



FINANCIAL SERVICES THREAT BRIEFING

Date: June, 2025



Contents

EXECUTIVE SUMMARY	3
KEY DETAILS	4
ANALYST COMMENTS	5
THE HUMAN ELEMENT	6
RANSOMWARE AND FRIENDS	10
GLOBAL TENSION, STATE ACTORS, AND POISONING THE WELL	14
CONCLUSION	22
REFERENCES	24
APPENDIX – PHISHING RED-FLAG CHECKLIST	27



Executive Summary

The finance sector has increasingly become a target of evolving and sophisticated cyber threats. Major breaches in recent years—such as those affecting Evolve Bank, Finastra, and the Lazarus Group's record-setting \$1.5 billion cryptocurrency heist—rank among the most significant fintech incidents to date. Ransomware attacks, a persistent threat across all industries, have intensified year over year in this sector. 2025 is shaping up to match or exceed the impact seen in 2024.

Phishing and social engineering remain the primary entry points for most threat actors, showing no signs of slowing. These attacks are increasingly executed at scale, driven by "as-a-service" cybercrime models. The growing use of stealer malware (designed to harvest credentials and crypto wallets), Android banking trojans, and access brokers (who sell initial entry to compromised networks) illustrates the increasing threat landscape. This rise is evident from heightened activity on underground forums that trade in these tools and services.

Geopolitical tensions are also reshaping the threat environment. Pro-Russian and pro-Palestinian hacktivist groups have launched DDoS attacks against banks and financial institutions. North Korean threat actors, in particular, continue to pursue financially motivated operations targeting the U.S. and Europe. Their tactics include advanced social engineering—such as luring finance-sector developers with fake job offers, placing operatives inside fintech organizations, and poisoning the software supply chain via malicious packages on GitHub and the VSCode marketplace.

Threats to the finance sector are expected to grow, especially through expanded social engineering campaigns, supply chain compromises, and exploitation of publicly accessible web assets. Threat actors are likely to exploit growing market instability following recent U.S. tariff announcements and the potential for a global trade war. This, combined with the wars in Ukraine and Palestine and a perceived lack of cybersecurity



investment and leadership from the current U.S. administration, creates an environment ripe for increased financially motivated attacks.

If current conditions persist, we will likely see a rise in financially driven threat groups leveraging proven tactics to capitalize on political and economic disruption.

Key Details

- The financial sector continues to attract a disproportionate share of social engineering attacks, making it one of the most consistently targeted industries.
- Over the past year, ransomware incidents affecting financial institutions have doubled. Early indicators suggest this trend will likely surpass last year's victim count.
- Industry data from multiple vendors places financial services firmly within the top five most frequently attacked sectors.
- Economic pressures—including new tariffs and the looming threat of a trade war—are expected to drive further exploitation by financially motivated threat actors.
- Groups like Lazarus, linked to North Korea, remain highly active. Their operations target financial entities and extend into broader financial crimes such as fraud and money laundering, often with the goal of bypassing international sanctions.
- Hactivist groups, though not focused on finance alone, have regularly disrupted banks and financial service providers through DDoS attacks. These actions are often politically motivated, aligning with pro-Russian or pro-Palestinian causes.
- Credential-stealing malware continues to gain traction. A recent example is Zhong Stealer, a tool attributed to Chinese threat actors that is being used to target the fintech space.
- Mobile-focused malware is on the rise, particularly variants designed to siphon off cryptocurrency and banking data from Android devices.



- Social engineering techniques are evolving. Beyond conventional phishing, attackers are increasingly using methods like ClickFix (which tricks users into running malicious code), fake IT support outreach, and SMS or voice-based scams (smishing and vishing).

Analyst Comments

Reducing risk across multiple fronts remains the most effective strategy for defending against both familiar and emerging threats in the financial sector. Phishing continues to be one of the top tactics used by attackers to gain a foothold—largely because it's simple, scalable, and increasingly enhanced by criminal services sold on underground markets.

What makes the threat landscape more complex is that cybercriminals aren't just targeting organizations—they're also going after individuals. A compromised user, whether an employee or a customer, can easily become the entry point into a larger network. With that in mind, the following practical steps can help reduce exposure and limit the potential fallout from security incidents:

- **Enable multi-factor authentication (MFA)** wherever possible. This helps prevent attackers from immediately reusing stolen credentials. Monitor the origin of login attempts to flag suspicious activity early.
- **Limit privileges** for all users. Whether it's a staff member, customer, or third-party contractor, only grant the minimum level of access required. This keeps the blast radius small if their account is compromised.
- **Run phishing awareness programs** regularly. Both employees and customers should know how to recognize a scam. (Refer to the Appendix for a quick-reference checklist.)
- **Vet all software downloads** and ensure they come from official, trusted sources. Unsanctioned apps are a common vector for malware.



- **Discourage browser storage of sensitive data.** Passwords, crypto wallets, and payment details saved in browsers are easy targets for stealer malware.
- **Secure SaaS platforms** by implementing key controls such as web application firewalls, runtime monitoring, and defense mechanisms against common vulnerabilities like SQL injection, insecure direct object references (IDOR), cross-site scripting (XSS), and broken business logic.
- **Stay current with patching.** Apply vendor security updates promptly and ensure only intended-facing systems—like your main public website—are exposed to the internet.

The Human Element

There have been several recent campaigns that illustrate just how aggressively phishing tactics are being tailored to the finance sector. One notable example is a campaign known as “ClickFix,” which has become increasingly common among threat actors—especially those linked to North Korea’s Lazarus Group.

These operations typically target individuals working in or applying for jobs in financial organizations—particularly developers. The scam starts with a fake job offer from a reputable fintech name like Coinbase, Kraken, Tether, or Bybit. Once initial contact is made, the victim is directed to a website that mimics a legitimate portal. They’re then told a portion of the site is broken and asked to copy and paste a snippet of code into their local machine—usually under the guise of fixing the problem. What actually happens is the download and execution of malware that steals credentials, drains crypto wallets, and in some cases, burrows deeper into the victim’s network.

While this technique is closely associated with North Korean actors, it’s not exclusive to them. Chinese and Russian threat groups have also adopted variations of ClickFix in their own campaigns, using it to scale attacks efficiently. For North Korea, this is just one prong of a broader social engineering strategy that includes placing operatives



within financial and security firms, or even approaching companies under the guise of legitimate business partnerships.

More broadly, phishing and social engineering remain among the most successful and widespread tactics used by threat actors across the board. Nearly every major group has employed some form of deception—whether email-based, voice-driven, or through fake support channels—to breach targets.

The threat is growing more sophisticated with the emergence of phishing-as-a-service (PhaaS) platforms and AI-generated lures. These include fake emails that appear to come from trusted vendors, as well as deepfake audio or video content that mimics real voices and speech patterns. The increasing frequency of MFA bypass attacks further complicates defense strategies, underscoring the need for organizations to adopt a layered, adaptive approach to protecting their users and systems.

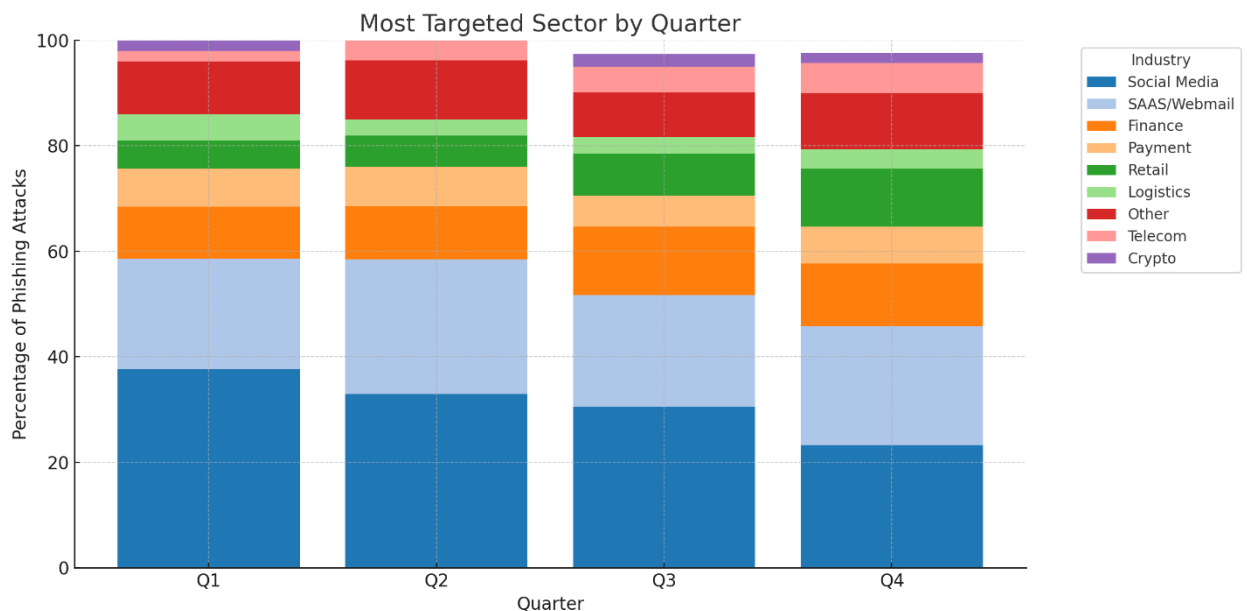


Figure 1 – Most targeted industries by quarter for phishing attacks

The finance sector remains one of the top targets for social engineering attacks—especially from threat actors motivated by financial gain. Reports from various vendors



consistently rank financial services among the most frequently exploited industries. Some data points are particularly striking: one provider recorded a more than 400% surge in vishing (voice phishing) incidents. According to APWG's data for Q4 2024, out of nearly one million phishing attacks, 11.9% were directed at financial sector targets, placing it as the third most attacked vertical. Quarterly breakdowns throughout 2024 show consistent targeting, with activity rising sharply between June and December. When factoring in both payment services and cryptocurrency exchanges, the broader finance category ranked among the top three attack surfaces throughout the year.

There's also been a noticeable shift in attacker focus. Instead of going after just institutions, many campaigns now target individuals—especially those with access to sensitive systems. One growing threat category is **stealer malware**. These tools are built to extract passwords, browser history, crypto wallet keys, and payment data from infected machines. A notable example is **Zhong Stealer**, a malware strain linked to Chinese cybercriminals. First reported in early 2025, Zhong has been used to infiltrate fintech companies by targeting customer support agents.

In these attacks, the threat actor typically creates a fake user account and submits an empty support ticket. Attached is an archive file—often a .zip or .rar—described as containing screenshots to help resolve the issue. Once opened, the contents execute malware that silently compromises the agent's system. Attackers often use broken or awkward language to mask intent, though increasingly this is being offset by AI-generated lures. Given the rapid adoption of language models by threat actors, spelling and grammar are no longer reliable red flags. The takeaway is simple: treat all unsolicited attachments—especially from unknown sources—with heightened caution.

Another emerging threat is the "**Smishing Triad**", a group of China-linked cybercriminals previously focused on logistics and toll fraud, now pivoting to target customers of financial institutions. This group is believed to be behind several **Phishing-as-a-Service (PhaaS)** platforms, including Darcula, Lighthouse, and the XinXin Group. Their tactics are familiar: smishing messages impersonating trusted brands, directing victims to fake sites, and requesting sensitive information such as



credit card numbers under the guise of fixing an error. Just like Ransomware-as-a-Service (RaaS), these phishing kits blur attribution. The same toolset may be used by multiple unaffiliated actors, affiliates, or even core operators acting on behalf of others.

Mobile malware is also evolving fast. Several new families of **banking trojans** are masquerading as legitimate crypto or finance apps on the Google Play Store. These trojans are designed to drain crypto wallets and steal payment credentials. Recent campaigns, such as **Crocodilus**, have hit users in Spain and Turkey. This malware abuses Android's accessibility features to trick users into exposing their seed phrases—the private keys that secure cryptocurrency transactions. Once installed, Crocodilus can take full control of the device: logging keystrokes, accessing messages, reading contacts, and more.

Similarly, **KoSpy**, a North Korea-linked Android spyware tool, has surfaced on Google Play and Firebase. It shares the same capabilities, with a heavier focus on surveillance and espionage. Although these malicious apps are eventually pulled down by platform maintainers, the damage is often already done by the time they're discovered. End users need to be vigilant: always verify the legitimacy of apps, and avoid installing anything from unfamiliar developers.

The larger picture is clear: social engineering—whether via phishing, smishing, or voice-based scams—isn't going away. Threat actors exploit the human element because it works, and no technical defense is perfect against it. Case studies like ClickFix, Zhong Stealer, and KoSpy represent only a fraction of the threat landscape.

With the rise of automated phishing platforms and generative AI tools, attackers can now create highly convincing lures, fake documents, and even audio deepfakes. Some have already used LLMs like ChatGPT to generate fake passports and bypass KYC (Know Your Customer) procedures. As these tools become more accessible, we can expect a sharp increase in high-quality social engineering attacks across the sector.



To help mitigate these risks, we've included a phishing red-flag checklist in the appendix of this report. It's designed to help users recognize suspicious behavior and make informed decisions before engaging with potentially harmful content.

Ransomware and Friends

Ransomware is a critical threat all organizations globally, especially for the Finance (and related) sectors given the direct correlation to threat actors with a financial motive. This is seen in past years, as 2023 had the most prevalent number of attacks and victims by industry reports. In analyzing open-source datasets from 2024 and the YTD for 2025, several items stand out.

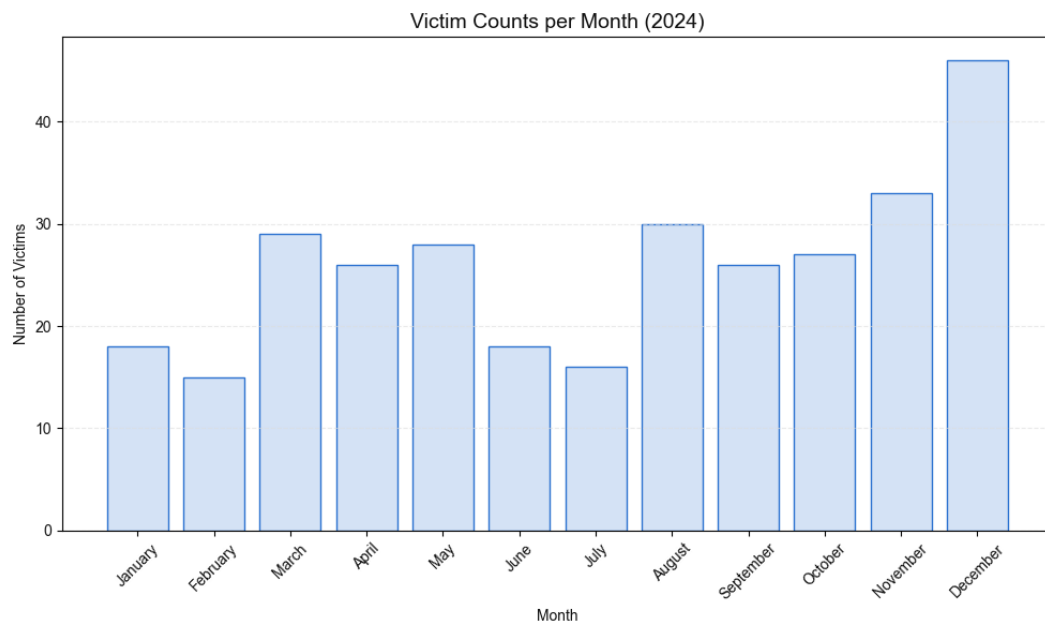


Figure 2 – Number of victims and their prevalence throughout the year of 2024.

We can see based on the figure above that the most prevalent months started around August and then having a slight downturn, before victims grew again in October, with



December reaching the most victims seen within the year. This has mirrored previous years with the most attacks usually happening during the winter holiday months.

As we forecast the rest of 2025, we see the initial data for the first 3 months of the year already beating number of victims from last year.

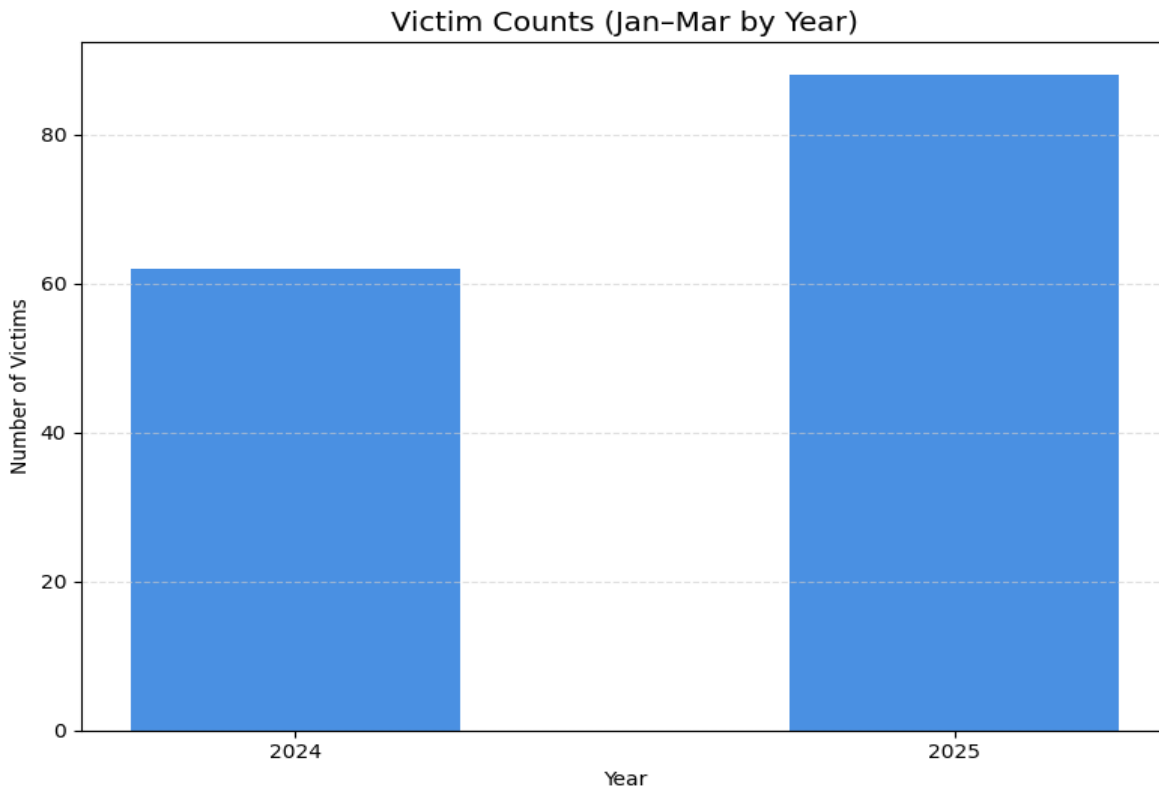


Figure 3 – Q1 comparison 2024 vs 2025.

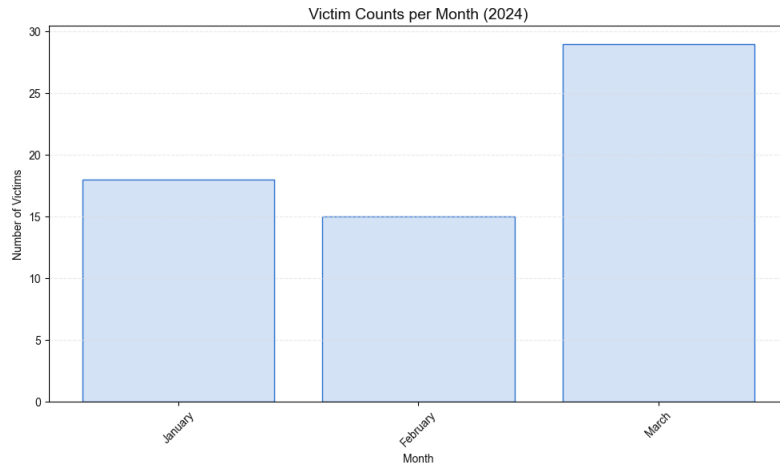


Figure 4 – Q1 2024

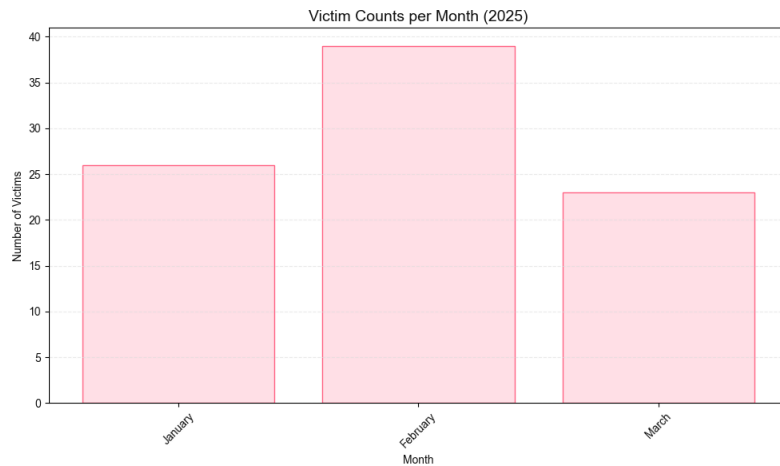
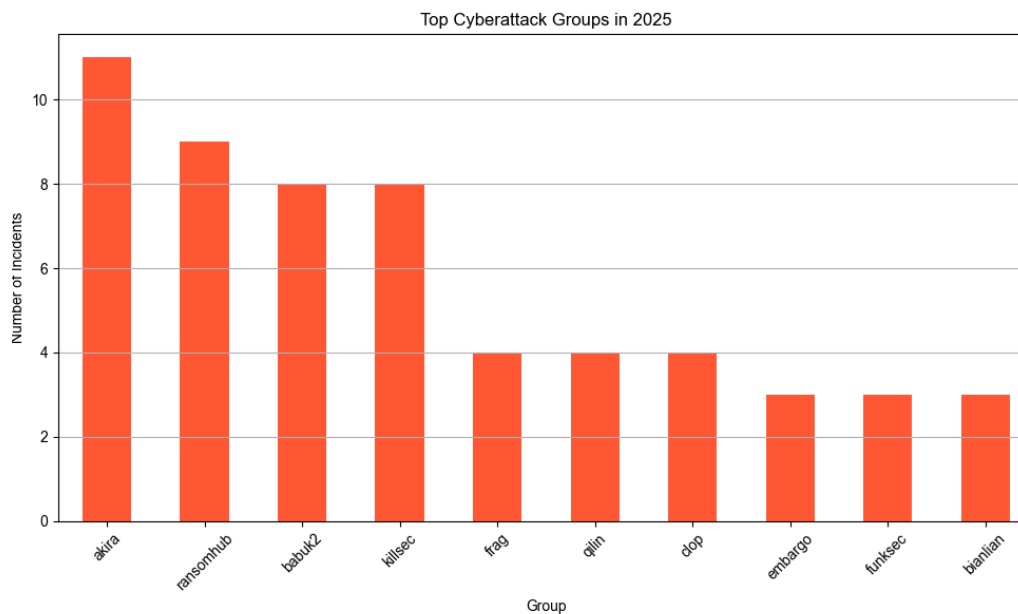
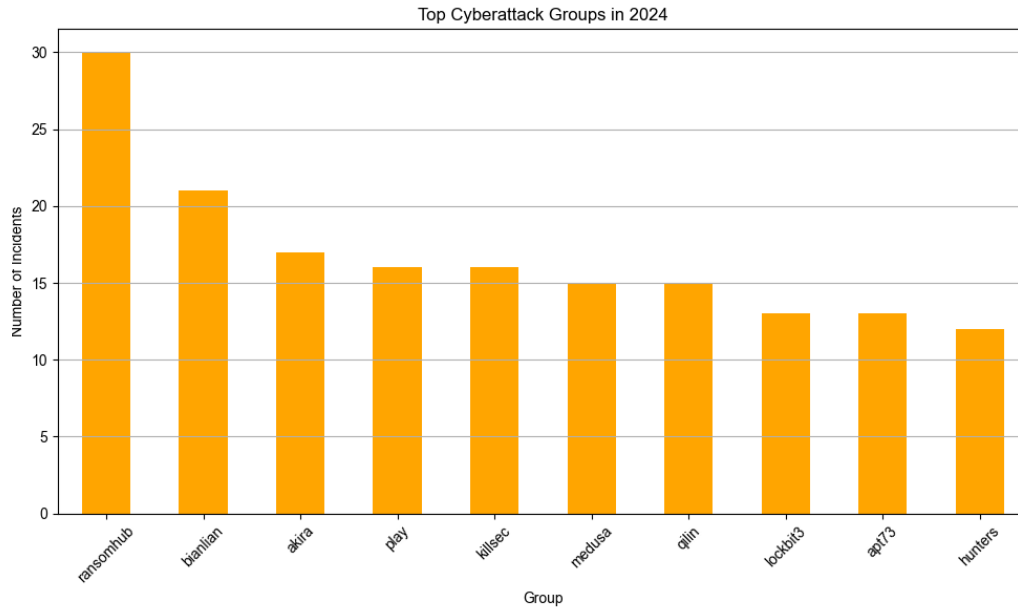


Figure 5 – Q1 2025

Given what we have seen in the first quarter this year it is highly likely that Ransomware attacks will be similar to 2024 or break the previous year's record.



Figures 6 and 7 – Most prevalent Ransomware groups by year with the Ransomwarehub (has ceased activity at the time of this document) and Akira most actively targeting the Finance sector.



Global Tension, State Actors, and Poisoning the Well

Geopolitical tensions, rising protectionist policies, and a surge in hacktivist activity are converging to elevate cyber risk across the financial sector. The imposition of new U.S. tariffs and the specter of a full-scale trade war have already rattled global markets. In parallel, hacktivism has become an increasingly disruptive force, with financially aligned institutions often caught in the crossfire.

Distributed Denial-of-Service (DDoS) attacks, in particular, have intensified. According to security research from Akamai, attacks targeting financial APIs—especially across layers 3, 4, and 7—have steadily increased since 2023. These attacks are often politically charged and linked to ongoing global conflicts, such as the wars in Ukraine and Gaza. Campaign hashtags like **#OpIsrael** and **#OpUSA** have become digital calling cards for these operations.

A number of hacktivist collectives are responsible for this uptick. Groups like **NoName057(16)**, **RipperSec**, **Dark Storm Team**, and **DieNet** are active on Telegram and operate under a broader umbrella alliance known as the **H0ly League**. This coalition focuses primarily on DDoS and DDoS-as-a-Service offerings, but it also engages in ransomware deployment, operational technology (OT) exploitation, and other high-impact cyberattacks.

Many of these groups are openly aligned with pro-Russian or pro-Palestinian causes. Some are thought to have direct ties to nation-state threat actors—**Sandworm/APT44**, for instance, is a well-documented example of a Russian state-sponsored unit with destructive capabilities. Regardless of their level of state sponsorship, these actors often treat financial institutions as legitimate targets, seeking to cause economic disruption in regions perceived as supporting adversaries in these geopolitical conflicts.



As financial systems become increasingly digitized and globally interconnected, these politically motivated cyberattacks present a serious and evolving threat to operational continuity, customer trust, and economic stability.

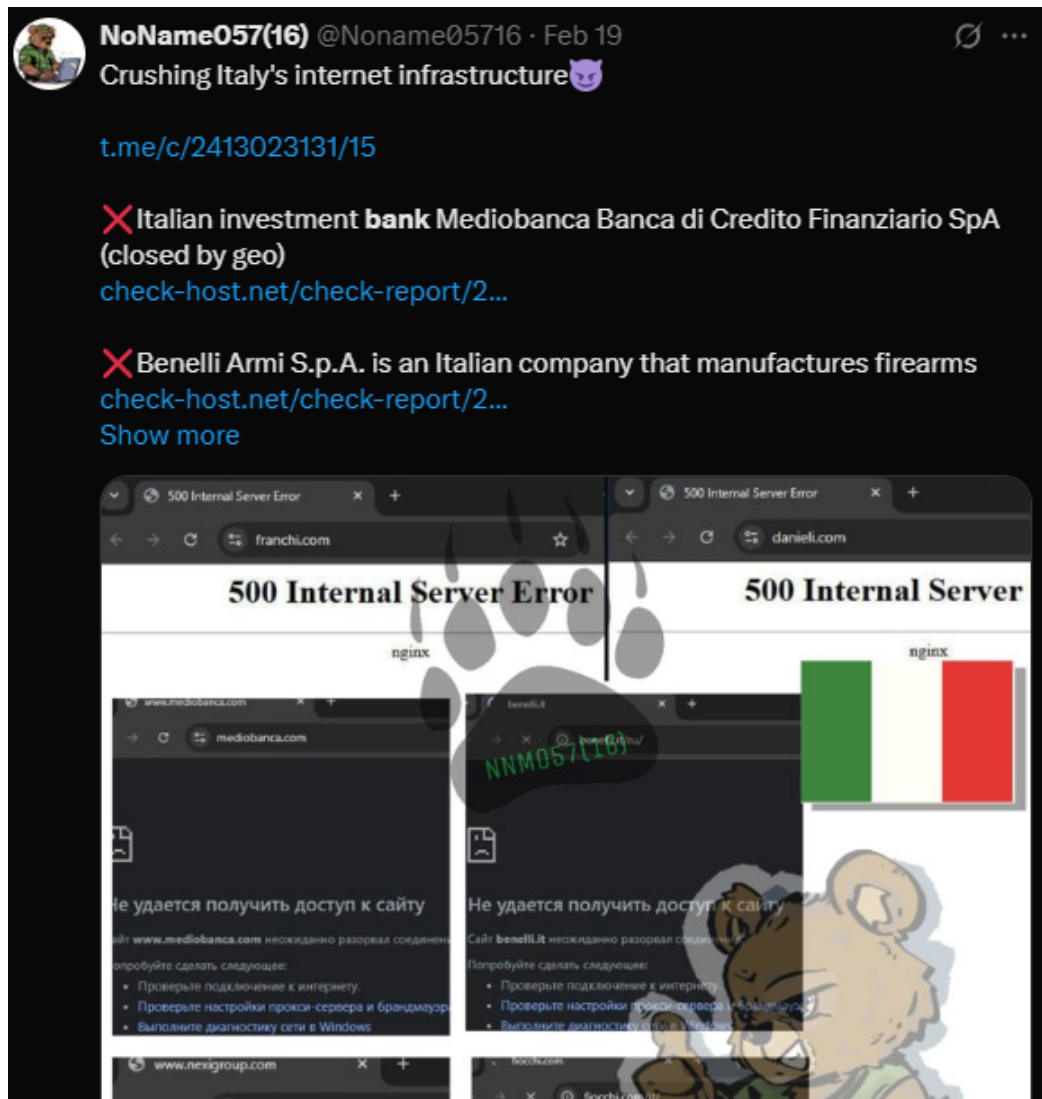


Figure 8 – NoName057(16) post claiming DDoS attack against Italian bank and firearms manufacturer.

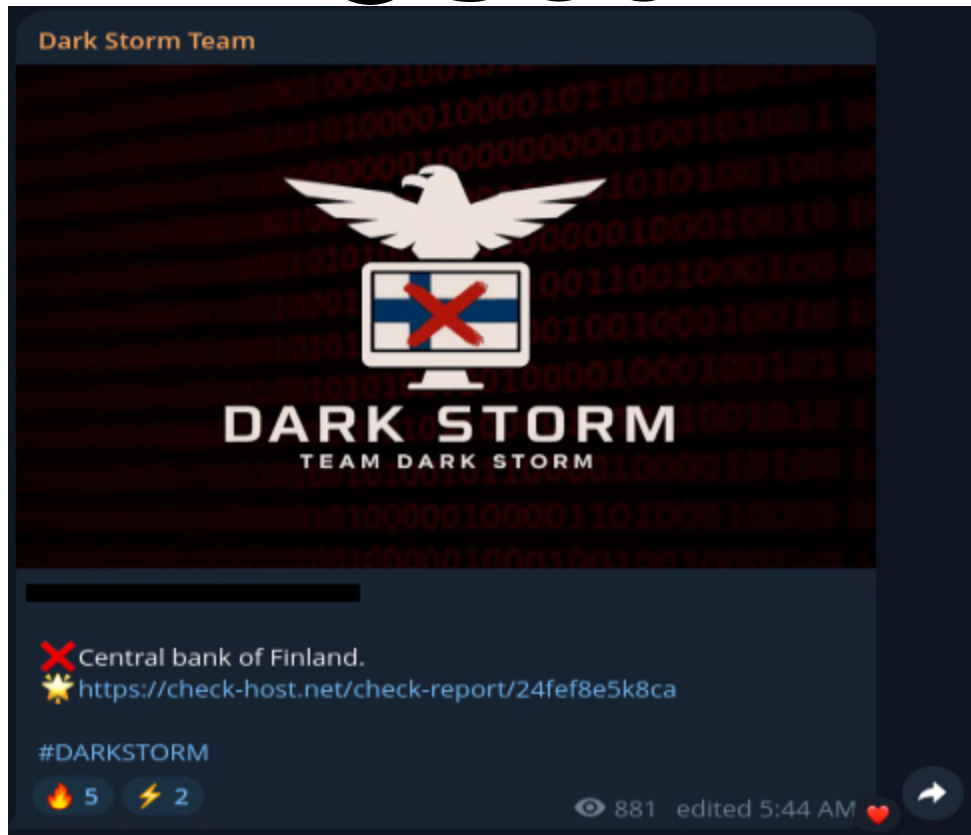


Figure 9 – Dark Storm team claiming DDoS attack against bank of Finland.

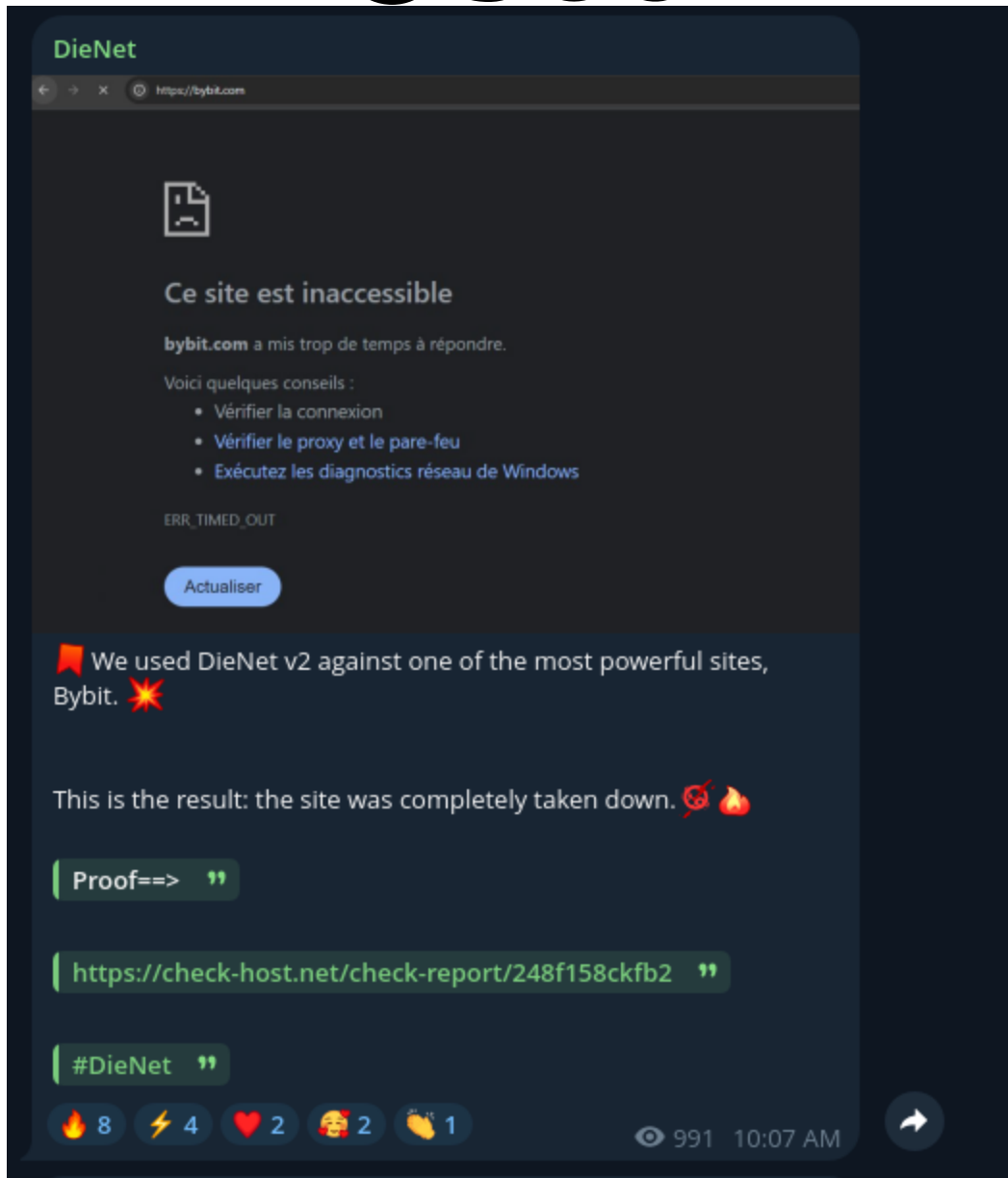


Figure 10 – DieNet claiming DDoS attack against ByBit using their own DDoS infrastructure.



RipperSec @RipperSec

RipperSec (ريفرسيك) ▾ Feb 2025

🔗 Summarize ▾

MegaMedusa V3.3.1 Released 📢

📘 Release Details :

- Domain block bug fixes on V3.3.0.

📘 Repo Git Clone :

```
git clone https://codeberg.org/RipperSec/MegaMedusa
```

📘 Codeberg Account :

🗨 <https://codeberg.org/RipperSec/MegaMedusa>

📘 Donate (BTC Only) :

🗨 `bc1q5z9kccxvwcx6dk9hsmezvhfg8yqjyj0hs3v52v`

Figure 11 – Malaysian hackers RipperSec advertising new versions of their DDoS tool MegaMedusa via a public repository (no longer available as of this document).

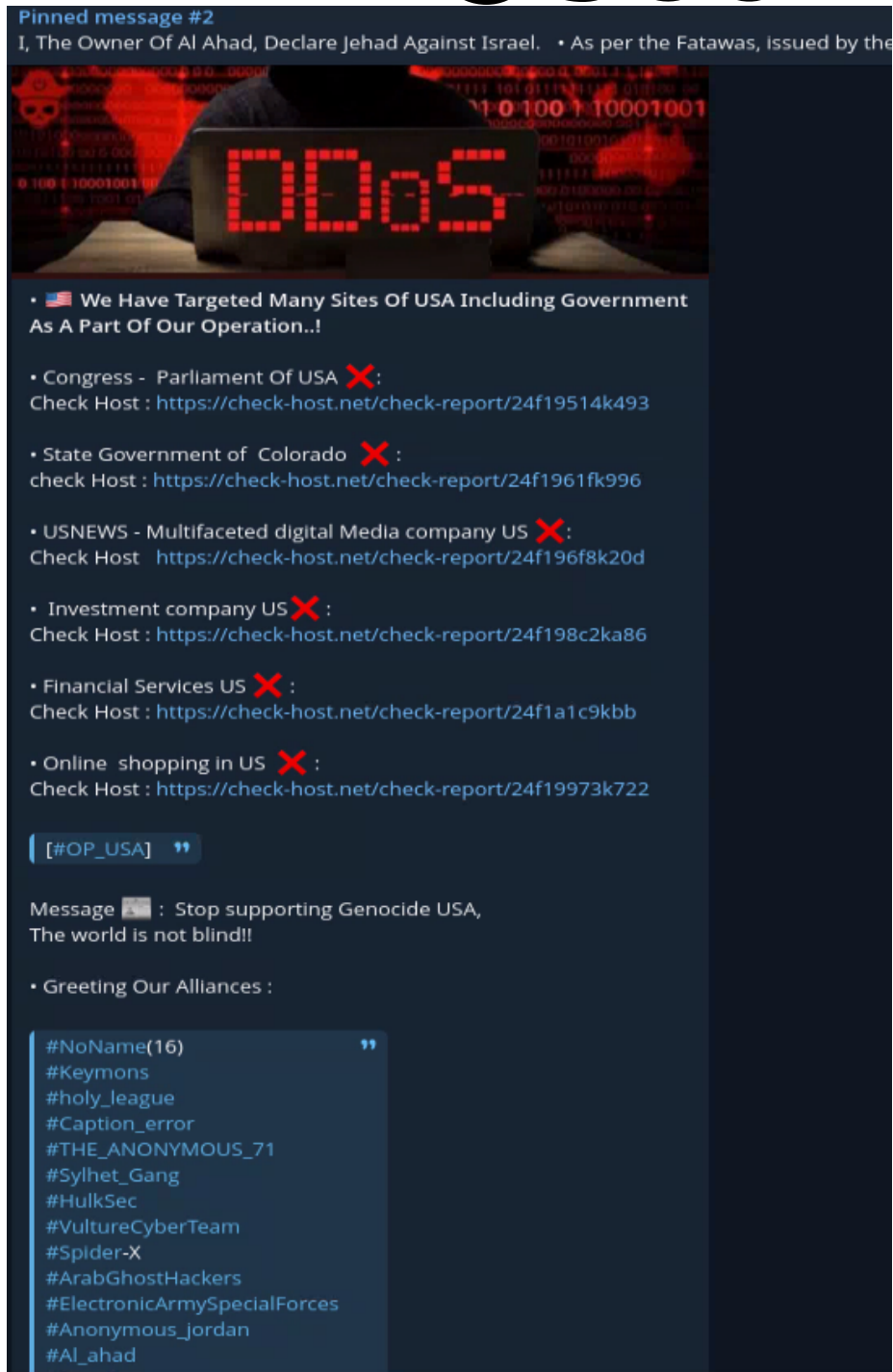


Figure 12 – AnonSec claiming attacks against several US targets including an unnamed shopping, investment and financial services companies under #Op_USA tag joined by other H0ly League aligned hacktivists.



Like many advanced threat actors, this group engages in espionage—often stealing intellectual property from universities and research institutions. But unlike most state-sponsored actors, what sets them apart is a heavy emphasis on financially motivated operations. Their goal is straightforward: generate revenue for the North Korean regime, which remains under heavy international sanctions and in dire need of foreign currency.

Because of this focus, the financial sector is a prime target. It offers not just monetary gain, but also opportunities to bypass regulatory controls like Know Your Customer (KYC) requirements and to exploit weaknesses in anti-money laundering systems. Embedding within fintech ecosystems gives the group both financial leverage and operational cover.

One of the most infamous examples of their activity is the 2024 breach of **Bybit**, a Dubai-based cryptocurrency exchange. The attack resulted in the theft of approximately **\$1.5 billion in Ethereum**, making it one of the largest known crypto heists to date.

The operation combined multiple attack vectors—social engineering, relationship-building with insiders, exploitation of zero-day vulnerabilities, and targeted malware deployment. It reflected the group's hallmark tactics: blending traditional espionage tradecraft with financially driven objectives to pull off highly coordinated, high-value cybercrimes.

FBI confirms Lazarus hackers were behind \$1.5B Bybit crypto heist

By [Sergiu Gatlan](#)

February 27, 2025 02:22 AM 0



Figure 13 – Article detailing the \$1.5b heist of cryptocurrency by Lazarus Group.

The group relies heavily on both supply chain compromise and social engineering to achieve its objectives. Their tactics include seeding malicious **NodeJS packages**, abusing **GitHub Actions**, and exploiting trust within developer ecosystems to distribute malware at scale. They also leverage **Ransomware-as-a-Service (RaaS)** tools—most notably the **PLAY** ransomware platform—to launch opportunistic attacks.

Unlike many traditional APT groups, they don't limit their targets to large enterprises. Individual users are often in the crosshairs, particularly via **watering hole attacks**—where malware is uploaded to widely used platforms, such as software marketplaces or repositories, in hopes of infecting unsuspecting visitors. Their Android malware campaigns have even made it onto the **Google Play Store**, disguised as legitimate applications.



In addition to technical exploits, the group actively engages in **long-term infiltration strategies**. These include applying for roles at financial or fintech companies under false identities, or approaching organizations while posing as venture capital firms or business partners. The goal is often to embed themselves within trusted networks where they can gather intelligence or stage future attacks.

These tactics highlight the importance of rigorous vetting processes—not only for software supply chains, but also for employee recruitment, business partnerships, and vendor relationships. Understanding who you're dealing with is critical, especially in sectors as sensitive as finance.

Conclusion

The finance sector isn't just another target—it's the target. That's been made clear by the volume and intensity of attacks over the last 18 months. What's also clear is that these threats aren't just coming from one direction. Criminal groups, state-backed actors, and politically motivated hackers are all circling the industry, each with different motives but often using the same tactics: phishing, social engineering, malware, and supply chain compromise.

This isn't a theoretical risk. Campaigns like ClickFix and tools like Zhong Stealer show how attackers are zeroing in on people—developers, support staff, even job applicants—to get inside the gates. Meanwhile, ransomware continues to hammer financial institutions, with early 2025 already outpacing 2024 in terms of victim numbers. And as long as there's profit to be made or chaos to sow, we can expect more of the same.

At the same time, broader geopolitical tensions are bleeding into cyberspace. DDoS attacks, data theft, and infiltration attempts are becoming tools of economic and political disruption, with banks and fintech platforms caught in the middle. Groups like Lazarus aren't just after money—they're looking to break into financial ecosystems and stay there.



All of this paints a challenging picture. But the situation isn't hopeless. There are clear steps organizations can take—like hardening access controls, improving phishing defenses, and being more skeptical about who gets in the door, whether they're a new hire, a vendor, or a piece of code from a public repo.

The bottom line is this: the threats aren't slowing down, and the targets aren't changing. But the organizations that invest in smarter, layered defenses—and that treat security as a shared responsibility across teams and customers—will be in a much better position to handle what's coming next.



References

1. 2024 Phishing By Industry Benchmarking Report. Published online 2024.
2. 2024 State of the Phish. Published online 2024.
3. Analysis 图片_20241220.exe (MD5: 778B6521DD2B07D7DB0EAEAB9A2F86B)
Malicious activity - Interactive analysis ANY.RUN. <https://app.any.run/tasks/a84e322a-a5e5-469e-98b3-1235f8069cbb>
4. APWG | Phishing Activity Trends Reports. <https://apwg.org/trendsreports/>
5. Lyons J. Are they really hacktivists or state-backed goons in masks?
https://www.theregister.com/2025/04/13/hacktivism_is_having_a_resurgence/
6. BlackBerry Quarterly Global Threat Report — January 2025.
<https://www.blackberry.com/us/en/solutions/threat-intelligence/threat-report#critical-infrastructure>
7. BlueNoroff Hidden Risk | Threat Actor Targets Macs with Fake Crypto News and Novel Persistence. SentinelOne. November 7, 2024.
<https://www.sentinelone.com/labs/bluenoroff-hidden-risk-threat-actor-targets-macs-with-fake-crypto-news-and-novel-persistence/>
8. China-based SMS Phishing Triad Pivots to Banks – Krebs on Security. April 10, 2025. <https://krebsonsecurity.com/2025/04/china-based-sms-phishing-triad-pivots-to-banks/>
9. Arghire I. “Crocodilus” Android Banking Trojan Allows Device Takeover, Data Theft. SecurityWeek. March 31, 2025. <https://www.securityweek.com/crocodilus-android-banking-trojan-allows-device-takeover-data-theft/>
10. European Union Agency for Cybersecurity. ENISA Threat Landscape: Finance Sector : January 2023 to June 2024. Publications Office; 2024.
<https://data.europa.eu/doi/10.2824/5410466>
11. Paganini P. Expert used ChatGPT-4o to create a replica of his passport in just 5 minutes bypassing KYC. Security Affairs. April 6, 2025.
<https://securityaffairs.com/176224/security/chatgpt-4o-to-create-a-replica-of-his-passport-in-just-five-minutes.html>



12. Fintech Giant Finastra Investigating Data Breach – Krebs on Security. November 20, 2024. <https://krebsonsecurity.com/2024/11/fintech-giant-finastra-investigating-data-breach/>
13. Firm hacked after accidentally hiring North Korean cyber criminal. October 16, 2024. <https://www.bbc.com/news/articles/ce8vedz4yk7o>
14. Guidance on the North Korean Cyber Threat | CISA. June 23, 2020. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-106a>
15. joshhighet. joshhighet/ransomwatch. Published online April 16, 2025. <https://github.com/joshhighet/ransomwatch>
16. Unit 42. Jumpy Pisces Engages in Play Ransomware. Unit 42. October 30, 2024. <https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/>
17. Lucid | Prodaft. <https://catalyst.prodaft.com/public/report/lucid/overview>
18. Intelligence MT. Microsoft shares latest intelligence on North Korean and Chinese threat actors at CYBERWARCON. Microsoft Security Blog. November 22, 2024. <https://www.microsoft.com/en-us/security/blog/2024/11/22/microsoft-shares-latest-intelligence-on-north-korean-and-chinese-threat-actors-at-cyberwarcon/>
19. New Android malware uses Microsoft's .NET MAUI to evade detection. BleepingComputer. <https://www.bleepingcomputer.com/news/security/new-android-malware-uses-microsofts-net-maui-to-evade-detection/>
20. New Chinese Zhong Stealer Infects Fintech via Customer Support. March 4, 2025. <https://hackread.com/chinese-zhong-stealer-infects-fintech-customer-support/>
21. New North Korean Android spyware slips onto Google Play. BleepingComputer. <https://www.bleepingcomputer.com/news/security/new-north-korean-android-spyware-slips-onto-google-play/>
22. North Korea Sanctions | Office of Foreign Assets Control. March 21, 2025. <https://ofac.treasury.gov/sanctions-programs-and-country-information/north-korea-sanctions>
23. News TH. North Korean Hackers Target Freelance Developers in Job Scam to Deploy Malware. The Hacker News. <https://thehackernews.com/2025/02/north-korean-hackers-target-freelance.html>



24. Russian money laundering networks uncovered linking narco traffickers, ransomware gangs and Kremlin spies. <https://therecord.media/russian-money-laundering-networks-trafficking-cybercrime-kremlin>
25. Rajic T, Brock J. The ByBit Heist and the Future of U.S. Crypto Regulation. Published online March 18, 2025. <https://www.csis.org/analysis/bybit-heist-and-future-us-crypto-regulation>
26. U.N. report: North Korea financing weapons program with cybercrime. Indo-Pacific Defense FORUM. <https://ipdefenseforum.com/2024/03/u-n-report-north-korea-financing-weapons-program-with-cybercrime/>
27. U.S. data compromises in financial services sector 2023. Statista. <https://www.statista.com/statistics/1318486/us-number-of-data-loss-incidents-in-financial-sector/>
28. Cofense. Wolves in Sheep's Clothing: Industry-Specific Targeted Phishing Attacks. Cofense. <https://cofense.com/blog/wolves-in-sheep-s-clothing-industry-specific-targeted-phishing-attacks>
29. Carpentier-Desjardins C, Paquet-Clouston M, Kitzler S, Haslhofer B. Mapping the DeFi crime landscape: an evidence-based picture. Journal of Cybersecurity. 2025;11(1):tyae029. doi:10.1093/cybsec/tyae029



Appendix – Phishing Red-Flag Checklist

The following is a checklist to help users identify a phishing email if they find one is suspected. Checking any of these items within these specific contexts might warrant that an email should have increased scrutiny made against it, especially if they only have one item checked against it. However phishing emails will typically have several indicators that might indicate it is suspicious or outright malicious, so communications exhibiting two or more should be regarded as such.

I get an email from an unfamiliar sender & generic red-flags:

- Who is the email from? Is it someone you know?
- What domain (e.g., somename@somedomain.com) is the email coming from?
- Does the email address look strange or fake?
- Does it have misspellings in the email such as within the content, title, or email domain?
- Did I expect this email?
- What is the content of the email? Is it trying to get me to navigate to a URL or Download a file?
- Are links using URL shorteners?
- Is there an attachment? Is it an archive or some other file format? Does it have a generic name? Are you expecting an attachment?
- Is the sender particularly aggressive in getting you to complete an action?
- Is the sender pressuring, threatening, or given you warnings/ultimatums (such as being arrested, leaking private details, and so on)?
- Does the email have an “external” or similar tagging applied to users outside of your organization?



I got an email from someone I know or work with:

- Do you know the person well? Are they a friend or simply a colleague you know about?
- Have you spoken or exchanged conversation before or have sent each other email, texts, or other methods of communication?
- Have you worked on projects together?
- Did you expect their email?
- Is their behavior typical to how you have interacted before?
- Have they shared an attachment? What is the file type and filename? Is it generically named?
- Can you contact this person via other modes of communication to confirm they sent you an email?

I got an email from IT Support:

- Is this normal behavior for IT support to send emails unprompted?
- What are the contents of the email? Is there anything strange about it such as misspellings, unknown names or individuals?
- Are they persuading you to navigate to a location or open a file to install or manage an update?
- Are they pressuring or threatening in the email contents?
- Are they asking you to copy and paste objects into a specific dialog, such as using the Windows run key (Win + R) or similar applications and appliances? Is this in the content of the email or when navigating to a URL that states something needs to be fixed with directions how-to?
- Are they asking you to navigate to a URL that does not belong to the company, or its partners?
- Can you reach out to IT support for clarity? Does the contact information match your company's IT department contact information?



- Can you contact the person through an alternate channel (call, chat) to confirm the email request?

I got an email from a well-known vendor or entity (Microsoft, AWS, Government and so on):

- A file has been shared, what is it? Were you expecting it?
- Is there a username or email associated with who sent the message or file through the noted vendors system?
- What is the filename of the attachment being shared? Is the filename generic? Was it expected?
- Did you receive an unprompted invite? Do you recognize the organizer or sender?
- Did you receive an email asking to give access to an application or person? Was this expected or unprompted?
- Are links using URL shorteners?
- Does the email domain match that vendor or entity?
- Does the email request urgent account actions, such as unlocking your account, verifying an account, logging into an account?
- Are they asking you to navigate to a URL that does not belong to the vendor or entity?
- Does the email include a support telephone number that contains non-numeric characters? (Os instead of 0s, etc...)

I got a message through support, SMS, Voicemail, Other:

- Did you expect the communication or was it unprompted?
- Are they sharing a file? What is its filename? Is it generically named and/or a dangerous file-type (.exe, .mmc, .lnk, .url)?



- Are you being persuaded to download a file? Navigate to a specific location?
- Are you being directed to input payment or personal details? Credentials such as username and passwords.
- Do they claim to be an authority? Police, government, vendor such as Microsoft, and so on.
- Are they pressuring or threatening you?
- Are they asking for some verification code that might be sent to you (via text, email, or other method)?
- Do they ask you to install some software or visit some site?
- Are they asking for a remote desktop session?