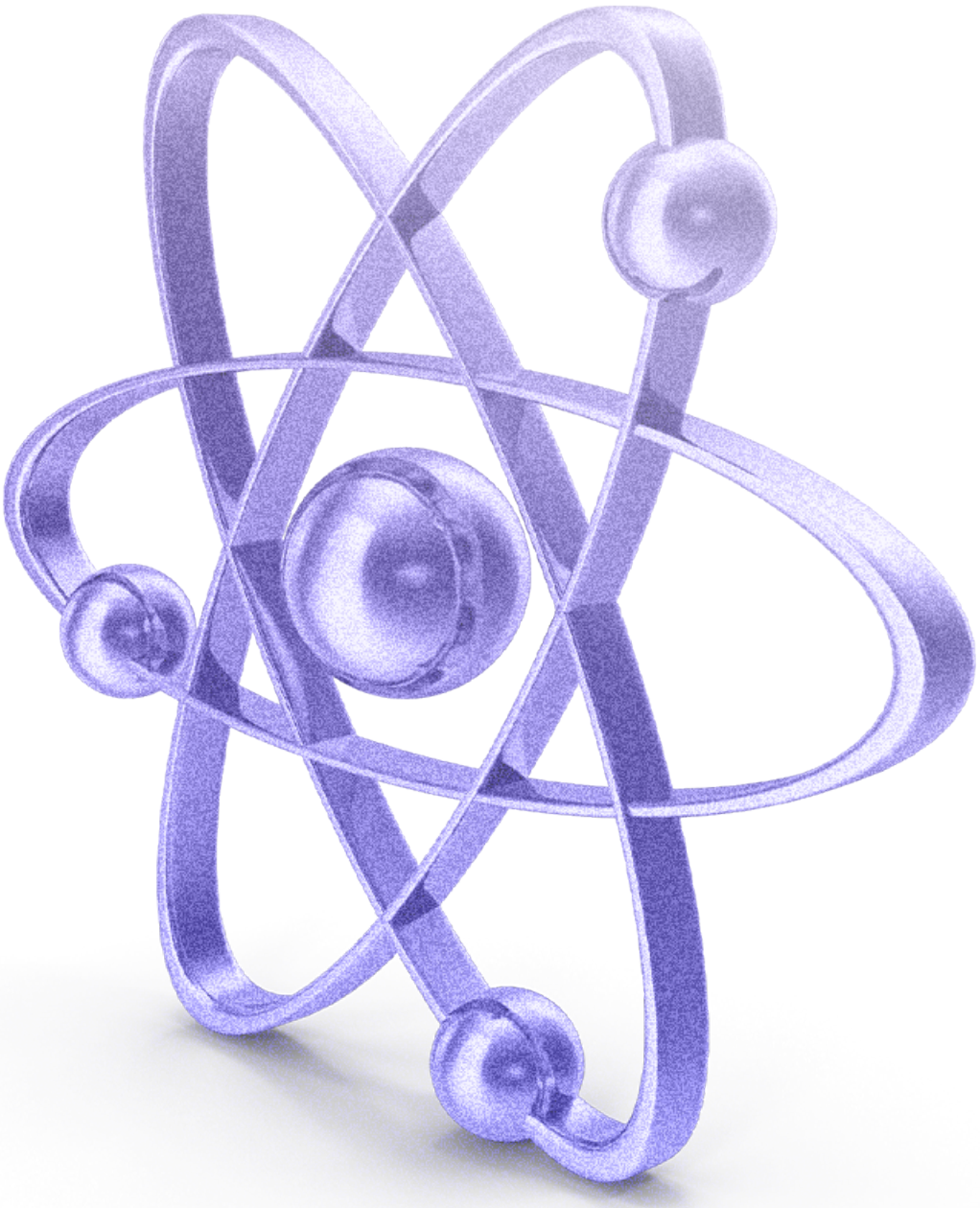
FS-ISAC

Navigating Cyber: Annual Threat Review and Predictions



March 2024

Contents

Executive Summary

The cyber landscape in the financial services sector was more stable in 2023, for the most part, than in years past. The sector's rigorous defenses – a product of the business mandate to maintain customer trust as well as a long history of regulation and a mature set of practices around intelligence sharing – continue to prove effective.

Nonetheless, cybersecurity trends are emerging that have disruptive implications for the sector's future.

1. **Generative AI** (GenAI) promises to radically transform financial services firms' operations in terms of automation and efficiency. But the same goes for fraudsters and threat actors; GenAI is a gamechanger in terms of automating and scaling attacks with very few skills required. More advanced threat actors could poison, manipulate, and exploit GenAI — for example, threat actors have already tricked ChatGPT into writing malicious code.[1] Financial institutions must decide how to make effective use of GenAI without taking on compliance and reputational risks. In terms of other emerging technologies, cybersecurity teams will be tasked with developing more agile encryption methods to prepare for the advent of quantum computing and dealing with a volatile — and vulnerable — cryptocurrency sector that is increasingly integrated with mainstream financial services.

2. **The supply chain** is a common adversarial target. Two key subsets of cyber-attacks – cloud file storage/transport solutions and clearing and trading platforms – have impacted the financial sector over the last year. Adversaries have exploited cloud systems to compromise software, steal customer data, insert malware, and hold data for ransom. Clearing and trading platforms have been victimized by difficult-to-mitigate ransomware attacks, which threaten to ripple through the global financial system when the victim disconnects to isolate the damage. Third-party supplier vulnerabilities will drive financial services firms to develop new data management programs, reduce the number of vendors under contract, develop new communication protocols with third parties (some regulations require it), and maximize the safety of information with in-house data storage.

3. **Geopolitical** events provide ideologically motivated hacktivists opportunities for disruption, as has been evident since the outbreak of the Russia/Ukraine and the Israel/Hamas wars. FS-ISAC expects hacktivism to increase in 2024 in response to those conflicts, the Summer Olympics, and the "Super Election," in which a world-record setting number of citizens will be eligible to vote in five countries' national elections. Financial services cybersecurity teams should expect an increase in hacktivists' favored techniques, like distributed denial-of-service (DDoS) campaigns. Last year, over a third of all DDoS attacks targeted the financial sector. DDoS attacks are increasing in size, scope, and sophistication, and are sometimes launched in layered attack patterns that are more difficult to mitigate.

4. **Regulation** is set to go into effect in the US, EU, UK, and Australia that will impact financial firms' cybersecurity in myriad ways. In the US, the SEC's 8-K rule on disclosure of material cyber breaches, which went into effect in December, gives public companies four days (184 days for small companies) to report certain information about cyberattacks. In the EU, financial institutions will be required to evaluate their suppliers to inhibit concentration risk and comply with comprehensive new AI and cryptocurrency regulations. Cyber teams in the UK will have new regulatory frameworks and accountability mechanisms. In Australia, regulators are considering the reclassification of 'customer data' as 'critical infrastructure.' And around the world, many financial services organizations will have a new mandate to share information on cyber breaches.

5. **Adversarial tactics, techniques, and procedures (TTPs)** include new applications of old crimes, such as QR code phishing and SEO attacks that deliver malware. Others, like ransomware and social engineering attacks, are

well-established attack patterns brought to new levels of sophistication and scope. Some, such as triangulation fraud, are wholly new methods of defrauding financial services customers and employees. These novel approaches to cybercrime will require financial firms' cybersecurity teams to stay constantly alert to adversaries' innovations.

FS-ISAC members are operating in a cyber landscape that is endlessly dynamic, with cybercrime and fraud converging, emerging technologies upping the ante for both threat actors and defenders, and more regulatory scrutiny than ever before.

The evolving cyber landscape will affect financial firms in various ways. Some of them may be quite positive, such as crypto agile encryption and legislation that encourages sharing. For those that aren't so positive, good cyber hygiene remains the best defense.

The 2023 Threat Landscape

Cyber Threat Levels

FS-ISAC has observed a lower and more stable level of risk in 2023 than in recent years. The Cyber Threat Level (CTL) — a barometer of the cyber threat landscape as determined by FS-ISAC members — was lifted to "ELEVATED" once in the AMER region in June but remained otherwise "GUARDED." Prior to 2023, members perceived substantial risks for the financial sector associated with zero-day vulnerability exploits, including SolarWinds (2020), Microsoft (2021), Kaseya (2021), and Log4j (2021). Though threat actors continued to exploit zero-day vulnerabilities throughout 2023, experienced cyber teams, having implemented lessons learned from previous years, responded quickly and effectively.

Despite significant and protracted geopolitical conflict in 2023, the CTL remained 'GUARDED' in both EMEA and APAC throughout 2023. The CTL for AMER was raised to 'ELEVATED' in June in response to the Cl0p ransomware exploitation of 'MOVEit Transfer,' a third-party file transfer system

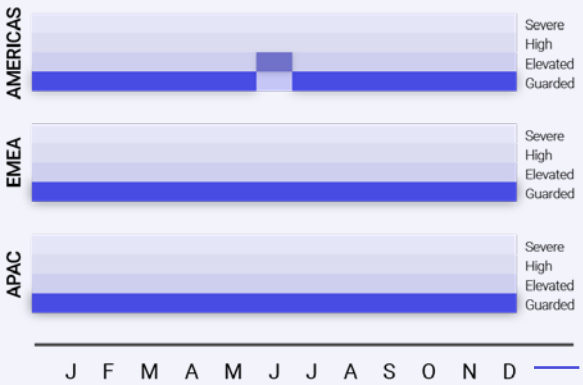


Figure 1: Regional Cyber Threat Levels in 2023

I. Threat Landscape Macro Trends

Generative AI

Though generative AI offers financial firms remarkable business and cybersecurity utility, cyberthreats relating to GenAI in financial services are a consistent concern.

The cybersecurity community's current consensus is that adversarial usage primarily relates to the creation of convincing phishing lures at scale. That said, threat actors can use generative AI to write malware and more skilled cybercriminals could exfiltrate information from or inject contaminated data into the large language models (LLMs) that train GenAI. The use of corrupted GenAI outputs can expose financial institutions to severe legal, reputational, or operational consequences.

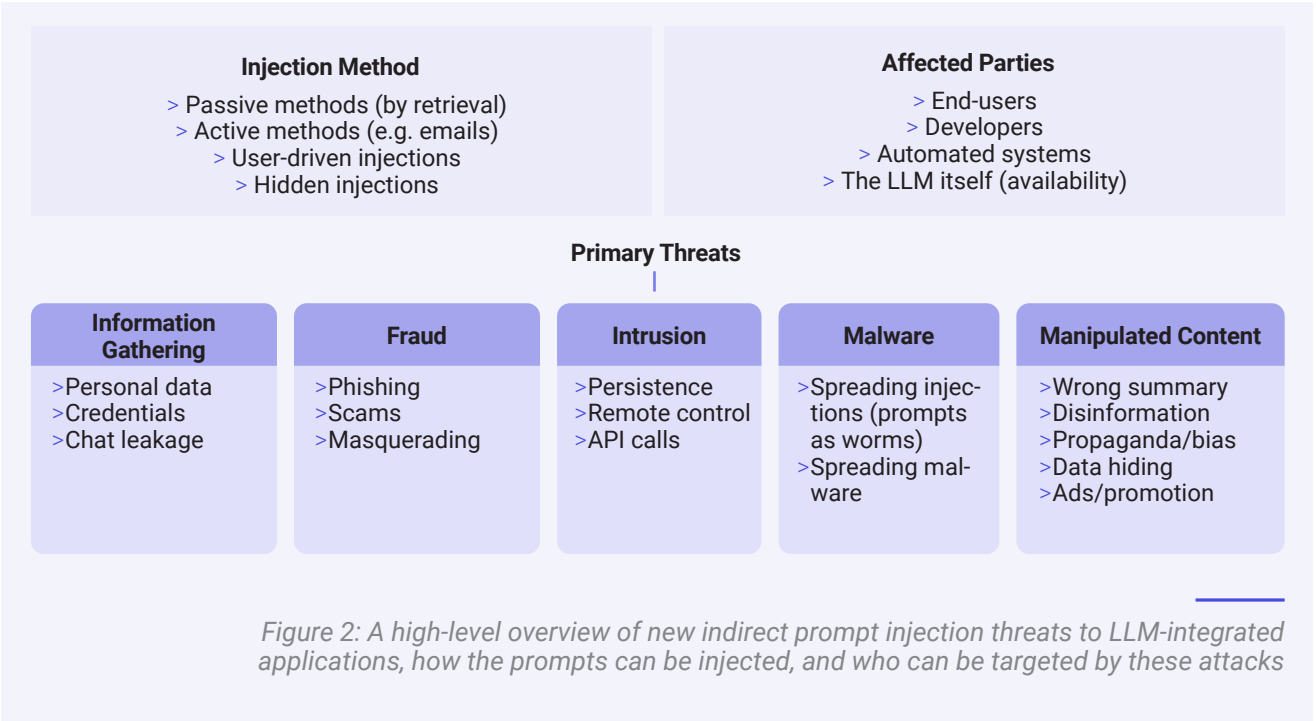


Figure 2: A high-level overview of new indirect prompt injection threats to LLM-integrated applications, how the prompts can be injected, and who can be targeted by these attacks

Not all AI risks are malicious. The LLMs that train GenAI typically use enormous datasets leveraging publicly available sources, which can contain privileged information (such as credit card numbers), or biased data. Using such outputs irresponsibly – or unethically – can cost financial firms the trust of regulators, consumers, and investors.

The FS-ISAC AI Risk Working Group published a holistic, practical perspective on the risks and opportunities associated with GenAI in these six white papers to help practitioners customize controls and mitigations at the organizational and sector level.

Supply Chain Incidents

The supply chain is a major threat exposure vector for the financial sector. Attacks on providers can disrupt various systems, such as those of clearing, trading, payments, and back-office service operations. The impact of a supply chain incident can cascade through the financial system.

Solution providers' lighter regulation and lower visibility make them easier prey than financial institutions for opportunistic attacks, and the supply chain provides more scope for lateral movement. In June 2023, FS-ISAC found that 57% of companies

whose data has been listed on ransomware group Cl0p's leak site after the MOVEit file share app compromise were financial institutions and financial services third parties.

Two key subsets of cyber-attacks – cloud file storage and transport solutions (a subset of IT supply chain threats) and clearing and trading platforms (a subset of financial services threats) – increased the severity of supply chain incidents in 2023.

Cloud file storage and transport solutions

These IT services are ubiquitous and, to many financial firms, operationally necessary. Adversaries exploit them to compromise software, exfiltrate sensitive customer data, and propagate malware.

> Between 2021 and 2023, Cl0p, a Russia-affiliated cybercrime group[2] (also known as TA505), carried out attacks on Accellion[3] (now known as Kiteworks), Fortra GoAnywhere, and MOVEit.

Clearing and trading platforms

FS-ISAC has observed that attacks on these providers can be difficult to immediately detect and remediate, sometimes causing cyber teams to disconnect from the compromised provider in precaution. That increases the adversary's impact, halts certain organizational operations, and affects downstream financial institutions.

> In January 2023, LockBit carried out a ransomware attack[4] against ION Cleared Derivatives, a subsidiary of trading firm ION Group. ION disabled some of its services in response, impacting derivatives trading services for dozens of major clients.

> In January 2024, a ransomware attack, also attributed to LockBit, on trading fintech EquiLend,[5] exfiltrated employees' personal and payroll information. Equilend shut down some of its systems for several days.

Notable Third-Party Cyber Events: 2023

> **March 2023:** a North Korean gang compromised 3CX phone and videoconferencing software in a malware attack and customers complained of malicious activity emanating from their desktop apps. The compromise of 3CX has been identified as part of a supply chain compromise cascade, following the compromise of another supply chain provider, Trading Technologies, a stock trading automation company. Such cascading impact is uncommon, making this a unique – and worrying – occurrence.

> **April 2023:** the Blackcat (AKA ALPHV) ransomware gang claimed to have breached and caused outages in NCR Corporation's Aloha point of sale platform, used extensively in hospitality services. The following September 2023, they attacked ATM and ITM solutions provider, QSI Inc.

> **November 2023:** the Industrial and Commercial Bank of China Financial Services (ICBC FS) was the victim of a ransomware attack, widely attributed to the Russian-affiliated LockBit gang, AKA Bitwise Spider (or an affiliate). While the initial point of access is unconfirmed, it is speculated that it may have been by exploitation of the Citrix Bleed vulnerability. ICBC FS disconnected and isolated its impacted systems, which disrupted the US Treasury market, causing equities clearing issues.

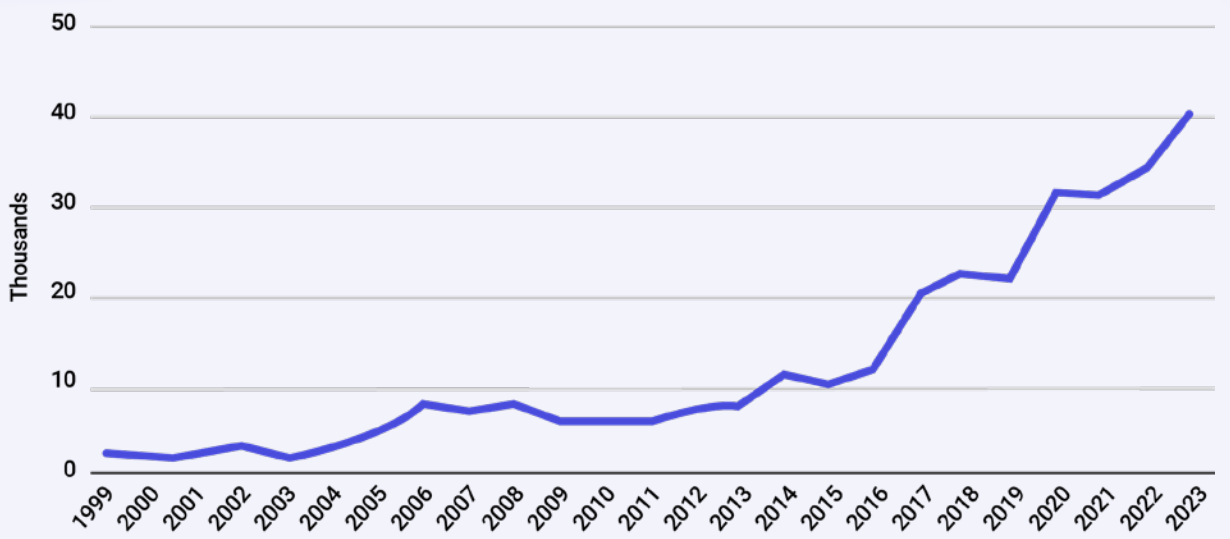


Figure 3: All vulnerabilities on record (source: CVE blog)

▶ Zero-Day Vulnerabilities

Zero-day vulnerabilities are unknown or unaddressed cybersecurity flaws, so called because cybersecurity teams have zero days to conduct remediation before threat actors exploit the flaw – the actor already has. Accurate asset lists and patching policies can mitigate the impact, but almost 40,000 new vulnerabilities were discovered in 2023,[6] up significantly since 2020.[7] In 2023, FS-ISAC members tracked impact from multiple zero days and other vulnerabilities exploited by threat actors.

Although full financial sector impact assessments were not achieved in all cases, the volume of cyber team investigations and patching imply at least a moderate impact.

▶ 2023 Major Incident Timeline

Jan

ION Trading platform: trades disrupted due to outage caused by LockBit ransomware (Financial Services)

Fortra GoAnywhere file transfer system zero-day compromise by Cl0p: multiple customers' data exfiltrated (File Storage & Transport)

Feb

LastPass password manager breach: customer data leaked (IT)

Mar

3CX VOIP/PBX software compromised as part of a cascade supply chain attack (IT)

Apr

NCR Aloha point of sale outages caused by Blackcat/ALPHV ransomware attack (Financial Services)

May

MOVEit zero-day compromise by Cl0p: data exfiltrated and ransom demanded from multiple victims (File Storage & Transport)

Jun

Fortigate VPN firewalls zero-day remote code execution vulnerability exploited by state-sponsored threat actors (IT)

Jul

Aug

Sep

QSI ATM operations impacted by ALPHV/ Blackcat ransomware (Financial Services)

Oct

Okta identity and access solutions breach: customer data leaked (IT)

Nov

ICBC hit by LockBit ransomware: US Treasury trade interrupted (Financial Services)

Dec

II. Geopolitical Trends

Russia-Ukraine

Since Russia's invasion of Ukraine in February 2022, ideologically-motivated hacktivist incidents have increased, but the impact on the financial services sector has been minimal – security-mature organizations can defend themselves from significant harm, and damage to smaller firms largely results from brief public website outages.

Critical or impactful incidents targeted solely on Ukrainian entities have done little damage outside the country.

Nonetheless, the financial services sector was announced as a DDoS target in June by the pro-Russian hacktivist group Anonymous Sudan in partnership with the more prominent KillNet hacktivist group and the ransomware operator REvil. FS-ISAC members accurately assessed Anonymous Sudan's capability as relatively poor in a 20 June 2023 Spotlight Call survey. Indeed, persistent DDoS attacks on Ukraine supporters in the second half of 2023 were either successfully defended or resulted in limited outages. A campaign using botnets launched by the less prominent pro-Russian hacktivist group UserSec targeted the financial sector in December and was similarly ineffectual.

More successful opportunistic attacks have been initiated by NoName057(16), another pro-Russia hacktivist group that emerged shortly after the invasion of Ukraine. The group's Telegram channel offers a DDoS toolkit called "DDosia,"[8] and claims to reward successful attacks in cryptocurrency. DDosia's target list includes dozens of organizations each day, many financial services firms among them, and is still active as of the publication of this report (though with limited impact).

These incidents underscore cyberthreat actors' investment in publicity and a shift from wiper attacks against businesses and government agencies in Russia, Ukraine, and affiliated nations to opportunistic DDoS attacks as part of the 'mixed media' warfare approach. It also highlights the importance of careful, independent threat assessments that evaluate intent, capability, and vulnerability.

Israel-Hamas

The Israel-Hamas war has had substantial geopolitical and economic impact but has not significantly or particularly affected the financial services cyber landscape, nor changed the regional cyber threat landscape overall. Financial institutions in Israel are remaining vigilant, but no high-profile attacks or significant impact have been reported. International organizations with a presence in the Middle East are monitoring and may operate at a heightened operational tempo but report no significant incidents.

Individual cyber-attacks and campaigns have been reported from both sides of the conflict, such as a phishing campaign targeting Israeli companies utilizing a zero-day vulnerability in F5 BIG-IP products, and an OpenAI ChatGPT outage in November. Anonymous Sudan claimed that attack, saying that AI is used by Israel for offensive and intelligence purposes and ChatGPT is biased towards Israel. However, the cyber crossfire campaigns only affect the countries involved.

III. Regulation

Legislation will be implemented in 2024 and 2025 that will shape financial institutions' cyber landscapes – especially in Europe, the UK, and Australia – for years to come. In many ways, new regulations will encourage a more secure, resilient financial services sector. However, it is important to note that threat actors have exploited regulatory changes by innovating new approaches or modifying old ones. Vigilant cyber hygiene is necessary as adversarial tactics may evolve with the regulatory environment.

Information and Communication Technology (ICT)

DORA (Digital Operational Resilience Act), part of the EU's Digital Finance Package (DFP), will impact all financial services operations in the EU. DORA is aimed at harmonizing digital resilience regulations using five pillars:

1. ICT risk management
2. ICT-related incident management, classification, and reporting
3. Digital operational resilience testing
4. Information-sharing arrangements

5. Management of ICT third-party risk and oversight framework of critical ICT third-party service providers.

DORA requirements have significant implications, particularly for those firms with hundreds or thousands of third-party providers. Financial services organizations will use 11 quantitative and qualitative indicators to identify their critical third-party providers, which will be directly regulated. Organizations must assess concentration risk in ICT and consider substituting providers and multiple contracts. International or global contracts will make this difficult, and financial services firms must continue to manage and oversee the resilience and security of their providers.

The FS-ISAC DORA Working Group's publication, Digital Operational Resilience Act (DORA) Implementation Guidance, helps financial firms become compliant before the Act goes into full effect on 17 January 2025.

Digital Assets

Major jurisdictions honed existing digital asset frameworks and implemented comprehensive regulations, signaling a move towards a more mature and regulated sector.

The key regulations include the European Union's Market in Crypto-Assets regulation (MiCA), and the United Kingdom's revised Financial Markets and Services Act 2023. Scheduled to take effect in 2024, MiCA introduces comprehensive regulations that enhance consumer protections, define conduct standards for the crypto industry, and introduce new licensing requirements. The Financial Markets and Services Act 2023 establishes new regulatory frameworks and accountability mechanisms.

Additionally, international financial regulatory bodies such as the International Organization of Securities Commissions (IOSCO), the International Monetary Fund (IMF), and the Financial Stability Board (FSB) have issued regulatory guidance and policy recommendations that establish clear guidelines and frameworks regarding the digital assets market.

Cybersecurity Regulation in Australia

Public interest has been increased by major cyber incidents in the last 18 months, such as the November 2023 ransomware attack on insurance provider, Medibank. Using a Medibank username and password stolen from a third-party IT service provider, the threat actors accessed almost 10 million customer names, addresses, birthdays, phone numbers, and email addresses and published Medibank customers on "naughty" and "nice" lists.[9] In January 2024, Australia sanctioned Russian national Aleksandr Ermakov in response to the attack.[10] US and UK authorities followed suit within 24 hours.[11]

These crimes have driven a robust regulatory response, particularly as it applies to critical infrastructure (including the financial sector).[12] Meanwhile, a 'no-fault, no liability' reporting requirement for ransomware attacks is being prepared. This approach aims to lift the visibility of ransomware incidents, support sharing within the industry, and build the sector's resilience.[13]

The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 lifted the penalty for breaches that result in the loss of customer data from AUD $2.2 million (USD $1.4 million) to whichever is the greatest:

1. AUD $50 million (USD $33 million)
2. 3x the value of benefits obtained by information misuse
3. 30% of adjusted turnover.[14]

The Australian government is also considering the reclassification of 'customer data' as 'critical infrastructure,' subject to the reporting requirements set out in the SOCI Act.[15] It is not clear yet whether this option will be pursued, considering the wide variability of 'customer data' and potential for increased compliance costs on the industry. Several FS-ISAC members in Australia report proactively moving to a more active and nuanced information management regime to balance the opportunities and risks associated with data retention and destruction.

IV. Member Observed Trends

Top malware

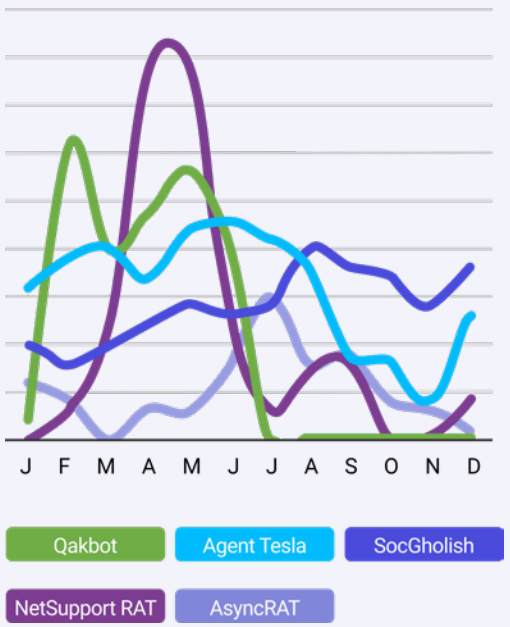


Figure 4: Top malware reported by FS-ISAC members, 2023

The top malware trends reported by FS-ISAC members are familiar and align with global malware trends across industries.

Agent Tesla – Likely used primarily in opportunistic "spray and pray" attacks on financial services institutions. The Agent Tesla Remote Access Trojan (RAT) infostealer offered as Malware-as-a-Service (MaaS) has been active since 2020.

SocGholish – A downloader malware attributed to TA569 – a financially motivated initial access broker selling access gained through SocGholish infections – is continuously active and reported by members in heightened numbers since mid-2022. FS-ISAC members reported that SocGholish and TA569 have demonstrated a novel and highly effective attack: compromising vulnerable websites to display fake-browser updates as the mechanism for malware delivery. Several new actors have taken cues from TA569 and are copying similar lures into their strategies. Noteworthy instances of such malware campaigns in 2023 include RogueRaticate, ClearFake, and ZPHP.

AsyncRAT – Malware with infostealing capabilities, sometimes used in connection with SocGholish/TA569 activity. NetSupport RAT is a repurposed version of the legitimate NetSupport Manager tool that allows remote access capabilities. This RAT is also associated with SocGholish/TA569 activity, although not exclusively. Member reporting peaked in Q2, then tapered off during Q3 and Q4. OSINT reports that NetSupport RAT use appeared to be focusing on other sectors such as education, government, and business services in the later parts of 2023.[16] The financial sector is likely to see more NetSupport RAT activity waves.

Qakbot – A modular botnet malware first reported in 2008, Qakbot was the target of a successful takedown operation carried out by the FBI in partnership with international law enforcement agencies in August. However, evidence of continued Qakbot activity in the wild was reported later in 2023.[17]

Interestingly, many trojans designed to target banking applications (Emotet, Qakbot, IcedID, Dridex, TrickBot) have evolved into modular toolsets that MaaS actors now deploy to compromise systems across sectors. The financial services threat landscape may soon be similar to the general global threat landscape as a result.

Ransomware

FS-ISAC analysis of ransomware leak sites data shows that finance and insurance were the fourth most targeted by ransomware and data extortion threat actors in 2023. FS-ISAC has worked with several members dealing with ransomware incidents throughout 2023.

Data exfiltration and encryption are the immediate concern of Ransomware-as-a-Service (RaaS) attacks, but financial institutions with experienced cybersecurity teams and/or cyber insurance are often more challenged by downtime and reconnection issues, which can erode customer trust.

The recent increase in financial sector third-party incidents has rekindled discussion of reconnection checklists/frameworks and resilience playbooks at the organizational and sector level.

Double and even triple extortion attempts have emerged in the last few years, in which attackers deploy ransomware in parallel with infostealers. If not paid, the threat actor threatens to release the stolen data or launch a DDoS attack. The malicious infrastructure – cyber and physical – created and developed to deploy ransomware and manage extortion operations has reached such a level of professionalism that some criminals are shifting their tactics to a new encryption-less "extortionware" approach. Some threat actors use their infrastructure to launch malware campaigns that abstain from ransomware and focus on data theft exclusively, and/or threaten to launch a DDoS attack and release stolen data unless a ransom is paid via the well-established ransomware extortion routes.

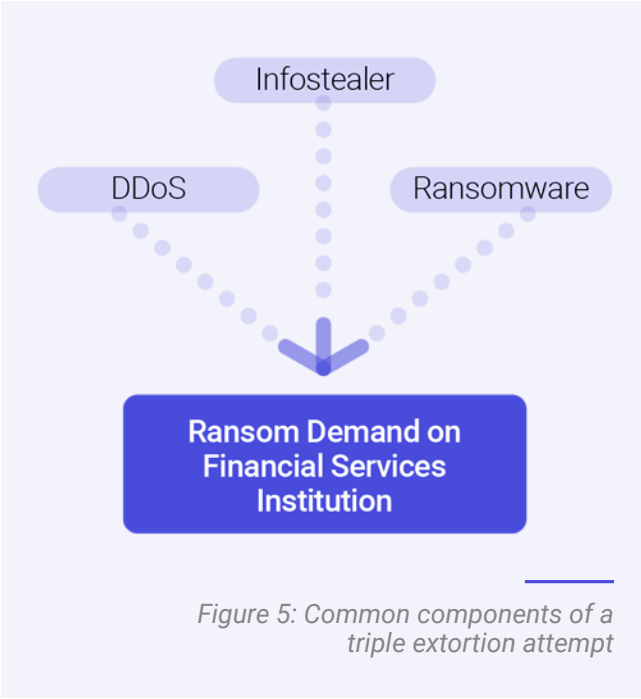


Figure 5: Common components of a triple extortion attempt

Mortgage Sector Targeted

The mortgage sector collects and stores a huge quantity of extremely sensitive information, making it a valuable target for cybercriminals. During the last quarter of 2023, non-bank mortgage companies and title insurance companies reported data breaches that affected millions of customers. Some computer systems were shut down, which affected closings, payments, and other activities. It is apparent from SEC 8-K filings and ransomware leak sites (and an ALPHV report to the SEC about a victim's failure to disclose the breach) that the majority of the companies were victims of ransomware attacks, probably by the RaaS ALPHV. FS-ISAC assesses with high probability that US victims were targeted by ALPHV's associate, Scattered Spider, which specializes in social engineering to obtain credentials to steal sensitive data for extortion.

In November, FS-ISAC and the Analysis and Resilience Center for Systemic Risk published Scattered Spider & Blackcat Ransomware: Mitigation Guidance to help financial firms deter and mitigate Scattered Spider and Blackcat ransomware exploits.

Fraud

▶ Social Engineering

FS-ISAC has observed that fraud-related social engineering usually involves business email scams (BES), with a small percentage involving business email compromise (BEC). Typically, the email scams incorporate executive impersonation, invoices, and payroll diversion using spoofed addresses.

Account takeover attempts are another common social engineering activity. Most commonly, attackers contact call centers impersonating a customer – "vishing" – and attempt to access accounts or information or use the firm's web presence to scam representatives or abuse credentials.

FS-ISAC has also noticed an increase in smishing (also called SMS-phishing), the use of social engineering in mobile texting. Most have involved executive impersonation, although some customer-facing smishing has been reported. The texts purport to be from a financial organization institution, often spoof sender names, and some use SMS short codes to appear more genuine. A common subterfuge is to notify the customer of (fake) activity in their account and invite them to "stop unauthorized transaction."

▶ Triangulation Fraud

Triangulation fraud unites online shoppers, a fake retail site, and a legitimate merchant in a fraud triangle. The fraudulent retail site attracts shoppers with substantially discounted items. The shopper makes an order (some post positive reviews about the experience, inadvertently reinforcing the ruse), which the criminal operators fulfill on a legitimate site using credentials stolen from a previous victim. The legitimate merchant fulfills the order, unaware of their involvement in a criminal operation until a shopper disputes the charge. Threat actors targeted large merchants during the 2022 Black Friday holiday sales, then pivoted to smaller merchants in 2023. It is difficult to assess the magnitude of impact of triangulation fraud on financial institutions because each party in the triangle sees only their side of the scam. This novel type of attack is an excellent use case in the importance of sharing in the fraud space. Pooling indicators of fraud makes it easier to identify trends and TTPs.

FS-ISAC's Triangulation Fraud Working Group Communications and Awareness Subgroup published a white paper regarding triangulation fraud, its indicators, and guidance to prevent and mitigate it.

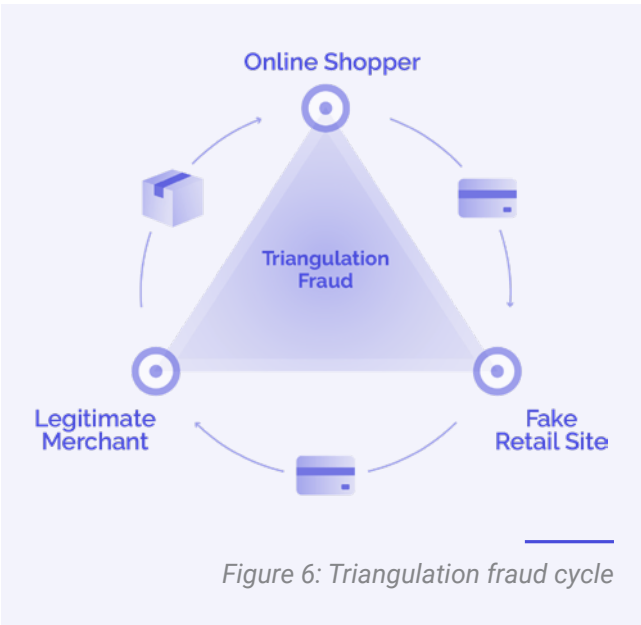


Figure 6: Triangulation fraud cycle

DDoS

Distributed Denial-of-Service (DDoS) attacks achieved greater reach and sophistication in 2023. According to Akamai, the financial sector is the top target across most of the world: 35% of all attacks targeted financial institutions in 2023. Hacktivists, who are intent on creating as much disruption and instability as they can, have been behind much of the upsurge in DDoS attacks since 2022. Ransomware attackers and criminal groups also incorporate DDoS attacks in layered attack patterns to distract cyber teams, disguise other attack operations, and/or add nuisance to the mitigation. Large-scale DDoS attacks cost little to provision and launch using readily available DDoS-for-hire services and underground markets.

Although FS-ISAC has seen many DDoS attacks on financial firms throughout 2023, third-party DDoS protection providers and web application firewalls can mitigate against all but the most massive DDoS attacks. Among institutions with such defenses, observed operational impact is typically low – largely confined to short-term website unavailability – which may cause some reputational damage.

For example, in September one of America's biggest and most influential financial institutions was attacked with a combination of ACK, PUSH, RESET, and SYN flood attack vectors. The attack was detected and halted within two minutes by the DDoS protection provider, but nevertheless disrupted internal system operations and the official website for a period of time. Anonymous Sudan claimed credit for the attack on its official Telegram page and disclosed its intention to shut the company's system down, although no further malicious activity was reported.

FS-ISAC's publication, DDoS: Here to Stay, produced in partnership with Akamai, details DDoS use cases, types, and mitigation best practices.

SEO Attacks Delivering Malware

In early 2023, FS-ISAC trends and open-source reporting indicated an increase in the use of search engine optimization (SEO) poisoning and malvertising.

Much of the reported activity combined elements of these two tactics, serving malicious advertisements for things like software downloads in search engine

SEO Poisoning: the use of search engine optimization techniques to insert malicious content in search results

Malvertising: usage of ads as a lure for malicious content

results. SEO poisoning and malvertising are not new, but prior to 2023 most SEO attacks observed by FS-ISAC were related to credential harvesting. These recent reports link the activity to malware.

Like many shifts and evolutions observed in 2022/2023 in common attack types, we assess that this too may be related to Microsoft's move in mid-2022 to block macros from untrusted sources. MS Office macros were a frequent malware vector, and the change drove threat actors to find new delivery methods, resulting in a string of known attacks now leveraged for malware.

QR Code Phishing

FS-ISAC observed a novel type of phishing attack in 2023: QR code phishing ("Qishing," "Quishing," or "QRishing"). Although not entirely unknown, usage was not widespread until mid-2023. At that point, attacks on the financial sector jumped, joining the X-ishing reports that had been dominated by email phishing, SMS phishing (smishing), and voice-phishing (vishing).

Reported TTPs involve a form of business email scam targeting financial services staff.

1. Attackers send emails from a spoofed/typo-squatted domain.
2. The emails contain an embedded JPG attachment with a QR code, which directs users to credential harvesting pages.
3. The QR code image attempts to circumvent corporate email security scanning defenses.

These scams typically purport to be from the company's HR, with lures themed with organizational benefits, HR functions, or MFA activation. This is particularly effective against victims using personal devices to scan the code because they are unprotected by the company's cybersecurity. Providers have quickly adapted to this new form of phishing by implementing email protection QR codes, extracting the URL for analysis, and improved staff awareness training and simulation.

V. Regional Close-Up

Latin America

The cyber threat landscape in the LATAM financial services sector is generally similar to the global landscape, but some cybercriminal groups operate exclusively in the region. In 2023, LATAM members focused on phishing and malware campaigns targeting banks in Mexico, Chile, Colombia, Panama, and others. Notable threat groups active in the region include Grandoreiro and CyberCartel. FS-ISAC observed activity associated with a Phobos-Faust Ransomware attack and an active campaign deploying a new variant of BBTok malware. The BBTok campaign targets computer systems in Mexico and Brazil via geofencing and utilizes a unique combination of LOLBins to spoof legitimate bank pages in the target countries.

EMEA

DORA and other pending EU regulations dominated member discussions throughout the year. FS-ISAC's DORA Working Group published compliance guidance and continues to work with regulators on the technical standards and other aspects of implementation.

As the EU cyber community assesses the implications of DORA on financial institutions, FS-ISAC monitors the cyber threat landscape for potential impacts of the two armed conflicts in the EMEA region.

The current assessment is that the Israel/Hamas war has not altered the threat landscape significantly. Pro-Russian hacktivists have continued to target EU and NATO countries, with a particular focus on government, transport, and telecommunications as well as the financial sector. In June, the Swiss parliamentary website was targeted by the threat actor NoName057(16) days before President Zelensky's address to the Swiss Parliament, followed by DDoS attacks on Swiss organizations. These exploits were largely mitigated.[18]

APAC

The use of ransomware has surged in frequency and severity. From January to October 2023, one in 20 APAC organizations was hit, with the overall rate increasing by 30% in 2022. Australia (77), India (50), and Japan (33) were the top three nations impacted. Financial services were the fourth most commonly affected sector in the region.[19] LockBit 3.0 was the most active ransomware operator, followed by ALPHV/Blackcat.[20]

That increase reflects rising cybercrime activity across APAC. In the first nine months of 2023, the region recorded a 15% year-over-year increase in cyberattacks. The average number of attacks in 2023 was 1,963 per week.[21] Threat actors employed more advanced TTPs and surveilling networks, many of which went undetected for extended periods in 2023. Drivers include rapid digitalization[22] resulting from COVID-19 lockdowns and accelerated remote working arrangements, increased internet penetration, and geopolitical tensions.[23]

An increase in state-sponsored cyber activities, including cyber espionage, poses significant geopolitical and security concerns for the region. Several local financial institutions reported the use of deepfakes to mimic senior financial services executives in 2023. The exploitation of vulnerabilities in supply chains – including but not limited to zero days – to gain unauthorized access to targeted organizations remains the greatest current concern for members.[24]

In 2023, threat actors from China, North Korea, and Russia launched increasingly sophisticated attacks against financial services operations in APAC. Groups affiliated with North Korea supported the development of the nation's nuclear warfare program in large part via cryptocurrency theft. Japanese exchanges have been heavily targeted. FS-ISAC is monitoring the collaboration between English-speaking and Russian-speaking cybercriminals to launch data extortion and ransomware campaigns.[25] In 2024, responses from China – whether diplomatic, miliary, and/or cyber – to the return of the Democratic Progressive Party in Taiwan in January will be closely tracked. Foreign interference, along with misinformation and disinformation, present significant risk to APAC countries holding elections in the first half of the year, including Indonesia (February), North and South Korea (April), the Solomon Islands (April), and India (April/May).

VI. Predictions

Driver

The 2024 Summer Olympics and a "Super Election" year.

Millions will view the Summer games, and 2 to 4 billion citizens will head to the polls, the most in world history, in national elections in Iran (1 March), Russia (17 March), India (April/May), the EU (6-9 June), and the US (5 November).

Prediction

Hacktivism attacks will increase, perpetrated by a more diverse range of threat actors and vectors.

Financial firms will see more disruptive attacks as the many national elections in 2024 will provide hacktivist groups opportunities to leverage geopolitical tensions and express their motives. A large proportion of exploits will be DDoS attacks aimed at critical infrastructure. As attacks increase, it can be expected that hacktivists' TTPs will expand as well, drawing on their experience and availability of cybercrime infrastructure.

Prediction

Increasing malinformation, misinformation, and dis-information campaigns will multiply scams and sow confusion.

Amplified by GenAI technology, election-based mal-, mis-, and dis-information[26] campaigns will likely increase X-ishing attacks -- more information gives fraudsters more opportunities for more lures – and will expand the cyber threat landscape. Such campaigns blur the distinction between truth and fiction (and scams), and often accelerate around geopolitical events, especially elections. These campaigns pose substantial threats to financial services, their customers, and the democratic process.

Driver

New legislation and regulation in relation to security standards, communication, and the use of AI.

Globally, regulation is increasingly focused on cybercrime and third-party risk. Regulations do or will require financial services organizations to adhere to new security standards, collaborate, share security events and incidents with peers, and report cybersecurity incidents to regulators. In 2023, legislation aimed at minimizing public risks associated with AI were passed in both the US and EU, providing a template for wider global regulation and driving rapid uptake. However, though excessive data collection and/or retention amplifies the risk of exfiltration attacks, extensive corporate datasets are necessary to train data for AI applications, as well as operations and for customer service.

Prediction

Financial services firms will adopt active data management programs.

The sector will increasingly require active data management programs to comply with regulations, minimize the risks, and maximize the opportunities presented by retention and destruction. Expect new strategies regarding in-house data storage, reducing the number of suppliers, and sharing information with third parties.

Prediction

Threat actors will weaponize legislation in ransomware campaigns.

Cybercriminals will not hesitate to use financial firms' compliance concerns to their own ends. In 2023, one threat actor alleged to the SEC that the organization they compromised and was extorting had failed to report the breach within four days. Having expanded their extortion tactics with threats of GDPR fines or SEC complaints, threat actors will continue to refine their extortion tactics to enhance their operational success and coerce their victims to pay.

Driver

Supply chain vulnerabilities are a threat vector.

As attacks on solutions providers accelerate, financial institutions' cyberthreat landscape broadens. DORA legislation requires financial firms in the EU to assess the "criticality" of providers and remove as many as is practicable as a security measure. Elsewhere, stricter regulatory scrutiny has been implemented to boost supply chain cyber hygiene, and some legislation will require suppliers to communicate incidents to the sector.

Prediction

Financial services firms will participate in third-party suppliers' cybersecurity.

Financial firms will work more closely with their suppliers to establish communications channels for incidents and help them improve their cyber defenses as regulators increase their scrutiny of the impact of third-party cyber vulnerabilities on financial services.

Driver

New technologies are rapidly evolving with effects beyond the cyber threat landscape.

Cryptocurrency and blockchain are established technologies that impact the financial services ecosystem in new – sometimes dangerous – ways. GenAI and quantum cryptography are both nascent technologies with proof of concept and use cases demonstrating the capacity and potential to radically reshape financial services operations.

Prediction

The financial sector will increasingly embrace "crypto agility," in which new encryption methods for information systems can be adopted rapidly without altering the underlying system infrastructure. Though claims of asymmetric RSA cryptography breakage were debunked last year, 2024 will deliver further advances in quantum computing and AI that will challenge established cryptographic algorithms. Financial firms will need to conduct cryptographic inventories, prepare their systems to replace algorithms, and most will likely roll out post-quantum cryptography schemes alongside traditional cryptography. In 2024, the FS-ISAC Post-Quantum Cryptography Working Group will release a report on the question of crypto agility in the financial sector.

Prediction

Volatility in cryptocurrency will attract malicious actors.

Following the pattern of previous Bitcoin halving cycles, the next halving event expected in April 2024 will catalyze a resurgence of interest and investment in cryptocurrencies, giving rise to a Crypto Spring. Alongside the expected increase in market activity, there will a heightened risk of cybersecurity threats and hacking incidents within the cryptocurrency space. More attention and investment during Crypto Spring will attract malicious actors seeking to exploit vulnerabilities in exchange platforms, wallets, and smart contracts due to the increase in Total Value Locked of the coins.

Prediction

Generative AI will enable more targeted phishing/BEC emails and deepfakes.

Financial institutions will need to reinforce processes for payments and other financial workflows, add more checks on known good channels internally, and augment employees' cyber training – employee impersonation is a big concern. Some may need to amplify collaboration across business units, specifically fraud, customer service, cyber threat intelligence and identity and access management to counter customer impersonations.

Contact

fsisac.com
media@fsisac.com

Endnotes

1 ChatGPT Tricked To Write Malware When You Act as a Developer (cybersecuritynews.com)

2 #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability | CISA

3 Exploitation of Accellion File Transfer Appliance | CISA

4 https://techcrunch.com/2023/02/02/ion-group-lockbit-derivatives-ransomware/

5 EquiLend Ransomware Attack Leads to Data Breach - SecurityWeek

6 CVE Website

7 Project Zero: 0day "In the Wild" (googleprojectzero.blogspot.com)

8 DDoSia Attack Tool Evolves with Encryption, Targeting Multiple Sectors (thehackernews.com)

9 Medibank Cyber Incident: What is Known About the Data Breach (gizmodo.com.au)

10 Australian Cyber Security Centre (2024). Cyber sanctions imposed on Russian cybercriminal for Medibank Private 2022 compromise. Published on 23 January.

11 US Department of the Treasury (2024). United States, Australia and the United Kingdom sanction Russian cyber actor for the Medibank hack. Published on 23 January.

12 The financial sector became part of Australia's critical infrastructure in 2018, with the introduction of the Security of Critical Infrastructure (SOCI) Act.

13 Department of Home Affairs (2023). 2023-2030 Cyber Security Strategy. Published on 22 November.

14 Australian Attorney General's Portfolio (2022). Parliament approves Government's privacy penalty bill. Press release published on 28 November.

15 Australian Strategic Policy Institute (2023). Interview with Hamish Hansford, Deputy Secretary of Cyber and Infrastructure Security, Department of Home Affairs on the 'Policy, Guns and Money' podcast. Published on 23 June.

16 VMware (2023). NetSupport RAT: The RAT King Returns. Published 20 November.

17 Cisco Talos (2023). Qakbot-affiliated actors distribute Ransom Knight malware despite infrastructure takedown. Published 5 October.

18 NoName Attacks Switzerland: A Page Out Of State-Sponsored APT Playbook (thecyberexpress.com)

19 Check Point (2023). A Continuing Cyber-Storm with Increasing Ransomware Threats and a Surge in Healthcare and APAC region. Published on 25 October.

20 Cyberint (2023). Top Asian/APAC Cybersecurity Threats of 2023. Published on 27 November.

21 Check Point (2023), A Continuing Cyber-Storm with Increasing Ransomware Threats and a Surge in Healthcare and APAC region. Published on 25 October.

22 Many APAC nations had extensive lockdowns during the COVID-19 pandemic, with the proportion of workers and students engaging online remaining relatively high well into 2023.

23 Cyfirma (2023). The changing cyber threat landscape: Asia-Pacific Region. Published on 14 December.

24 CYFIRMA (2023). THE CHANGING CYBER THREAT LANDSCAPE: ASIA-PACIFIC (APAC) REGION. Published on 14 December.

25 BushidoToken Threat Intel (2023). Top 10 Cyber Threats of 2023. Published on 12 December.

26 https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation