Under the Lens

Financial Services:

Challenger Banks

Cyber Threat Operations

Q1 2020

Contents

Introduction

The financial services sector is constantly evolving, whether in response to technology advancement or regulatory changes, and nowhere is that more evident than amongst challenger banks – both those that are 'bricks and mortar' and those that are technology-based. Yet the cyber threat landscape is also evolving, and the cyber threats facing the challenger banks also adapt to this changing attack surface.

A sometimes nebulous term, 'challenger banks' mainly comprise new retail banks that have been given banking licences within the last ten years and are directly competing with longer-established banks. In many instances, they have changed the way in which consumers interact with their banking providers. Some of these operate in the same way as established high-street banks; others are on a 'branchless', purely digital platform. Regardless, their lack of legacy infrastructure and traditional organisational structure means that they are often able to leverage new technology and digital applications to a greater extent than some more established banks.

Although a term covering a diverse range of entities, many challenger banks will offer niche products or services to customers, rather than necessarily a full retail bank offering. Their predominant role is – as with wider financial services – the management of money, making them an attractive target to criminals and anti-capitalist hacktivists alike. They provide services to a wide gamut of customers, and will therefore hold sensitive data on these customers that is attractive to espionage threat actors, including state-backed threat actors. Indeed, a number of challenger banks themselves have been recipients of large amounts of investment capital, which itself could be target of espionage campaigns seeking insight into deals or private equity activity. More broadly, financial services are often classed as critical infrastructure,[1,2] making the sector an attractive target for sabotage threat actors looking to cause disruption.

The sector as a whole is highly regulated, and it recorded the second highest average cost of a breach in the 2019 Cost of a Data Breach Study.[3] Yet financial services customers have high expectations for the protection of their data and money, and are more likely to turn to competitors if they do not believe their needs are being met.[4,5]

[1] 'Critical National Infrastructure', Centre for the Protection of National Infrastructure, https://www.cpni.gov.uk/critical-national-infrastructure-0

[2] 'Critical Infrastructure Sectors', Department of Homeland Security, https://www.dhs.gov/cisa/critical-infrastructure-sectors

[3] 'Ponemon Institute Cost of a Data Breach Study 2018', Security Intelligence, July 2018, https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018/

[4] 'Ponemon Institute Cost of a Data Breach Study 2019', IBM, July 2019, https://www.ibm.com/security/data-breach

[5] 'Brits would change their bank following a cyberattack', ieDigital, https://www.iedigital.com/resources/press-releases/half-brits-change-bank-following-cyber-attack-research-reveals/ (13th September 2017)

It is therefore vital for financial institutions to not only develop a secure environment, but to develop the means to detect and respond to cyber incidents so that any impact is minimised. The challenges inherent in identifying and retaining cyber talent can in turn magnify the complexity of this landscape.

Digital transformation plays a key part within the challenger bank space, including in the software and backend of the provision of financial services. This specific importance and reliance on technology - including cloud - amongst many technology-driven challenger banks, means that maintaining visibility of the continuously evolving cyber threat landscape is particularly vital. This is in particular the case for those that operate solely with a digital presence, given the potential for business interruption, reputational and regulatory implications, for example Strong Customer Authentication (SCA) under PSD2.

The open technological ecosystems of some digital banking platforms, their partnering with FinTech companies and adoption of new technologies may also create new potential avenues of attack, as demonstrated by Operation Cloud Hopper. It is also important to consider that technology not only underpins challenger bank's back-end infrastructure but also actual client offerings, for example, in the form of credit decision models.

This report provides an overview of the most common cyber threats facing the financial services sector, and challenger banks in particular, in order to generate awareness and illustrate the motivations behind such attacks, as well as support intelligence-led defence.

Our analysis is informed by our own in-house intelligence datasets maintained on cyber attacks and targeting from a variety of threat actors, intelligence gleaned from our incident response engagements around the world, as well as publicly-available reports on attacks in the sector.

Timeline of attacks

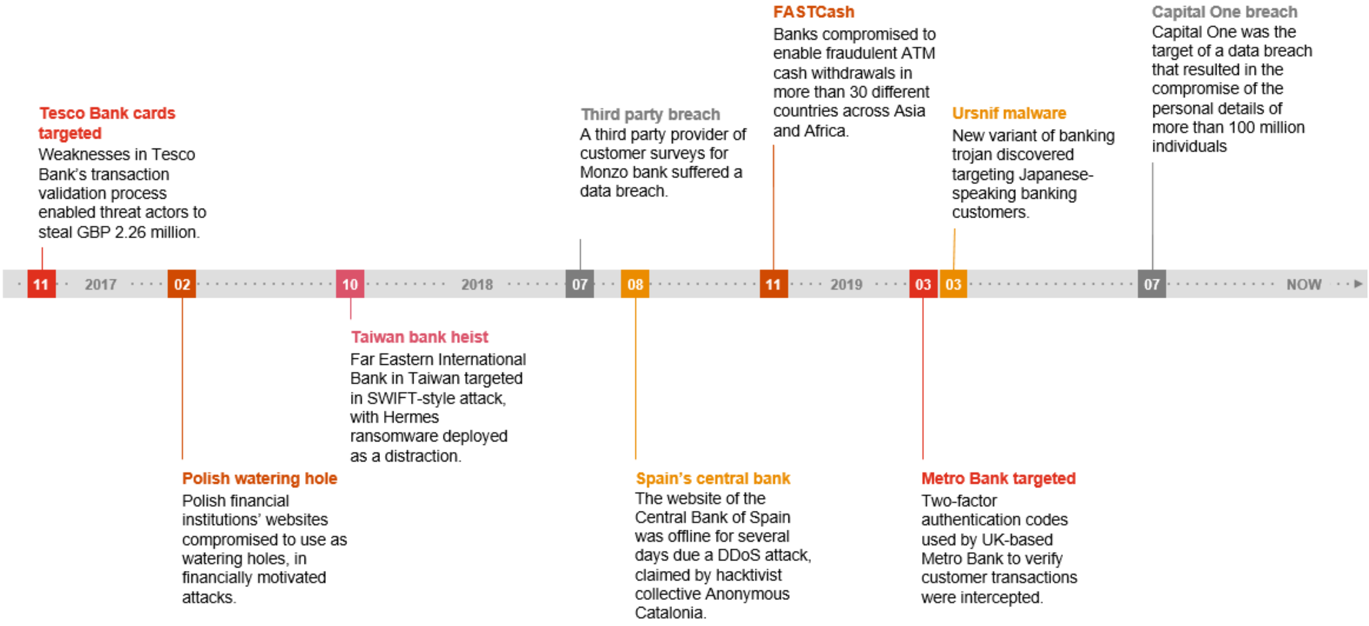
The threat actors targeting the financial services sector as a whole vary in their motivations and in their sophistication – from low-resourced, opportunistic threat actors, through to persistent, highly targeted state-sponsored attackers that seek to obtain information from specific organisations.

In particular, PwC intelligence reporting over the past few years shows a consistent trend of criminal threat actors becoming more sophisticated, both in their technical capability but also in their ability to target increasingly higher levels in the financial services value chain for larger payoffs; from individuals (with banking trojans, identity fraud), to companies (with payment processing systems, ATM hijacking, monetising stolen data), to targeting banking infrastructure itself. Whilst low-level tools, techniques, and procedures (TTPs) remain prevalent, over the last few years more sophisticated attacks have targeted banks and banking networks around the world.

For several years, there has been a steady stream of attacks that involve compromising banks with low levels of security maturity – and this is as relevant for challenger banks as it is for their more established peers. Threat actors pivot to the banks' systems that access payment platforms which they leverage to transfer funds to attacker-owned accounts. North Korea-based, state-backed threat actor Black Artemis (*a.k.a.* Lazarus, Bluenoroff, APT38) is known to be responsible for more than ten such heists, and more recently has also targeted the Mexican electronic payment system SPEI, compromised banks in Asia and Africa to enable fraudulent ATM cash withdrawals, and has been active in parts of Africa and the Middle East in 2019.

> *'In the past decade, the capability and motivation of threats to the financial sector have transformed from small-scale opportunistic crimes to efforts to compromise entire networks and payment systems.'*
>
> Carnegie Endowment for International Peace

The timeline below documents some of the key attacks targeting challenger banks and financial services more widely, which are discussed in this report. Further real-world examples are included in the Case Studies section of this report.



Tesco Bank cards targeted
Weaknesses in Tesco Bank's transaction validation process enabled threat actors to steal GBP 2.26 million.

Polish watering hole
Polish financial institutions' websites compromised to use as watering holes, in financially motivated attacks.

Taiwan bank heist
Far Eastern International Bank in Taiwan targeted in SWIFT-style attack, with Hermes ransomware deployed as a distraction.

Third party breach
A third party provider of customer surveys for Monzo bank suffered a data breach.

Spain's central bank
The website of the Central Bank of Spain was offline for several days due a DDoS attack, claimed by hacktivist collective Anonymous Catalonia.

FASTCash
Banks compromised to enable fraudulent ATM cash withdrawals in more than 30 different countries across Asia and Africa.

Metro Bank targeted
Two-factor authentication codes used by UK-based Metro Bank to verify customer transactions were intercepted.

Ursnif malware
New variant of banking trojan discovered targeting Japanese-speaking banking customers.

Capital One breach
Capital One was the target of a data breach that resulted in the compromise of the personal details of more than 100 million individuals

Incident themes

Based on past incidents and sector trends, PwC assesses that financially motivated threat actors are most likely to target the financial services sector - including challenger banks. For criminal threat actors, organisations controlling the flow of money are a prime target. According to PwC's Global Economic Crime and Fraud Survey 2018, cyber crime represented the third most prevalent form of fraud for financial services.

A detailed explanation on how PwC categorises threat actors by motivation is located in Appendix 1 of this report.

Criminal

Due to their role managing and controlling large volumes of money, organisations in the financial sector are highly attractive targets for criminal threat actors, whether that is through bank heists, stealing valuable data, or DDoS extortion. PwC research shows criminal threat actors executing more innovative and sophisticated forms of attack, while others continue to thrive using more traditional threat vectors.

The sections below outline prevailing focuses for criminal attackers targeting the financial sector, from conducting large-scale cyber heists, to targeting banking users with commodity malware.

Bank heists and banking networks

On the more sophisticated end of the spectrum are financially motivated attacks targeting banks and core banking networks. Prominent examples are the Black Artemis campaigns, which involve compromising banks and pivoting through the network to reach and abuse poor implementation of access controls and business processes around SWIFT servers in order to transfer funds to attacker-owned accounts. This has taken place, with varying levels of success, in the Philippines, Vietnam, Bangladesh, Taiwan, India, Malaysia, Chile, Ecuador, Mexico, and Sierra Leone – and it is likely other countries have and will be targeted.

SWIFT is not the only interbank network to which access has been sought by criminal threat actors. SPEI is the real-time gross settlement system in Mexico and, in 2018, threat actors targeted five banks' networks in order to reach SPEI's transaction servers. Using this privileged access, the threat actors fraudulently transferred between USD 15 and 20 million from non-existent bank accounts.

While these examples target major interbank networks, the threat also applies to ATM switches, card issuing platforms, and domestic payment schemes, which will also impact smaller organisations.

Organised criminal syndicates

PwC intelligence reporting shows an increase in criminal syndicates working together to have the maximum impact. This includes international coordination, for example, Black Artemis' use of global money mules to enable cashing out from countries around the world, including India, the Philippines, and Sri Lanka.

As well as working with criminal organisations to manage its cash out operations, reports suggest Black Artemis has been contracting with a criminal syndicate, TA505, which acts as a distribution network for some of the most prevalent criminal threat actors, as well as operating its own bespoke malware. TA505 is a sophisticated threat actor that has been attributed to distributing Dridex, Locky ransomware, and Trickbot. TA505 tools include:

- GraceWire – a custom backdoor used in the early stages of an intrusion; it has been seen on systems compromised by Black Artemis;[6]
- ServHelper – this backdoor has been used since the end of 2018, most notably in an attack against a financial institution where the malware was signed with a legitimate certificate;[7] and,
- FlowerPippi – first reported on in July 2019, this backdoor has been used in campaigns targeting Japan, India, and Argentina.[8]

ATM jackpotting

Although this type of attack is more relevant for the 'bricks and mortar' challenger banks rather than those that are digital-only, the threat should nevertheless also be considered in the context of the wider financial services sphere. Attacks are increasingly sophisticated, with prominent campaigns including:

- FASTCash: Since at least late 2016, Black Artemis has targeted banks in Africa and Asia in order to gain access

[6] 'A new breed of ATM hackers gets in through a bank's network', Wired, https://www.wired.com/story/atm-hacks-swift-network/ (10th April 2019)
[7] *CTO-TVB-20190515-01A – Threat Vector Bulletin – April 2019*
[8] 'Latest spam campaigns from TA505 now using new malware tools Gelup and FlowerPippi', TrendMicro, https://blog.trendmicro.com/trendlabs-security-intelligence/latest-spam-campaigns-from-ta505-now-using-new-malware-tools-gelup-and-flowerpippi/ (4th July 2019)

to payment switch application servers and enable fraudulent ATM cash withdrawals;

- Cobalt Group: In 2017 and 2018, another criminal threat actor known as the Cobalt group carried out a series of attacks affecting ATM systems in the Asia Pacific and Eastern European regions;
- In 2019, reporting uncovered attacks against banks in Bangladesh, India, Sri Lanka, and Kyrgyzstan that resulted in ATM jackpotting. These are attributed to a criminal threat actor, White Jackalope (*a.k.a.* Silence); and,
- Redbanc: In 2018, Black Artemis compromised the corporate network of the Chilean ATM interbank network. While the incident was mitigated before any money was stolen, it was likely financially motivated.

Data theft

The theft of personal and financial data through social engineering and data breaches is a major contributor to fraud losses.[9] As well as being leveraged to carry out direct 'cash out' activity, it can also be used to facilitate wider identity theft. This could include, for example, opening a credit card in someone else's name, or taking over an account. Although challenger banks' investment in technology solutions – such as AI-based systems to flag suspicious activity – can help to mitigate this activity, they remain a high-profile target for this type of activity.[10]

Attacks targeting retail and hospitality

Over the past few years, PwC has seen more sophisticated criminal threat actors focusing on the retail and hospitality sector. Since 2018, the various criminal threat actors that fall under the umbrella group known as Magecart have compromised a wide variety of organisations to place digital card skimmers on e-commerce sites to steal payment details. Similarly, White Giant (*a.k.a.* FIN6) and Blue Gulon (*a.k.a.* FIN7) are criminal threat actors that focus on retail and hospitality, using point-of-sale malware to steal payment card details. Both have been active since at least 2015 and have compromised a wide variety of major companies around the world.

While these attacks do not directly target the financial sector, victims often look to banks or other financial institutions to reimburse losses. This remains relevant to the challenger bank space although some of the challenger bank community are reported to be sceptical about the continuation of a so-called 'fraud fund'.[11]

Banking trojans

Banking trojans remain extremely popular; the most prevalent malware families include Ursnif, Dridex, and Trickbot – designed to surreptitiously steal credentials as victims type them into the web browser. These malware families have been around since 2007, 2011, and 2016 respectively, yet are regularly evolving to encapsulate new techniques. They also have a disproportionate impact on financial institutions, both from direct attacks and attacks against their customers.

Mobile banking trojans are a growing threat, with several malware families targeting Android users. For example, the Anubis mobile banking malware has configurations for over 100 banks internationally, and is delivered through fake apps on Google Play and through SMS phishing attacks. In the UK, Financial Fraud Action reported that losses from mobile banking fraud grew from GBP 2.8 million in 2015 to GBP 7.9 million in 2018, although some of this growth may reflect the greater use of mobile banking apps over the same time period.

[9] Fraud The Facts 2019, UK Finance, https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2019 (21st March 2019)
[10] 'Fraud: here's how scammers get away with it', The Guardian, https://www.theguardian.com/money/2018/jul/07/heres-how-scammers-get-away-with-it (7th July 2018)
[11] 'What will happen to the fraud fund in 2020?', ThisIsMoney, https://www.thisismoney.co.uk/money/saving/article-7701249/What-happen-banks-fraud-fund-2020-banks-squabble.html (19th November 2019)

Espionage

Financial services are also frequently targeted by espionage threat actors, with attacks originating from state-sponsored attackers and financially motivated threats actors alike. For state-backed threat actors, the motive could be to benefit the country's economy, or gain sensitive information on an organisation's customers; for criminals, the motive may be to gain an advantage in a market. For example, for five years leading up their capture in 2017, Ukrainian threat actors made a total of USD 100 million selling on information stolen from three major business newswires.[12] The threat actors sold unpublished press releases, regulatory announcements, and other market-moving information while under embargo, to Moscow-based distributors. The distributors then sold to stock traders, for a cut of the profit.

Different techniques are used depending on the sophistication of the threat actor. Phishing emails and other social engineering tactics are prominent infiltration vectors – used to lure a victim into providing sensitive information, or to pivot to other networks or victims. In the Cloud Hopper campaign, espionage threat actor Red Apollo (*a.k.a.* APT10) carried out a supply chain attack in order to compromise its victims. Red Apollo compromised major managed service providers in order to reach their customers, and one of the end-goal victims was a global financial institution. This type of attack vector threat is particularly relevant for challenger banks given the likelihood of technology being outsourced.

Hacktivist

Victims of hacktivism are often selected seemingly at random as the attackers seek any avenue through which to gain additional notoriety. In some cases, however, their victims are targeted, due to an organisation or individual's perceived actions or support of an issue.

Financial institutions periodically catch the attention of anti-capitalist individuals or groups who believe that the financial services sector generates too much profit.

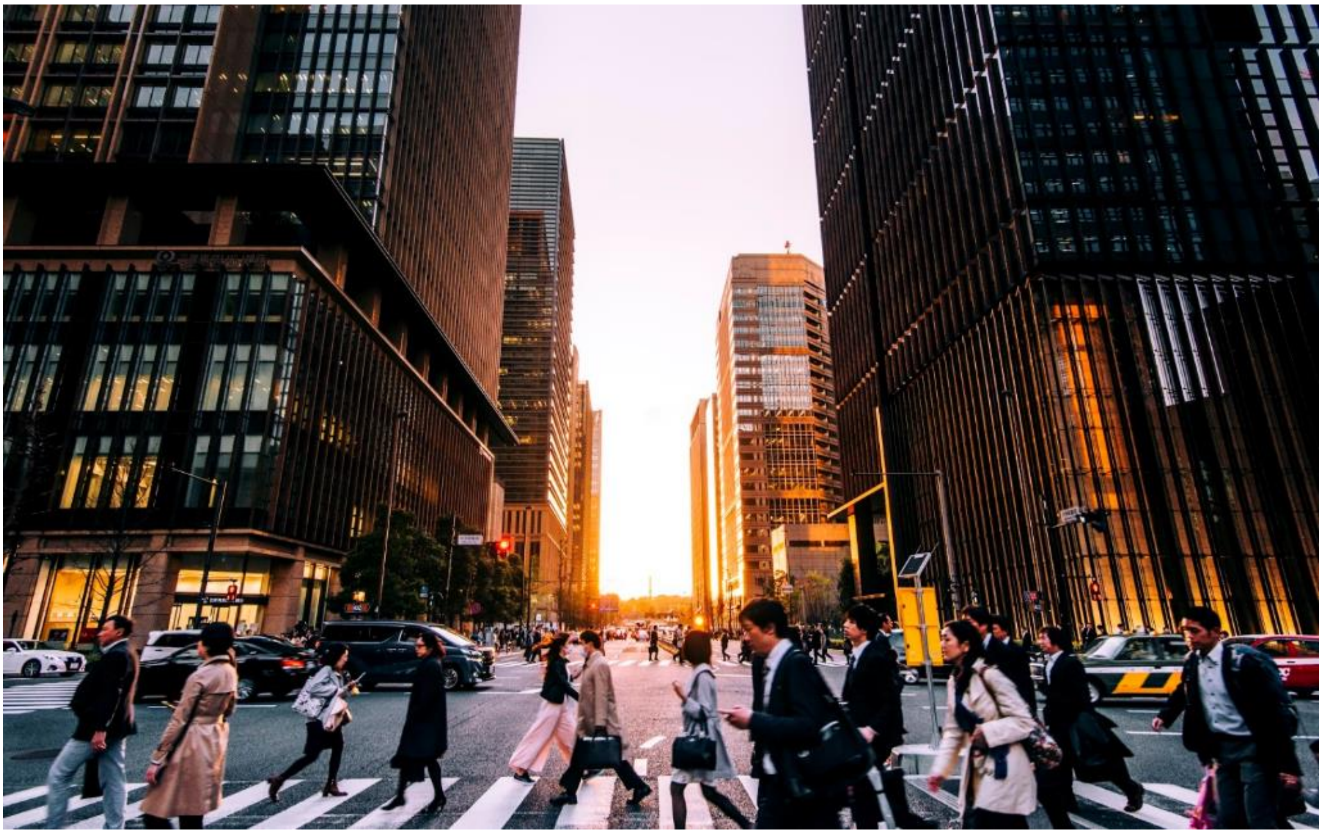
For example, in June 2018, Grey Ares (*a.k.a.* Anonymous) launched its #OpIcarus2018 campaign targeting global financial institutions and banks in protest against perceived corruption and capitalism. Grey Ares uses cyber attacks to raise awareness of the cause, and uses a variety of low sophistication techniques, including DDoS attacks, SQL injection, and cross site scripting.

Sabotage

Sabotage attacks rose to prominence in 2011, with the infamous campaign targeting Iran's nuclear programme using destructive malware, dubbed Stuxnet. Since then, the use of destructive malware has evolved to no longer be entirely motivated by sabotage.

StoneDrill is a sophisticated wiper used predominately to cause destruction with the oil and gas sector in the Middle East; however, StoneDrill also contains espionage tools in its arsenal indicating the destructive malware serves multiple purposes.

[12] 'How an international hacker network turned stolen press releases into USD 100 million', The Verge, https://www.theverge.com/2018/8/22/17716622/sec-business-wire-hack-stolen-press-release-fraud-ukraine (22nd August 2018)



PwC has also seen sabotage attacks used for diversion. In more recent cyber heists, Black Artemis has employed destructive malware to draw attention away from the true motivation of the attack; the threat actor deployed Hermes ransomware as a distraction technique in Taiwan, and KillDisk wiper malware when targeting banks in Mexico and Chile in 2018.

Of course, traditional destructive attacks purely seeking to cause destruction still occur. In November 2017, seven of the UK's largest banks were hit by DDoS attacks generated by the DDoS-for-hire website, Webstresser. The definitive motivation is unknown; however, none of the victims reported extortion attempts or other financially motivated attacks occurring simultaneously.

Previous incidents involve disgruntled insiders deleting files and backups of systems to cause the most damage, or negligent insiders doing the same unintentionally. In 2016, a former systems administrator for software company ClickMotive, was sentenced to ten years in jail for deleting files before leaving his job; ClickMotive claimed this resulted in USD 140,000 worth of damages. Given that many challenger banks have experienced fast rates of growth and are often based on small dynamic teams and open access principles, these threats should be given particular attention.

In addition to this, for some financial institutions, complicated algorithms and machine learning are critical to operations and accidental or malicious changes could have a high impact. For example, if investment decisions are made using an algorithm for which the data feeds are manipulated, this could incur serious financial loss. This is particularly true for challenger banks, where this is often a high level of reliance on technology-based solutions, both for back-end operations and customer-facing applications.

Finally, it is also important to consider cyber attacks that are not targeting financial institutions, yet have still impacted them. NotPetya and WannaCry are both examples of this. While it can be debated whether these attacks were financially motivated, the significant destruction they caused cannot. WannaCry targeted victims indiscriminately, and government organisations, hospitals, railways, and banks were among the victims. NotPetya predominately compromised (and arguably targeted) organisations in Ukraine, and victims spanned all sectors.

Case studies

The below case studies provide an overview of publicly-reported attacks that have taken place in recent years. These examples also illustrate the wide-ranging motivations of the threat actors which have targeted the financial services sector, including challenger banks.

1. Tesco Bank cards targeted

Threat Actor Motivation	Target	Year
Financial	Bank	2016

Criminal threat actors exploited weaknesses in Tesco Bank's transaction validation processes that made processing transactions with some invalid data (e.g. expiry dates) an easier task.[13] In addition, Tesco Bank issued debit cards with sequential account numbers, making it easier for threat actors to identify legitimate credit card details.[14] Over one weekend, the threat actors initiated fraudulent transactions from more than 8,000 customer accounts, which amounted to more than GBP 2 million. The Financial Conduct Authority has since fined Tesco Bank GBP 16.4 million for the breach.

2. Polish watering hole

Threat Actor Motivation	Target	Year
Financial	Financial institutions	2017

Black Artemis compromised the websites of at least three financial institutions – the Polish Financial Supervision Authority, the National Banking and Stock Commission of Mexico, and a state-owned bank in Uruguay – to use as watering holes in financially motivated attacks.[15] Multiple Polish banks were compromised by Black Artemis as a result.

3. Taiwan bank heist

Threat Actor Motivation	Target	Year
Financial	Bank	2017

Black Artemis compromised the Far Eastern International Bank in Taiwan and launched fraudulent transfers to attacker-owned accounts in Cambodia, the US, and Sri Lanka.[16] Simultaneously, the threat actor deployed Hermes ransomware as a form of distraction; despite this, the attack was uncovered and the majority of funds recovered.

4. Third party data breach

Threat Actor Motivation	Target	Year
Financial	Third party	2018

In July 2018, challenger bank Monzo revealed that a third-party company it uses for customer surveys had experienced a data breach. The third party, Typeform, had been compromised by attackers who were able to access data back-ups for surveys conducted by the firm on the bank's behalf. Monzo estimated that about 20,000 of its users had been impacted in the incident, with some personal information, such as email addresses, being revealed.

[13] 'Tesco Bank blames "systemic sophisticated attack" for account losses', BBC News, https://www.bbc.co.uk/news/business-37891742 (7th November 2016)

[14] 'Final notice; Tesco Personal Finance plc', Financial Conduct Authority, 1st October 2018, https://www.fca.org.uk/publication/final-notices/tesco-personal-finance-plc-2018.pdf

[15] 'Lazarus and watering hole attacks', BAE Systems, https://baesystemsai.blogspot.com/2017/02/lazarus-watering-hole-attacks.html (12th February 2017)

[16] *CTO-QRT-20171031-01A – Taiwan heist malware*

5. Spain’s central bank targeted

Threat Actor Motivation	Target	Year
Hacktivist	Central bank	2018

The website of the Central Bank of Spain was offline for several days in August 2018 due a DDoS attack, claimed by hacktivist collective Anonymous Catalonia. The incident was part of the so-called ‘#OpCatalonia’ in support of Catalonian independence protesters. The bank’s normal business operations were not reported to have been affected by the outage.

6. FASTCash

Threat Actor Motivation	Target	Year
Financial	Bank	2018

In October 2018, the US-CERT issued an alert detailing Black Artemis’ FASTCash campaign.[17] Since at least 2016, the North Korea-based threat actor had stolen tens of millions of dollars through injecting malware into banking application servers. The targeted servers all ran unsupported versions of the AIX operating system that allowed the threat actor to generate fake approval messages for fraudulent transactions and dispense cash from ATMs across Asia and Africa.

7. Capital One data breach

Threat Actor Motivation	Target	Year
Hacktivist	Bank	2019

US-based bank Capital One was the target of a data breach that resulted in the compromise of the personal details of more than 100 million individuals, including the names, addresses and phone numbers of people who applied for the bank’s products. Some 140,000 social security numbers and 80,000 linked bank account numbers were compromised in the US. Other information accessed in the breach included credit scores, limits, balances, payment history and contact information.

8. Metro Bank targeted

Threat Actor Motivation	Target	Year
Financial	Bank	2019

Threat actors intercepted text messages containing two-factor authentication codes for customer transactions with UK-based Metro Bank.[18] They exploited flaws in the Signalling System 7 (SS7) protocol to bypass the two-factor authentication used by Metro Bank, defrauding a small number of customers.

9. Ursnif malware

Threat Actor Motivation	Target	Year
Financial	Banking customers	2019

Ursnif is a banking trojan first seen in 2016. In a recent campaign, criminal threat actors have used a new variant of the Ursnif malware to target Japanese-speaking bank customers.[19] This demonstrates that banking trojans are still being used and updated by criminal threat actors.

[17] ‘HIDDEN COBRA – FASTCash Campaign’, US-CERT, 2nd October 2018, https://www.us-cert.gov/ncas/alerts/TA18-275A

[18] ‘Criminals hit Metro Bank with multi-factor authentication bypass SS7 attack’, SC Media, https://www.scmagazineuk.com/criminals-hit-metro-bank-multi-factor-authentication-bypass-ss7-attack/article/1524670 (4th February 2019)

[19] ‘New Ursnif variant targets Japan packed with new features’, Cybereason, https://www.cybereason.com/blog/new-ursnif-variant-targets-japan-packed-with-new-features (12th March 2019)

Conclusion

In the last few years, financially motivated attacks have become more prominent, and espionage threat actors more audacious in their techniques – even incorporating destructive components into their attacks. As the cyber threat landscape evolves, so do the attacks targeting the financial sector – and with that, the challenger bank space.

Based on incident trends, case studies of attacks, and our own in-house analysis, PwC assesses that criminal threat actors pose the greatest threat to financial services. The sophistication of criminal threat actors varies considerably, with threat actors on the higher end of the scale reaping in millions. On the other hand, low-level tools, techniques, and procedures used against the financial services, including banking trojans, ransomware, and DDoS extortion, are still met with success.

In comparison, espionage, hacktivist, and sabotage attacks against the sector are far less prevalent. In fact, prominent sabotage attacks against financial institutions have been linked to financially motivated attacks (as in the cases of ransomware and wipers used in cyber heists).

However, PwC has observed activity where company competitors have sought to gain competitive advantage through espionage cyber attacks, and hacktivists targeting financial institutions in the name of their beliefs.

Knowing which threat actors are relevant to a given sector is an important step toward strategically directing investment in appropriate defences. The overall view presented in this report, however, spans the entire financial services sector, incorporating challenger banks specifically, and more granular threat analysis should be done on a per-organisation basis.

Analysis of how threats would navigate your organisation's infrastructure to achieve their objective can help to identify the gaps that exist in your security controls, and enable you to tailor your preparation efforts appropriately. Having the ability to protect, defend, respond and recover is key to ensuring that threats can be minimised, and that incidents can be addressed when they manifest.

Appendix 1: Analysis methodology

Most cyber attacks have an underlying and ultimate motivation. Although attacks by separate threat actors might share objectives, separate threat actors do not always share the same motivation. Examining the motivation of an attack can enable the identification of the category of attacker.

PwC divides the threat landscape according to the motivation of those behind cyber attacks. For each, some common tactics, techniques, and procedures (TTPs) observed by PwC's Threat Intelligence team are included. The divisions are as follows.

Motivation	Description
Espionage For the information	Espionage threat actors (often referred to as "Advanced Persistent Threats", or APTs) typically seek to steal information which will provide an economic or political advantage to their benefactor. Attacks motivated by espionage usually originate from either industry competitors or state-sponsored threat actors. Often the benefactor is a nation state, and espionage activity aligned to state objectives will reflect geopolitics and real-world events. Usually, the information sought out by espionage attackers is only found at specific organisations, meaning they repeatedly target the same organisation and their suppliers until they have completed their mission.
Criminal For the money	Cyber criminals are largely indiscriminate in who they attack as they simply seek to monetise their attacks. The range in sophistication of cyber criminals is vast, and displays a widely different set of Tactics, Techniques and Procedures (TTPs). Low-level criminals target individuals, commonly using ransomware, or banking trojans like Dridex or Trickbot, which steal credentials from users as they type them into their web browser. More sophisticated threat actors target organisations to monetise stolen data. Attacks include the use of inserting card skimming malware onto retail websites via third party provider access, ATM hijacking, or using point-of-sale malware.
Hacktivist For the cause	Hacktivists conduct attacks to increase their public profile and raise awareness of their cause .This is typically done through the disruption of services such as denial of service (DoS) attacks, and website defacements. In many cases such attacks are random; they care little how this is done or who is affected, so long as their message is promoted. In some cases, however, their victims are targeted, due to an organisation or individual's perceived actions or support of an issue. As with espionage, attacks from hacktivists are sometimes influenced by real-world events, meaning the risk of such attacks is subject to change.
Sabotage For the impact	Saboteurs seek to damage, destroy or otherwise subvert the integrity of data and systems. Sabotage attacks are not always deliberate and have been used to mask other malicious activity. Sabotage operations designed to be a diversion can still result in significant collateral damage. Examples of attacks include wiping hard drives, causing SCADA systems to malfunction or altering trade data. As with espionage attacks, attacks from saboteurs tend to be influenced by real-world events, making the risk of attacks specific to geography and company actions in relation to political events/issues.

Appendix 2: PwC Threat Intelligence

About Us

PwC is globally recognised as a leader in cyber security and as a firm with strong global delivery capabilities and the ability to address the security and risk challenges our clients face. We underpin our board-level security strategy and advisory consulting services with expertise gleaned from the front lines of cyber defence across our niche technical expertise in services such as red teaming, incident response and threat intelligence.

Our threat intelligence team specialises in providing the services which help clients resist, detect and respond to advanced cyber-attacks. This includes crisis events such as data breaches, economic espionage and targeted intrusions, including those commonly referred to as APTs. We differentiate ourselves with our ability to combine strong technical capabilities with strategic thinking, with our research conducted by our in-house experts recruited primarily from governments, the military, and the security services- giving us a unique perspective and a vast array of contacts.

We offer a range of threat intelligence products and services designed to enable an effective defence against advanced cyber threats.

Cyber threat intelligence subscription

Access to PwC's targeted attack indicator feeds, network and endpoint signatures and tactical and strategic reporting.

Directed research and assessments

Direct access to PwC's threat research team for tasks relating to ad-hoc or long term enquiries – both tactical and strategic research into malicious samples, threat actors or analysis support.

Cyber threat intelligence monitoring

Continuous, bespoke and focused research which would augment our subscription services.

Consulting and advisory

Advisory services to help organisations define requirements, consume, apply and produce threat intelligence in a way which best suits their organisation.

If you would like more information on our services, or to discuss any of the threats contained in this report please feel free to get in touch at cyber.austria@pwc.com.

Notes

pwc.at/cyber

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.