BRIGHTER

Financial services threat landscape report 2021

Illuminating insight from Countercept

WITH secure

Executive summary

Methodology

The objective of this report is to provide a summary of key themes and threats facing the financial services vertical. The report is based on interviews with experts in the vertical: threat intelligence and cyber security leads in EU banks, EU financial regulatory institutions, and global investment organizations.

WithSecure™ identified key themes and threats to the vertical based on these discussions and WithSecure's own first-hand knowledge working with the vertical through our managed services and consulting engagements. The report also draws on threat data from WithSecure's proprietary sources as well as Open Source reporting.

Key Judgements

- Supply chain was the highest priority theme concerning financial services organizations WithSecure™ interviewed. Nation-state threat actors such as NOBELIUM currently dominate this space, but a development of concern is the breakout of tradecraft to cybercriminal groups, as demonstrated by REvil ransomware group in the recent supply chain attacks against Kaseya. With the proliferation of tradecraft, **WithSecure™ assesses it is likely that some cybercriminal threat actors will have the capability and intent to conduct supply chain attacks in the future that could impact financial organizations.**

- Cloud was the second-highest priority theme for financial services organizations WithSecure™ interviewed. Organizations highlighted challenges faced in this space with diverse strategies for cloud adoption, lack of monitoring and detection capabilities, and skills shortages. **WithSecure™ assesses it is likely that cloud-offensive capabilities will grow among state-based groups and start to trickle down and proliferate among cyber criminal groups. The threat to cloud will not only stem from direct compromises to the cloud, but as an end objective that threat actors look to laterally move to from on-premise infrastructure, as was seen in the NOBELIUM compromises.**

- Financial services organizations are struggling to effectively manage vulnerabilities in their infrastructure among a backdrop of increased exploitation by both state-based and cybercriminal threat actors. Open Source and WithSecure's data suggests that the exploitation of vulnerabilities is a key intrusion vector in many high-impact intrusions, **and the adoption of effective asset management strategies will be important for the long-term resilience of financial services organizations.**

- Financial services technologies such as SWIFT, Open Banking and ATMs present an ongoing risk to financial organizations as offensive techniques deployed against these technologies evolve. Cryptocurrency-related attacks have increased and securing digital currency infrastructure is identified as an important trend as central banks increase their cryptocurrency holdings and roll out their own digital currencies. **Securing cryptocurrency technologies will be a prominent future trend in financial services security.**

- Ransomware was the number one threat for financial services organizations WithSecure™ interviewed. This was based on the perceived impact a ransomware attack could have on the resiliency of an organization, resulting in considerable financial, operational, and reputational damage.

Exploitation of vulnerabilities is a notable trend that used to be the exclusive remit of state-backed threat actors and is now more commonly employed by ransomware actors. **The risk of impact to financial services organizations from ransomware lies not only with direct attacks but also to those of their suppliers, who can suffer significant business disruption and downtime that negatively impacts the operations of financial services organizations**. Organizations should ensure they keep track of the evolutions in tradecraft from these groups and continue to focus efforts both on mitigating the intrusion vectors, as well as reducing the impact of any footholds gained on their networks by these groups.

- Financially motivated state-backed groups continue to conduct ATM cashouts, fraudulent abuse of compromised bank-operated SWIFT system endpoints, and cryptocurrency theft. **WithSecure™ assesses that it is likely the evolution of tradecraft towards cryptocurrency theft is likely to continue, particularly as banks' digital currency and cryptocurrency holdings grow. Chinese and Russian state-backed groups have demonstrated advanced capabilities to conduct supply chain attacks**. Both have the intent to target financial services regulatory bodies with the objective of gaining information of intelligence value. In addition, Chinese state-backed threat actors have further been seen targeting private sector financial services organizations with the intent of stealing data to further political and economic objectives.

Key themes:

Supply Chain

Recent high-profile supply chain incidents, such as SolarWinds and Kaseya, have increased public awareness of supply chain as an attack vector. Securing against this vector of attack was the top area of concern and strategic focus for almost all financial organizations WithSecure™ spoke to. One organization WithSecure™ spoke to has begun a project to classify not only their third-party suppliers but also their fourth-party suppliers. This work was focused towards understanding upstream concentrated dependencies of suppliers that may present high-impact risks to this organization. This picture would allow them to manage their risks through supplier selection that reduces these concentrated dependencies.

The European Union Agency for Cybersecurity (ENISA) recently published its research of 24 supply chain attacks conducted over the past 18 months. The report defined a new taxonomy for discussing supply chain attacks, breaking the subject into four key parts.

It was notable in discourse of the Kaseya attack that there was confusion over how to classify this supply chain attack. ENISA's taxonomy to define the different elements of a supply chain attack should help bring more clarity to these discussions and help organizations be more informed in developing their strategies to counter this threat. The ENISA report highlighted that most supply chain attacks took advantage of supplier trust, focused on suppliers' code to compromise customers, deployed malware, and were aimed at gaining access to data. While data loss is a major concern for all organizations, this picture is likely heavily influenced by the type of victim organizations.

A development of concern for supply chain attacks is the breakout of this tradecraft from an exclusively state-sponsored capability to also including cybercriminals. The Kaseya supply chain attack, where customers of MSSPs operating Kaseya VSA appliances were compromised, was attributed to the REvil threat actor[1] . REvil is a ransomware threat actor, and while the supply chain attack did not display the same degree of capability as other supply chain attacks – like the one conducted against SolarWinds customers – it did evidence a high degree of technological and operational capability. WithSecure™ assesses it is likely that some cybercriminal threat actors will have the capability and intent to conduct supply chain attacks in the future that could impact financial organizations.

The ENISA report attributed around half of the supply chain attacks it studied to APT state-sponsored activity. These groups have clearly shown their ability to conduct these attacks with a high degree of technical and operational capability. With their motivations usually being espionage-focused, the intent to target financial organizations is less concrete; however, reasonable assessment can be made that financial organizations could meet the targeting criteria of a number of these groups, as they are classified as Critical National Infrastructure (CNI). The recent SolarWinds incident did impact some state financial institutions, lending credence to this assessment and risks of future exploitation with any data gathered from these intrusions.

[1] https://www.huntress.com/blog/rapid-response-kaseya-vsa-mass-msp-ransomware-incident

WithSecure's insight

The events of the past 18 months have highlighted the need for organizations to review their approach to supply chain security.The common approach of compliance and due diligence questionnaires may provide some comfort for businesses' stakeholders but in reality do little to protect organizations from supply chain attacks. It is important that financial services organizations work to an assumed breach mentality of suppliers, where they consider the access of external suppliers to their environments and consider the impact of the compromise of these organizations. Developing controls to reduce the impact of these intrusions, combined with developing more open communication with suppliers on their security, will be important steps to ensure resilience against future supply chain attacks.

Cloud

There has been steady and growing adoption of cloud infrastructure across all financial organizations we interviewed, which placed cloud as second only to supply chain in priority as a key theme they are focused on securing. There are mixed views on long-term strategies for cloud usage, with some organizations, such as BNP Paribas, Citi and Standard Chartered, committing to using on-premise cloud solutions.[2] These banks have been reluctant to outsource to vendors because they worry about the risk of a security breach, risk being concentrated on one vendor, and the potential of regulatory crackdowns on where data is located. New legislation, such as the proposed Digital Operational Resilience Act[3] (DORA), provides some regulatory guidance for organizations, but also restrictions on potential cloud suppliers[4]. In contrast, other organizations are adopting use of multiple public cloud providers, such as HSBC, which has signed cloud usage agreements with Google, AWS and Microsoft over the past two years.[5] In addition, some newer fintech organizations have built their entire business model around cloud and operate entirely in the cloud without little to no on-premises infrastructure.

What was common across all organizations WithSecure™ spoke to, as well as in our consulting engagements, is the challenges organizations face in securing these new technologies. As the rate of cloud adoption increases, so does the amount of sensitive data being stored in cloud-based environments, and thus the need to secure it becomes ever more important. Many of the big-name cloud service providers have the telemetry and supporting functionality to allow for monitoring; however, financial services organizations are facing challenges due to lack of expertise in how to effectively make use of these to defend their environments.

This year saw the publication of several new cloud threats, with evolving tradecraft and malware being deployed against cloud environments. In WithSecure's discussions with financial services organizations, the techniques employed by NOBELIUM were of foremost concern. In its recent campaign, NOBELIUM successfully pivoted in to victim's cloud infrastructure by exploiting ADFS trusts, and forged new SAML tokens to move laterally and persist within victim networks.[6] These Golden SAML[7] attacks were new tradecraft and came as a surprise to most organizations that did not have detection in place for this type of threat activity.

The recent four OMIGOD vulnerabilities[8] in Microsoft's Open Management Infrastructure (OMI) framework revealed critical vulnerabilities that highlight the fact that this infrastructure is not infallible and, as with any technology, exploitation will occur. Threat actors are also developing new capabilities to exploit cloud services; for example, this year saw the discovery of the first ever 'cloud-native' malware, which was targeting Windows Containers dubbed as Siloscape.[9] The malware is designed to open a back door into poorly configured Kubernetes clusters to run malicious containers. With the right privileges, this would enable the theft of credentials, pivoting within a victim's cloud environment, and work towards a final objective, be that motivated by financial gain or espionage.

[2] https://www.digfingroup.com/hsbc-cloud/
[3] https://www.WithSecure™.com/gb-en/consulting/our-thinking/exploring-dora
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595
[5] https://www.digfingroup.com/hsbc-cloud/
[6] https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forg es-authentication-to-cloud-apps;
[6] https://us-cert.cisa.gov/ncas/alerts/aa21-008a
[7] https://www.sygnia.co/golden-saml-advisory
[8] https://msrc-blog.microsoft.com/2021/09/16/additional-guidance-regarding-omi-vulnerabilities-within-azure-vm-management-extensions/
[9] https://unit42.paloaltonetworks.com/siloscape/

WithSecure's insight

Almost all industry experts WithSecure™ interviewed raised ongoing concerns around securing cloud infrastructure in the next 12 months, particularly as cloud becomes the default for many organizations where it isn't already. As cloud usage grows, medium-to-large organizations with hundreds of workloads in the cloud will face challenges in securely scaling this activity. Similarly, securing Software-as-a-Service (SaaS) will increasingly become a bigger problem for most financial sector organizations, due to proliferation of different and more niche products, and a lack of good research and experience in securing them.

WithSecure™ therefore recommends that organizations seek expertise and advice on enforcing secure configuration at scale. For organizations developing in-house cloud detection, then cloud-specific threat simulation through purple teaming can form a valuable pursuit for organizations to develop detection capabilities and validate them. The collaborative nature of these engagements can also help to grow expertise in organizations to help bridge some of the skills gap shortages being experienced in the industry as a whole.

With the evolution of new capabilities in the cloud, WithSecure™ assesses it is likely that cloud-offensive capabilities will grow among state-based groups and start to trickle down and proliferate among cybercriminal groups. The threat to cloud will also not only stem from direct compromises to the cloud, but as an end objective that threat actors look to laterally move to from on-premise infrastructure, as was seen in the NOBELIUM compromises.

Vulnerabilities and Legacy Infrastructure

The risk of legacy software and applications was a strong theme for financial services organizations WithSecure™ interviewed, which were unable to move away from this infrastructure due to key operational dependencies. The financial services sector is relatively heavily regulated for cyber security standards and assurance practice, but it still faces considerable challenges with asset identification, as well as vulnerability management of often large, complex sprawling environments.

In July, US Cybersecurity and Infrastructure Security Agency (CISA), the Australian Cyber Security Centre (ACSC), the UK's National Cyber Security Centre (NCSC), and the US Federal Bureau of Investigation (FBI) published an advisory[10] on the top 30 vulnerabilities routinely exploited by threat actors in 2020 and 2021. The report highlighted how threat actors continue to target vulnerabilities in externally facing technologies. Among those highly exploited in 2021 are vulnerabilities in Microsoft (Exchange), Pulse Secure, Accellion, VMware, and Fortinet devices.

Public reporting of the exploitation of these vulnerabilities identifies a few financial services sector organizations being compromised by threat actors using these intrusion vectors. For example, an unpatched critical vulnerability in Pulse Secure VPN servers was likely the vector used in a 2020 REvil ransomware attack against the foreign exchange company Travelex in London.[11] The attack forced the company to shut down all operations across 30 countries.[12] DarkSide ransomware affiliates were seen exploiting SonicWall VPN vulnerability to hack targets in the US.[13] Phineas Fisher's Cayman Bank hack targeted a bank's network using a vulnerable SonicWall VPN appliance, demonstrating that VPN vulnerabilities still provide a route to compromise against financial services organizations.[14]

Also on the list of vulnerabilities identified by CISA was CVE-2017-11882, a 17-year-old memory corruption issue in Microsoft Office (including Office 365). WithSecure™ telemetry identifies this as one of the most actively exploited vulnerabilities on Windows endpoints over the past year. This vulnerability can be exploited during phishing campaigns and requires little interaction from the user. It has been historically used by financially focused threat actors such as the Cobalt Group.[15]

[10] https://us-cert.cisa.gov/ncas/alerts/aa21-209a

[11] https://portswigger.net/daily-swig/travelex-ransomware-attack-pulse-secure-vpn-flaw-implicated-in-security-incident

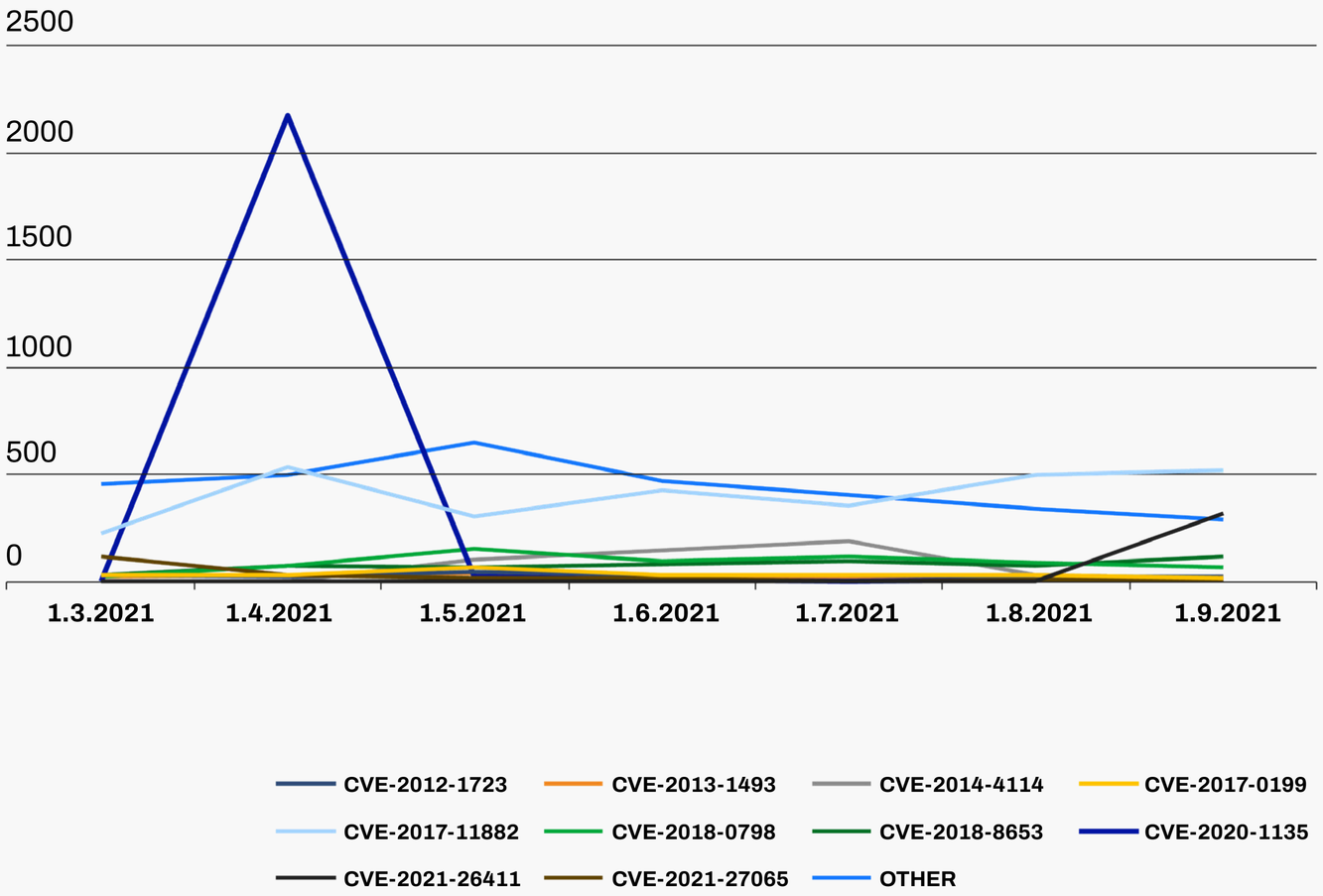
[12] https://www.bitdefender.com/blog/hotforsecurity/pulse-secure-vpn-server-exploit-opens-the-way-for-sodinokibi-ransomware-travelex-falls-victim

[13] https://www.securitynewspaper.com/2021/05/12/darkside-ransomware-affiliates-are-using-sophos-firewall-and-vpn-vulnerability-to-hack-researchers-track-down-5-affiliates-of-them

[14] https://github.com/Alekseyyy/phineas-philes/blob/master/cayman-english.md

[15] https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/17-year-old-ms-office-flaw-cve-2017-11882-actively-exploited-in-the-wild

Most commonly exploited vulnerabilities identified by WithSecure™ epp data between March and September 2021



WithSecure's insight:

The relevance of vulnerability exploitation is supported by the data from WithSecure's incident-response engagements, where the exploitation of externally facing vulnerabilities is a prevalent intrusion vector for all types of actors. In particular, WithSecure™ has observed a growth in adoption and speed to exploit vulnerabilities in ransomware intrusions over the past 12–18 months.

WithSecure™ recommends organizations conduct external attack surface testing to understand their exposure to breach, to identify and remove vulnerabilities. There are always going to be some parts of a perimeter that are more exposed than others: places where, for operational reasons, vulnerable assets cannot be taken out of the public domain, and attack surfaces cannot be reduced. Understanding where such vulnerabilities lie can help organizations map potential attack paths and prioritize their spending on detection and response. For example, WithSecure's External Attack Surface Management (EASM) team investigations have found that some organizations had far higher email credential exposure than might be expected. There aren't necessarily patches to help with this kind of information, but this information can be fed back into phishing awareness and security training, to help build a more resilient company culture in the future.

Financial Services Technologies

Financial services-specific technologies, such as SWIFT and Open Banking, were the last key theme from WithSecure's discussions with financial services organizations. Intrusions involving these technologies grab headlines due to their novelty and general public bank-robbing voyeurism. The level of capability required to conduct these attacks means they are predominately the purview of advanced groups with nation-state capability and resourcing. As will be discussed in the Nation-State section, DPRK groups have demonstrated the intent and capability to exploit SWIFT infrastructure and deploy networks of criminals to launder money that is funneled back to the DPRK regime.[16]

SWIFT

SWIFT is a financial telecommunications infrastructure that links banks' networks together to facilitate messaging and the global transfer of funds between banks. The targeting of SWIFT dates back to at least 2013, when threat actors used it to process fraudulent bank transfers.[17] Perhaps the highest profile case was the 2016 attack on the Bank of Bangladesh by a DPRK threat actor that resulted in the theft of US$150 million. Following the 2016 attack, there was a cluster of threat actor activity targeting the SWIFT infrastructure of banks in Russia, Ukraine and Vietnam.

After the Customer Security Controls Framework (CSCF) was implemented by SWIFT banks, they segmented their operational networks with SWIFT infrastructure and adopted 'secure zones' with security controls and real-time monitoring. These measures have limited the opportunity for threat actors to laterally move from other exposed elements of a banks' networks to target the SWIFT system and have helped reduce the frequency of attacks. It is WithSecure's view that the impact of lockdown measures during the global pandemic are likely to have further disrupted threat actors' ability to mobilize logistical resources that are required to 'cashout' proceeds from fraudulent SWIFT transactions. As will be discussed in the Nation-State section of this report, another contributor to the drop in frequency of attacks has been the shift of focus by Lazarus, the threat actor most attributed to targeting SWIFT, to cryptocurrency infrastructure-focused attacks.

Open Banking

Open Banking is a standard aimed to help organizations meet the Second Payment Services Directive (PSD2)[18], to enable the access of data held by banks by other financial organizations. There is little public discourse about the exploitation of Open Banking in the wild. However, there is wider adoption of this infrastructure with the growth of online banking and banks that are now operating fully online. Open Banking is very reliant on APIs to operate, and there is more public evidence[19] of the exploitation of APIs across many technologies with their increasing proliferation.

WithSecure's consultants have conducted threat-modeling exercises with financial services organizations based on Open Banking infrastructure, which concluded that exploitation would require significant technical expertise or insider knowledge. WithSecure™ assesses that it is likely opportunistic exploitation could rise as Open Banking is adopted by a wider circle of organizations, many not subject to as stringent cyber security regulation or standards. Transaction data is valuable

[16] https://us-cert.cisa.gov/northkorea
[17] https://www.WithSecure™.com/content/dam/WithSecure™/en/business/common/collaterals/WithSecure™-threat-analysis-swift.pdf
[18] https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en
[19] https://salt.security/api-security-trends

information revealing pattern of life information and financial standing that can be exploited by a highly capable threat actor. However, WithSecure™ assesses there is a reasonable possibility that exploitation that seriously impacts financial services organizations will not proliferate unless a profitable monetization method is found for data gained through Open Banking exploitation.

ATMs

ATM attacks present an ongoing operational risk and cost for banks; however, in the interviews conducted by WithSecure™ those organizations did not see this as a growing area of concern or major cost compared with other risks. In reporting earlier in 2021, the EU EAST Expert Group on ATM and ATS Physical Attacks (EGAP) noted that the number of physical ATM attacks had fallen 19% since the start of the pandemic, even if the overall costs associated with the attacks remained constant. In contrast, ATM logical and malware attacks have risen 44% in frequency and 14% in total costs for the same period.[20] The report did note that most of such attacks were unsuccessful despite this rise.

It is clear that some ATM models are still vulnerable to compromise, and as new technologies and malware are developed, criminal groups will continue to find novel ways to exploit the evolving attack surface.[21] WithSecure's incident-response team has observed the use of simple ATM malware such as Alice[22] on ATMs in Europe in 2021. ATM 'jackpotting' can raise significant income for threat actors, with two individuals arrested this year, having stolen at least €230,000 in attacks targeting one brand of ATM across at least seven countries in Europe.[23] These losses for banks are, however, not a huge impact and remain limited by the physical amount of currency contained within these devices, a limitation for example not in place for SWIFT or ransomware attacks.

More capable threat actors, such as nation-state groups operating in the interests of the DPRK, have successfully conducted ATM heists that deployed 10 different malware samples in the FASTCash cyber attacks that compromised ATM machines and SWITCH application servers to facilitate fraudulent transactions and cashouts. The Cybersecurity and Infrastructure Security Agency (CISA) stated that "since February 2020, North Korea has resumed targeting banks in multiple countries to initiate fraudulent international money transfers and ATM cashouts. The recent resurgence follows a lull in bank targeting since late 2019."[24] These attacks are notably more complex than standard ATM jackpotting attacks and involve the compromise of wider banking infrastructure before monetization through ATM terminals. Figure 2 that follows is an example overview of a DPRK-backed attack reported in 2020.

[20] https://www.association-secure-transactions.eu/tag/atm-physical-attacks/
[21] https://www.finextra.com/newsarticle/36242/diebold-nixdorf-warns-banks-of-compromised-atms
[22] https://www.trendmicro.com/en_us/research/16/l/alice-lightweight-compact-no-nonsense-atm-malware.html
[23] https://www.europol.europa.eu/newsroom/news/russian-speaking-hackers-arrested-in-poland-over-atm-jackpotting-attacks
[24] https://us-cert.cisa.gov/ncas/alerts/aa20-239a

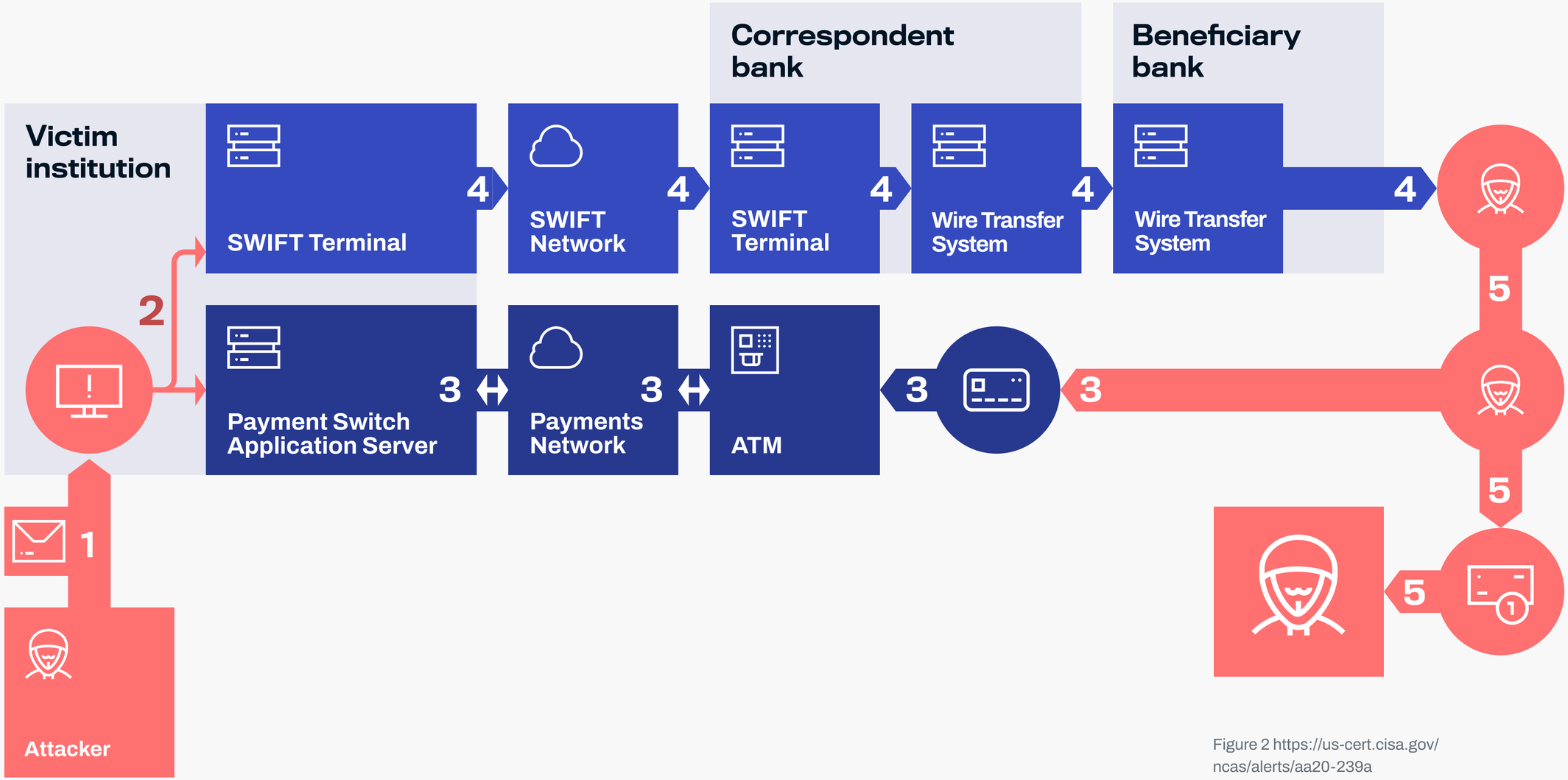


Figure 2 https://us-cert.cisa.gov/ncas/alerts/aa20-239a

WithSecure's insight:

A growing trend moving forwards will be more banks holding cryptocurrency assets as central banks in countries and regions including the US, UK, China and EU have announced proposals for their own Central Bank Digital Currency (CBDC). Therefore, securing CBDC platforms will be a prominent trend in financial services technologies. User interaction will be conducted via mobile applications, which will likely be at risk from the threat of criminal organizations to state-backed threat actors. The threat actors targeting CBDC platforms will likely be financially motivated actors, such as DPRK state-based groups or cybercriminals who commonly conduct fraud attacks through capabilities deployed against existing banking apps such as click bots, mobile malware, credential stuffing, overlay attacks and banking trojans.[25] In addition, money-laundering and other fraud-related activities are likely to attract threat actors who already are literate in cryptocurrencies and see them as an appealing form of currency to operate with.

[25] https://www.finextra.com/blogposting/20408/a-central-bank-digital-currency-challenges-and-opportunities26

Key threats:

Cybercrime

All interviewees have witnessed a significant rise in cybercrime activity, ranging from phishing, the continued evolution of initial access brokers and the associated threat of ransomware, which proves an ongoing major concern for the financial organizations we spoke to. The technical capability of some cybercrime groups has also grown in sophistication: one respondent noted that in the past 12 months, a criminal group had successfully bypassed MFA, enabling them to compromise consumer banking apps.

Ransomware

Ransomware was consistently highlighted as the highest priority threat across WithSecure's discussions with financial services organizations. This was based on the perceived impact a ransomware attack could have on the resiliency of an organization, resulting in considerable financial, operational, and reputational damage. This view is supported by recent statistics published by Sophos, which show that 34% of financial services organizations were hit by ransomware in the last year; 51% of those hit said the cybercriminals succeeded in encrypting their data.[26] Furthermore, in instances where financial organizations paid the ransom, on average, a third of data was still unrecoverable, according to the research.

The risk of impact to financial services organizations from ransomware lies not only with direct attacks but also to those of their suppliers, who can suffer significant business disruption and downtime that negatively impacts the operations of financial services organizations. Supply chain risks from ransomware are therefore not only direct but also indirect risks from the impact to an organization's suppliers.

The threat actors and the ecosystem enabling ransomware attacks have evolved in scale and capability over the past two years, with increasing specialization and capability among the top threat actors. Operational and monetization models, such as data-related extortion, have also evolved to continue to increase the costs of ransomware for organizations. Sophos's research suggested that the average cost of a ransomware incident for a financial services organization was US$2.1 million – a significant impact for any organization.

[26] https://www.finextra.com/blogposting/20408/a-central-bank-digital-currency-challenges-and-opportunities26

WithSecure™ research suggests ransomware attacks leverage three principal intrusion vectors

- Phishing: attackers typically seek to install ransomware malware directly, or in cases where clients have more effective filtering in place, harvest credentials through phishing to gain access to a target's machine.

- Exposed RDP servers: attackers often try to brute force their way in or make use of leaked credentials.

- Exploitation of vulnerable software: ransomware attacks can often start with exploitation of externally facing vulnerable software such as firewall or VPN appliances.

The rise in exploitation of vulnerabilities is a notable trend, as this was tradecraft that used to be the exclusive remit of state-backed threat actors, and has instead become more commonly employed by ransomware actors. As discussed in the Vulnerabilities section earlier, ransomware actors27 impacting financial services have been seen exploiting vulnerabilities in SonicWall and Pulse Secure VPN devices. WithSecure™ can corroborate this from incident-response engagements, both for financial services organizations and organizations in other verticals.

What traditionally were banking trojans, such as TrickBot, have evolved to become enablers of ransomware and a shifting focus to monetization through these means instead of their traditional banking roots. This evolution is not a seismic shift but highlights the profitability of ransomware. Financial services organizations should ensure their response activities are updated appropriately to account for this shift in the threat posed by these malware families.

[27] https://www.WithSecure™.com/content/dam/WithSecure™/en/business/g/WithSecure™-threat-highlights-report-2021-08.pdf

WithSecure's insight:

Ransomware

The impact of ransomware will continue to pose a predominant threat to financial services organizations moving into the next 12 months. Organizations should ensure they keep track of the evolutions in tradecraft from these groups and continue to focus efforts on both mitigating the intrusion vectors, as well as reducing the impact of any footholds gained on their networks by these groups. The reality is, it is likely they will gain a foothold at some point, but the cost of this can be reduced to a few hours of work if detection and response capabilities are adequately employed.

Ransomware actors focus their efforts on the easiest targets of opportunity who are most likely to pay the ransom. This means, as noted above, the risk of ransomware for financial services organizations extends to supply chain risk if third-party suppliers are the victims of an attack. These organizations are likely to invest less in cyber security controls than financial services organizations but can still have a big impact on their operational resilience. Management of this supply chain risk, adopting an assumed compromise mindset for suppliers, will prove valuable if brought into wider procurement and business decision-making processes.

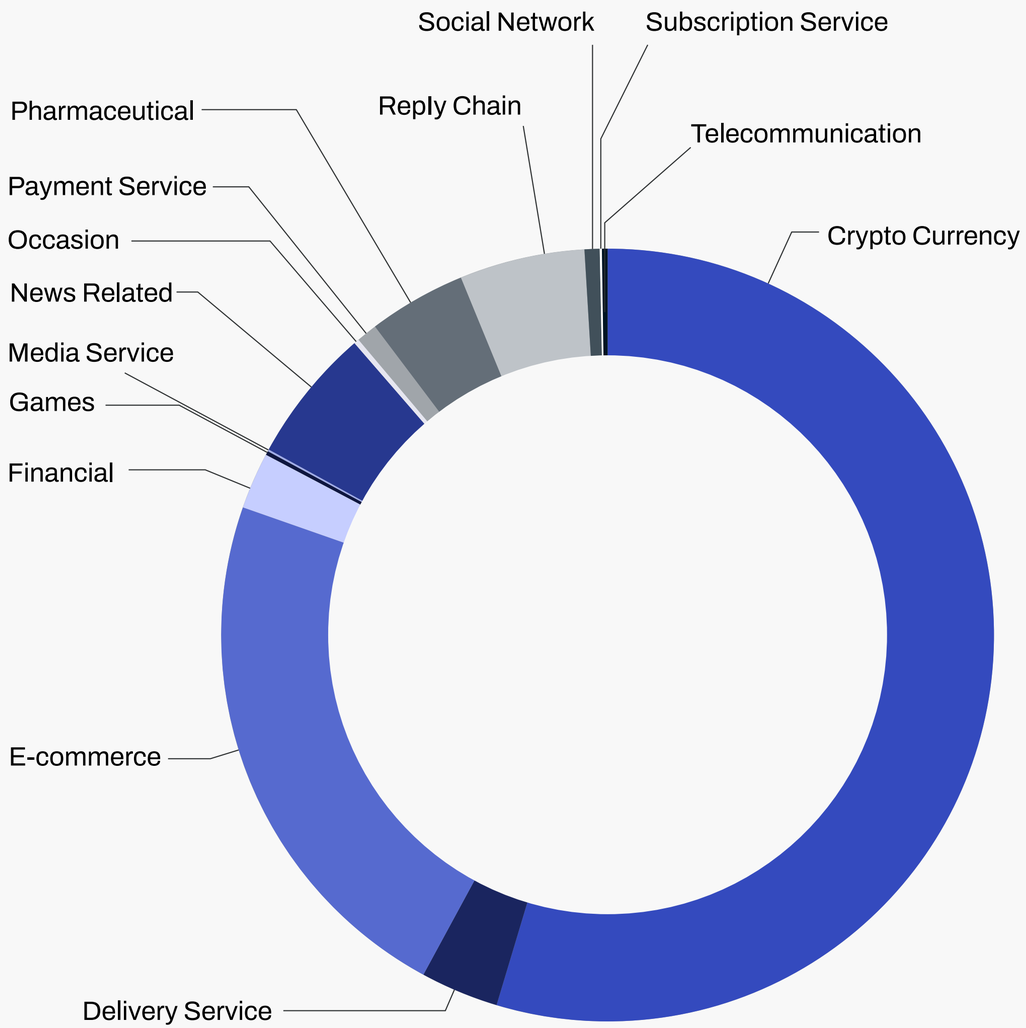
Phishing

Last year (2020), WithSecure™ saw evidence in incident-response cases of advanced phishing campaigns targeting financial services organizations using compromised accounts belonging to the client of the target organization. CEO fraud or 'whale phishing' was only raised as a concern by one organization WithSecure™ spoke to, which claimed this was an ongoing threat but had seen no escalation in the past 12 months.

Most organizations WithSecure™ spoke to, however, assess the level of sophistication of phishing emails they had seen was low, not highly targeted, and matched general trends of phishing in terms of theme, such as Covid-related content. This is in line with WithSecure™ data that shows most phishing campaigns witnessed were standard phishing campaigns, delivering a range of adware, malware, and credential harvesting.

One government cyber security body in Europe noted a huge increase in cyber-enabled crime focused against consumers – in particular, smishing has "gone through the roof since October 2020…it dominates what we are doing". Further, they had observed a very organized campaign, where one financial organization would be exclusively targeted one week and then the campaign would target another financial organization the following week. Prior to more coordinated collaboration and information-sharing between local private sector and government organizations, the connection between attacks and prevalence of the threat from coordinated phishing campaigns would not have been identified, limiting the opportunity to prevent and respond to the threat. This highlights the value in collaboration and information-sharing between financial organizations.

Most common spam themes identified by WithSecure™ epp data



Nation-State

Nation-state threat actors were deemed a lesser risk than ransomware actors in WithSecure's discussions with financial services organizations. When asked to support this judgement, organizations said that, financially motivated DPRK groups aside, they were likely to only be a tertiary target for nation-state actors. In this situation, the threat actor would be seeking onward further access to reach financial regulatory bodies or government institutions with access to data of intelligence value, and the impact for the financial services organization would be lower than in a ransomware attack.

DPRK

DPRK state-backed groups have traditionally been the most prominent groups targeting financial services. The UN security council has historically reported on the DPRK's cyber capabilities that have been directed "to steal funds from financial institutions and cryptocurrency exchanges"[28] to finance the regime's military and nuclear programs. These priorities remain for the DPRK regime and provide a constant motivation for conducting financially motivated cyber attacks.

Since 2015, Lazarus (APT38) group has been responsible for the FASTCash ATM cashouts, as well as fraudulent abuse of compromised bank-operated SWIFT system endpoints. According to CISA, BeagleBoyz, a group that has overlaps with Lazarus, has attempted to steal nearly US$2 billion since at least 2015: "They have manipulated and rendered inoperable critical computer systems at banks and other financial institutions."[29]

However, in the past two years, these groups have shifted their focus to conduct lucrative cryptocurrency theft. Another CISA alert highlights Lazarus group's employment of malware masquerading as cryptocurrency trading platforms in in more than 30 countries in the past year. WithSecure's own reporting[31] identified a long-running Lazarus group campaign targeting cryptocurrency organizations for financial gain in 2020. ClearSky researchers identified further activity from this group focused on theft from cryptocurrency wallets that they estimate may have resulted in the theft of hundreds of millions of dollars.[32]

DPRK-backed threat groups have clear intent and capability to conduct attacks against financial services organizations, causing reputational damage, financial loss and recovery costs. WithSecure™ assesses that it is likely the evolution of tradecraft towards cryptocurrency theft is likely to continue, particularly as banks' digital currency and cryptocurrency holdings grow. The impact of successful attacks from these threat groups is considerable, and financial organizations would be wise to track the activities of these groups and develop controls to counter these threats.

[28] https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf
[29] https://us-cert.cisa.gov/ncas/alerts/aa20-239a
[30] https://us-cert.cisa.gov/ncas/alerts/aa21-048a
[31] https://labs.WithSecure™.com/assets/BlogFiles/WithSecure™LABS-tlp-white-lazarus-threat-intel-report2.pdf
[32] https://www.clearskysec.com/cryptocore-lazarus-attribution/

Russia

Russian-backed threats relating to, and following on from, the SolarWinds intrusion[33] have been prominent in many discussions in 2021. These intrusions have brought into focus the risk of supply chain compromises and the high level of capability that Russian groups can employ. These intrusions have resulted in some impact for financial services organizations, with victims including central banking institutions. However, the intent to directly compromise private sector financial services organizations appears less clear.

In WithSecure's discussions with financial services organizations, the consensus was that the capability of NOBELIUM to exploit cloud and supply chain vectors outweighed the low-level confidence of intent; therefore, a threat to take note of and invest in countering it. This judgement was also influenced by an expected trickle down of tradecraft into other groups that may have more direct intent to target financial services organizations. Some evidence of attempted emulation could arguably be made in the Kaseya REvil attack that involved a supply chain element earlier this year.

Russian-based threats continue to display high degrees of capability to conduct targeted intrusions with a focus on cloud infrastructure.[34] The compromise of state financial organizations does pose future risk to private financial services organizations that information gained during these intrusions could be weaponized against them. These groups have not displayed a clear intent to target private sector financial services organizations, but WithSecure's assessment is that there is a reasonable probability in the future that geopolitical dynamics could bring financial services into the targeting scope of these groups due to its role as CNI. Financial services organizations should be aware of these threats and novel tradecraft that may permeate into wider use by other threat groups; however, compared with threats from ransomware and DPRK-backed groups, these should be less of a priority.

[33] https://msrc-blog.microsoft.com/2020/12/21/december-21st-2020-solorigate-resource-center/

[34] https://us-cert.cisa.gov/ncas/alerts/aa21-116a

China

In WithSecure's discussions with financial services organizations, concerns were highlighted of the exploitation of zero-day vulnerabilities by Chinese state-backed groups. The HAFNIUM attacks that exploited zero-day vulnerabilities in Microsoft Exchange Server[35] and Pulse Secure VPN[36] attacks are the most recent demonstrations of that capability. In both instances, financial services organizations were reported to be directly impacted by this activity.

Chinese state-backed threat actors are exploiting supply chain as a vector of compromise in attacks that date back to at least as early as 2017, when Chinese state-backed threat actors compromised over 2.27 million users of Avast, planting a malicious update. A small subset of those victims was infected with a second stage trojan, likely for espionage.[37] Recent reporting has also highlighted the extent of Chinese state-backed groups' capabilities, as groups linked to the Chinese People's Liberation Army (PLA) have the logistical support from a range of state-level resources, including the use of HUMINT (human intelligence) operations that aide computer network exploitation (CNE) operations.[38]

In 2017, credit reporting agency Equifax announced that Chinese state-backed hackers stole the credit information of 147.9 million Americans.[39] Recent activity such as the HAFNIUM Microsoft Exchange Server attacks demonstrate an intent to collect data from the emails of the European Banking Regulator, the European Banking Authority (EBA), which was targeted in the HAFNIUM attacks.[40] The EBA gathers and stores large amounts of sensitive data about banks and their lending. It was reported the threat actor remained in the victim's email servers, and did not attempt to move laterally within the compromised network, indicating the objective of the threat actor was exfiltration of data from the email servers. Recent reporting suggests there is a possibility that data stolen by HAFNIUM in the Microsoft Exchange Server attacks could be used to feed into China's AI machine.[41] Although this claim lacks sufficient evidence to support it, there is evidence that Chinese state-backed cyber operations have, over recent years, accumulated huge swathes of personal identifiable information of general citizens.

Chinese state-backed cyber operations are to be considered an extension of China policy in the political, economic, and military agendas. As such, WithSecure™ assesses it is highly likely that threat actors operating on behalf of the Chinese government will target financial organizations in operation under cyber espionage objectives: to collect information of intelligence value to the Chinese state, which extends beyond a traditional intelligence agenda to include economic advantage, intellectual property theft, and collection of personal data.

[35] https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
[36] https://www.fireeye.com/blog/threat-research/2021/05/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices.html
[37] https://www.recordedfuture.com/china-pla-unit-purchasing-antivirus-exploitation/
[38] https://asia.nikkei.com/Business/Technology/Japan-lashes-out-against-alleged-Chinese-military-cyberattacks
[39] https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020
[40] https://www.reuters.com/article/us-microsoft-hack-eba-idUSKBN2B01RP
[41] https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying

Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of WithSecure™ Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

W / T H
secure