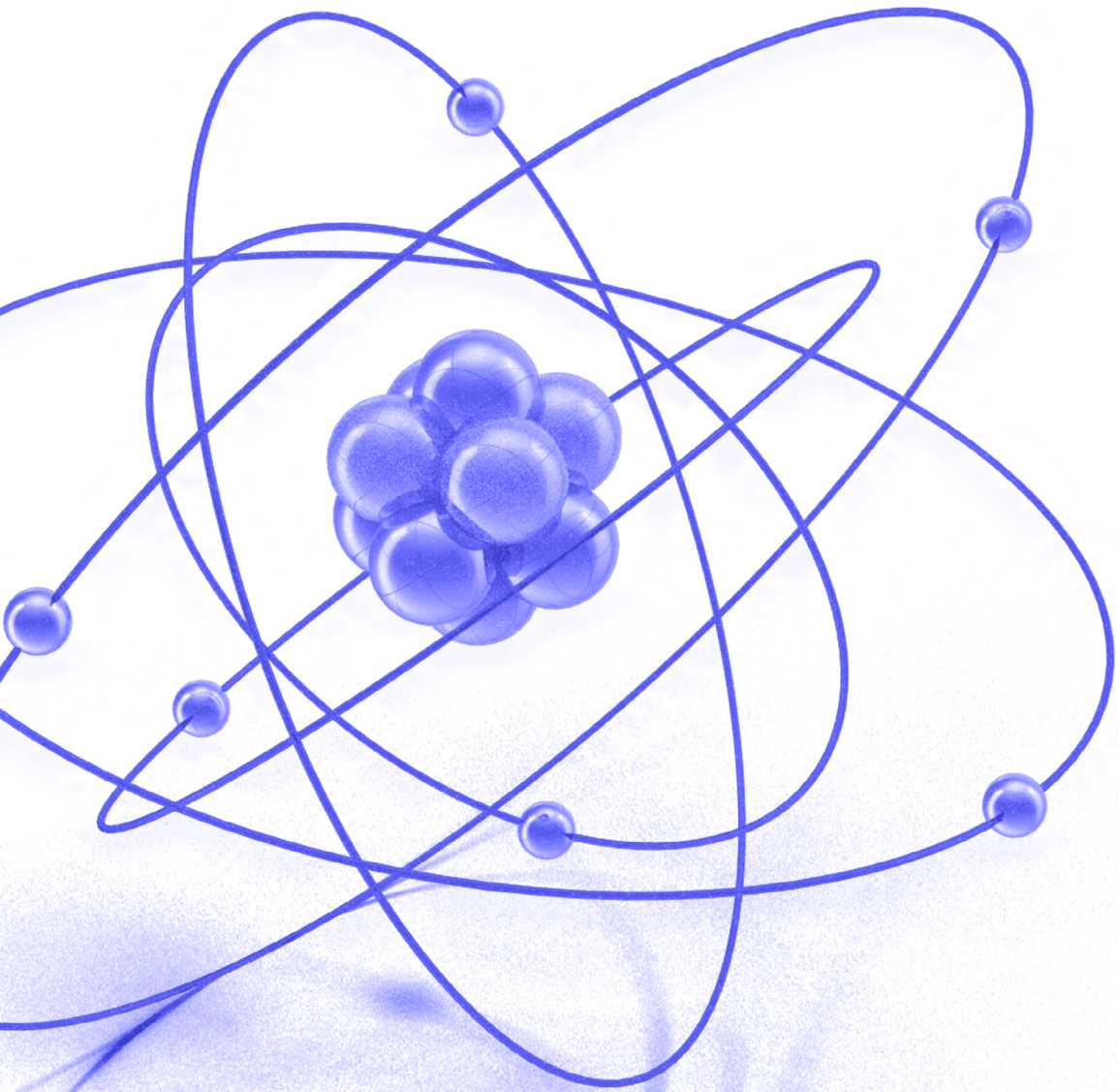
FS-ISAC

Navigating Cyber: Annual Threat Review and Predictions



May 2025

Contents

Executive Summary

The stability and continuity of the global financial system are under constant threat. Lone hackers in a basement, organized criminal gangs, and nation-state threat actors – motivated by profit, espionage, or politics – challenge the operational resilience of the financial sector and its supplier ecosystem on a daily basis. Attackers and defenders alike are aided by rapid technological advances. Given the complexity and interdependence of the digital economy, tiny errors can cause widespread disruption. Regulators seek to ensure that the necessary investments are made to protect citizens and consumers, while larger geopolitical tensions test the efficacy of those investments every day.

2024 upped the ante for FS-ISAC's global community of cybersecurity, resilience, and fraud professionals defending the financial sector from threats on multiple fronts, including:

Supply chain incidents: The sector's reliance on third-party vendors increases its exposure to disruptions that — whether malicious or unintended — can have widespread impact, underlining the necessity for robust incident response plans.

Fraud: Scams and fraud are surging across multiple sectors, targeting firms, customers, and employees. Generative AI (GenAI) gives threat actors powerful new tools for more effective fraud campaigns.

Ransomware: The financial services sector is a perennial target for ransomware threat actors, and the payouts are getting bigger. Law enforcement has hobbled many groups, but ransomware gangs have continually disbanded and re-formed to evade sanctions, takedowns, and prosecution.

DDoS attacks: Criminal and hacktivist groups continue to make the financial services sector a primary target for Distributed Denial of Service (DDoS) attacks – including some of the largest-ever volumetric attacks – a concerning trend that could affect service availability.

Emerging technologies: Deepfake-enabled fraud is only one of a long list of threats to the financial sector brought by the explosion of GenAI, while unpredictable progress on quantum computing increases the urgency to migrate to quantum-resilient and agile cryptography.

Geopolitically-motivated cyber activity: Ongoing hostilities and new tensions present opportunities for threat actors to target the financial sector. Nation-state threat actors increasingly attack providers crucial to business operations.

Regulation: Regulation of financial firms' cyber and resilience postures is increasing around the world. The EU's Digital Operational Resilience Act (DORA) is seen as a watershed in its direct regulation of critical third-party suppliers to the sector. The UK and other countries are enacting similar requirements.

2025 has already brought dynamic shifts in the cyber landscape as geopolitics continue to influence attack trends and the world's defense systems, regulations, and approaches to international cooperation. Still, the financial sector's long-established information-exchange mechanisms demonstrate that sharing advanced warnings about threats, developing mitigation advice, and exercising to prepare for incidents protects the global financial system and the people it serves.

Incident Timeline

Jan

Ivanti Connect Secure and Policy Secure
Zero-day exploitation

Malicious npm packages uploaded onto GitHub [1]

Feb

ConnectWise
ScreenConnect authentication bypass vulnerability exploitation [2]

Malicious update in PyPI package used to push infostealer [3]

Mar

XZ Utils backdoor discovery

Apr

Snowflake
Databases of up to 165 customers accessed via stolen login credentials [4]

DDoS extortion campaign
Swiss financial sector web servers, e-banking portals, firewalls, APIs, and mail servers attacked [5]

May

Scattered Spider
Targeted the financial sector for extortion after conducting thorough reconnaissance [6]

Jun

Fortigate
VPN firewall vulnerability exploited by state-sponsored threat actors [7]

Jul

CrowdStrike Falcon Sensor
Faulty update caused global IT outage [8]

DDoS attack on Microsoft
10-hour Office, Outlook, and Azure outage impacted financial sector users [9]

Oct

Global DDoS campaigns
Record-high volumetric attacks with a notably sustained campaign in APAC in late 2024

Dec

BeyondTrust
US Department of Treasury breach via provider, attributed to Chinese state-sponsored threat actor. [10]

Cyber Threat Levels

FS-ISAC sets regional Cyber Threat Levels (CTLs) periodically to reflect attack activity and responses within geographic areas. While some regional CTLs changed during the year, the Global CTL, which is based upon a holistic worldview, remained at GUARDED throughout 2024.

The overall ratings in each region were more stable than they have been in years past, but FS-ISAC's regional Threat Intelligence Committees (TICs), comprised of threat intelligence experts in FS-ISAC member firms, have raised significant concerns about specific elements of the threat environment.

The relative stability of the CTLs reflects the sector's ability to manage the changing threat landscape; however, each CTL comes with a range of details that convey the changes financial institutions need to be aware of. Caveats to the CTL can be made for industries or specific countries. The CTL for countries affected by the invasion of Ukraine, for example, was caveated at ELEVATED.

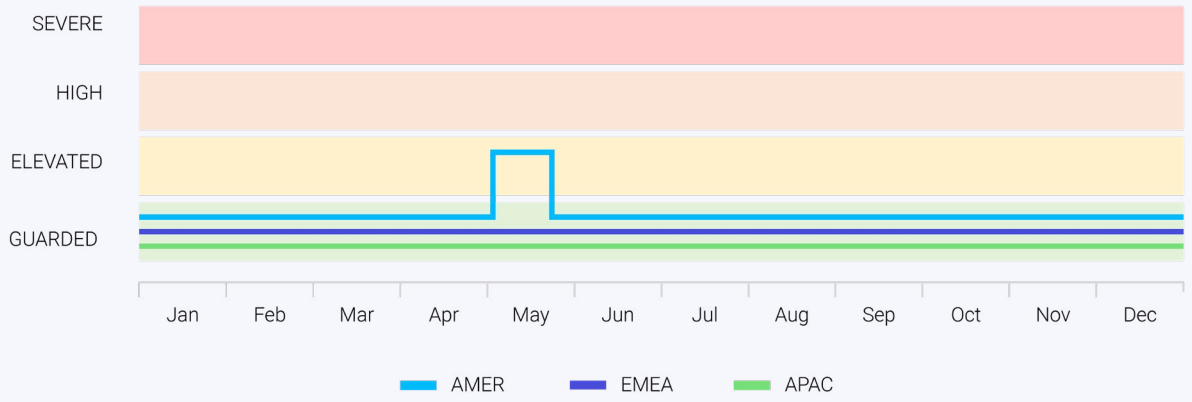
Firms should consider making threat management and residual cyber risk assessment a multi-team function, taking the FS-ISAC regional CTL into context as they calculate their individual stance.

Regional Cyber Threat Levels

On 2 May 2024, the AMER Cyber Threat Level increased from **GUARDED** to **ELEVATED** during an out-of-cycle TIC vote.

The TIC voted to raise the Cyber Threat Level to **ELEVATED** as ongoing Scattered Spider activity increased the cyber threat from a credible, sophisticated actor. In an **ELEVATED** situation, implementation of additional cybersecurity measures may be warranted. FS-ISAC published detailed guidance for members on mitigating the threat from Scattered Spider.

On 23 May 2024, the AMER Cyber Threat Level decreased from **ELEVATED** to **GUARDED**.



Supply Chain Incidents

Supply chain risk is one of the top concerns of the financial sector globally. Because many firms rely on the same service providers, an outage at one can impact many firms simultaneously. This concentration risk applies throughout the supply chain.

The financial sector must therefore ensure the security and resilience of companies vital to its IT infrastructure and other critical services. To that end, many in the sector are investing in enhanced third-party risk management infrastructure and processes.

Several high-profile issues have proved the efficacy of that approach as software vulnerabilities impacting the supply chain — such as the discovery of an XZ Utils backdoor and the Polyfill CDN service [11] — and zero-day vulnerabilities keep the sector on high alert.

Zero-day vulnerabilities are those without patches. These incidents offer adversaries a head start until a patch is developed and can pose a substantial threat if the target is critical to a firm's operations.

Such vulnerabilities were discovered in Cleo managed file transfer (MFT) products in 2024. MFT platforms offer enhanced encryption for sensitive data in flight and at rest and can automate many financial sector transfer processes. As noted last year, attacks on MFT vendors are a concerning trend: a breach can expose the vendor's clients' data to threat actors and cause significant financial, compliance, and reputational harm. The Russian-speaking Cl0p ransomware group claimed responsibility for the Cleo incident and the breach of the MOVEit MFT in 2023. [12, 13, 14, 15]

XZ Utils

XZ Utils is a widely used open-source data compression software package present in almost all Linux distributions and other Unix-like operating systems. In March 2024, it was discovered that malicious code had been deliberately inserted into the XZ libraries that could permit unauthorized remote access to the victim's entire system. [16]

Predictions

- Prompted by direct regulatory mandate and/or pressure from financial services clients and other large customers, the financial sector's supply chain will increase cybersecurity and resilience investments to reduce risk exposure.
- Financial institutions will seek diversification by utilizing smaller or more local suppliers. That will reduce concentration risk, but if those vendors are less cyber mature than those they replace, the move could increase cyber risk and pressures on firms' risk management functions.

Fraud

Fraud is surging in the financial sector, as well as in sectors where financial channels are used, such as social media and telecoms. Real-time payments infrastructure, cryptocurrencies, and decentralized finance mechanisms make it virtually impossible to retrieve stolen funds.

Meanwhile, fraud and scam operators increasingly function with the rigor of legitimate businesses. Indeed, scams-as-a-service operations have become more structured, efficient, and effective in the last one to two years. Scam compounds — facilities where human trafficking victims are forced to conduct cybercrimes — scaled up in 2024, increasing the potential for social engineering frauds.[17] Moreover, money mule intelligence shows that fraud usually crosses borders, so global collaboration on fraud intelligence is essential. Using cyber intelligence and network tools to fight fraud is a fast-growing trend in the financial sector, enabling cyber, fraud, and other teams to combine their unique skillsets into a holistic approach of fraud prevention.

Top 10 Fraud Attack Patterns

FS-ISAC Member Reporting, July - December 2024

1. Business email scam
2. Impersonation
3. Account takeover
4. Payroll diversion
5. Social engineering
6. Card fraud
7. Manipulated invoice
8. Domain spoofing
9. Extortion
10. Check fraud

Leveling Up:
A Cyber Fraud Prevention Framework for Financial Services

Read here ↗

Use this Framework to improve coordination across cyber and fraud departments.

Examples of Innovative Frauds in 2024

- Impersonating law firms in social engineering schemes to trick victims into paying fake overdue invoices.
  - Crimson Kingsnake imitated a UK law firm using Microsoft's cloud services onmicrosoft.com domains to appear legitimate.
- Fabricating invoices to lure victims with indicators of urgency and vague or nonexistent formal documentation.
  - One threat actor attempted to make an invoice appear legitimate with a fake backdated email chain containing a conversation between an executive within the institution and a vendor. The invoice was flagged as fraudulent when the recipient realized there were no email banners in the chain, indicating the "vendor's" emails were falsified.

Predictions

- Fraudsters will exploit uncertainties caused by changes in political, regulatory, and business environments (i.e. investment scams leveraging economic trends).
- Online scammers will continue to develop complex operational structures with highly differentiated roles and functions and add more "staff," many of them kidnapping victims.
- Scam compounds will become better resourced through the rising value of stolen cryptocurrency, which will make the compounds' operators more attractive targets for other thieves.
- Cybersecurity, fraud, and other teams will champion smart friction, i.e., strategically placed obstacles in the user experience designed to increase security and slow payment authorizations. Firms will determine that these temporary obstacles are needed to limit fraud and help maintain trust in the financial system.
- Firms across industries will step up investments in fraud prevention and detection to stop fraud before it happens as opposed to mitigation after it has already occurred. Such efforts include real-time transaction monitoring, new authentication solutions, and updated employee and customer training and awareness programs to meet evolving fraud methods. Fraud intel shared internally, with peer organizations, with other sectors, and across geographies will enable faster, more targeted defense.
- The cross-border, cross-sector nature of fraud will require more private- and public-sector partnerships across multiple industries.

Ransomware

Ransomware continues to be a serious and pervasive threat to business continuity, reputation, and profitability across sectors. Low-skill threat actors have powerful tools — Ransomware-as-a-Service (RaaS), GenAI, open-source code, etc. — to enable their crimes. Ransomware operators have shown their ability to rebrand, re-organize, and adapt their tactics despite, and in some cases because of, law enforcement's disruptive actions.

$75M USD

Ransomware payment made by an undisclosed victim in 2024, the largest ransomware payment on record.

In 2024, the number of reported ransomware attacks decreased, but the amounts threat actors demanded to release stolen data increased. Indeed, reports indicate that 2024 was one of the highest-grossing years yet for ransomware operators, largely due to fewer but higher profile attacks that deliver larger payouts (known as "big game hunting"). [18]

Ransomware Essentials: A Guide for Financial Services Firm Defense

> Ransomware mitigation best practices
> Incident response
> Crisis management
> Considerations on paying ransoms

Read here ↗

To publicize their activities, gain notoriety, and name and shame victims, ransomware groups typically make use of leak sites on Tor or other channels such as Telegram. Leak site data from 2024 shows that the "financial and insurance" sector — as it is termed in the US Census Bureau's North American Industry Classification System (NAICS) [19] — is the fourth most affected sector and accounts for around 8% of all identified leaks. Analysis of leak site data shared with FS-ISAC by our partners suggests that ransomware attacks are now more dispersed across a wider pool of ransomware threat actors.

However, victims are still likely to be opportunistically chosen rather than specifically targeted. Many victims are the third-party services and providers that make up the NAICS Professional, Scientific, and Technical Services sector. That sector accounted for almost 19% of victims, highlighting the increased exposure of the financial sector via third-party incidents.

The trend of ransomware operators using double- and triple-extortion tactics to coerce victims into paying persists, as does the rebranding of RaaS operators.

Double- and Triple-Extortion

Incidents in which a ransomware attack is combined with other tactics, such as a DDoS attack, divulging the incident to the victim's customers and clients, or data exfiltration combined with the threat of disclosing the stolen data publicly.

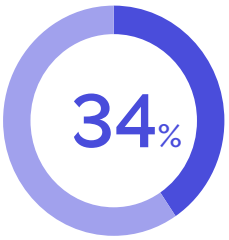
RaaS operators may rebrand when targeted by government sanctions (as the affiliates and associates of high-impact ransomware groups often are) because paying a ransom to a sanctioned entity is a legal offense. By rebranding, threat actors appear to be unsanctioned, which deludes victims and potentially increases the likelihood of payment. RaaS groups may also rebrand if they have drawn too much attention from law enforcement, which endangers the group and its affiliates. For example, an affiliate of the DarkSide ransomware group is believed to have rebranded as BlackMatter after the 2021 Colonial Pipeline attack.

Predictions

- In 2025, ransomware groups will continue to evolve and adapt, leveraging endpoint detection and response (EDR) evasion toolkits, BYOVD (Bring Your Own Vulnerable Driver) techniques, and GenAI for automation and content customization.
- As law enforcement continues to target high-profile ransomware operators that disrupt critical services, more threat actors will drop encryption and resort to data extortion.
- Stricter reporting mandates and penalties for ransomware incidents will be introduced by governments and regulatory bodies to encourage organizations to enhance their cybersecurity postures and transparency.
- Relaxed cryptocurrency regulation in the US could lead to increased opportunities for ransomware actors to monetize their activities.

DDoS

The sector continues to be a primary target for Distributed Denial of Service (DDoS) attacks. Akamai reported that financial services was the most frequently targeted sector in 2024, accounting for 34% of attacks last year. [21,22]



Financial services accounts for over a third of DDoS attacks. [20]

Cybercriminal and hacktivist groups employ DDoS tactics to disrupt operations and undermine trust in the global financial system through impacting the availability of customer-facing websites and apps. In the last year, geopolitically-driven events – including the US elections, escalating Middle East hostilities, and the ongoing Russia/Ukraine conflict – were key catalysts for hacktivist-driven DDoS campaigns. Threat actors frequently targeted organizations, including financial institutions, that were peripheral or non-players in related events.

The outcomes of DDoS campaigns can be severe – attacks on Japanese, Indian, and Australian firms had impacts on many digital financial operations. [23,24,25] Moreover, monitoring the hacktivists' activity continues to be a challenge for the defending organizations, given the wide range of active threat actors, their varying degrees of sophistication, and the amount of noise they generate.

DDoS: Here to Stay

Read our report written with Akamai to learn how financial services firms can mitigate the impacts of DDoS attacks.

Read here ↗

Predictions

- As firms and suppliers expand their use of application programming interfaces (APIs), attackers will target mission critical endpoints across a wide range of technology resources. These attacks will be precise, carried out by threat actors who know their targets' architectures well.
- Private operators will generate income with destructive "DDoS-as-a-service" offerings.
- Threat actors will try to circumvent DDoS defense mechanisms by testing attack vectors across numerous institutions in a systematic and methodical approach, then deploy multivector, high-volume DDoS attacks.
- Threat actors will become increasingly agile and analytical, employ more reconnaissance, and use DDoS as a smokescreen for higher-value attacks. That may affect firms' material risk calculations.

Emerging Technologies

Generative AI

Generative AI's beneficial use cases have proliferated among financial services firms and vendors, primarily to automate and expedite business operations.

However, GenAI is a tool that can be used maliciously as well. Threat actors have leveraged large language models (LLMs) – a form of GenAI – to increase the volume and sophistication of their attacks. Though some feared that LLMs would be used to create new types of exploit, thus far, threat actors are more likely to employ LLMs to lower their barriers to entry and more rapidly leverage known vulnerabilities and opportunities. [26]

For example, content generated by AI can make adversarial social engineering campaigns more effective – phishing emails in particular are increasingly crafted with convincing business language and information specific to the targeted individual. Observers have noted an increase in emails written in languages not often associated with such campaigns, as GenAI makes it easier to execute phishing attacks in many languages.

GenAI's business use cases in financial services can include:

- Detecting fraud
- Summarizing documents
- Analyzing and reporting financial data
- Automating technical support and customer service
- Market research
- Coding

Because threat actors can use GenAI to innovate on existing threat vectors, financial institutions are encouraged to strengthen their fraud detection controls — particularly their employee training on phishing — as well as:

> Implement careful governance of personally identifiable information (PII) in AI-backed systems

> Exclude proprietary, sensitive, or confidential data in publicly accessible LLMs

> Use a human-in-the-loop approach in which employees are accountable for providing input and oversight to enhance the accuracy, reliability, and adaptability of AI systems

Predictions

State-sponsored threat actors will continue to attack via "AI poisoning," i.e. sabotaging training datasets or overwhelming them with propaganda or inaccurate data so that outputs will be incorrect or incoherent.

As businesses develop new GenAI use cases, employees will become more likely to use it inappropriately or without cybersecurity's oversight (i.e. "shadow AI"). That will challenge firms' ability to meet regulatory requirements, manage data properly, ensure the validity of company information, and adhere to copyright protections.

AI usage in some functions may remain in experimental stages longer than expected to mitigate against over-confidence in outputs caused by anthropomorphization (e.g. assigning human traits to non-human things). As AI proliferates across the sector and the broader economy, firms will need robust quality assurance processes to correct for anthropomorphization.

Deepfakes

Similarly, rather than create new threat vectors, adversaries are using deepfakes to execute more sophisticated — but familiar – exploits, notably C-Suite impersonation and social engineering scams. In such incidents, a threat actor uses GenAI tools to create synthetic, interactive versions of company officials or fellow employees that trick victims into giving the cybercriminal money, information, or access to the firm's systems. This was observed in a February 2024 attack in which a Hong Kong finance worker paid cybercriminals $25 million USD when tricked by a deepfake of the company's chief financial officer in a video conference call. [27]

These impersonation attacks are often powered by easily accessible and inexpensive deepfake and voice-cloning technologies. These tools allow low-skilled threat actors to achieve large-scale thefts, adapt quickly, and maintain longer dwell times without detection.

Mixed online/offline strategies make it hard to detect malicious activity, which can facilitate cyber espionage, destruction, and fraud activities. Deepfakes are also being used to impersonate job candidates, as noted in the section on the Democratic People's Republic of Korea, with implications for national security as well as business compromises.

Deepfake frauds may be more effective as the image of a known person can be exceptionally convincing. However, existing controls and fundamental cyber hygiene — notably training — are effective defenses for these attack vectors, when executed properly.

Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks

Read here ↗

For guidance on mitigating the impact of deepfakes, read the FS-ISAC AI Risk Working Group's 2024 white paper.

Predictions

- Impersonation attacks will increase over the coming 12 months. Threat actors have thus far tended to impersonate executives, but may soon impersonate a broader spectrum of employees to facilitate entry points for lateral movements. That will present new challenges for customer and staff authentication systems.
- North Korean IT worker impersonation campaigns will expand and evolve in 2025 to fund government operations.

Quantum Computing

Though still not commercially available, quantum computing is advancing. In December 2024, Google unveiled its "Willow" quantum processor and in February 2025, Microsoft and Amazon announced significant progress in the production of their quantum chips, Majorana and Ocelot, respectively. [28, 29]

Nation-states are also key contestants in the race for quantum supremacy. Given the national security and espionage advantages of keeping advances classified, the true state of progress of the technology among countries is not publicly known, and may not be until well after major quantum breakthroughs are achieved.

From a commercial perspective, widespread availability of quantum computing is likely to create positive benefits — particularly for solving complex problems quickly — but it also introduces a threat to current cryptography, as quantum computers could break asymmetric cryptography algorithms commonly used today.

This progress underscores the sector's need to address the migration to quantum-resilient cryptography algorithms. FS-ISAC recommends that firms adopt a cryptographically agile approach now — i.e. develop the ability to quickly change algorithms — so they can more easily adapt to evolving cryptographic algorithms, protocols, and standards without disrupting the firm's infrastructure significantly. It could take some financial institutions years to inventory their cryptography usage and mature their operations. Starting before quantum computers are released enables institutions to begin prioritizing risks, resolving complex issues around compatibility and integration with legacy systems, and replacing at-risk algorithms with quantum-resilient cryptography. The timeline on quantum is still uncertain, but given recent breakthroughs and investments in the technology, the sector can't afford to wait on the shift to crypto agility.

Quantum Cryptography and Cryptographic Agility Guidance

FS-ISAC's Post Quantum Cryptography Working Group released several advisories on post quantum cryptographic agility to assist firms in migrating to a more crypto-agile posture.

Read here ↗

Predictions

- Leaders will struggle with the decision to make meaningful investments in post quantum cryptography as more immediate needs take precedence. Firms that delay the migration to quantum-resilient algorithms may face elevated risk exposure.
- At first, quantum computers will be so expensive that only their manufacturers and governments will have them. Financial firms will rent time on quantum systems, as many do on cloud systems today.

Geopolitically-Driven Cyber Activity

People's Republic of China

Threat actors associated with the People's Republic of China (PRC) tend to be among the most sophisticated in the world. Their activities tend towards espionage aligned with Chinese foreign and military policy. The financial sector's key providers, such as technology and telecoms operators, are often direct targets of Chinese state-sponsored cyber activities. Therefore, the financial sector tracks Chinese threat actors closely.

Threat actors linked to the PRC conduct extensive target research, possess the tools and knowledge for successful attacks, and dedicate ongoing resources to maintaining persistence within a target environment after initial compromise.

Targets

While financial institutions are rarely priority targets at time of publication, it is conceivable that PRC-related threat actors may conduct more cyber espionage related to sanctions, tariff disputes, opposition funding, Taiwanese defense funding, and other financial information moving forward. As disputes over trade and tariffs accelerate, cyber groups linked to the Ministry of State Security (MSS) may focus their espionage efforts against business targets. MSS is thought to be connected to Salt Typhoon, [30] which infiltrated several major US telecommunication companies and internet service providers, potentially gaining troves of information including US government communications. [31]

Impacts

With the growing tensions in Taiwan, state-sponsored cyber activity appears to be turning towards pre-positioning — rather than information and intellectual property theft — on network infrastructures in multiple countries for attacks against critical infrastructure sectors. [32] Reports from government agencies, including those of the Five Eyes group, [33] indicate that Volt Typhoon attacks could disrupt or destroy critical services within strategic targets.

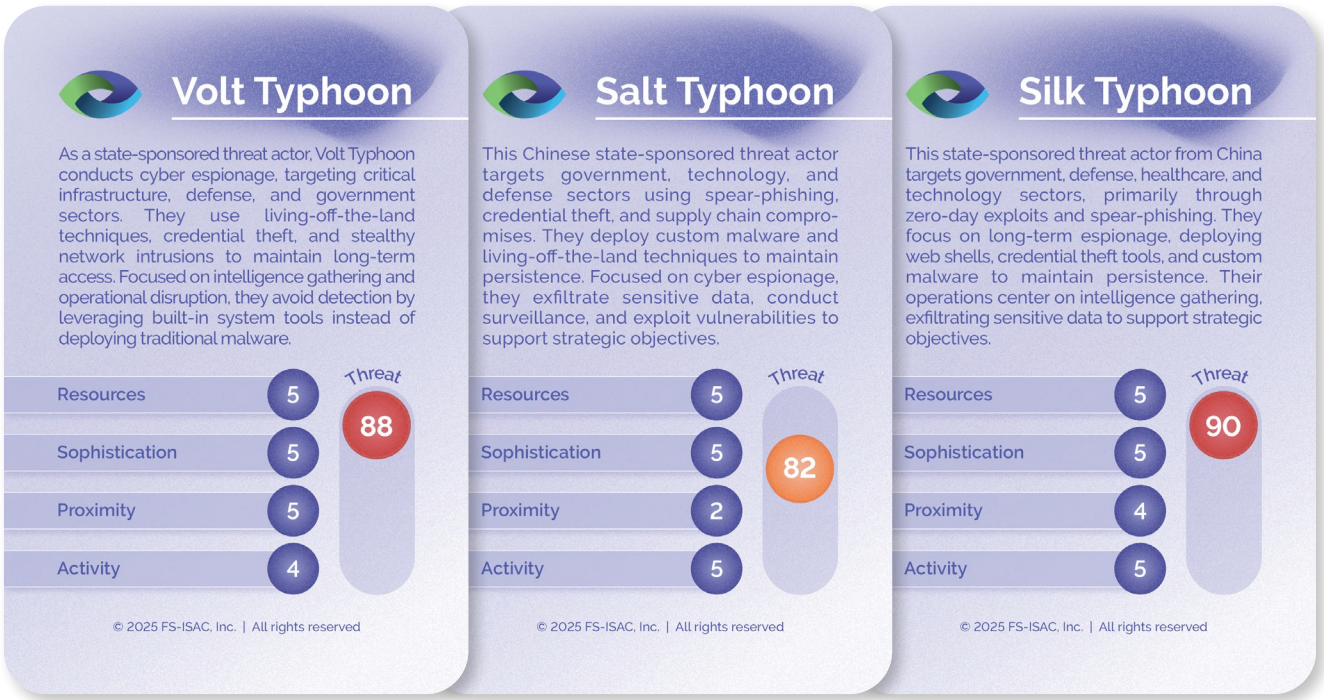
Pre-Positioning

Pre-positioning refers to an intrusion into IT networks in order to launch disruptive or destructive cyber attacks and enable lateral movement in the event of geopolitically-driven tensions and/or military conflicts.

New national security and data laws mandated by the PRC could negatively impact the business activities of foreign companies operating in China or that have relationships with PRC firms. In response, some have modified core operational activities, reviewed business travel protocols, and limited the export of sensitive technology to China. [34]

Further, it is possible for financially motivated groups affiliated with state agencies to use the tactics employed by state-sponsored threat groups — such as exploiting vulnerabilities, targeting systems on the network edge, and compromising suppliers or the supply chain — to steal money or data.

Notable Chinese Threat Actors



These threat actors cards -- and those in the sections covering the Russian Federation, the Islamic Republic of Iran, and the Democratic People's Republic of Korea -- are examples of threat actor cards distributed to members at our regional Summits around the world. The Global Intelligence Office determines the Threat Score by assessing, weighting, and calculating threat groups' intent and capability on a scale of 0 to 100.

The Russian Federation

Russian state-sponsored cyber activities have largely focused on the conflict in Ukraine. However, connections between state-sponsored and financially motivated threat actors may exist in various forms.

Though geopolitically-driven cyber activity remains highly relevant to the war effort, state-affiliated cybercriminals do target the financial sector. These attacks can be noisy, such as denial of service attacks or intrusion campaigns.

With peace negotiations tenuously starting with Ukraine and international power dynamics shifting, it is likely that state-sponsored cyber activities will mirror the changing political and military landscape. That may increase the potential for cyber espionage exploits and destructive cyber attacks unrelated to the Ukraine war. Sanctions may encourage state-sponsored cyber threat actors to leverage their ties to cybercriminal networks for financially motivated cyber attacks.

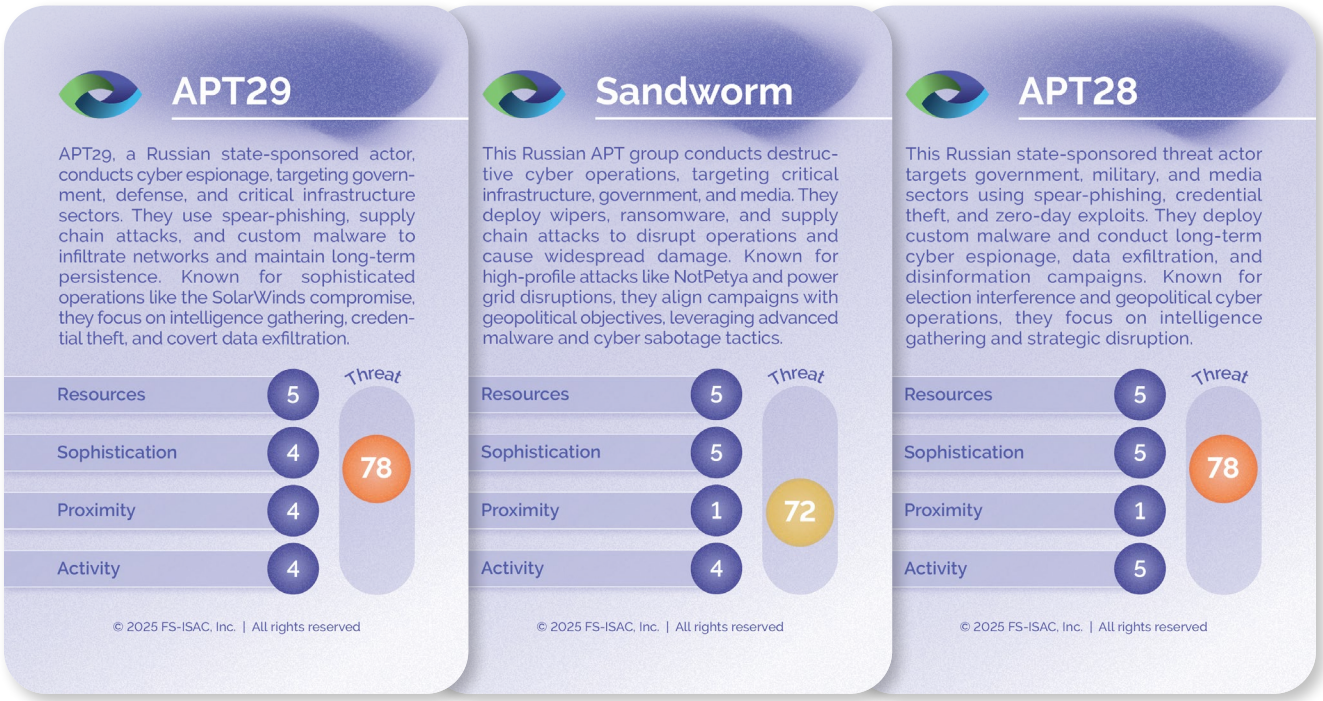
Targets

Typically, Russia deploys its espionage, disruption, and disinformation cyber campaigns in the West, the North Atlantic Treaty Organization (NATO) countries, and countries that either provide support to Ukraine or otherwise oppose Russia's objectives. Russia is known for its influence operations and is actively operating across many countries to undermine alliances.

Impacts

One of the most impactful exploits of the first half of 2024 was Midnight Blizzard's attack on Microsoft. The incident resulted in a major intrusion of Microsoft's systems, including the email accounts of senior executives. While most of the impact on the financial sector from Russian nation-state cyber operations is indirect, some campaigns directly affect the sector. In June 2024, for instance, the European Banking Authority warned of misinformation campaigns that could lead to runs on bank deposits amid fake news of liquidity problems. [35] Such campaigns could be initiated by Russian disinformation and propaganda networks.

Notable Russian Threat Actors



The Islamic Republic of Iran

Iranian government cyber operations include espionage, but Iran is more prone to cyber warfare activities such as disruptive or destructive attacks. Israel is a primary focus for Iran's cyber activities, which may impact financial services firms that rely on Israeli third-party suppliers. [36]

Iranian state-run cyber groups' activity largely aligns with national interests, which now focus on re-establishing Iran's allies in the region, suppressing opposition, and stabilizing Iran's economy amidst sanctions. Several hacktivist groups support Iranian goals — some are accused of being state-run groups in disguise – including a coalition that announced in early November that it would launch a coordinated cyber campaign against Israel, including its financial sector.

The Iranian financial sector experienced a cyber attack as well, which disrupted the operations of the Central Bank of Iran and several other Iranian banks in August 2024.

Targets

Financial institutions are not a primary target of Iran's adversarial cyber activity, but Iran's growing interest in conducting supply chain attacks is likely to increase the middle- to long-term threat to financial services. [37]

Impacts

There is a realistic possibility that attacks on Israeli targets — whether by state actors or hacktivists — could disrupt suppliers in Israel, with potential impacts on service provision and data security for the global financial services sector.

Notable Iranian Threat Actors

MuddyWater

This Iranian APT group conducts cyber espionage, targeting government, defense, and telecom sectors. They use spear-phishing and PowerShell-based malware for initial access, deploying backdoors and remote access tools to maintain persistence. Their operations focus on intelligence gathering, leveraging social engineering and credential harvesting to infiltrate and monitor targeted networks.

Resources	5
Sophistication	5
Proximity	1
Activity	4
Threat	72

Charming Kitten

Charming Kitten in an Iranian APT that conducts cyber espionage, targeting government, media, and human rights organizations. They use spear-phishing, social engineering, and credential harvesting to gain access to sensitive data. Deploying custom malware and impersonating trusted entities, they focus on long-term infiltration, surveillance, and intelligence gathering to support strategic objectives.

Resources	5
Sophistication	5
Proximity	3
Activity	3
Threat	74

OilRig

OilRig is an Iranian state-sponsored group that targets government, financial, and telecom sectors using spear-phishing and supply chain attacks. They deploy custom backdoors, credential harvesting tools, and PowerShell-based malware to establish persistence. Focused on cyber espionage, they exfiltrate sensitive data, leveraging compromised accounts and lateral movement to maintain long-term access to networks.

Resources	5
Sophistication	3
Proximity	3
Activity	4
Threat	68

Democratic People's Republic of Korea

The financial sector has become increasingly aware of the clear insider threat posed by Democratic People's Republic of Korea (DPRK) remote workers applying for IT-related jobs around the world. These fraudulent workers often use front organizations and sometimes deepfake technology to apply for and gain employment to enable malicious cyber intrusions, steal money or information, or conduct espionage. [38, 39] In May 2024, the US Department of Justice reported that over 300 such fraudulent employees were hired in US companies, including banks and other financial service providers. [40]

Sanctions on North Korea inhibit legitimate financial activity, so state-sponsored cyber groups are known to generate revenue through cryptocurrency heists and ransomware attacks (or collaborating with ransomware actors who provide initial access points). [41]

DPRK Cyber Characteristics

North Korean nation-state cyber activity can be sophisticated, agile, and possess both the intent and the capability to carry out destructive cyber activities against a diverse range of targets.

Targets

DPRK threat actors are highly proficient in conducting tailored, elaborate social engineering campaigns against employees of decentralized finance ("DeFi"), cryptocurrency, and "Web 3.0" companies to deploy malware and steal cryptocurrency. [42] While crypto-related companies are a potential target, financial institutions that invest or deal with cryptocurrencies could be impacted by future DPRK thefts. [43, 44]

Impacts

DPRK threat actors are also adept at launching skillful software supply chain attacks, giving them unrestricted access to and impact on a wide range of organizations. It is also expected that DPRK threat actors will continue exploiting vulnerabilities in blockchain technology, gaming companies, and cryptocurrency exchanges to generate and launder funds to support the government and its weapons programs. [45]

$2.2B USD

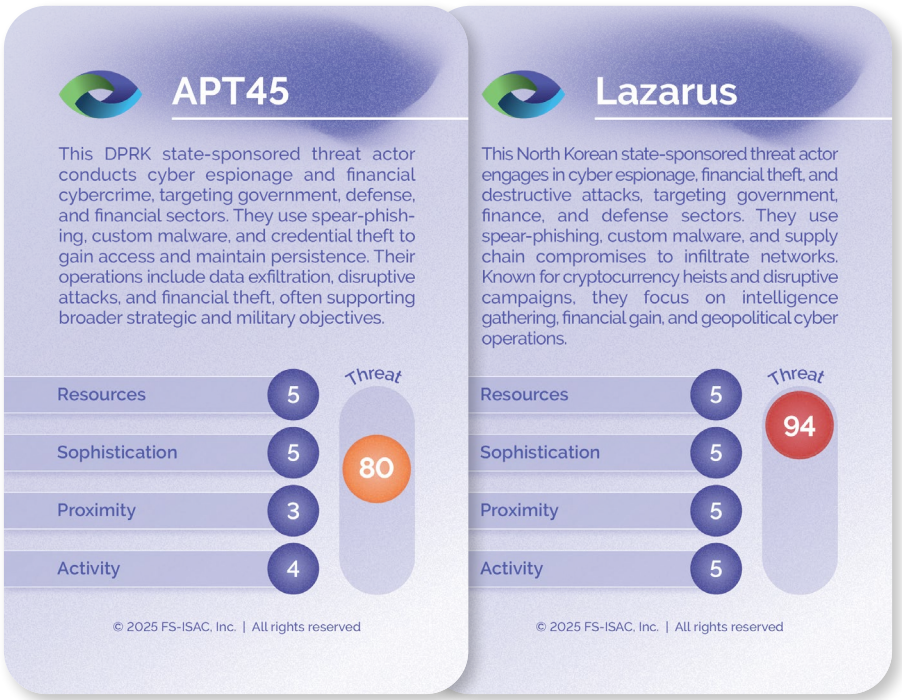
stolen by DPRK threat actors from cryptocurrency platforms in 2024

61%

of all stolen cryptocurrency in 2024 stolen by DPRK cybercriminals

Chainanalysis [46]

Notable North Korean Threat Actors



Predictions

- More geopolitically-driven attacks will occur, impacting multiple industries and countries. In particular, military action in the Middle East and Ukraine will continue to drive politically and ideologically motivated attacks against governments, companies, industries, and citizens.
- Threat actors in sanctioned nations, such as the DPRK, will attempt more financially motivated crimes to fund their governments' activities.
- Threat actors will increasingly target terrestrial infrastructure, subsea cables, and low-Earth orbit satellites.
- Volatile geopolitical environments will increase firms' threat surface and offer cybercriminals more opportunities for attack, such as mis- and disinformation campaigns feeding on political and social uncertainty.

Regional Close-Up

EMEA

- DORA went into effect 17 January 2025. More information is in the Regulation section.
- The EMEA financial sector was the target of 49% of DDoS attacks in 2024, down from 66% in 2023, according to Akamai research.

APAC

- Scam compounds run by complex criminal networks are a growing concern across Southeast Asia.
- Australia passed the Cyber Security Act in November 2024, mandating minimum cybersecurity standards for smart devices and ransomware, as well as reporting obligations for certain businesses targeted for cyber extortion.
- Australia, Japan, and India were attacked with a coordinated series of DDoS campaigns starting in October.

LATAM

- Mexico experienced over half of all cyber attacks in Latin America, mainly due to its economic proximity to the United States. [47]
- In March, Chile became the first country in the region to establish both a cybersecurity agency and a regulatory framework.

NAM

- The financial services sector was targeted in large-scale typosquatting campaigns, in which criminals deliberately misspell legitimate names in URLs to trick users and harvest sensitive information.
- Scattered Spider, believed to be based primarily in the US, the UK, and Canada, launched highly targeted attacks that repeatedly impacted the financial services sector.
- Firms across the US and Canada hired DPRK threat actors who posed as IT professionals in order to misappropriate data, steal money, and conduct espionage.

New Regulations in 2024

After years of discussion around regulatory harmonization, the global regulatory environment is becoming more fragmented, a reflection of shifting geopolitical dynamics. Firms operating in multiple jurisdictions are expected to face increasingly complex compliance challenges as cyber regulations continue to diverge in a rapidly evolving regulatory landscape.Recent legislation in many jurisdictions has extended regulatory focus on financial firms' cybersecurity and resilience to that of their most important suppliers.

DORA and NIS2

The EU's Digital Operational Resilience Act (DORA) applies to applies to financial services institutions conducting business in the EU, including banks, credit unions, insurance companies, investment firms, cryptocurrency-asset service providers, and crowdfunding platforms. [48] Many organizations are applying DORA regulations to their operations outside the EU to gain efficiency through consistency.

A key aim of the DORA regulation is to harmonize digital resilience regulations throughout the EU, which brings Information and Communication Technology Critical Third-Party Providers (ICT CTPPs) into the direct scope of financial regulation. FS-ISAC members consistently report that third-party risk management is one of their most substantial cybersecurity challenges. [49]

DORA's Article 45 requires firms to share indicators of compromise (IOCs), adversaries' tactics, techniques, and procedures, cybersecurity alerts, and configuration tools in a safe, secure, and trusted manner. FS-ISAC membership enables firms to fulfill Article 45's conditions by using FS-ISAC offerings to share information and intelligence.

By 17 October 2024, the Network and Information Security 2 Directive (NIS2) [50] required EU member states to regulate cybersecurity, ICT systems, and networks on a national level in 18 sectors. [51] NIS2 and DORA often overlap but DORA requirements take precedence, so DORA compliance is the focus in many financial firms.

DORA Guidance and Advice

FS-ISAC facilitated members' DORA compliance throughout 2024 with white papers produced by the FS-ISAC DORA Working Group and FinCyber Today podcasts featuring leading EU financial services executives. See them here:

Digital Operational Resilience Act (DORA): Implementation Guidance

Read here ↗

Burim Bivolaku: Financial Sector Collaboration is Key to Third-Party Risk Management

Watch here ↗

DORA Information Sharing Requirements and FS-ISAC Membership

Read here ↗

Beate Zwijnenberg: Can Cyber Risks be Quantified?

Watch here ↗

Contact

fsisac.com

media@fsisac.com

References and Resources

1 Mascellino, A. (2025) 'NPM packages target GitHub SSH keys', Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/news/npm-packages-target-github-ssh-keys/

2 Ivanti (2024) 'CVE-2023-46805 Authentication Bypass, CVE-2024-21887 Command Injection for Ivanti Connect Secure and Ivanti Policy Secure Gateways', Ivanti Forums. Available at: https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

3 SC World (2025) 'Nova Sentinel infostealer deployed via inactive PyPI package', SC World. Available at: https://www.scworld.com/brief/nova-sentinel-infostealer-deployed-via-inactive-pypi-package

4 Google Cloud. (2025) UNC5537: Snowflake Data Theft and Extortion. Google Cloud Blog. Available at: https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

5 NCSC (2024) 'Halbjahresbericht 2024/1', NCSC. Available at: https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/berichte/lageberichte/halbjahresbericht-2024-1.html

6 Cybersecurity and Infrastructure Security Agency (CISA). (2023) Title of the advisory. CISA. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

7 Gatlan, S. (2025) Chinese hackers breached 20,000 FortiGate systems worldwide. BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/chinese-hackers-breached-20-000-fortigate-systems-worldwide/

8 Jones, D. (2025) CrowdStrike mismatch causes Falcon sensor outage. Cybersecurity Dive. Available at: https://www.cybersecuritydive.com/news/crowdstrike-mismatch-falcon-sensor-outage/723569/#:~:text=CrowdStrike%2C%20in%20a%20root%20cause,leading%20to%20the%20system%20crash.

9 Forbes (2024). Microsoft Confirms New Outage Was Triggered By Cyberattack. Published 31 July.

10 DocumentCloud (2025) Letter to Chairman Brown and Ranking Member Scott. Available at: https://legacy.www.documentcloud.org/documents/25472740-letter-to-chairman-brown-and-ranking-member-scott/

11 D'Agnolo, C. (2025) More Than 100k Websites Targeted in Web Supply Chain Attack. Available at: https://cside.dev/blog/more-than-100k-websites-targeted-in-web-supply-chain-attack

12 Cleo. (2024) Cleo Product Security Advisory CVE-2024-50623. Cleo Support. Available at: https://support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623?ref=labs.watchtowr.com

13 Huntress (2024). Threat Advisory: Oh No Cleo! Cleo Software Actively Being Exploited in the Wild. Published 09 December.

14 IBM (2025). What is managed file transfer (MFT)? Available at: https://www.ibm.com/think/topics/managed-file-transfer#:~:text=Managed%20file%20transfer%20(MFT)%20is,in%20compliance%20with%20applicable%20regulations

15 Rapid7 (2024). Authentication Bypasses in MOVEit Transfer and MOVEit Gateway. Published 25 June. Available at: https://www.rapid7.com/blog/post/2024/06/25/etr-authentication-bypasses-in-moveit-transfer-and-moveit-gateway/

16 Goodin, D. (2024) What We Know About the XZ Utils Backdoor That Almost Infected the World. Available at: https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/

17 Regan, H., Watson, I., Rebane, T., and Olarn, K. (2025) Myanmar scam center crackdown. CNN.

Available at: https://www.cnn.com/2025/04/02/asia/myanmar-scam-center-crackdown-intl-hnk-dst/index.html

18 Chainalysis (2024). 2024 Crypto Crime Mid-year Update Part 1: Cybercrime Climbs as Exchange Thieves and Ransomware Attackers Grow Bolder. Published 15 August.

19 North American Industry Classification System (NAICS) U.S. Census Bureau

20 Akamai Technologies. (2024) Financial Services Trends 2024. Akamai. Available at: https://www.akamai.com/lp/soti/financial-services-trends-2024

21 Akamai (2024). Akamai Finds Geopolitical Tensions Driving Surge in DDoS Attacks on Financial Institutions. Published 17 September.

22 Microsoft Tech Community. (2024) Understanding the Evolving Threat of DDoS Attacks in 2024. Microsoft Tech Community. Available at: https://techcommunity.microsoft.com/blog/azurenetworksecurityblog/understanding-the-evolving-threat-of-ddos-attacks-in-2024/4362031

23 Chakravarti, J. (2025) Japanese businesses hit by surge in DDoS attacks. BankInfoSecurity. Available at: https://www.bankinfosecurity.com/japanese-businesses-hit-by-surge-in-ddos-attacks-a-27216

24 CM Alliance. (2024) December 2024: Major Cyber Attacks, Data Breaches, Ransomware Attacks. CM Alliance. Available at: https://www.cm-alliance.com/cybersecurity-blog/december-2024-major-cyber-attacks-data-breaches-ransomware-attacks

25 Radware. (2025) Pro-Russian and Pro-Palestinian Hacktivists Targeting Australian Organizations. Radware. Available at: https://www.radware.com/security/threat-advisories-and-attack-reports/pro-russian-and-pro-palestinian-hacktivists-targeting-australian-organizations/

26 TechRepublic. (2024). OpenAI GPT-4 exploit vulnerabilities. Retrieved from https://www.techrepublic.com/article/openai-gpt4-exploit-vulnerabilities/

27 CNN (2024). Deepfake CFO scam in Hong Kong. Published 4 February. Available at: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk#:~:text=A%20finance%20worker%20at%20a,according%20to%20Hong%20Kong%20police

28 Microsoft Azure. (2025). Microsoft unveils Majorana 1: The world's first quantum processor powered by topological qubits. Retrieved from https://azure.microsoft.com/en-us/blog/quantum/2025/02/19/microsoft-unveils-majorana-1-the-worlds-first-quantum-processor-powered-by-topological-qubits/

29 Amazon. (2025). Quantum computing: AWS Ocelot chip. Retrieved from https://www.aboutamazon.com/news/aws/quantum-computing-aws-ocelot-chip

30 Wall Street Journal. (2024, October 7). China cyberattack on internet providers. Retrieved from https://archive.ph/20241007181947/https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835

31 Wall Street Journal. (2025, October 5). U.S. wiretap systems targeted in China-linked hack. Retrieved from https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b

32 US Cybersecurity and Infrastructure Security Agency (2024), PRC State-Sponsored Actors Compromise and Maintain Persistent Access to US Critical Infrastructure. Published 07 February.

33 Office of the Director of National Intelligence. (n.d.). ICIG FIORC. Retrieved from https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc

34 US Office of the Director of National Intelligence (2024). Annual Threat Assessment of the U.S Intelligence Community. Published 05 February.

35 Reuters (2024). Beware of wartime fake news triggering a run, EU banks told. Published 01 April.

36 Microsoft (2024). Iran surges cyber-enabled influence operations in support of Hamas. Published 26 February 2024.

37 Microsoft (2024). Microsoft Digital Defense Report 2024. Published on 15 October 2024.

38 Google Cloud. (2024, September 23). Mitigating DPRK IT worker threat. Retrieved from https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat

39 U.S. Department of the Treasury. (2022, May 16). Guidance on the Democratic People's Republic of Korea Information Technology Workers. Retrieved from https://ofac.treasury.gov/media/923126/download?inline

40 United States Department of Justice (2023). Charges and seizures brought in fraud scheme aimed at denying revenue to workers associated with North Korea. Published 16 March. Available at: https://www.justice.gov/archives/opa/pr/charges-and-seizures-brought-fraud-scheme-aimed-denying-revenue-workers-associated-north

41 Microsoft (2025). Microsoft Digital Defense Report 2024. Published 2025.

42 FBI (2024). North Korea Aggressively Targeting Crypto Industry with Well-Disguised Social Engineering Attacks.Published 03 September.

43 US Cybersecurity and Infrastructure Security Agency (2020). Guidance on the North Korean Cyberthreat. Published 23 June.

44 Cybersecurity and Infrastructure Security Agency. (2024, July 25). FBI, CISA, and partners release advisory highlighting North Korean cyber espionage activity. Retrieved from https://www.cisa.gov/news-events/alerts/2024/07/25/fbi-cisa-and-partners-release-advisory-highlighting-north-korean-cyber-espionage-activity

45 US Cybersecurity and Infrastructure Security Agency (2022). TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies. Published 20 April.

46 Chainalysis (2024).$2.2 Billion Stolen from Crypto Platforms in 2024, but Hacked Volumes Stagnate Toward Year-End as DPRK Slows Activity Post-July. Published 19 December.

47 Reuters (2024). Mexico faces over half of Latin American cybercrimes due largely to US ties. Published 9 October. https://www.reuters.com/world/americas/mexico-faces-over-half-latin-american-cybercrimes-due-largely-us-ties-2024-10-09/

48 PwC. DORA and its impact on UK financial entities and ICT service providers. Retrieved from https://www.pwc.co.uk/industries/financial-services/insights/dora-and-its-impact-on-uk-financial-entities-and-ict-service-providers.html

49 The Register of Information under DORA is a standardized central database that records all contractual agreements of a financial company with ICT third-party service providers.

50 ENISA. (n.d.). Network and Information Systems. Available from: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems

51 European Commission. (2025). NIS2 Directive. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive