Cyber Threats to the Financial Services Industry

QBE

Contents

Executive summary

- The threat of extortion-based attacks is unsurprisingly one of the top cyber threats to financial services.
- In 2023, financial services was the fourth-most targeted sector, with the United States being by far the most affected country, according to ransomware leak sites.
- The exploitation of vulnerabilities, especially before they are disclosed or soon afterwards, is a key threat to financial services. Ransomware actors have demonstrated the capability to quickly exploit critical vulnerabilities in popular software used by organisations.
- Attacks in 2023 and 2024 against financial services businesses have often led to disruption for the wider sector. Given the interconnectedness of the sector, supply chain attacks pose a very high threat.
- Phishing and credential harvesting remains a key access vector for all sectors, including financial services.

Introduction

This White Paper was produced by the QBE Cyber Threat Intelligence Team. It provides a snapshot of the current threat landscape, highlighting notable developments towards the end of 2023 and into 2024, and is intended to provide brokers and businesses insights into the types of threats faced by the financial services sector.

Ransomware and Extortion

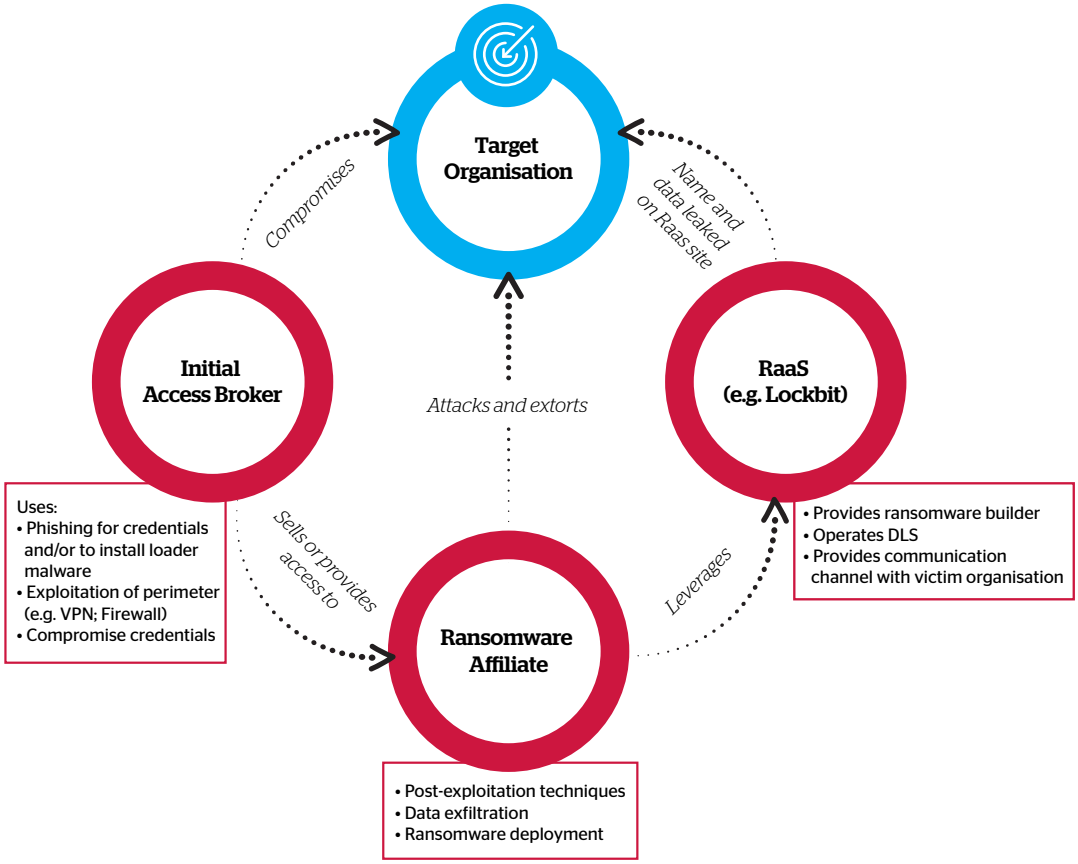
In terms of likelihood and potential impact, the threat from ransomware remains high to all organisations, including those operating in financial services. More broadly, extortion (i.e. the use of ransomware and/or the threat of leaking stolen data) is the go-to tactic for financially motivated threat actors.

The criminal ecosystem has developed in such a way that there is a myriad of methods that threat actors can gain access to corporate networks, from the exploitation of vulnerabilities and phishing, through to the purchasing of credentials and remote access on dark web forums. The sophistication of some prominent threat groups means they are capable enough to leverage this access, pivot around the network, steal data, and deploy enterprise-wide ransomware.

Despite increased investment in security tools and awareness throughout the financial services industry, the sector is by no means immune to this threat. More advanced threat actors are able to adapt to the environment they are in and evade detection using a variety of malware and techniques.

Much of the ransomware landscape is dominated by ransomware-as-a-service (RaaS), which is reflected in the interplay between three key elements:

- Initial access brokers
- Affiliates
- RaaS operators[1]



Ransomware in Financial Services

Key Facts:

- In 2023, Financial Services was the fourth-most targeted sector, behind business services (first), retail (second), and manufacturing (third). There were 346 instances of FSI organisations listed as victims in 2023.[2]

By ransomware:

1. CLOP – 96
2. Lockbit – 66
3. Black Basta – 61
4. ALPHV – 38
5. INC Blog – 20

By geography:

1. North America – 219
2. Asia – 50
3. European Union – 42
4. Europe – 22
5. Caribbean – 16

- A report by Mandiant published in June 2024 noted that the top initial access vector in ransomware attacks (based on their investigations) was the use of exploits.[3]

Notable Cyber Incidents in the Financial Services Sector[4]

February 2023

ION, a financial trading services group based in Dublin, Ireland suffered a ransomware attack by Lockbit. It impacted the firm's cleared derivatives platform, affecting multiple customers including banks, brokerages and hedge funds in the US and the EU. These firms were unable to process their transactions and had to find alternative means to do business. ION reportedly paid Lockbit to get their systems back online.

March 2023

Latitude Financial, an Australian firm that provides loans, credit cards and insurance suffered an extortion attack by an undisclosed group. The personal and medical information of 7.9 million customers in Australia and New Zealand was reportedly compromised. Latitude believe that the attackers used the account of a third party who had privileged access into their network. Latitude did not pay the ransom.

May-July 2023

Roughly 100 (actual number likely to be much higher) companies in the broader financial services sector worldwide were impacted by the mass exploitation of the MOVEit file transfer application by the **Clop** extortion group. One of the many victims was Fiserv, a global payments processing provider. They were forced to notify their customers, including Flagstar who had 830,000 customers impacted.

November 2023

In November, it became apparent that threat actors were actively exploiting a severe vulnerability in Citrix Netscaler software, known as **Citrix Bleed**. The same month, several major organisations, including those in the financial services sector were seemingly compromised by ransomware actors. Whilst few organisations admitted it (Boeing did), researchers noted that many firms that had suffered ransomware attacks had apparently failed to patch this vulnerability, meaning it was possible that Citrix Bleed was used. Breached FSI firms in November 2023 included:

- **Industrial and Commercial Bank of China (ICBC)**: The US subsidiary of the "world's largest bank" confirmed they suffered a ransomware attack at the hands of Lockbit. ICBC could not access their systems, forcing the bank to inject capital into its US Division to settle trades and repay debts.
- **TCW**: The Global Asset Management firm with $202 billion under management was compromised by Lockbit.
- **MeridianLink**: This US company provides software tools to the financial services industry. Affiliates of the ALPHV ransomware operation took to submitting the incident to the SEC in the US themselves to add pressure to MeridianLink to pay the ransom, something not previously seen from a ransomware actor.
- **Fidelity National Financial (FNF)**: Was attacked by ALPHV, and later admitted that 1.3 million customer records were compromised. The attack caused major disruption for customers trying to manage their loans and mortgages.

December 2024

Equilend, a securities lending platform admitted to a ransomware attack that reportedly led to 14 days of disruption where clients could not use their trading platform, which is used by a large portion of the market. The attack meant that banks could not properly allocate capital against trades, increasing the cost. It also forced users to adopt manual trading. Whilst Equilend did not confirm who was behind the attack, the Lockbit crew claimed responsibility.

Intrusion Vectors: How are threat actors getting in?

Direct Exploitation

One of the primary ways attackers breach organisations is through the exploitation of external-facing infrastructure.

In 2023, security teams grappled with a series of critical vulnerabilities that were enabling threat actors to breach networks. What made the attack campaigns so serious was that the vulnerabilities were leveraged either before they were known to the vendor (so there was no patch or mitigation) or exploited shortly after disclosure, meaning that organisations didn't have enough time to roll out fixes. These vulnerabilities are referred to as 'zero-day' vulnerabilities.

Exploitation of zero-day vulnerabilities like MOVEit and Citrix Bleed led to spikes in numbers of victims, catching many large organisations off guard, as there was no knowledge of how the exploitation was being carried out and no patches available.

Ultimately, the time available to organisations to patch after the disclosure of a vulnerability has become shorter.

Once, the difficulty of developing zero-day attacks meant that they were generally exclusive to advanced nation-state actors. Now, they are available to more threat actors due to the growing technical proficiency of organised crime groups, as well as the availability of zero-day vulnerabilities, and this means it's likely the intrusion trend will continue.

It is almost inevitable that zero-days and other high impact vulnerabilities will continue to be discovered and leveraged by dangerous actors such as ransomware operators. The most prominent of these, based on the trends observed in 2023, will be in 'edge' systems such as VPN services, email exchange servers, firewalls, file transfer applications, etc.[5] It is therefore important that organisations ensure they are closely monitoring these types of systems for unusual activity; they are hardened with appropriate endpoint controls, MFA, and are segmented as much as possible to prevent an actor from easily pivoting into other parts of the network. It is also imperative that organisations have processes in place to monitor vulnerability and intelligence sources to detect and react to high severity vulnerabilities and zero-days.

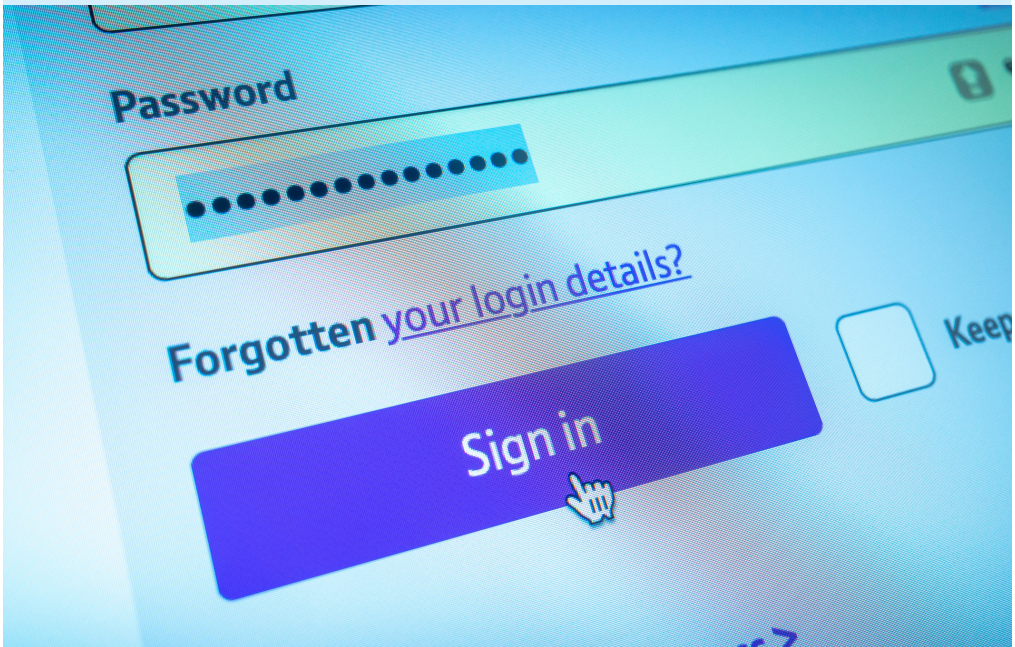
Malware Delivery through Phishing

While threat actors continue to rely heavily on phishing for initial access, they must consistently adapt to overcome new security controls. As such, there is not one consistent malware delivery format.

There is a "follow-the-leader" approach, meaning when one prominent actor adopts a successful technique, many others will likely start adopting that same technique. For example, after a surge in a new delivery format, such as OneNote in early 2023, endpoint detection engines were initially caught off guard.[6]

A recent report by Egress provides insights into the state of phishing in 2024:[7]

- Finance, alongside legal and healthcare sectors, are the most targeted.
- Finance, accounting, HR, and marketing are the most targeted teams within businesses.
- DocuSign and Microsoft are the most abused brands in phishing emails.
- The use of HTML attachments has seen the biggest increase in adoption by threat actors.
- PDF and Word attachments have also seen an increase. These types of documents now typically contain links to malicious sites.
- There has been an increase in the use of file sharing sites to host malware. These sites include DropBox, Google Drive, and attacker-controlled SharePoint sites.
- Using multi-channel attacks are more likely to lead to success for threat actors. These are when an attacker uses two or more different means to approach a target, for example sending an email and following up on Teams or with a phone call.
- Artificial Intelligence is likely to be adopted extensively in the near future for target reconnaissance and the creation of more convincing phishing lures and at scale.



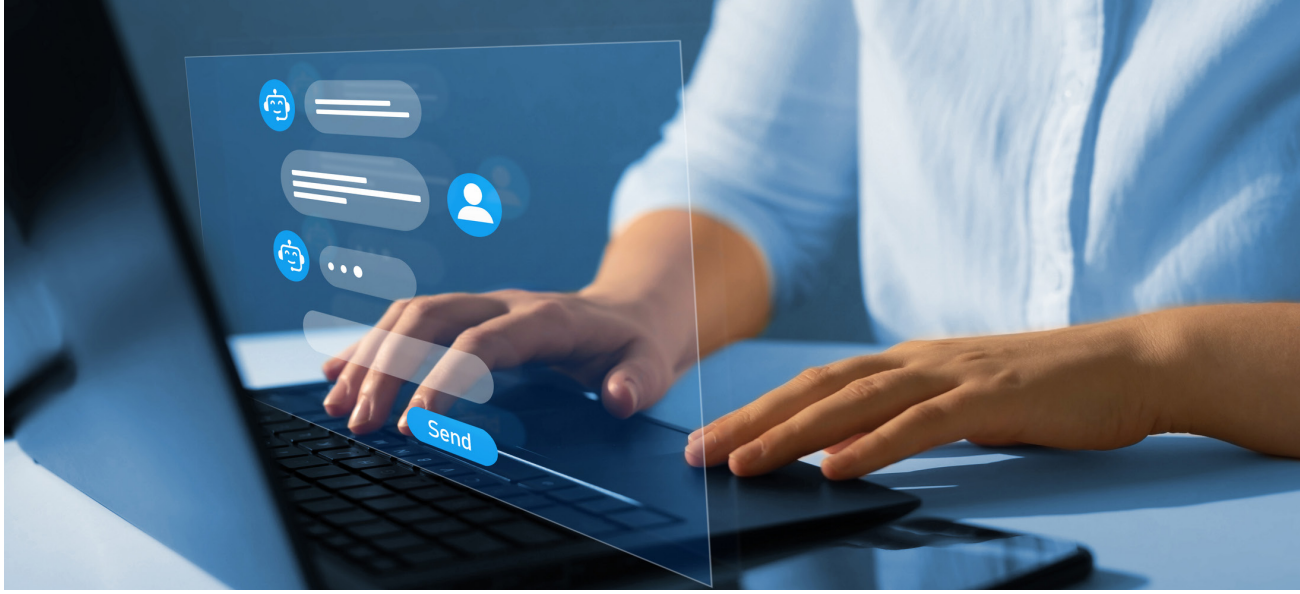
Credential Harvesting

The theft and use of credentials to gain initial access to networks is common and continues to be a highly effective technique.

How are threat actors getting access to credentials?			
Stealer malware	**Password guessing**	**Credential harvesting pages**	**Forums and marketplaces**
A PC is infected with malware with the primary goal of **harvesting credentials**. The malware picks up credentials as they are entered into a log-in page, then sends them to the attacker's server. **"Stealer logs,"** which are vast sets of credentials stolen by malware, are often sold on dark web marketplaces (see far right column).	The process of forcing access into an account by simply guessing the user's password is done through **brute-forcing:** attempting multiple different passwords against the same account, or **password spraying:** attempting a lower number of password guesses against a wider range of accounts.	Threat actors use **phishing emails** and other forms of social engineering to direct users to a **malicious website** that steals credentials by tricking users into entering them. Often these websites imitate Office365 login pages or other widely used tech platforms to trick users. Advanced **phishing kits** are available to automate attacks (e.g. EvilProxy).	Actors can advertise stolen credentials on dark web sites. These are often referred to as **initial access brokers** that have acquired valid credentials through some of the means mentioned previously. Threat actors buy the credentials and perform post-exploitation activities like the theft of data or ransomware deployment.

What about multi-factor authentication?

While multi-factor authentication (MFA) can protect against credential harvesting, threat actors have found success with bypass techniques. An example of this is MFA-fatigue attacks, where the user is pestered to accept MFA requests multiple times until they tap 'accept' on their mobile device. Phishing kits (mentioned above) can offer actors the ability to bypass MFA as well. This is often achieved through the use of a reverse proxy which relays the multi-factor code to the attackers in real time.[8]



Web compromise

Another way threat actors can drop malware onto victims' systems is through fake or compromised websites.

When a user visits the website they may be presented with a pop-up urging them to update their browser (for example, a prominent campaign doing this is the FakeUpdates/SocGholish operation).

Similarly, another technique (malvertising) that is being observed widely is the use of websites that imitate legitimate brands or applications to trick users into thinking they are downloading a legitimate program. Popular IT applications like VMware, AnyDesk, KeePass, Steam, etc., may be packaged alongside malicious files that kick-off the infection chain.[9]

To push fake websites to the top of search results, actors often employ **search engine optimisation (SEO) poisoning**, which tricks users into perceiving a malicious application as legitimate.

In the financial services sector, organisations should be on the lookout for fake websites that appear to offer tools, or software applications that are often used by employees of that organisation, which a bad actor may imitate to trick users into installing malware.

Supply Chain

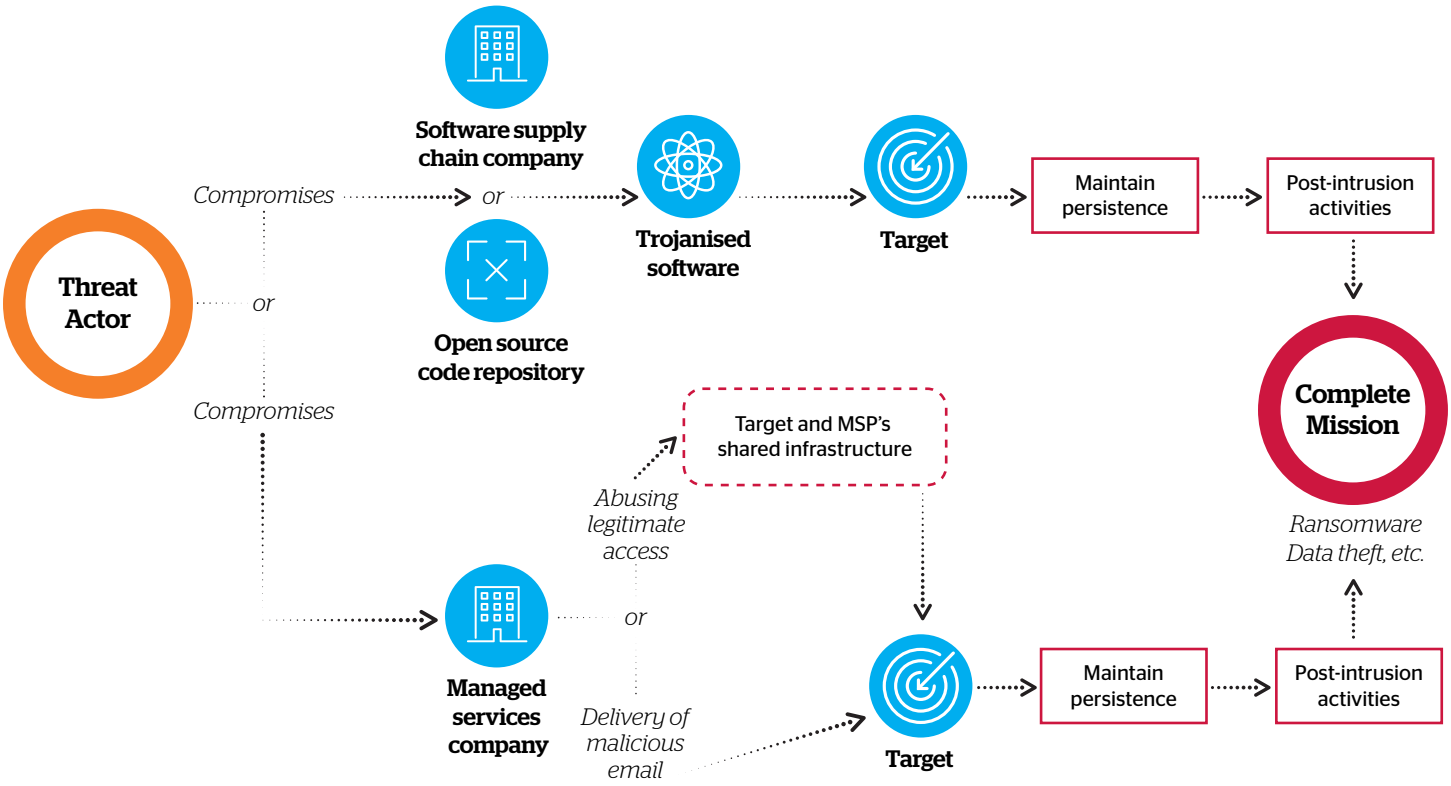
The supply chain represents a major threat for financial services organisations. There are several scenarios where a supply chain breach can lead to potentially catastrophic consequences.

- **Breach of data hosted by third party:** Perhaps the most common of scenarios, in which a third-party provider entrusted to manage an organisation's data is attacked by a threat actor. The perpetrator may demand payment of a ransom to unencrypt systems, or threaten to dump customer data unless a ransom is paid. (An example of this type of incident is outlined above in the Notable Incidents section in which Fiserv was required to notify Flagstar Bank that a breach by Clop exposed data of 800,000 of Flagstar's customers.)
- **Breach of managed service provider (MSP):** In this scenario, a threat actor compromises an MSP and leverages its trusted access to pivot into customer networks. A good example of this technique is the Cloud Hopper operation from 2016-2017, a well-known historical campaign.

Breach of software supply chain: In this scenario, a threat actor compromises a vendor that provides software to numerous organisations. The actor injects malicious code into the vendor's application and pushes it out into the networks of the vendor's customers, establishing a backdoor. Two examples of this are the SolarWinds campaign, carried out by Russian threat actors, and the 3CX campaign, carried out by North Korean threat actors.

- **Open-source software:** A threat actor places malicious code into open-source code repositories used by organisations in their own applications. In 2023, a report by security company Checkmarx was published about malicious code packages and was uploaded to NPM (a platform that hosts JavaScript packages to help with development), in which actors specifically targeted the banking sector. In one case, the actors attempted to use malicious code to act as a stager for a second-stage exploitation framework called Havoc. In another case, the actors developed malicious code to harvest log-in credentials through a bank's mobile application.[10]

High level view of potential supply chain attack scenarios



Geographic Hot Spots and Implications for Financial Services

North America

- USA is heavily targeted by ransomware.
- Some large FSIs targeted.
- High criminal intent to target US companies for 'big game hunting'.
- Likely some direction from Russian intelligence to target US financial sector.

South America

- South America is often associated with dangerous banking trojans that target individuals and their banking information.
- The are numerous banking trojans such as Casbaneiro, Guildma, Mekotio, and Grandoreiro, that are all developed to infect user's personal computers and mobile phones to facilitate banking fraud.
- A recent report on the Chavecloak trojan which targets Brazilian users is the most recent example.

Ukraine & Europe

- Financial services targeted by nation state actors and hacktivists in support of the war.
- Counter-attacks by Ukrainian intelligence services and pro-UA hackers on Russian FSIs.
- Potential large scale disruptive (wiper) attack by Russian APTs against Western financial infrastructure. Potential damaging spillover from cyber attack on Ukraine (akin to NotPetya).
- Pro-Russian DDoS attacks against multiple European and US FSIs (but generally low impact).

Middle East & Africa

- The financial sector in the MEA region was one the most targeted in 2023.
- The region is associated with rising instances of impersonation scams, creating social media and WhatsApp accounts to impersonate executives and attempt to steal data or money.

Asia and Australia

- Australia has dealt with the breaches of some major companies including financial and insurance companies.
- While the country has taken steps to improve the resilience of their critical sectors, threat actors are still likely to consider Australian and New Zealand companies as weaker targets compared to big firms in Europe or North America.
- The geopolitical tension relating to Chinese aspirations over Taiwan has driven a large amount of espionage attacks against Taiwanese, Asian and US organisations.
- Whilst financial services is less likely to be a focus area for Chinese threat actors compared to government or technology, for example, it nevertheless represents a critical sector that they are likely intent on gaining a foothold in.

Outlook

Despite the sector being associated with generally higher levels of security investment and maturity, financial services will likely remain a top target for financially motivated threat actors. As incidents in 2023 showed, some major organisations in the sector were exposed when critical vulnerabilities emerged. This situation is highly likely to continue into 2024 and beyond, given how successful criminal groups have been at weaponizing vulnerabilities.

The increasingly complex and interconnected nature of the sector means that when a key provider is breached, and threat actors use ransomware and/or steal data, the disruption may be extensive, as we saw in 2023–2024.

Being a critical sector, the possibility remains that the financial services sector will be targeted during times of heightened geopolitical tension and conflict. Russian actors continue to wield dangerous wiper malware against critical Ukrainian sectors, and there is potential for spillover into other industries and geographies.

The role of artificial intelligence and how it can bolster threat actor capabilities is still being assessed. However, intelligence agencies and firms like Microsoft have taken the position that while it can help to improve efficiency and effectiveness of tactics like social engineering, code development, and vulnerability research, AI has not yet been observed to provide threat actors with novel, more dangerous, or undetectable malware that cannot be countered. Nevertheless, financial services organisations should continue to monitor this area closely in case this situation changes.

[1] https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

[2] This data is based on victims listed on publicly available ransomware leak sites

[3] https://cloud.google.com/blog/topics/threat-intelligence/ransomware-attacks-surge-rely-on-public-legitimate-tools

[4] https://www.reuters.com/technology/ion-starts-bring-clients-back-online-after-ransomware-attack-source-2023-02-07/;

https://www.theguardian.com/technology/2023/apr/11/latitude-financial-vows-not-to-pay-ransom-to-hackers-in-wake-of-massive-data-breach

Clop victims based on open-source data leak site information;

https://www.reuters.com/technology/cybersecurity/icbc-paid-ransom-after-hack-that-disrupted-markets-cybercriminals-say-2023-11-13/;

https://twitter.com/FalconFeedsio/status/1729825029867684282;

https://therecord.media/meridianlink-confirms-cyberattack-after-sec-threat;

https://www.malwarebytes.com/blog/news/2024/01/fidelity-national-financial-acknowledges-data-breach-affecting-1-3-million-customers;

–

[5] https://www.sentinelone.com/resources/watchtower-end-of-year-report-2023/

[6] https://www.proofpoint.com/sites/default/files/misc/pfpt-us-threat-research-2023-05-12-cybercrime-experimentation.pdf

[7] Egress Phishing Threat Trends Report (April 2024)

[8] https://www.proofpoint.com/uk/blog/email-and-cloud-threats/tycoon-2fa-phishing-kit-mfa-bypass

[9] https://www.crowdstrike.com/cybersecurity-101/attack-types/seo-poisoning/

[10] https://checkmarx.com/blog/first-known-targeted-oss-supply-chain-attacks-against-the-banking-sector/