disruptive** attacks. This country adapted its strategy in 2014 to focus on targeting banks, cryptoassets entities and financial technology companies in order to maintain its economy despite international sanctions and finance its ballistic missile and nuclear weapons programs.



North-Korean intrusion sets conducting operations against financial institutions are concentrated in the **Reconnaissance General Bureau (RGB)**, which is part of the State Affairs Commission. Of note, **Lazarus** is one of the most active intrusion sets operating the RGB lucrative campaigns for the purpose of North Korea's military development, followed by **Andariel** and **Bluenoroff**, two Lazarus sub-groups.

Lazarus has been active since at least 2009 and is known to encompass a broad range of activity from cyberespionage and destructive operations to lucrative campaigns. Its operations focus mainly on the defence industry as well as finance and cryptocurrencies platforms and users. Lazarus campaigns are particularly sophisticated due to their creative spearphishing techniques to lure victims and the constant evolution of their tools, techniques, and procedures.

Lazarus has used **fake job offers** several times to target high-profile individuals and infect strategic companies' networks like banks. It was the case with the **Operation Dreamjob** discovered in 2020, and more recently with the **VMConnect campaign** identified in August 2023. During the VMConnect campaign, the attacker impersonated a major US financial services firm, CapitalOne, recruiting individuals working in the financial sector.

In a fake process of recruitment, jobseekers have to complete a Python exercise provided via a link sent on LinkedIn and directing to a GitHub repository. In a short time, the candidate has to find a bug, resolve it and push changes that address the bug, leading the victim to execute the project on his/her machine. Once executed, it delivers a Python backdoor sending HTTP POST requests to a C2 and executing Python commands.

Spearphishing techniques leveraging job offers

It is interesting to note that Lazarus' campaigns leveraging job offers to lure the victims constitutes a **constant modus operandi over time**.

An individual is contacted via direct messaging on a community forum, LinkedIn, WhatsApp, or Telegram to be offered an attractive position.

The candidate for the job can be invited to **conduct an online interview**, to **complete a skills assessment document** or to **pass a test on a private GitHub repository**, which will be used to make the victim execute malicious payloads on his/her machine.

In a 2024 campaign, researchers identified Lazarus relied on Chat GPT to make its job offers even more credible.

These operations, ongoing since at least 2019, are targeting critical sectors, such as defense, IT, finance, and especially developers and engineers. This aims at taking profit of human error to conduct **supply chain attacks** on widely used products and compromise critical targets.

These malicious campaigns are well-documented by security vendors and translate the **constant evolution of tools, techniques, and procedures** of this intrusion set. In a 2024 report, Securelist researchers analysed the evolution of the Operation Dreamjob. They highlighted that between 2023 and 2024, the infection chain of this campaign totally changed. Even if Lazarus still heavily rely on weaponised open-source software, such as VNC and PuTTY, latest investigations unveiled it switched to malicious ISO files instead of ZIP files to evade detection, and used new malicious programs or variants, like MISTPEN, LPEClient, RollMid, and CookiePlus.

Lazarus is an umbrella under which other sub-groups conducting operations against financial institutions are located. Among them is **Bluenoroff**, a North Korea-nexus intrusion set who has been active since at least 2014 and subordinated to the **RGB 121 bureau**. It conducts financially-driven campaigns against banks, ATMs, cryptocurrency exchanges and venture-capital related entities in line with North Korea's strategic objective of sanction evasion. Their targets are from various parts of the world, as Bluenoroff's objective is to maximise the profit of its operations, instead of collecting precise information. It explains why it has a particularly broad victimology compared to other APTs.

This intrusion set especially developed macOS malware to target financial institutions. This is a three-stage malware dubbed **RustBucket**, which allows C2 communication and the execution of various payloads. First seen in 2022, it was leveraged by Bluenoroff in the **SnatchCrypto campaign** to target companies dealing with cryptocurrencies, DeFi, blockchains, and smart contracts, as well as the FinTech industry. The threat actor infiltrated internal and external business communications to map the interactions and identify topics of interest. The objective of the campaign was to collect credentials, as well as stealing cryptocurrencies.

Lazarus

Motivations
- Espionage, lucrative, sabotage

Victimology:
- Countries: USA, South Korea, Japan, Europe, Taiwan, the Middle East, Latin America
- Sectors: finance, cryptocurrencies, technology, defence, media, healthcare, chemical Industry

Infection vectors:
- Watering hole, spearphishing, social media messaging, public-facing apps, malicious package (NPM, Pip), supply chain attacks, insider threats

Tools & Malware:
- Malware: BeaverTrail
- Wiper: Sharpknot
- Spyware: Manuscrypt
- Trojanized applications: PondRAT, DacisRAT, DeFi wallets
- Rootkit: FudModule
- Ransomware: VHD
- Custom malware framework: MATA, Gopuram Loader
- Exploit of open source and zero-day vulnerabilities

For further insights into the Lazarus intrusion set, please check the dedicated page on the Sekoia CTI platform.

In 2024, **Bluenoroff** was also considered **responsible for the largest crypto hack of the year**, according to the FBI, the Defense Department and the National Police Agency of Japan. Indeed, the **theft of $308 million in cryptocurrency** from the Japanese platform DMM has been attributed to Bluenoroff and leveraged the **TraderTaitor** malware.

First seen in 2022, TraderTraitor is a malicious application derived from various open-source projects. It pretends to be cryptocurrency trading or price prediction tools to lure the victims.

TraderTraitor campaigns feature websites with modern design advertising the alleged features of the applications. An "update" function downloads a payload using a HTTP POST request to a PHP script hosted on the C2.

Among payloads executed are included **updated macOS and Windows variants of Manuscrypt**, allowing to collect system information, execute arbitrary commands and download payloads.

Bluenoroff

Motivations:
- Lucrative

Victimology:
- Countries: South East Asia, Latin America, Africa, Middle East, Europe, North America.
- Sectors: blockchain technology, cryptocurrency, DeFi protocols, NFTs

Infection vectors:
- Watering hole, spearphishing, social media messaging, public-facing apps, insider threats, use of initial access via IABs

Tools & Malware:
- MacOS malware: RustBucket
- Malicious applications: TraderTraitor
- Remote Access Trojan: SparkRAT
- MacOS backdoor: RustDoor, SpectralBlur
- Spyware: Manuscrypt
- Windows OS malware: YamaBot

For further insights into the Bluenoroff intrusion set, please check the dedicated page on the Sekoia CTI platform.

Another sub-group under the Lazarus umbrella is **Andariel**. It is an intrusion set related to the **RGB 3rd Bureau** who has evolved from conducting destructive attacks against US and South Korean entities, to cyber espionage and ransomware operations. One of its **principal objectives is to collect information for Pyongyang's nuclear and defence programs**, while ransomware campaigns serve to fund its espionage activity. It already targeted financial institutions with ransomware attacks because of the **lucrative nature of financial activities**.

While investigating a 2024 Play ransomware incident, researchers from Unit42 assessed with high confidence that the initial access was obtained by **Andariel** in May. It indicated that the North Korean APT would proceed as an **IAB** or an **affiliate of the Play ransomware** group and shift towards a deeper involvement in the cybercrime ecosystem.

Indeed, this incident brought to light the **first case of known collaboration** between this intrusion set and a ransomware group. The Play ransomware group declared on its leak site that it does not provide a Ransomware-as-a-service ecosystem (RaaS). If this is true, Andariel might only have acted as an IAB, according to Unit42. In any case, the involvement of sophisticated North Korean APTs in ransomware campaigns represents an emerging trend potentially leading to more damaging attacks.

Andariel

Motivations:

- Espionage, lucrative, sabotage

Victimology:

- Countries: South Korea, USA, India, Japan, Vietnam, Russia, Europe, South America, Nigeria
- Sectors: finance, defence, aerospace, Government, nuclear, industry, healthcare, telecommunications, transportation, education, NGOs, manufacture, retail

Infection vectors:

- Watering hole, spearphishing, public-facing apps, supply chain attacks, insider threats

Tools & Malware:

- Custom tools and malware for discovery and execution.
- Leverage legitimate proxy and tools tunneling (Sliver, Impacket, Mimikatz).
- Native tools and processes (LOTL)
- Malware: DTRack, SmallTiger, HOTCROISSANT and Phandoor, Rifdoor, MonoRAT, and ApolloZeus
- Ransomware: custom Maui ransomware, BMPScriptCrypt ransomware

For further insights into the Andariel intrusion set, please check the dedicated page on the Sekoia CTI platform.

APTs and cybercrime operators collaboration

As well as North-Korea-nexus intrusion sets, other state-sponsored threat groups turned to financially-motivated operations against the financial sector in addition to cyberespionage. These lucrative campaigns aim at bypassing international sanctions, but also at taking profit from the cybercrime ecosystem to **improve the cost-benefit tradeoff of strategic cyber operations**.

APTs and cybercriminal operators' collaboration

In order to maximise the cost-benefit trade-off of an operation and harden attribution to an attack, state-sponsored threat actors were observed cooperating with cybercriminal operators for their operations.

Once an APT has gained initial access to a targeted entity and conducted its operation, it can act as an **IAB** and collaborate with ransomware groups in exchange for a percentage of the ransom payments.

This technique has already been adopted by the Iran-nexus APT33 intrusion set since 2017, and was still ongoing in 2024.

In August 2024, the FBI and CISA reported that **APT33**, an **Iran-nexus intrusion set** active since at least 2013, was conducting **IAB campaigns** under the aliases "Br0k3r" and "xplfinder" on cybercrime forums and marketplaces. Acting as an IAB, APT33 focused on gaining and maintaining technical access to victim networks to facilitate future ransomware attacks. The Iranian cyber actors' role extends beyond providing access. The FBI identified that these actors worked directly with ransomware affiliates, assisting in encryption operations in exchange for a share of the ransom payments. Documented incidents revealed APT33 collaborating with ransomware groups such as **NoEscape**, **Ransomhouse**, and **BlackCat**.

APT33 is an Iranian state-sponsored threat group active since at least 2013. It has targeted organisations in the United States, Saudi Arabia, and South Korea, with a strong focus on the aviation and energy sectors. Given its destructive capabilities, overlapping activities with other Iranian APTs, and shared victimology, it has been attributed to the Islamic **Revolutionary Guard Corps (IRGC)**. APT33, as other groups subordinated to the IRGC, pass contracts to operate under the guise of a private company to harden attribution. Among them is **Danesh Novin Sahand**, who is associated with the APT33's sub-group **Fox Kitten**.

Historically, APT33 has been associated with **hack-and-leak campaigns**, such as the **Pay2Key operation** in late 2020, an information warfare operation designed to undermine the cybersecurity of Israeli infrastructure. In the case of APT33's ransomware activities, they appear to be primarily focused on **stealing sensitive information**.

APT33

Motivations:
- Espionage, sabotage

Victimology:
- Countries: USA, Israel, Azerbaijan, Saudi Arabia, South Korea
- Sectors: financial institutions, aviation, energy, education, Government, healthcare

Infection vectors:
- Use of proxy groups, spearphishing, public-facing apps, social media messaging
- Malicious package (NPM, Pip), watering hole, supply chain attacks

Tools & Malware:
- Wiper: Shamoon
- Custom backdoor: Tickler, FalseFont
- Remote Access Trojan: QuasarRAT

For further insights into the APT33 intrusion set, please check the dedicated page on the Sekoia CTI platform.

On a different model from Iran-nexus intrusion sets, several **state-sponsored cyber threats attributed to China** rely on the cybercrime ecosystem for their malicious campaigns.

ChamelGang, a China-nexus intrusion set active since at least March 2021, was observed carrying out cyberespionage campaigns against critical infrastructure in various countries. In addition, Positive Technologies, Sentinel One and TeamT5 assessed that this APT pursues objectives beyond intelligence gathering, like Personally Identifiable Information (PII) theft and financial gain operations. For that purpose, it was reported that ChamelGang used the **CatB ransomware**.

Indeed, since at least 2022, this intrusion set leveraged ransomware to target high-level victims, such as the major Indian healthcare institution AIIMS and the Presidency of Brazil. The use of RaaS by state-sponsored threat actors can be interpreted as a way to **make additional profit**, but also as a **way to distract victims from its cyberespionage focus**. Indeed, it can help to cover the track of a compromise, as well as leading to misattribution of cyber espionage campaigns to cybercrime operators.

As ChamelGang used to deploy ransomware at the end of its operations, an hypothesis is that it is used as a cover for **intelligence gathering**.

ChamelGang

Motivations:

- Espionage, lucrative, influence operations

Victimology:

- Countries: Taiwan, Vietnam, Philippines, Thailand, India, Turkey, Brazil, Hong Kong, Russia, US, Japan, Afghanistan, Lithuania, Nepal
- Sectors: Government, finance, aviation, telecommunications, healthcare

Infection vectors:

- Supply chain, typosquatting of legitimate IT services

Tools & Malware:

- Malware: ChamelDoH, CatB Ransomware, Cobalt Strike Beacon
- Backdoor: AukDoor, DoorMe, ProxyT, BeaconLoader
- Tools: ProxyShell vulnerabilities, Tiny shell, SweetPotato, SharpToken, FRP

For further insights into the ChamelGang intrusion set, please check the dedicated page on the Sekoia CTI platform.

Double motivation due to outsourcing of cyber capabilities in APT operations

The dual interest of some APTs for intelligence gathering and financial gain can be explained by the hack-for-hire ecosystem. In China, state units are known to **outsource part of their cyber operations to private companies**. Companies operating part of state-sponsored operations can then use the access for their own benefits, explaining this double objective.

Indeed, the 2024 I-SOON leaks revealed that several cyber range businesses operate part of state-sponsored cyber campaigns. For instance, I-SOON proceeds by gaining access to various systems and selling them to state entities, especially to Provincial and City-level State Security Bureaus, for strategic operations. This profit-driven way of operating is likely to be adopted by other companies similar to I-SOON, such as **Chengdu 404**, **Integrity Technology**, and **Sichuan Silence**.

The difference between private and front companies in cyber operations

It is important to note that private companies related to state-sponsored operations attributed to China can either be **profit-driven companies** likely motivated to increase their income, or **front companies**, without real business activity. According to Natto Team, the Chinese company Sichuan Juxinhe, recently sanctioned by the US Office of Foreign Assets Control (OFAC), is likely a front company, whereas I-SOON, Chengdu 404, Integrity Technology and Sichuan Silence are real private companies.

Chengdu 404 and I-SOON are operating for State Security Bureaus, under the Ministry of State Security (MSS), and linked to **APT41**. This intrusion set is known for conducting both intelligence gathering, as well as financial gain campaigns. An hypothesis is that private companies operating for state-sponsored operations attributed to APT41 also use access, malware and tools for their own profit and complete their revenues.

APT41

Motivations:

- Espionage, sabotage, lucrative

Victimology:

- Countries: Europe, South Asia, North America
- Sectors: financial Services, transportation, telecommunications, Government, industry, defence, healthcare, media, entertainment, technology

Infection vectors:

- Use of proxy groups, spearphishing, public-facing apps, social media messaging, malicious package (NPM, Pip), watering hole, supply chain attacks

Tools & Malware:

- Framework: DeepData
- Malware: PlugX, ShadowPad, MoonWalk, KEYPLUG, StealthVector, Cobalt Strike, SideWalk, DodgeBox
- Spyware: LightSpy, WyrmSpy
- Tools: VMProtect, UPX, netstat, rakshasa, Tailscale, MEGAcmd

For further insights into the APT41 intrusion set, please check the dedicated page on the Sekoia CTI platform.

An overview of hacktivism activities impacting the financial sector

Hacktivism nowadays can refer to two types of actors. The first one refers to malicious cyber campaigns, mainly leveraging DDoS or data leaks, conducted by individuals or groups to promote political or ideological agendas. These threat actors typically target governments, corporations or entities they oppose, aiming to disrupt operations, spread propaganda, or cause reputational harm.

The second type of hacktivism is what we call nationalist hacktivism, conducting the same kind of operations on political entities, in order to support the interests of their own country. Those groups are often partially supported by intelligence services (financially, access, targeting). Nationalist hacktivism rose on a larger scale starting from 2022, in conjunction with Russia's invasion of Ukraine. Over this period, multiple groups such as KillNet, Anonymous Sudan or NoName057(16) conducted hacktivism-like operations to support Moscow. Moreover, it was further amplified by other major events, in particular political and geopolitical ones such as the Israel-Hamas war.

Over the past years, the **hacktivist threat expanded across most sectors, including the financial industry**. From July 2023 to June 2024, banking and insurance represented the third most targeted sector by hacktivists groups within the European Union. The hacktivist groups most actively targeting the financial sector were NoName057(16) and Killnet, which is in line with the global landscape of the hacktivist activities. In 2024, NoName057(16) targeted around 140 financial related entities among the millions of targets in Europe of its DDoS campaigns. However, it is worth noting that cybersecurity teams regularly face DDoS attacks that remain unclaimed and therefore harder to attribute.

A significant event occurred in January 2024 when NoName057(16) launched a DDoS attack against a website labeled "SWIFT card authorization." Interestingly, the targeted website was unrelated to the Society for Worldwide Interbank Financial Telecommunication (SWIFT), the secure messaging network enabling financial institutions to exchange transaction data. Instead, the attack targeted a website associated with a bus card system named SWIFT. This incident highlights that, beyond the operational disruption caused by a DDoS attack on financial entities, such cyberattacks can result in substantial reputational damage, even affecting entities that experience no technical issues with their services. Beyond the operational concerns related to targeted services' unavailability, another expected impact is the erosion of public confidence in these services, which could be critical to the functioning of democratic institutions. Nevertheless, the intensity of the hacktivist rhetoric claiming massive campaigns against financial assets are often followed by **limited or isolated impact**. This is likely indicative of the financial entities' resilience, alongside anticipated cybersecurity measures.

Conclusion

This report summarises the latest intelligence on key **cybercrime** and **state-sponsored** intrusion sets conducting malicious campaigns **against the financial sector**.

Advanced intrusion sets that engage in **lucrative campaigns** are continuously **expanding their capabilities** and **targeting new regions**. The most prolific among them include Initial Access Brokers, banking Trojan operators, phishing enablers, ransomware and extortion actors.

The report also explored the diverse motivations of **state-sponsored** threat actors in targeting financial entities, ranging from **intelligence gathering** and **destabilisation** to **financial gain**. Notably, APTs attributed to **North Korea** historically targeted the sector to finance their economy and support their ballistic nuclear missile programme.

Meanwhile, other APT groups are **increasingly collaborating with cybercrime actors**, particularly IABs and RaaS operators, to reduce costs, enhance efficiency, and cover their tracks within compromised systems.

Finally, the **outsourcing** of certain APT operations to **private entities** created opportunities for profit-driven actors to exploit access to strategic targets for financial extortion.

About Sekoia.io TDR team

TDR is the Sekoia Threat Detection & Research team. Created in 2020, TDR provides exclusive Threat Intelligence, including fresh and contextualised IOCs and threat reports for the Sekoia SOC Platform. TDR is also responsible for producing detection materials through a built-in Sigma, Sigma Correlation and Anomaly rules catalogue.

TDR is a team of multidisciplinary and passionate cybersecurity experts, including security researchers, detection engineers, reverse engineers, and technical and strategic threat intelligence analysts.

Threat Intelligence analysts and researchers are looking at state-sponsored & cybercrime threats from a strategic to a technical perspective to track, hunt and detect adversaries. Detection engineers focus on creating and maintaining high-quality detection rules to detect the TTPs most widely exploited by adversaries.

About Sekoia.io

Sekoia.io is the European cybertech, leading provider of Extended Detection and Response (XDR) solutions based on Cyber Threat Intelligence (CTI). Its mission is to provide businesses and public organizations with the best protection technologies against cyber attacks.

By combining threat anticipation through knowledge of attackers (Sekoia Intelligence) with automation of detection and response, the Sekoia SOC platform (Sekoia Defend – XDR) provides security teams a unified view and total control over their information systems. Its interoperability with third-party solutions and compliance with international technical standards enable organizations to take full advantage of their existing technologies.

Sekoia.io gives its customers the means to focus their human resources on high value-added missions, optimize their cyber-defense strategy and regain the advantage against advanced cyber threats.

Find more publications on blog.sekoia.io

Please don't hesitate to provide your feedback on our publications by clicking here.
You can also contact us at tdr@sekoia.io for further discussions.