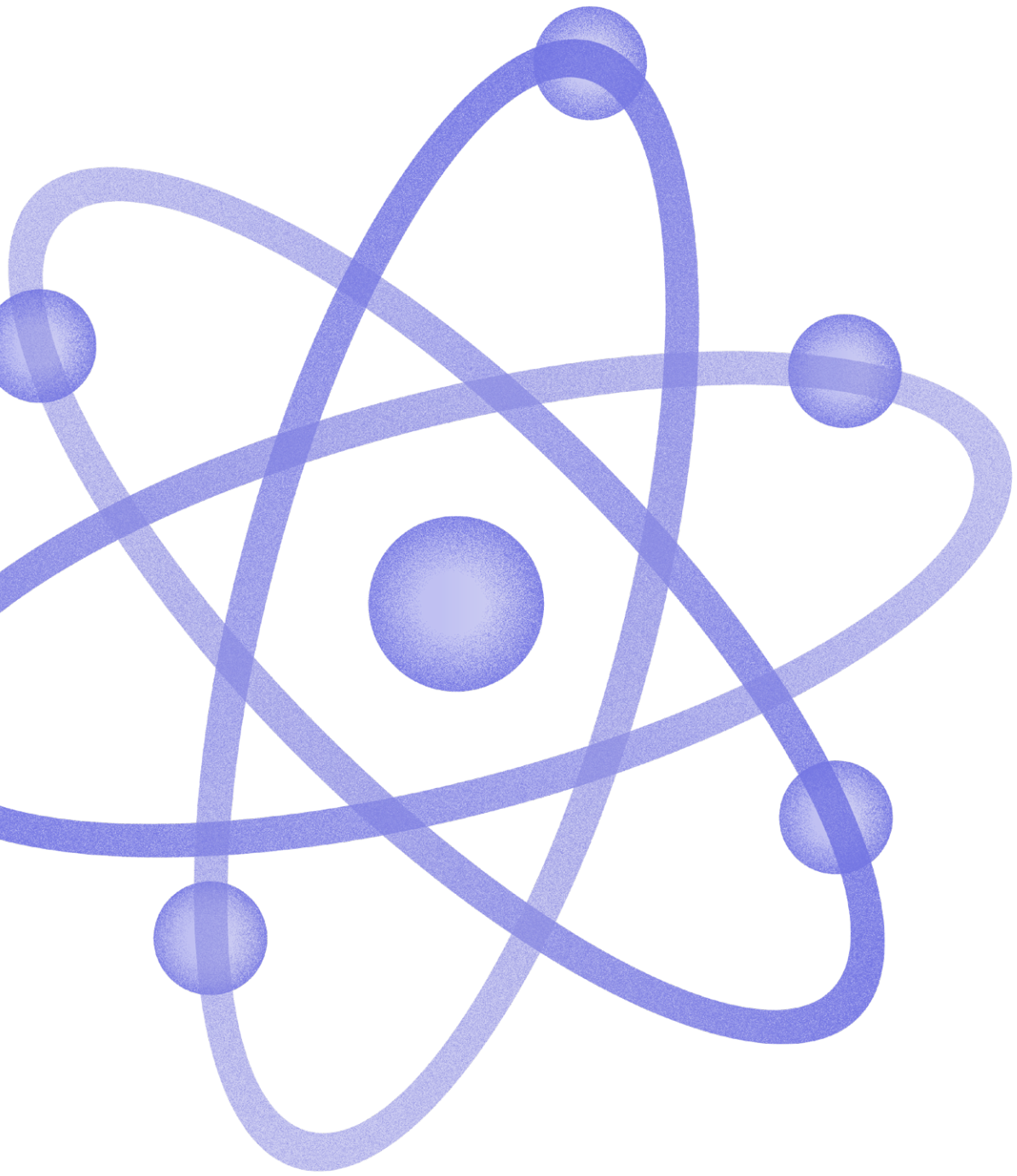
FS-ISAC

Navigating Cyber 2023



March 2023

Contents

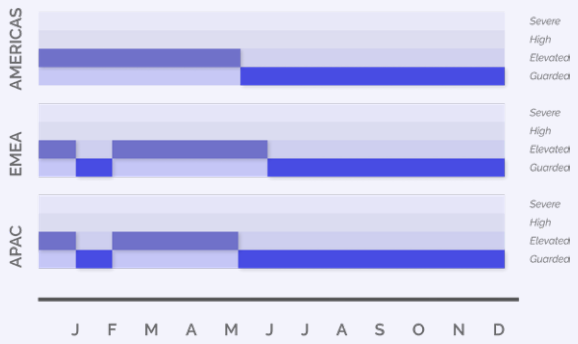
EXECUTIVE SUMMARY

By far, the most significant impact on the financial services cyber threat landscape in 2022 was the Russia-Ukraine war.

FS-ISAC's Cyber Threat Level, an industry barometer of cyber threats facing financial services, remained at Elevated for much of the year across all regions and remained Elevated for longer in EMEA. As the global volume of cybercrime rose, financial services organizations remained a prime geopolitical target.

▸ Regional Cyber Threat Levels

In January 2022, Elevated regional Cyber Threat Levels due to impact of the December 2021 Log4j vulnerability were lowered to Guarded. In February, the regional Cyber Threat Levels increased due to the Russian invasion of Ukraine and only lowered back to Guarded later in the year.



KEY TRENDS OF 2022

▸ **Geopolitical conflict** goes cyber at scale as existing tensions, exacerbated by Russia's invasion of Ukraine, sparked a flood of hacktivist activity that continues unabated. China and its goal of Taiwan unification, and Iran's ideologically motivated attacks on Western financial institutions contribute to the geopolitical cyber threat landscape.

▸ **Denial-of-Service (DoS) and Distributed DoS (DDoS) Attacks** are increasing globally due to the increased availability of 'as-a-service' options and are frequently associated with extortion. While most of these attacks have low or no impact, the financial services sector remains one of the most targeted.

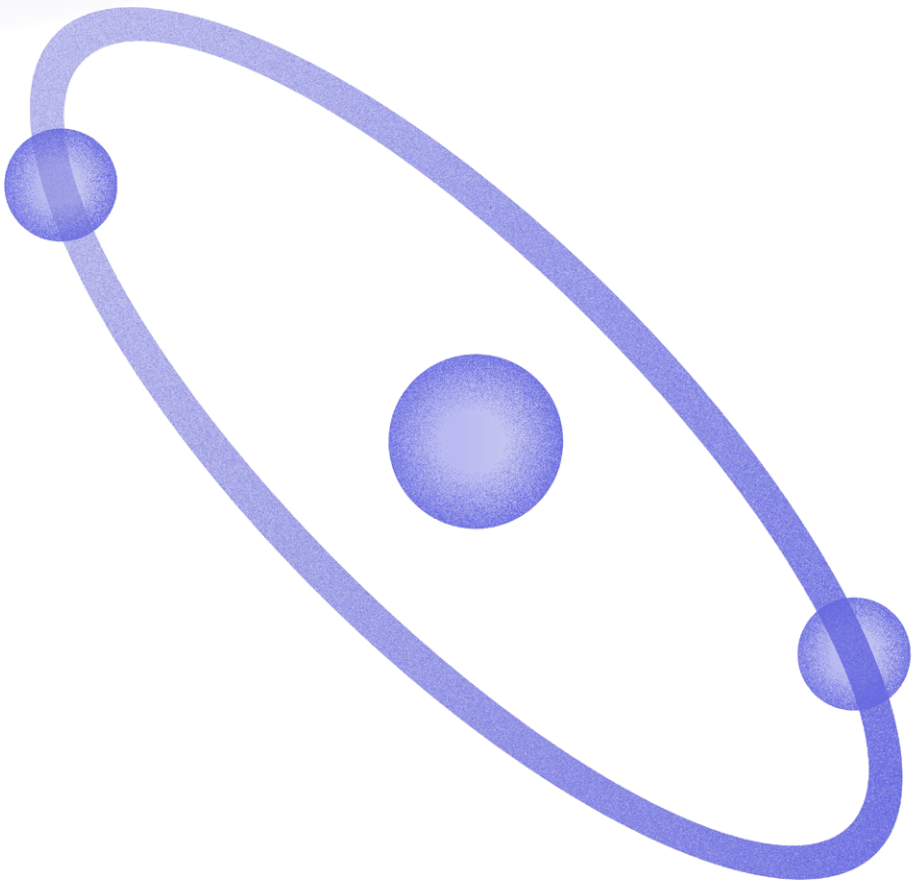
▸ **Ransomware attacks** regularly dominated headlines throughout 2022. Almost all security vendors agree that ransomware attacks are getting worse. Ransomware-as-a-service (RaaS) providers, who give affiliates access to their ransomware suite in exchange for a cut of the illegal profits, are likely to blame for this growth.

▸ **Business email compromise (BEC)** has become one of the most common and costly frauds impacting firms around the world. BEC can take several forms but the most reported to FS-ISAC are payroll diversion requests or fraudulent payment requests, either as part of an impersonation scam or vendor fraud.

▸ **Cryptocurrencies** present a range of challenges to financial institutions globally. Threat groups finance their operations using cryptocurrency in ransom demands, among other methods. The increase in cryptocurrency investment holdings highlights the need for better oversight and protections for this asset class.

▸ **Supply chain threats** impacted a more digitized business environment. Open banking and APIs, mobile banking apps, and exposure to partner breaches contributed to making financial services organizations vulnerable to hackers via third-parties. In 2022, the most prevalent supply chain attacks reported by members were the hijacking of software updates, fraudulent code signing, and the compromise of open-source code.

Member financial firms reported on the top malware strains hitting the financial sector, as well as emergent attack methods such as using Microsoft OneNote Attachments, telephone-oriented attack delivery, and "Adversary-in-the-Middle Attacks." In Asia Pacific, cyber incidents related to impersonation are on the rise, but ransomware remains the top concern for APAC members.



Key Predictions for 2023 and Beyond

Where geopolitical tensions escalate in 2023, we will see a further fragmentation in the cyber landscape via the increased involvement of non-state actors attacking on an ideological basis. The use of mis-, dis- and mal-information – potentially leveraging generative text engines to spread – will continue to sow uncertainty, both politically and in the perceived impact of hacktivist campaigns. In turn, this is likely to increase the cyber and/or reputational risk to financial sector firms operating in (or affiliated with) the nations engaged in conflict.

As DDoS as-a-service subscriptions get cheaper and cheaper, it will be easier for threat actors to launch devastating attacks anonymously and disrupt business uptime. Accordingly, third-party risk management is likely to become a more important part of an organization's overall strategy for managing risks. To bolster those efforts, governments around the world will begin to implement new regulations and compliance requirements.

Despite the crypto crash, threat actors will continue to be lured by the large sums they can directly steal from crypto infrastructure firms and exchanges. As businesses integrate crypto into traditional financial infrastructure, they may seek to protect investments via cyber insurance. However, there will be significant changes to the cyber insurance market. Many companies will not qualify without rigorous transformations to their security infrastructure.

Even the most advanced defenses can be penetrated through simple social engineering attacks such as impersonation through business email compromise. Emerging artificial intelligence tools will make detecting fraudulent communications and verifying identities more challenging; however, AI will also be leveraged on the cyber defense side.

2022 THREAT LANDSCAPE: MACRO TRENDS.

I. Geopolitical Conflict Goes Cyber at Scale

Existing geopolitical tensions exacerbated by Russian's invasion of Ukraine sparked a flood of hacktivist activity that continues unabated. Hacktivist groups on both sides of the Russia-Ukraine war have been involved in DDoS attacks, data leakage, and website takeovers since the invasion began. Financial firms in countries that Russia considers hostile have been singled out for attacks and called out by name as targets on Telegram and other hacktivist forums. While the attacks have yet to cause significant impact, they are notable in their ability to temporarily disrupt major businesses and governments while also garnering media interest.

Hacktivists are just one example of a range of cyber activity that has been seen since the invasion of Ukraine. According to the Ukrainian CERT, the Russian government unleashed cyber attacks against more than 2000 organizations in Ukraine in 2022, including in the financial, commercial facilities, and telecommunications sectors. It is likely that cyber attacks will continue and may increase as the conflict in Ukraine persists. FS-ISAC members with operations in geopolitically conflicted jurisdictions could encounter severe business disruption.

Russia's invasion of Ukraine sparked intense speculation on whether China would do the same to Taiwan. China's government has long stated their belief that Taiwan is already part of the country; recent downturns in diplomatic relations and threats against how other countries treat Taiwan suggest they are willing to take military action if necessary. While this is unlikely in the short term, the possibility of sanctions against Chinese government leaders could create ripple effects from trade and supply chain disruptions, especially on semi-conductor manufacturing, which would have direct impact on the financial sector.

II. The DDoS Threat is Here to Stay

Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks are increasing globally – in part due to increased availability of 'as-a-service' options - and are frequently associated with extortion. While most of these attacks have low or no impact, the financial services sector remains one of the most targeted sectors. FS-ISAC's joint report with Akamai showed that 2022 saw a 73% increase in DDoS attacks on financial firms in Europe and a 22% increase globally compared to the previous year.

DDoS poses serious threats when dealing with third-parties and dependencies which can impact business operations for customers like financial institutions. For example, a vulnerable service provider is brought offline, or impacts the operation of a higher order service. In the context of financial services, which operate in a highly regulated, highly complex environment, DDoS can potentially cause compliance issues via the unavailability of a service.

A key actor in the DDoS space in 2022 is the Russia-based Killnet cyber criminal group. During the Russian invasion of Ukraine, Killnet declared allegiance to the Kremlin and hostility to anyone opposed to Russia. DDoS attacks targeted both state and privately-owned sites. A notable wave of attacks targeted governments, airports, and financial targets including FS-ISAC members in October, many months after the war began.

III. Cryptocurrency as a Destabilizing Factor

Cryptocurrencies present a range of challenges to both financial institutions and the general cybercrime landscape globally. As international agencies and law enforcement ramp up defenses against ransomware campaigns, threat actors have been persistent in adopting new techniques. Threat groups finance their operations using cryptocurrency: in ransom demands, and in parallel through

unauthorized cryptomining malware on Internet-of-Things devices, corporate networks, and cloud environments. North Korean cyber criminal groups such as CryptoCore (aka TA444) and the Lazarus Group-based BlueNoroff were seen as some of the most active threats in the cryptocurrency space. North Korean actors were also linked to several employment scams, leveraging text from online job posts and publicly available resumes to secure remote positions at cryptocurrency firms, likely to function as insiders.

As cryptocurrency grows in investment portfolios, the gap in regulation and security becomes apparent. Beyond the already dubious reputation of decentralized digital currencies as a tool for money laundering, criminal funding, and illegal purchases, the crypto market is vulnerable to cybercrime, as evident – among many other instances – by the over $1 billion in cryptocurrencies stolen from DeFi platforms in February 2022. It is also rife with fraud – most notably the collapse of the FTX cryptocurrency exchange in December.

The increasing global proliferation of digital assets has spurred many governments to look into their own implementations of Central Bank Digital Currencies (CBDC) that will be pegged to the country's fiat currency. CBDCs may significantly impact the payments industry in countries that implement them and may well encroach on some services currently provided by financial institutions.

IV. Ransomware: A Better Business Model than Ever

Ransomware attacks continued to regularly dominate headlines throughout 2022. In previous years we saw innovations such as data exfiltration prior to encryption and extortion, the use of leak sites to shame and coerce victims into paying, and DDoS attacks against victims already struggling to cope with the ransomware attack. What 2022 lacked in innovation, it made up for in volume. Security vendors almost unanimously highlight not only an upward trend in ransomware attacks, but also ransomware as the most significant threat in the cybersecurity environment. Such growth is likely due to the many ransomware-as-a-service (RaaS) operators who provide affiliates with access to their ransomware suite for a share of the criminal profits. Organizations who follow cryptocurrency payments to ransomware actors noted a significant dip in 2022, attributing this to sanctions against such payments. However, FS-ISAC noted a continued stream of attacks despite this trend.

Ransomware is of specific concern in terms of supply chain risk. Trending analysis of ransomware attacks conducted by FS-ISAC on data shared from a partner identified the Manufacturing and Professional, Scientific, and Technical Services sectors as the top two industries targeted by ransomware threat actors, with the Finance and Insurance sector third. Professional, Scientific, and Technical Services represent the majority of third-party suppliers and vendors to the financial sector.

Ransomware Attacks on Third-Party Suppliers to the Financial Sector in 2022

Irish banking software company CR2 – *AvosLocker*

Finance and accounting solutions provider Exela – *Hive*

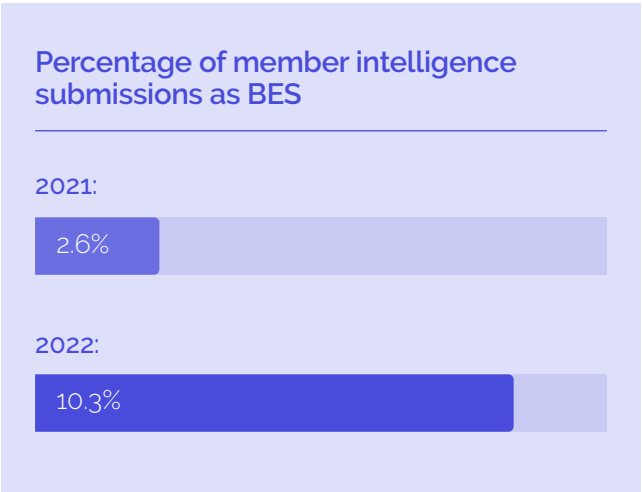
Digital security software firm Entrust - *Lockbit*

Lockbit was the most prolific ransomware operator throughout 2022. Lockbit, like other RaaS operators, target public and private sectors indiscriminately, capitalizing on the availability of compromised networks sold by initial access brokers. Other notable groups from throughout the year include Black Basta, BlackCat, AvosLocker and Hive.

One significant development in the ransomware scene was the splintering of the notorious Conti group. At the onset of the Russia/Ukraine war, the Conti group briefly posted their support for Russia during the conflict. Consequently, a Ukrainian researcher leaked a huge trove of chat files from the Conti gang's private chat server detailing the group's internal workings. Not long after this, the group fragmented but continued to operate.

V. Business Email Scams – Not Just Email Anymore

Business email scams (BES) have become one of the most prolific and costly frauds to plague industries globally. While there are no global figures to estimate the cost of BES, in the US in 2021, the FBI's Internet Crime Complaint Center (IC3) received complaints of BES amounting to damages of nearly USD 2.4 billion. In the same period, ransomware complaints only amounted to damages of around USD 49.2 million. In FS-ISAC member reporting, BES saw a 300% increase between 2021 and 2022.



BES scams can take several forms, but typically manifest as payroll diversion requests, or fraudulent payment requests, either as part of a CEO or impersonation scam or vendor fraud. The majority of reports shared with FS-ISAC are payroll diversions.

While email is the principal attack vector for these scams, fraudster TTPs (tactics, techniques, and procedures) have begun to increasingly include the use of other media, such as WhatsApp. Taking the scam outside of the corporate email system decreases the likelihood of discovery and gives fraudsters the opportunity to introduce other technology to dupe their victims. Advances in artificial intelligence (AI), deepfake and text-to-speech technologies have been demonstrated to be effective in executive impersonation schemes.

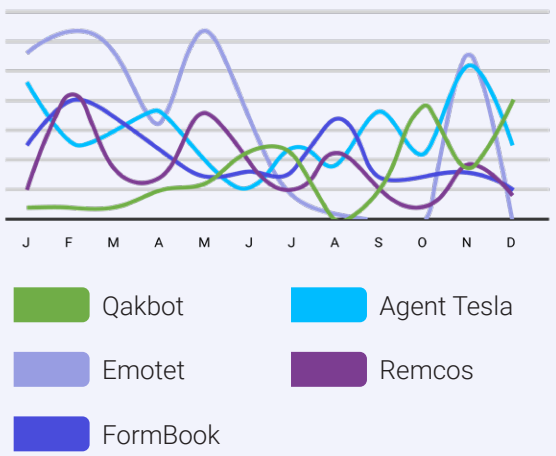
VI. Supply Chain Threats Are Not Just a Nuisance

As organizations become increasingly interconnected and complex, the supply chain threat is growing. In last year's report, we covered in detail the Solarwinds, Accellion, Kaseya, and Log4j incidents that affected the financial sector. As detailed above, in 2022 multiple suppliers to the financial sector experienced ransomware compromise. Although actual cascade of compromise is rare, each incident does have impact. At the very least, customer firms must divert resources to gather information and investigate potential impact on themselves and the sector. Critical vulnerability exploits – for example, the "Follina" Microsoft Office zero-day remote execution vulnerability discovered in May 2022 – similarly cause at least some operational impact for many affected organizations while they investigate and patch.

Some supply chain incidents are not easily mitigated. A notable incident occurred in July 2022 when Rogers, a major ISP in Canada, suffered prolonged outage that caused disruption throughout the financial sector impacting corporate operations (including remote work), online banking services, payments, and ATMs of multiple FS-ISAC members in the region. With telecom providers in particular, it is often not practical or possible to switch providers quickly and easily even when there are contracted backups. In today's world of remote working, cloud-based services, and internet customer-facing services, telecom outages may be especially destructive.

MEMBER-OBSERVED TRENDS

Top 5 malware reported by FS-ISAC members, 2022



Malware

Emotet

Emotet typically operates during periods of marked activity and inactivity. Following a break from July to November 2022, Emotet returned to installing malware to exfiltrate data, extorting money, and launching other forms of attack including ransomware and DDoS. FS-ISAC members observed the use of thread hijacking to encourage recipients to open malicious Excel attachments and new strategies such as encouraging recipients to re-open the attachment in a 'Templates' folder to bypass Microsoft's Protected View.

Remcos

Remcos is a remote access software used to grant full control of a machine to a remote user. Peaks in observed activity in April-May 2022 coincide with the publication of code improvements.

Agent Tesla

Agent Tesla is an advanced remote access trojan (RAT) that functions as a keylogger and information stealer, as frequently reported by FS-ISAC members. Although ever-present in the threat landscape, Agent Tesla is estimated by Checkpoint to impact as much as 7% of all organizations worldwide. Its activity saw a significant increase in October-November 2022. Phishing lures observed by the membership to spread Agent Tesla utilized financial themes such as purchase orders, bank statements, shipment notifications, invoices, and remittances.

FormBook

FormBook member submission volumes have been fairly consistent between 2021 and 2022, showing a slight increase in 2022. However, towards the end of the year, FormBook's presence tapered off. This impact in member submissions is consistent with global OSINT trends. FS-ISAC members reported financially themed campaigns, including invoices, purchase orders, shipment notifications, quotes, and outstanding balance themes.

Qakbot

Qakbot is a modular stealer observed in an increasing trend in member reporting and in the wild during the latter half of 2022. Its considerable growth can be attributed to newly observed TTPs in which Qakbot was used as an initial entry point for the deployment of Black Basta ransomware. A smaller peak seen in June 2022 could be related to attempts to use Qakbot to take advantage of the Follina vulnerability. The Qakbot volume of FS-ISAC member submissions increased by nearly 50% from 2021 to 2022. Notably, Qakbot is reported by a wide range of industries within the financial sector, indicating its prevalence outside of the realm of banking and payments.

Microsoft OneNote Attachments

Since December 2022, FS-ISAC members have reported the distribution of malware and embedded files via OneNote, Microsoft's note-taking application that enables cross-organization collaboration. Hackers have been embedding executable code and script formats to run malicious code on the systems of recipients. Sometimes they use "click to view" banners to trick recipients into downloading attachments and clicking through warning messages. Security researchers observed malicious actors experimenting with a variety of alternative tactics before settling on OneNote, taking advantage of the new delivery vector while its endpoint security is unable to detect malicious code.

Telephone-Oriented Attack Delivery

FS-ISAC members observed hybrid cyber campaigns known as 'telephone-oriented attack delivery' (TOAD). TOAD campaigns combine elements of phishing, malspam, and vishing to social engineer potential victims into downloading malware or exposing sensitive information. Some TOAD campaigns entice potential victims to contact fraudulent call centers managed by threat actors in an attempt to steal credentials or infect systems with malware. While TOAD campaigns require more threat actor resources than traditional phishing and malspam, they also often avoid security defenses that are aimed at more traditional campaigns.

Adversary in the Middle Attacks

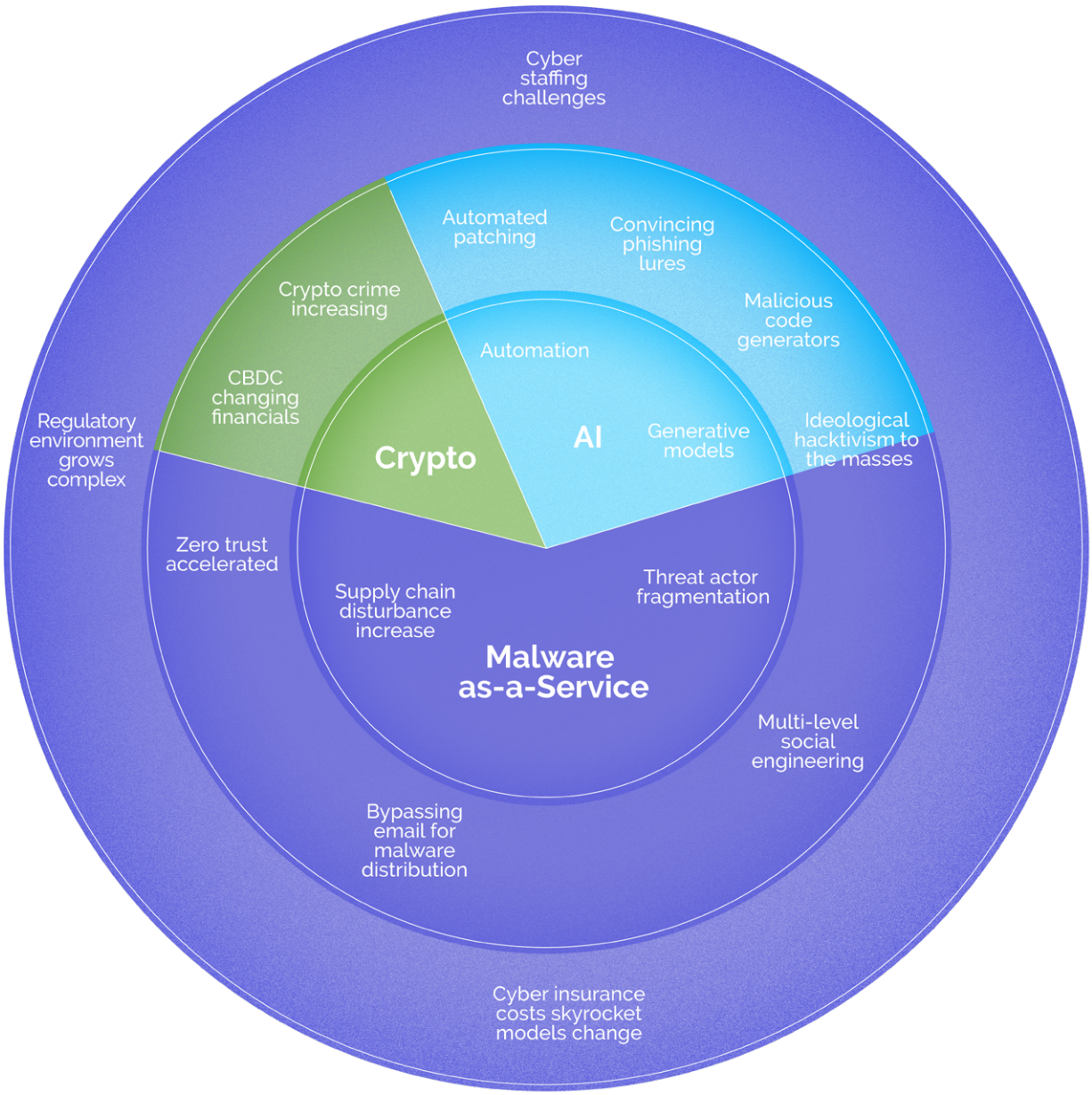
Midway through 2022, FS-ISAC members observed an increase in phishing campaigns attempting to harvest credentials from Office 365 users. This technique, known as "Adversary in the Middle" (AitM), involves placing a proxy between a target and a website they are visiting in order to intercept information. This information often includes credentials and session cookies, which is then leveraged for business email compromise. Access to session cookies allows threat actors to bypass multi-factor authentication (MFA) and gain access to the target's account. In mid-2022, AitM approaches were deployed against financial institutions in the US, UK, New Zealand, and Australia.

REGIONAL SPOTLIGHT: RANSOMWARE A TOP CONCERN IN APAC

As with the counterparts around the world, the first half of the year saw increased concerns from Asia Pacific (APAC) members on the cyber impact of the Russia-Ukraine War, as well as concerns relating to state-sponsored attacks by China and North Korea. In the second half of 2022, there was an increase in member reports of cyber incidents relating to cyber impersonation of specific individuals. A mid-December survey of members indicates that ransomware is a primary concern of APAC members, alongside reports of increased cyber insurance premiums and exemptions for ransomware.

- **May:** Black Basta ransomware observed
- **July:** Members report use of YamaBot Malware by North Korean affiliated Lazarus Group
- **September/October:** Heightened ransomware concerns following attacks on telecoms provider Optus and health insurer Medibank
- **October:** Cyber impersonations: fraudulent loan applications using false identification, impersonating bank executives regarding crypto investments

- **May:** Ransomware attack on Nikkei Singapore
- **February:** Chinese state-sponsored actors targeted financial firms in Taiwan
- **February:** Darkside targets financial firms in Phillippines
- **June:** Man-in-the-Middle Attacks targeting Office 365 users in Australia and New Zealand
- **July:** Hive ransomware attack on Australian arm of security firm GS4



PREDICTIONS FOR 2023 AND BEYOND

In 2022, we observed the effects of change driver pillars operating at the global and regional levels. These drivers are the root causes of many of the key trends impacting the financial services cyber threat landscape. The diagram shows the identified change drivers and their predicted impact, radiating from the center outwards.

▶ Driver

Malware-as-a Service

The commodification and professionalization of cybercrime operations has long been a major driver of the threat landscape. As threat actors become specialized in specific aspects of the kill chain and offer their services in skills and code for sale, cyber attacks become easier to orchestrate, more accessible, less attributable and of lower risk, and therefore more prevalent.

▶ Impact

Supply chain threats will continue to grow with the easy availability of malware-as-a-service, as the opportunities to impact third-parties connected to financial services proliferate. Third-party breaches against key software suppliers, authentication providers and services, technology services and providers, and cloud and managed software service providers will increase in volume and impact. Dedicated third-party teams focused on mitigating risk and building resilience will become an integral cybersecurity function. Movement towards zero trust approaches will accelerate.

Social engineering activity will increase. The success of social engineering in several high-profile criminal and nation-state attacks in 2022 will create the momentum for more. Social engineering attacks will increasingly incorporate SMS and hybrid tactics like telephone-oriented attack delivery, branching out beyond email. New and emerging machine learning generative tools like ChatGPT may be used to craft more convincing campaigns, but collaboration between the telecommunications and financial services sectors will also grow to address the problem. Increased impersonation of known individuals – such as senior banking executives – is likely to continue and may be amplified by deepfake technology and new-generation AI bots.

While employee education and vigilance will continue to be a primary defense against social engineering threats, technical controls like MFA enhancements, email security tools, and network segmentation can support non-technical defenses.

The increased involvement of hacktivists related to geopolitical tensions, with easy access to malware-as-a-service, will cause a further fragmentation in the threat landscape. The use of mis-, dis- and mal-information – potentially leveraging generative text engines to spread – will continue to sow uncertainty, both politically and in the perceived impact of hacktivist campaigns. This is likely to increase the cyber and/or reputational risk to financial sector firms operating in (or affiliated with) the nations engaged in conflict, which is likely to trigger decisions to reduce or withdraw operations in those locations (often irrespective of formal sanctions).

▶ Driver

Artificial Intelligence

ChatGPT is a generative-text chatbot system that performs a variety of tasks from simple to complex using human language interface. The simplicity of the tool's interface, and the level of success it already seems to be achieving in creating convincing, working texts from simple prompts, promise a multitude of potential uses by virtually anyone.

▶ Impact

AI-enabled attack tactics: since its release to the public by OpenAI in November 2022, ChatGPT has successfully responded to prompts to generate malicious code and to design convincing phishing lures. More broadly, generative language models have already been used to create infostealer malware, encryption tools, and dark web marketplace automations for illegal goods such as stolen bank accounts or payment cards along with drugs and ammunition.

AI-enabled defenses: positive applications include the automation of detection rules and lifting intelligence capability. The current threat from generative language models is limited by their current capability and modulated by their operators monitoring for policy violations; however, neither of these factors can be relied on as a long-term mitigation as the tools become smarter and their code more widely available.

The increasing number of vulnerabilities and the growing speed with which these are exploited – coupled with cyber staff shortages and increased regulatory focus on vulnerability and patch management -- may drive organizations toward an increased investment in automated approaches to patching and prioritizing vulnerabilities, both new and aged. Despite this, automated patching will likely only be good for handling non-critical cases in low complexity architectural environments. Automation will not replace the judgment and expertise of trained professionals for the foreseeable future.

▶ Driver

Cryptocurrency

Although the value of most cryptocurrency has not rebounded significantly since its decline in the past year, the TTPs surrounding cryptocurrency cybercrime continue to evolve. Profiting from fraud schemes and ransomware payments is more likely to result in the engagement of law enforcement. This gives cyber criminals more reason to target crypto infrastructure and assets further in the years ahead.

▶ Impact

Cryptojacking will continue. Requiring no infrastructure or fuel of their own, cyber criminals and sanctioned nation-state actors such as North Korea will continue to leverage unauthorized cryptomining on networks via vulnerabilities and malware to turn a profit.

Crypto will become more integrated into financial infrastructure. In January 2023, the US Office of Science and Technology Policy (OSTP) issued a request for information on research and development subjects surrounding digital assets and the surrounding technology. This feedback is likely going to help drive the integration of cryptocurrency and digital assets into global financial infrastructure. As such, it is pertinent to understand the threat landscape and take a defense-in-depth approach to all related integrations both internally and as extended to users.

2023 will undoubtedly see an increase in the adoption of central bank digital currencies. Given the variation models that are being adopted - retail, wholesale and hybrid - this is likely to generate a complex regulatory environment for multinational firms. The financial sector will need to invest in careful navigation of these complexities and understand the cybersecurity implications of different approaches.

CONCLUSION

As the effects from all of these change drivers converge, interact, and overlap, they will bring massive changes in the operating environment of financial services firms. Three key areas firms need to consider are increased regulation, the future of cyber insurance, and the ongoing cybersecurity talent shortage.

Increased regulation will impose new challenges for multinational firms. Multiple large scale cyber incidents in 2021-2022 will serve as the catalyst for change, in particular the management of data and information holdings to reduce risk in the event of exfiltration. For example, regulators may require public and/or private sector firms to establish data destruction programs or to provide departing customers with the option of having their records deleted. The potential to introduce legislation to explicitly make ransom payments illegal is currently under discussion in some nations (e.g. Australia). Similar to the adoption of CBDCs, regulation is likely to continue to fragment, making the already challenging global environment even more complex to navigate.

Cyber insurance will undergo an identity crisis. Following substantial year-on-year premium increases coupled with more and more exclusions and growing requests to establish minimum security standards and practices (e.g. the engagement of specialist ransom negotiators on retainer), some financial sector firms are beginning to reconsider cyber insurance. In some cases, premiums rise so high that firms are considering ring-fencing capital equivalent to the estimated premiums as an alternative to purchasing insurance coverage altogether. Although unclear in what direction the field of cyber insurance will evolve as it matures, drastic changes seem likely. As cyber regulation increases, regulators may contemplate alternatives to cyber insurance for individual firms to ensure the continued security of the financial sector and other elements of critical infrastructure.

Cybersecurity staffing will continue to be challenging. The field of cybersecurity is notorious for rapidly growing on one hand, yet never seemingly having sufficiently trained professionals to staff more senior positions. There is a constant tension between growing cybersecurity requirements and the allocated resources. Staff shortages and pressure to reduce operating costs are both drivers to adopt new technologies to provide effective security in the context of increased demands and reduced resourcing; however, ironically, technology and automation are likely to replace the lower tier of cybersecurity professionals, exacerbating the problem of growing senior staff and leadership further.

Contact

fsisac.com
media@fsisac.com