Blueliv.

Cyber Threat Intelligence for Banking & Financial Services

FOLLOW THE MONEY

1. Introduction

Banks and other financial institutions handle some of the most valuable information to cybercriminals, from account and credit card data to sensitive PII (personally identifiable information). As such, these organizations remain at the forefront for risk as cybercriminals become increasingly sophisticated and malicious in their methods. A new generation of cybercriminals is also evolving - no longer satisfied with simply stealing funds and holding companies' information hostage, instead, aiming to infiltrate and manipulate companies and environments, threatening the credibility and integrity of the institution, leaking sensitive information to the public, or committing fraud at different levels.

The COVID-19 pandemic has only bolstered these threats, as financial institutions' already large exposure to such risks has been amplified by sudden shifts to remote working practices and other operational challenges. As a result, many financial organizations saw employees access data from remote, unprotected networks, compared to the highly regulated and sophisticated environment they had typically used in the office. This exposed their systems to a plethora of threats that could infiltrate the enterprise's network easier than ever before.

The second edition of this whitepaper is intended to act as a reference document for organizations in the banking and financial services sector, providing a broad overview of threats, certain relevant threat actors and how organizations can manage their digital risk more effectively, with updated information about the cyberthreat landscape.

Despite the financial services sector being among the most secure industries when it comes to cybersecurity, the risk of cyberattack cannot be overstated. Attacks and breaches hit and disrupt financial services firms particularly hard and often cost them more in damages and recovery than institutions in any other sector. This is due to the fact that financial institutions today are 300 times more likely to be targeted by an attack than any other industry[1].

This whitepaper will provide some detail around some of the most relevant cybersecurity issues targeting the financial services sector, offering threat intelligence insight and guidance to meet some of the challenges they face today.

In industries as mature as financial services, it is critical to build defenses that are comprehensive, resilient and end-to-end. Managing cyber-risk is, as EY puts it, "a team sport and is everyone's responsibility, from the boardroom to the front line."[2] With that in mind, organizations across the board are using integrated cybersecurity risk management strategies, involving resources, activities and the cooperation of the entire organization.

Cybersecurity is based on a combination of people, process and technology. A successful approach focuses on a cybersecurity-aware culture and includes regular training, as well as using best-in-breed targeted cyber defense technology. Beyond awareness and education, everyone has an active role to play, all the way from CISOs, to risk compliance and auditing professionals, to operational teams and beyond.

1 https://web-assets.bcg.com/d4/47/64895c544486a7411b06ba4099f2/bcg-global-wealth-2021-jun-2021.pdf
2 https://www.ey.com/en_us/innovation-financial-services/cybersecurity

2. Why is the financial services sector targeted?

The financial services sector has always been highly targeted due to the tremendous value of and access to extremely sensitive data (financial, personal…) and the possibility to quickly make a lot of profit. Cyberattacks can undermine the integrity of a financial organization's underlying infrastructure as well as the systems that drive its operations. Recent high-profile attacks that were more persistent, elaborate and far-reaching have demonstrated this. The end game varies - the attackers' objective may be to extort profit from their victims, to cause reputational damage or to cause a political stir, to mention just a few.

2.1. Financial institutions manage money - lots of it

As consumers expect high quality digital solutions, such as online and mobile banking and online shopping, the attack surface increases, affording cybercriminals an increased ability to infiltrate networks to achieve their objectives. Data held and processed by FSIs can be monetized in many different ways, from insider trading, pump-and-dump schemes, customer account take over, manipulating payment information to many more methods that will be discussed later in this paper.

2.2. Pushing political or personal agendas

Many cybercriminals, from APTs down to script-kiddies and hacktivists, tend to view the finance sector as a key target due to its importance across the global economy. For example, hacktivists typically seek to target particular organizations as a way of drawing attention to their agendas. At a lower level, disgruntled current or former employees of an organization seeking to cause damage could be another source of attack. At a higher level, many attacks can be attributed to nation states who are acting on a political agenda.

2.3. Cybercriminals crave recognition

Among the cybercriminal community, individuals or larger groups may target large, well-known organizations in the hopes of gaining notoriety within the hacker community. This goes for all industries, but the status payout for infiltrating financial institutions is high, given that they are usually much better defended than organizations in other sectors.

3. State of the Industry

We are in the midst of a constantly changing threat landscape, during a time when shifting business priorities continue to change how organizations approach risk management and mitigation. With financial services institutions being such high-profile targets for cybercriminal activity, it is important to get a sense of the current risk landscape so organizations can create effective strategies before, during and after an attack.

The COVID-19 crisis has brought about years' worth of digital transformation and disruption in a matter of

months, forcing industries, governments and individuals to abandon traditional working practices and adopt new, uncertain practices almost overnight. This mass disruption - from the sudden digitalization and remote management of banks, to shifting and uncertain customer expectations in light of the pandemic - created a breeding ground for new threats and risks.

According to a 2019 Ponemon report[3] the industry is very much aware of and concerned by online threats, but acknowledges that it is not doing enough to protect its systems, networks and data.

While the global financial services sector is well versed in seeking solutions to increase efficiency and keeping with user demand, the sprint to adopt the latest digital technologies sometimes means weaknesses can appear in the network infrastructure. The increasing number of channels, not to mention core integrations with third parties (aka supply chain), has also led to an increase in attack surface and has upped the complexity of attacks themselves. Currently, a robust cybersecurity posture goes well beyond protecting sensitive information and systems from malicious external attack. It means guarding identities, higher levels of data privacy than ever before and vulnerability management on a vast scale.[4]

3.1. Recent attacks

We have established that the potential value of the information within financial institutions' IT systems makes them frequent targets of cybercriminals, either directly or via a third party. It is important to study recent attacks that have occurred in the financial services sector and lessons learned

3.1.1. SolarWinds

In December 2020, the business software application Orion, created by the popular IT management company SolarWinds, was infected with nation-state malware that affected all versions of the application released between March and June 2020.

Following the successful installation of the tainted software update, attackers identified high-value targets among the compromised SolarWinds clients and moved to elevate credentials and steal signed certificates. Considering how labor intensive such activities are known to be, it is widely believed that significant advanced planning was carried out prior to the successful launch of the Trojanized update.

It is now known that the SolarWinds victims spanned not only to financial institutions, such as Denmark's Central Bank, but government, consulting, technology, telecommunications, and other industries worldwide, affecting victims in the United States, Canada, Mexico, Belgium, Spain, UK, Israel, UAE, and elsewhere.

In short, the SolarWinds attack quickly became one of the biggest attacks in recent history, highlighting not only the danger of supply-chain attacks but also how unprepared some of the world's largest organizations operating in the financial or any other sector are to prevent and detect such threat. The hack saw more than 250 federal agencies and businesses compromised by a state-sponsored actor, which prompt the US to impose new sanctions on Russia in the aftermath.

3 https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/software-security-financial-services-ponemon.pdf
4 https://www.ey.com/en_gl/advisory/how-financial-services-organizations-can-manage-cyber-risk

3.1.2. Flagstar Bank

US-based bank Flagstar Bank fell victim, alongside other organizations, to an Accellion software zero-day vulnerability early in 2021, which resulted in credential theft from "numerous" Flagstar clients and a devastating Cl0p ransomware attack. As well as the bank subsidiary, which provides mortgages and financial services to US customers, this vulnerability also impacted banks and financial institutions across Australia and New Zealand.

The Accellion program, File Transfer Appliance, is a commonly used product for the transfer of large files in an enterprise environment. It has long been discontinued but legacy versions are continued to be used globally. It was in these legacy versions that the zero-day vulnerability was found that lead to this exploitation by attackers.

3.1.3. CNA Financial

In March 2021, CNA Financial reportedly paid $40 million after a ransomware attack stopped the financial insurance company from accessing its company network and data. The staggering ransom is predicted to be one of the largest payments met by a victim to date, surpassing the infamous Colonial Pipeline attack of 2021 by almost ten times by comparison.

In a Consumer Protection Bureau notification[5], CNA Financial reported the threat actor gained access to an employee workstation with a fake browser update executed upon accessing a legitimate website. Then the threat actor conducted further malicious activity to steal credentials with elevated privileges, ultimately destroying back-ups and deploying ransomware. Prior to encryption, the attackers exfiltrated data from the affected systems to a MEGA cloud-based account.

The insurance company was swift to bring in outside aid in the form of cybersecurity experts and law enforcement but ultimately this was too little too late, and should serve as a warning for other financial institutions when it comes to the potential severity of ransomware attacks.

4. Cyberthreats targeting the finance sector

This section outline some, but not all, cyberthreats which are actively targeting the financial services sector, supported by intelligence gathered by Blueliv's infrastructure. Each of these areas should be a focus as they enable cybercriminals to commit fraud, successfully breach enterprises, cause reputational damage and lead to non-compliance penalties.

4.1. Credential theft

Credential theft is often the initial access vector of a successful attack. We go into significant detail on this topic and use cases in our dedicated report on The Credential Theft Ecosystem. All it takes is a single good credential to gain access to an organization and cause havoc. Once credentials are captured, they can be used in a variety of ways, depending on their type.

5 https://www.doj.nh.gov/consumer/security-breaches/documents/cna-financial-20210712.pdf

All industries are impacted by credential theft and can be used to commit many different types of fraud when an account is taken over, from transfers and purchases to money laundering and insurance scams. In some specific cases compromised accounts can be used to perform fraudulent actions like sharing malicious links with other users.

These account takeovers can also lead to blackmail. With access to accounts or systems, sensitive and confidential information is not sold but ransomed to the legitimate owners. There are a variety of ways cybercriminals can turn a profit, regardless of sector, from using phishing techniques to exploiting vulnerabilities to using malware. The faster detect compromised credentials, the better. Detecting compromised credentials at an early stage – within days after they are compromised – can massively reduce the impact of an attack.

Get started with our Credentials Module

4.2. Phishing

Phishing is a seminal technique used by cybercriminals to steal credentials and personally identifiable information (PII) from its victims. It remains one of the most effective attack vectors, due to the fact that it is normally used together with social engineering techniques to extract information from its victims. The goal is to trick the email recipient into believing that the message is important and/or something they need to act on, say, a request from their bank, or a note from someone in their company. The attack typically comes in the form of a link or an attachment.

What really distinguishes phishing is the form the message takes: the attacker cleverly disguise themselves, posing as a trusted entity of some kind, often as a real or conceivably real person or company. Phishing techniques are becoming increasingly sophisticated and continue to have a decent return of investment (ROI).

Get started with our Domain Protection Module

4.3. Business Email Compromise (BEC)

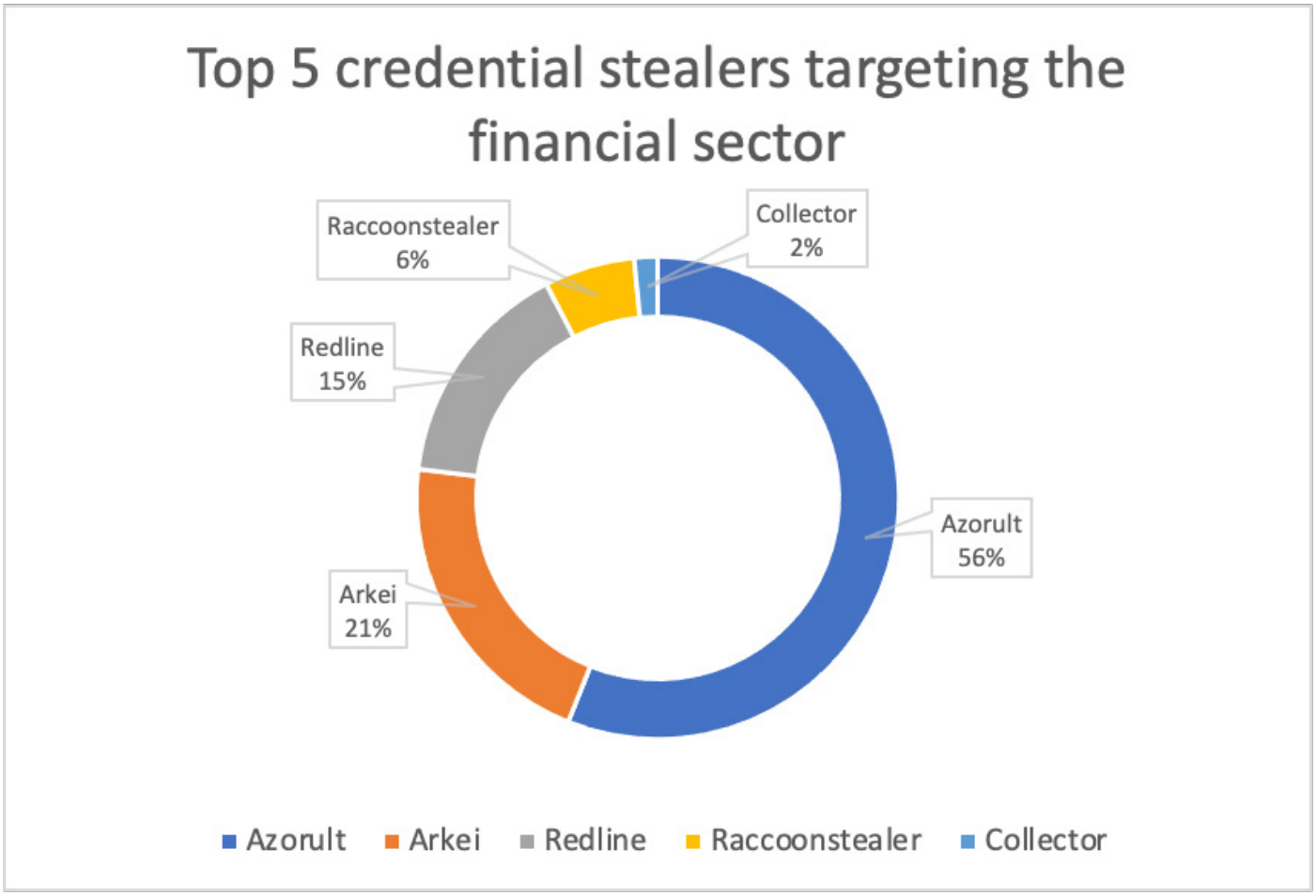
A business email compromise (BEC) attack is a type of exploitative hack in which malicious actors obtain access to a business email account and imitate the owner's identity or use a spoofing email address to look like the legitimate email address. Their objective is to defraud the company and its employees, customers or partners. In this way, BEC attackers are able to gain access to critical data and infiltrate all sorts of company systems and networks.[6] In many instances, attackers will focus their efforts on the employees with access to company finances and attempt to trick them into performing wire transfers to bank accounts owned by the criminals.

4.4. Malware infection

Malware distribution campaigns may use email as an attack vector amongst a variety of others. The malware could have different purposes, including stealing credentials. According to Blueliv's data, the top five malware stealers used for credential theft specifically targeting the financial services sectors as of October 2021 are Azorult, Arkei, Redline, Raccoonstealer and Collector.

Get started with our Malware Module

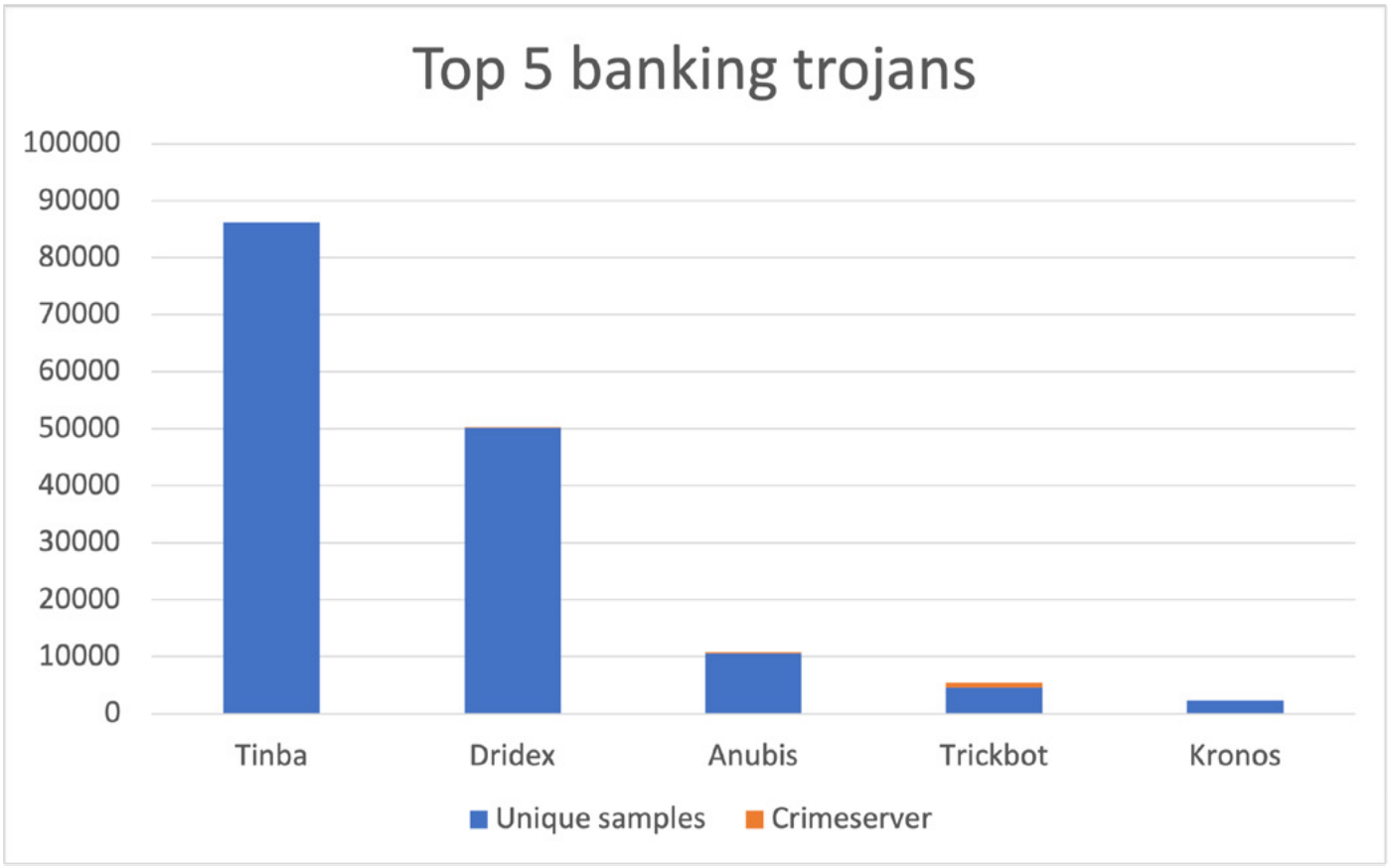
6 https://www.weststarbank.com/our-info/bec-attacks--what-they-are-and-how-to-protect-yourself



4.5. Banking trojans

Malware infections are among the most popular attack vectors used by adversaries. A banking trojan is a malicious computer program designed to steal sensitive and confidential information stored or processed through online banking systems. Banking trojans may use form-grabbing, code injection and specific stealer modules dropped in the infected machines to harvest sensitive data and may masquerade as a legitimate piece of software in order to dupe victims into downloading the malware.

According to data collected by Blueliv's infrastructure, this chart represents the most used banking trojan botnets targeting the financial sector since the beginning of 2021.



(Sorted by total = unique + crimeservers)

Most observed infections are related to Tinba (aka TinyBanker), a banking trojan discovered in 2012 known for its small size of approximately 20KB. Back in July 2014, Tinba source code was leaked, leading to the release of variants with new features.

Dridex is the second most distributed trojan during this period. This malware is especially dangerous because it is often used to deploy second-stage malware such as the BitPaymer and DoppelPaymer ransomware. Comparing the statistics to our 2019 report, Emotet was the most distributed trojan and currently is not active anymore. On the other hand, Trickbot is still active, but it has decreased from second to sixth position.

4.5.1. How a banking trojan campaign works?

Blueliv analyzed a campaign successfully targeting financial entities in Spain and Latin America. The immediate objective of the campaign is the installation of a banking trojan on the users' systems, with the goal of stealing sensitive financial information that can be used to perform fraud. The malware is distributed through a massive email phishing campaign, delivering what appears to be electronic invoices in PDF with a download link. The link downloads a ZIP file impersonating a PDF, but in fact leads to its payload hosted in Dropbox.

4.6. Webinjects

Trojans have at their disposal multiple functionalities that allow them to steal the victim's information, such as

man-in-the-browser techniques, keystroke logging, and form grabbing. Blueliv monitors botnet configurations as new functionalities have started to spread among banking trojans in recent years. These functionalities include webfilters, dnsfilters and webinjects.

A webinject is a tool used to intercept data after it is decrypted from SSL but prior to its display in the browser. Consequently, it gives the trojan the ability to manipulate the way the web page renders in the victim's browser. They allow attackers to steal credentials when they are inputted on the web page as well as the opportunity to create requests for additional information not requested by the bank, such as PIN numbers. Inserting malicious Javascript code allows the attackers to perform a multi-stage attack where different HTML code is injected depending on the online banking page the user is visiting at that moment.

4.7. Ransomware

Ransomware is a form of malware that encrypts the victim's files. The attacker holds the victims' information and files hostage, demanding a ransom to restore access to the data upon payment. A particular window of time is usually specified in which to deliver the ransom, and the cybercriminal usually requires payment in Bitcoin or another anonymous form of payment. After receiving payment, the cybercriminal may provide an avenue for the victim to regain access to the system or data.

Since 2020, many prominent ransomware gangs have implemented double extortion to the attacks, exfiltrating data from targeted systems prior to the encryption and threatening victims with data leak if the ransom is not paid. Leveraging this new strategy, many ransomware gangs have increased the ransom amounts and escalated the number of attacks, buying compromised corporate access from initial access brokers[7] offering their services in underground forums. Ransomware targets are mostly opportunistic, aimed at obtaining the ransom amount as possible.

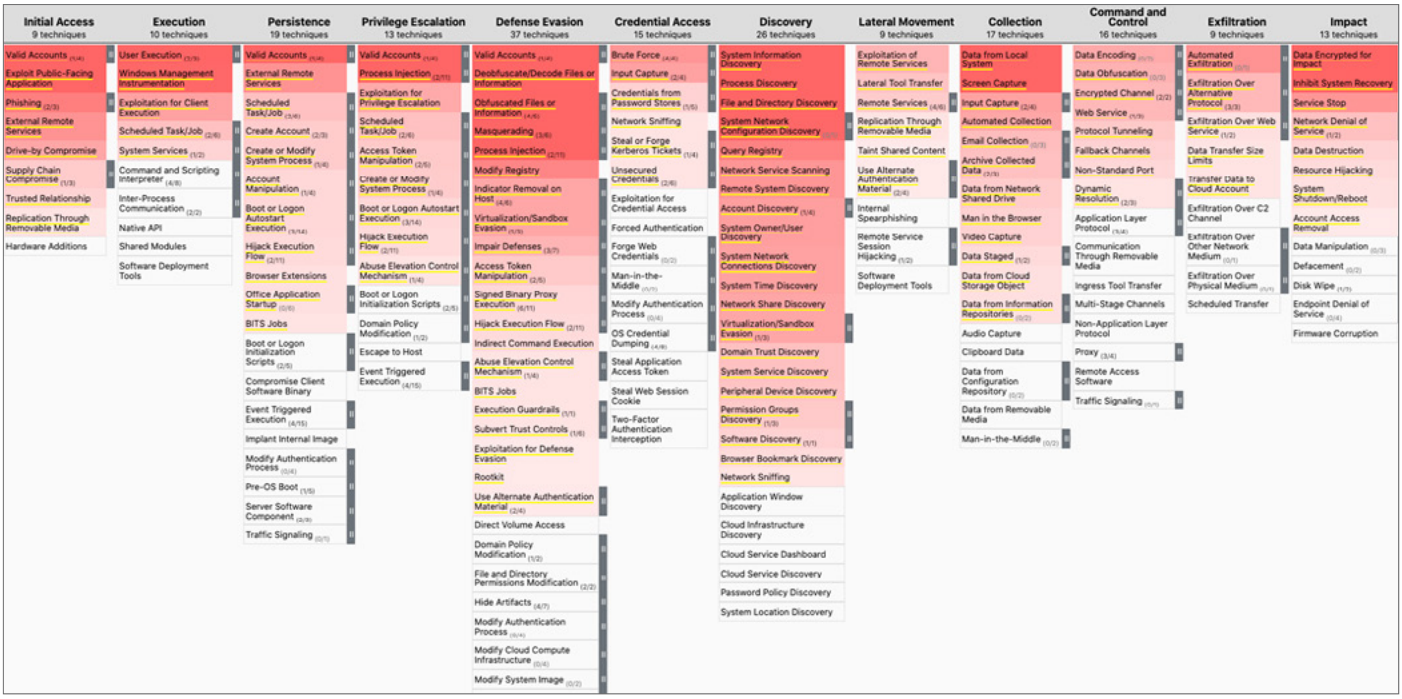
There are a number of ways individuals and organizations can fall prey to ransomware. One common way that ransomware can be delivered and gain access to a computer is spam – attachments that come to the victim in an email, masquerading as a file they trust. Once they are clicked on, downloaded and opened, they can take over the victim's computer. Moreover, more aggressive forms of ransomware, like NotPetya, exploit security holes to infect computers without needing to trick users.[8]

Many researchers have asserted that the majority of ransomware incidents are the result of a cybercriminal gaining access to a poorly-secured or misconfigured remote desktop protocol (RDP) servers. RDP servers represent a direct entry point into an organization's network and, in a departure from many of the attack vectors that security professionals typically deal with, rarely rely on victim interaction to be weaponized. Others use malware such as Dridex and Trickbot as entry points.

In order to prevent ransomware attacks it's crucial to understand how ransomware gangs operate, learning how the attackers typically gain initial access to networks, establish persistence, move laterally, and exfiltrate stolen data. Blueliv analysts have gathered and highlighted the most common TTPs used by prominent ransomware gangs from the MITRE ATT&CK for enterprise framework. In the image below,

7 https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/use-of-initial-access-brokers-by-ransomware-groups/

8 https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html



Most used MITRE ATT&CK TTPs by ransomware gangs

Financial institutions must take the necessary precautions to protect themselves from ransomware and know how to proceed when suffering an attack. The most effective measure is to have properly stored backups – which are separate from the main systems – so systems can be easily restored with data intact. All employees should be trained in cybersecurity to lower the chance of human error as an infection vector, and systems should always be up to date with the latest patches to protect against publicly known exploits. It is also advised that organizations should never pay the ransom. The losses may be higher, but it is the most effective way to dissuade actors from using this kind of malware in the future.

4.8. Mobile apps malware

Despite high levels of intended security, many banking apps have flaws and vulnerabilities that can be exploited which put user data at risk. Mobile banking trojans in particular are "one of the most rapidly developing, flexible and dangerous types of malware,"[9] and have functionalities that include credential theft as well as stealing funds from mobile users' bank accounts.

Recent research highlights a year over year increase of 129% in malicious actors targeting smartphones since 2019, in part due to an increased use of mobile banking applications.[10] Malware builders are available to purchase in underground forums, often developed with advanced evasion techniques to remain undetected on infected devices – such as Anubis, which utilizes device motion sensor information. If it does not detect movement, the malware will not deploy its payload in case it is in a sandbox environment.[11] It is recommended that users check permissions requested by any app they download - ideally from an official app store - and try to ensure these permissions correspond with the app's actual tasks.

9 https://www.finextra.com/pressarticle/78517/kaspersky-reports-rise-on-mobile-banking-malware
10 https://www.threatfabric.com/blogs/the-rage-of-android-banking-trojans.html
11 https://www.zdnet.com/article/these-malicious-android-apps-will-only-strike-when-you-move-your-smartphone/

Get started with our Mobile Apps Module

4.9. Point of Sale malware

When consumers purchase goods or services from a retailer, the transaction is initially handled by Point of Sale (PoS) systems. PoS systems consist of the hardware (e.g. the equipment used to swipe a credit or debit card and the computer or mobile device attached to it) as well as the software that tells the hardware what to do with the information it captures.

The information collected when consumers SWIPE a credit or debit card at a PoS system consists of the card's track data, the information about the card encoded on the magnetic stripe. In recent years, malware affecting PoS systems has gained popularity among cybercriminals. Unrelated to malware, in some circumstances criminals attach a physical device to a PoS system to collect card data, called skimming which will be covered in a later section on Credit card theft.

In other cases, cybercriminals deliver malware which acquires card data via RAM scraping, then passing the stolen information to the criminal. The data can be used for immediate gain or sold on other bad guys who use the data to create fraudulent cards. A combination of hard-to-detect data-exfiltrating malware, legacy hardware, which is difficult to patch, and general OS vulnerabilities mean that this particular threat is common and tricky to defend against.

Get started with our Credit Cards Module

4.10. ATM malware

ATM malware is malicious software designed to compromise ATM machines. The malware is often physically installed in the targeted ATM by the criminal or their associates themselves. ATM malware is used in "jackpotting" in which attackers install malware that causes ATMs to dispense large sums of cash on command. ATM malware can also be used to steal personal financial information at ATM terminals, such as payment card numbers and PIN numbers.[12]

4.11. Pharming

Some malware families perform what are known as pharming attacks. These attacks modify legitimate DNS responses to return malicious IPs rather than the legitimate website IP, by modifying the host's file or hijacking and modifying DNS responses via API hooking. The attackers then redirect the victims to the malicious server where a phishing page is normally hosted.

4.12. Digital card skimmers

Digital skimmers have received attention recently as online retailers are attacked alongside instore transactions. The number of threat actors operating under the researcher-coined umbrella term "Magecart" and leveraging digital skimmers increased significantly, demonstrating that steps to eradicate payment card-related fraud has shifted cybercriminal resources.

12 https://www.cyber.nj.gov/threat-center/threat-profiles/atm-malware-variants/

Digital skimmers are scripts designed to steal data entered into online payment forms, and threat actors use these on the compromised websites of entities or third-party suppliers. Research suggests that the actors often use vulnerabilities in the website/CMS or take over the hosting/CMS accounts to facilitate crime.

Magecart groups got its name from the first attack identified back 2015 targeting the e-commerce platform Magento. Later in 2016, they hacked numerous e-commerce websites using the CMS such as Magento Commerce, Powerfront CMS, and OpenCart.

The groups injected Javascript code into the sites thereby allowing the attackers to capture the payment card information introduced in the payment form. Since these attacks, it seems that these various Magecart threat actors have established the modus operandi of injecting Javascript code in order to capture and steal the customer's payment data. This is clearly a major problem for financial institutions.

4.13. DDoS attacks

A distributed denial-of-service (DDoS) attack is when a website or network is made unavailable by flooding or crashing the website with too much traffic.[13] DDoS attacks inflict damage by utilizing multiple compromised computer systems as sources of attack traffic. These can include computers and other networked resources such as IoT devices.[14]

An increased availability of off-the-shelf tools as well as a proliferation of "stressor" and "booter" DDoS-for-hire websites means that the barriers to entry have massively decreased in recent years. Attacks target the bandwidth of sites and are designed to disrupt business function, severely damaging traffic and databases. As a result, a successful attack can lead to huge losses. Even a smaller attack which overloads servers and takes a site down for a few seconds could frustrate customers enough to look elsewhere. Equally, attackers might seek to extort money from an organization by simply threatening a DDoS attack, a technique that we observed ransomware groups recently.

These types of attacks are a significant risk to financial services institutions since revenue will likely be disrupted as a direct result of an attack. Furthermore, costs for remediation and even customer compensation should be added to the bill. We expect that DDoS attacks will continue in the near future, surpassing 2 Terabyte Per Second (Tbps) and include more ransom demands to increase the financial benefit.

4.14. Cryptojacking

Cryptocurrency is an ever-present market that moves millions each day with little to no control by authorities. With increased popularity, there are now trading with cryptocurrency and online wallets managing and exchanging different cryptocurrencies, both of which present a target to attackers.

The fact that many of these cryptocurrencies are designed with privacy and anonymity in mind makes it difficult to protect the victims, minimize the damages and catch the criminals, leaving investigation and compensation in hands of the affected companies.

Cryptojacking is the unauthorized use of someone else's device to mine cryptocurrency. Cybercriminals can

13 https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html
14 https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

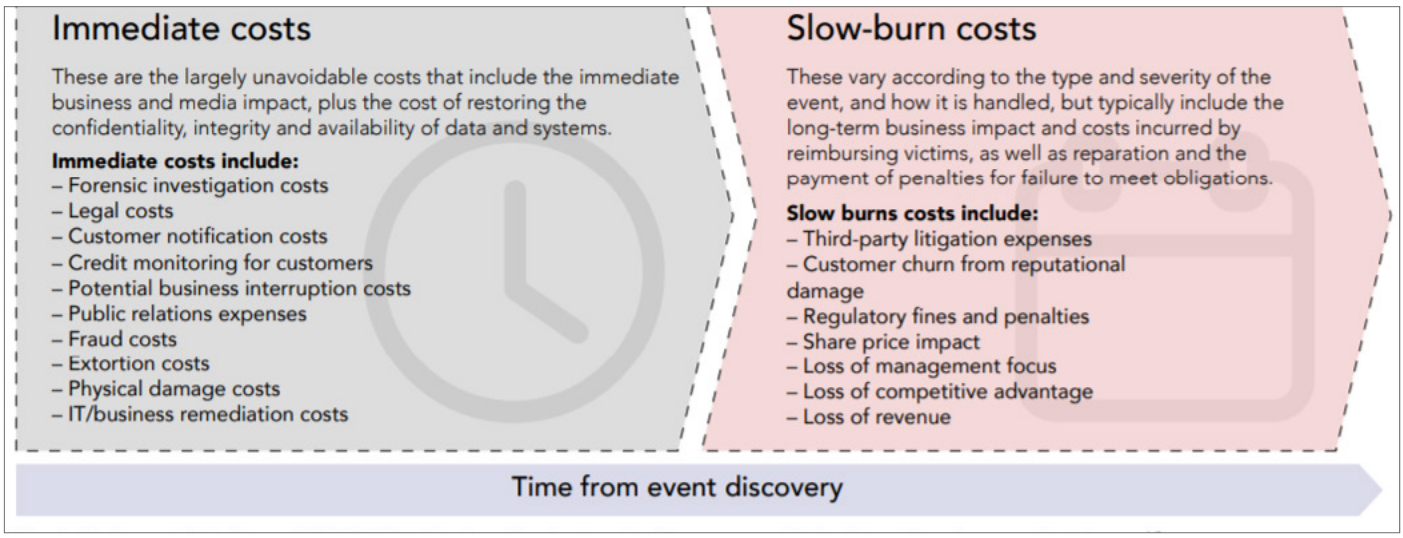
accomplish this objective a number of ways, such as getting the victim to click on a malicious link in an email that loads cryptomining code on the computer, or by infecting a website or online ad with JavaScript code that infects once loaded in the victim's browser, among other surreptitious techniques.

Whichever method is used, the cryptomining code then works in the background, undetected, as unsuspecting victims use their computers normally, albeit with potentially slower performance or lags in execution.[15]

Since the malware cybercriminals use to gain control of vulnerable online assets is delivered directly to end points, there is unfortunately little institutions can do to prevent attacks. However, detection is key. Detection is an extremely important and valuable tool within the context of an overarching mitigation program. If banks can pinpoint treacherous code, they can jump on it and quickly take steps to reduce the likelihood of infection.

4.15. Data leakage

Data leakage is the unauthorized transmission, or leak, of data from within an organization to an external recipient. This can refer to data that is transferred electronically or physically. Data leakage threats usually occur via the internet and email but can also happen via mobile data storage devices like USB drives and laptops. The damage caused to any organization can be extremely difficult for them to dig themselves out of both on a technical and regulatory level.[16] The below diagram illustrates the costs associated with a breach.



KPMG July 2017, Closing The Gap: Cyber security for the Insurance Sector, p.5 [17]

Get started with our Data Leakage Module

4.16. Account Takeover

Account takeover (ATO) is a form of identity theft in which a malicious threat actor gains unauthorized access to a legitimate user account. Once in control, the attacker can change the personally identifiable information related to this account, change the password, make fraudulent wire transfers, and purchase or request a new bank card, for instance.

15 https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html
16 https://www.forcepoint.com/cyber-edu/data-leakage
17 KPMG July 2017, Closing The Gap: Cyber security for the Insurance Sector, p.5

In fact, financial services organizations are one of the most lucrative targets for account takeover fraudsters since they can not only directly steal funds from users but also obtain personal information that can be later sold on the dark web.

The tactics that attackers use are sometimes as simple as sending bank-themed phishing emails that ask users to click on a malicious link and log into a legitimate-looking web page that is in fact created and controlled by the attackers. Another tactic that fraudsters use is to search for publicly available leaked databases containing credible user credentials which they then upload to and process through free automated tools such as Sentry MBA. If the credentials were also valid on another website, then this is known as a credential stuffing attack which typically happens when users reuse passwords across different accounts and platforms. Unfortunately, credential stuffing attacks can be very effective as a Google Security Survey from 2018[18] found that 52% of individuals reuse the same password for multiple (but not all) accounts, and 13% reuse the same password for all their accounts. In fact, attackers often use scripts that contain potentially thousands of usernames and passwords. They also perform the so-called dictionary attacks during which threat actors use common passwords and dictionary terms to guess passwords. Account takeover fraudsters demonstrated creativity in that they also started calling potential victims directly on the phone pretending to be bank officers. The purpose of this call is to notify users of suspicious transactions and offer them help once they verify their identity, together with the code sent in a text message or push notification. In separate cases, fraudsters can also ask users to install malicious software which typically enables remote access.

Account takeover fraudsters could also be seen sending phishing emails from an account of an employee of a financial organization that they took over. This could be, for example, the account of a financial director who is asking a member of his team to urgently pay an invoice to a client. This social engineering tactic is also known as whaling. Access to someone's mailbox can also be extremely valuable since attackers could exfiltrate data that they can sell later to other threat actors in the underground who would like to easily gain initial access to a specific target.

Financial loss and reputational damage are amongst the consequences of a successful account takeover attack against financial sector organizations. In fact, according to a 2021 study from Aberdeen Group[19], companies in the financial services sector can lose 1.9 to 8.3% of their annual revenue due to an ATO or $3.38 million on average.

4.17. Third-party exposure

Data breaches often start with the compromise of suppliers, contractors and vendors, and it is not only the individual victim's problem if their data is exfiltrated. Third-party risk management is an issue that is increasingly causing stress for many security leaders.

59% of organizations attribute security issues involving data loss to vendors or other third parties, according to a 2018 study from Opus and Ponemon Institute. It is common in today's interconnected business world for companies to share data with vendors. Whether it's sharing data or allowing other companies system access, it is no longer enough just to ensure that your organization's network and enterprise web presence are secure. Your risk management program must look beyond your own organization to properly scrutinize and vet the third and fourth-party vendors who will have access to your data without being privy to your internal risk management

18 https://services.google.com/fh/files/blogs/google_security_infographic.pdf
19 https://www.perimeterx.com/resources/reports/quantifying-the-impact-of-credential-stuffing-and-account-takeovers/

process.[20]

This risk also extends to talent. There are considerable difficulties in hiring and training IT professionals, and so outsourcing to vendors for backend development (for cloud integrations, app development, mobile payments, for example) can leave financial institutions at risk to new cybersecurity challenges.

4.18. Hacktivism

With the heightened sense of political awareness across society in recent years, criminals regularly engage in agenda-driven attacks as opposed to spreading malware for purely financial reasons. Hacktivism is the act of exploiting a computer system or network for a socially or politically motivated reason. Hacktivism, at a baseline level, describes groups or individuals who plan to affect political change and damage their ideological opponents.[21] Hacktivist attacks generally comprise DDoS attacks, publishing confidential information, website defacements, website redirects, and doxxing.

In the current climate the financial services sector is particularly vulnerable to this type of cyberthreat.

Get started with our Hacktivism Module

5. Threat Actors

Certain threat actors are responsible for the most complex and longer-lasting campaigns and attacks in the cybersecurity landscape. They present a major threat against the availability, integrity and confidentiality of the information of any entity and usually target big corporations and governments

In this section, we highlight some of the key actors and campaigns targeting organizations in the banking and financial services sector. All of this information and considerably more detail is available using Threat Context, Blueliv's powerful enrichment tool.

5.1. Lazarus Group

Lazarus Group has been linked to some of the most notorious cyberattacks in recent history, and some researchers have suggested that it may be backed by the North Korean government. In the past few years, the group has carried out several heists at traditional financial institutions and cryptocurrency exchanges around the world.

Lazarus Group's activity dates back to 2009, with some analysts suggesting that the group has been active since as early as 2007. The group has been linked to some of the most notorious hacks in history, including the 2014 attack against Sony Pictures Entertainment, the 2016 Bangladesh Bank heist, and the 2017 WannaCry ransomware outbreak. In late 2015, Lazarus Group began to move away from the use of DDoS and wiper malware in their attacks and began to experiment with compromising financial institutions and carrying out SWIFT heists – that is to say, successfully initiating and cashing out fraudulent SWIFT transfers. This also represents a possible change in motivation - pursuing financial gain for the first time.

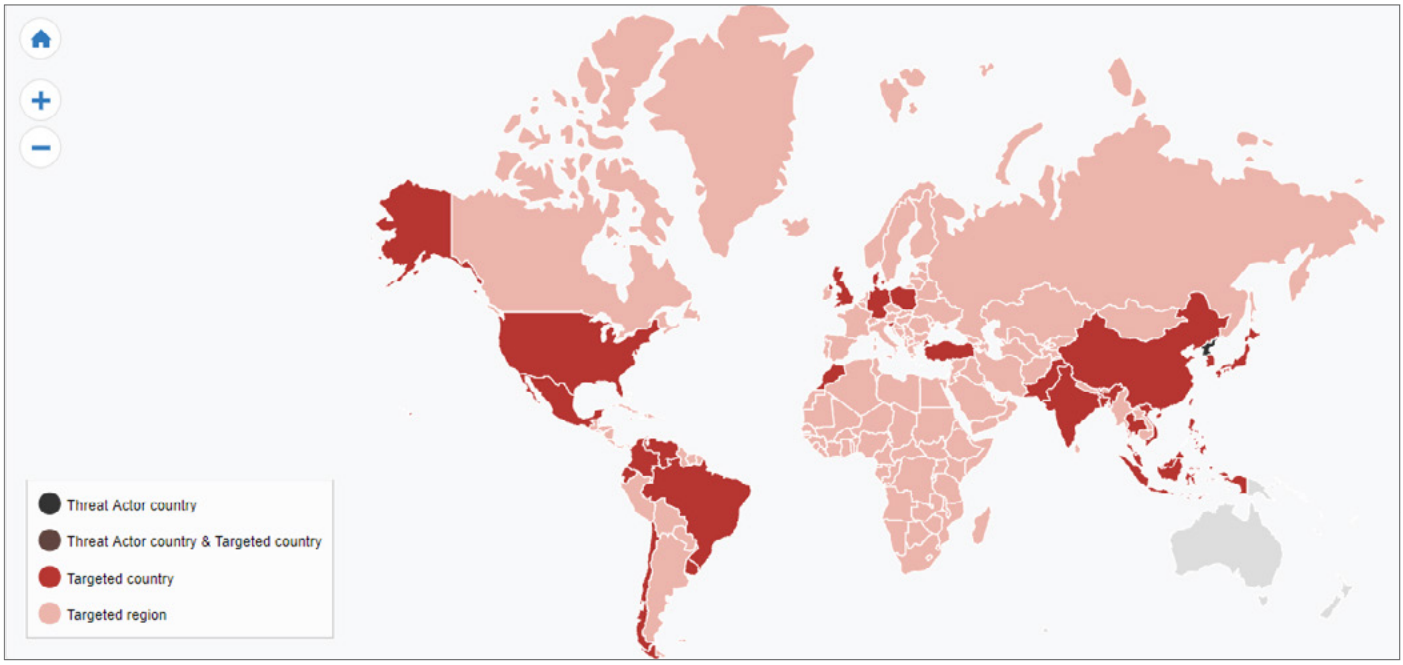
20 https://www.upguard.com/articles/five-things-to-know-about-third-party-risk
21 https://www.itpro.co.uk/h acking/30203/what-is-hacktivism

Since that time, Lazarus has continued to target financial institutions with the goal of carrying out SWIFT heists. In recent years, targets included financial institutions in the US, Mexico, Brazil, Chile, Venezuela, Colombia, Uruguay, UK, Denmark, Poland, Turkey, China, Taiwan, and Hong Kong. Lazarus Group also targets cryptocurrency exchanges, with Chinese firm 360 Security linking the theft of funds from cryptocurrency exchanges Etbox, Biki, and Dragonex to Lazarus Group.

Much of Lazarus Group's original targeting has historically focused on South Korea and the United States. With time, however, the group has displayed more opportunistic targeting, compromising entities from around the globe. This shift in targeting is in line with Lazarus Group's shift towards pursuing financial gain. Lazarus Group is considered highly sophisticated and adaptive. Some analysts have suggested that the threat group may interact with Russian-speaking cyber criminals due to their use of crimeware products such as Hermes ransomware.

In 2021, the US Department of Justice indicted three North Korean military personnel associated with this threat actor. While this is unlikely to slow the group down, the three's trial indicates the success and ambition of the Lazarus Group and should serve as warning to financial institutions globally of the scale of these attacks.

Among the convictions was the theft of over $1.3 billion of cash and cryptocurrency, as well as a further attempted theft of $1.2 billion from banks across Africa, Bangladesh, Malta, Mexico and Vietnam after infiltrating their networks and launching fraudulent messages through the Society for Worldwide Interbank Financial Telecommunication.



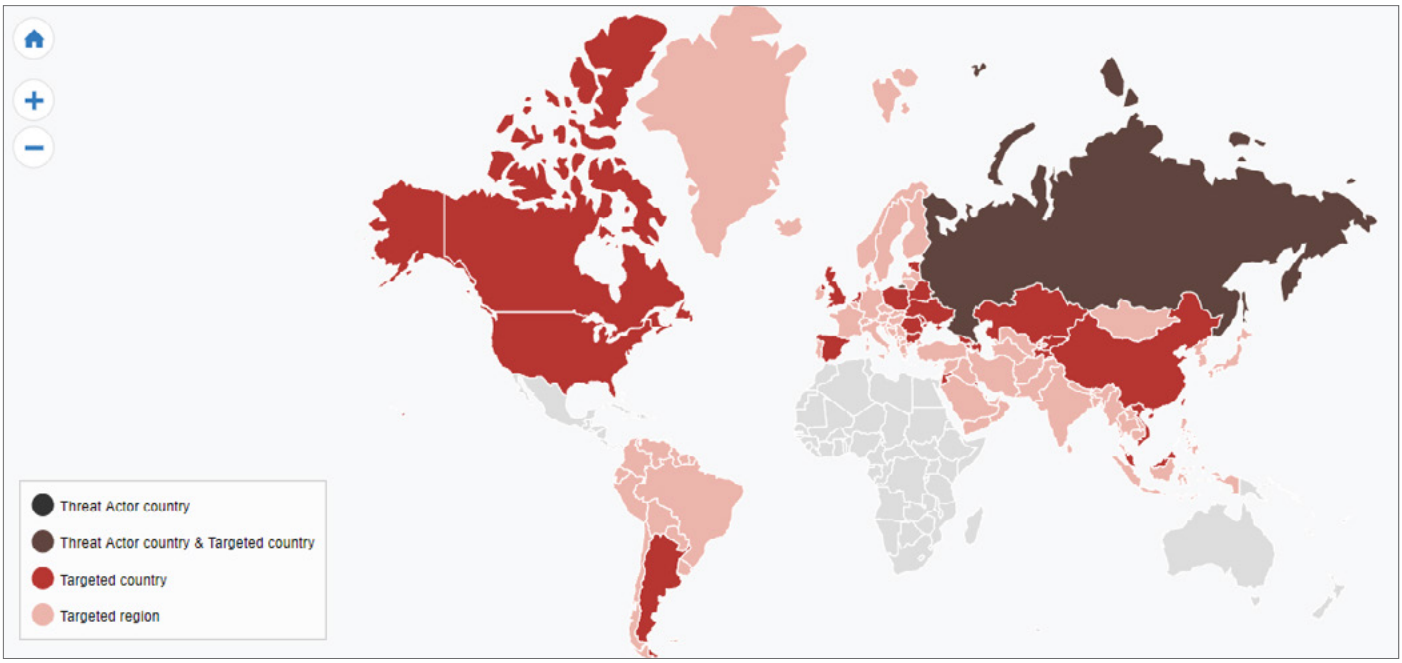
5.2. Cobalt Gang

The Cobalt Gang is one of the biggest threats to global financial institutions. This threat group has targeted FSIs around the world, including dozens of targets primarily located in Western Europe, Eastern Europe, and Central Asia. The group has proven a willingness and ability to adapt to changing circumstances.

Cobalt Gang first came onto the scene in 2016 with the ATM jackpotting attack on First Commercial Bank in

Taiwan. It typically sends spear-phishing emails to distribute malware, then pivots in order to gain valuable access before cashing out via several different money-making schemes. The group has been found responsible for ATM jackpotting and supply chain attacks as well as attacks on payment gateways and card processing systems. Researchers have uncovered a good deal of evidence connecting the Anunak Gang to the Cobalt Gang.

In March 2018, Europol announced that one of the leaders of the Anunak/Cobalt Gang - simply referred to as Ukrainian "Denis K." - had been arrested. Despite this, the Cobalt Gang is believed to be alive and still operating as the group continued to attack financial institutions across the globe, shifting from POS campaigns to conducting ransomware attacks[22].



5.3. FIN7

FIN7 has aggressively targeted various entities in several major sectors, including financial services. While this financially motivated cybercrime group is primarily known for their theft of payment cards from dozens of US-based retailers and restaurants, the group has also targeted European and Asian targets, and it is capable of compromising big companies.

The group uses techniques to distribute point-of-sale (PoS) malware, often combined with remarkably bold social engineering techniques, such as calling up victims to ensure they open malicious files. Since appearing in 2015, the group has compromised hundreds of companies, thousands of PoS terminals, and millions of payment cards. FIN7 has been linked to high profile breaches at Arby's, Chili's, Chipotle, Red Robin, Jason's Deli, and Sonic. After a successful breach, FIN7 typically offers the compromised cards for sale on the underground card shop 'Joker's Stash'.

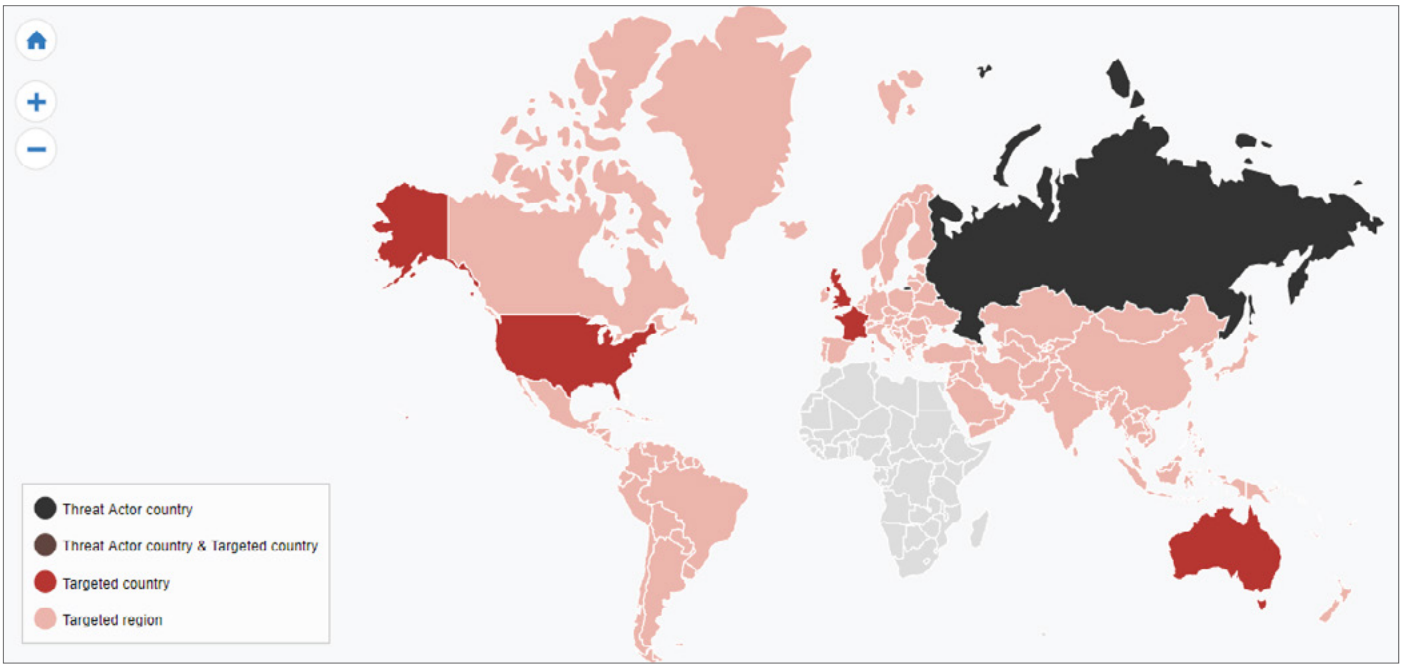
Researchers have uncovered that in addition to large compromises of payment cards, FIN7 occasionally chooses to utilize their access to pivot towards finance departments. US law enforcement has also reported FIN7-linked phishing emails posing as the US Security and Exchange Commission (SEC) targeting individuals with access to

22 https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/

documents that may prove useful to those who want an advantage in stock trading.

In August 2018, the US Department of Justice (DOJ) announced that three members of FIN7 had been arrested. In the announcement, the DOJ revealed that FIN7 used a front company called "Combi Security" to carry out at least a portion of their activities. Combi Security masquerades as a legitimate company headquartered in Russia and Israel and has posted on job recruitment boards in Eastern Europe and Central Asia. Membership of the group is primarily Eastern European. As recently as 2020, FIN7 also added ransomware and data exfiltration attacks to its arsenal, selecting targets according to revenue using the ZoomInfo service. ZoomInfo is a popular tool for identifying sales opportunities.

Throughout 2020 and 2021, the group continued to target financial and other industries globally, including financial attacks in Panama, IT organization attacks in Europe, and several healthcare and educational institutions across the US.



5.4. Dridex Gang

The Dridex Gang has evolved during the past years from managing a successful banking botnet and targeting bank clients to dropping backdoors and ransomware in specific computers previously infected with Dridex. There are several cases where big companies have suffered major losses when this group targeted them and infiltrated their networks. The Dridex Gang is linked to Dridex, Locky, and BitPaymer.

The group is primarily focused on developing, distributing, and profiting from banking trojans and ransomware. The Dridex Gang has been linked to Dridex (a successor of Bugat, Cridex, and Feodo) and Locky; researchers at ESET have also linked the developers of Dridex to BitPaymer (also known as FriedEx). The group is primarily comprised of cybercriminals from Eastern Europe, including cybercriminals from Moldova, Romania and Russia, with Westerners enlisted for help in conducting money laundering schemes.

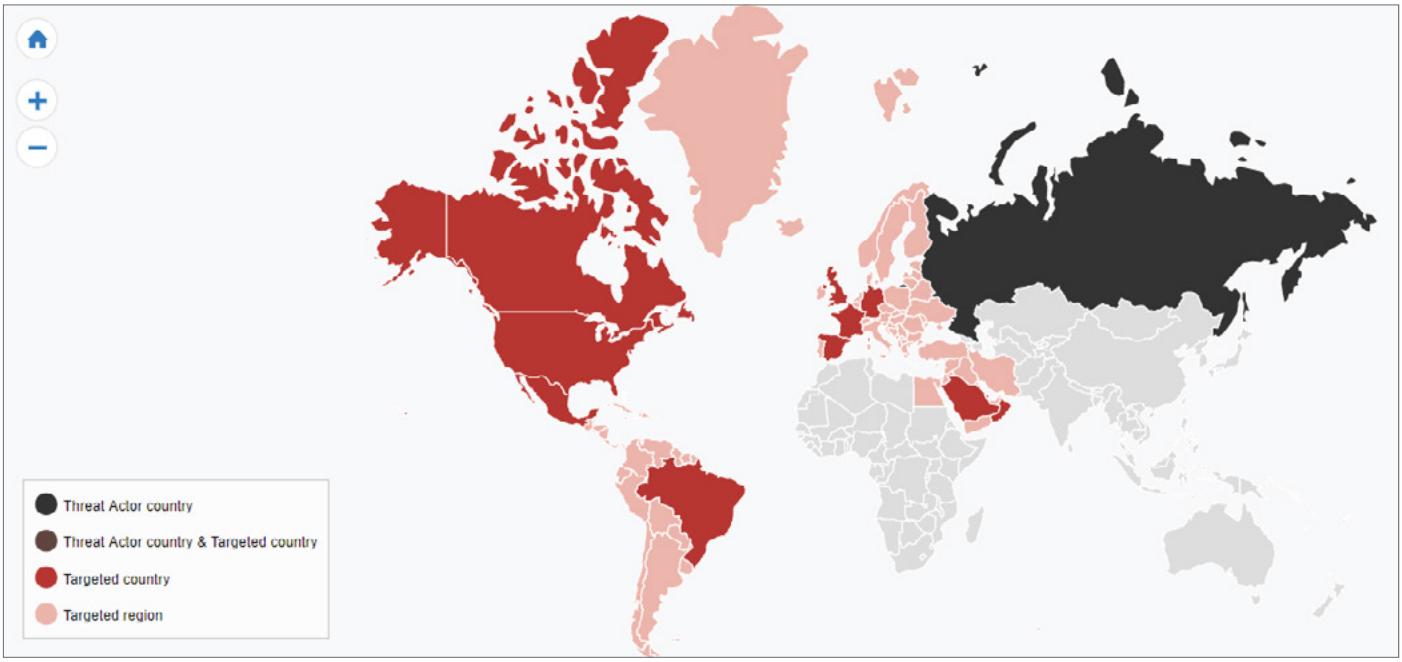
Dridex first appeared in July 2014, only a couple months after the May 2014 law enforcement takedown of

GameOver Zeus. For this reason and others (such as code similarities between GameOver Zeus and Dridex), the Dridex Gang is hypothesized to be an offshoot of the gang behind GameOver Zeus (also known as the "Business Club"). One of the supposed leaders of the Dridex Gang, Andrey Ghinkul, was arrested in October 2015. While Ghinkul's arrest led to a drop in Dridex infections in the short term, the gang has proved resilient, despite this high-profile arrest.

In its early years, the Dridex Gang operated like many similar cybercriminal gangs of the time: developing malware, distributing that malware via phishing emails, and cashing out compromised bank accounts. In recent years, however, the Dridex Gang's TTPs appear to be shifting, deploying ransomware on infected systems, and focusing on compromising high value targets. Dridex Gang continues to use the Dridex banking trojan to commit financial crimes and has even updated the trojan to target cryptocurrency exchanges.

In July 2019, a new malspam campaign was discovered spreading fake eFax messages. This campaign was designed to drop two different malwares: the Dridex banking trojan and RMS RAT. By delivering a banking trojan and a RAT, the cybercriminals ensured that they didn't just steal their victims' credentials, but also have a more complex tool to manage the infected computers at their disposal. This strategy also increases the chances of persistence in case one of the malware families happened to be detected, since the second one could still be used as a backup communication channel.

After a brief hiatus following the arrest of two members in 2019, the group continued with low level activity in early 2020 before emerging once more, this time with a new strain of ransomware in its arsenal. The WastedLocker ransomware adds the .wasted extension to encrypted files and is believed to be almost entirely new, despite similarities to existing ransomware in its ransom note. The gang has been transitioning between tools since early 2020, on the occasion of a US Treasury Department's Office of Foreign Assets Control action[23] that prevents companies to pay ransom demands of ransomware attacks attributed to this threat group. As a result, in December 2020 they developed the Hades ransomware, a Wastedlocker variant, in an attempt to mislead attribution and evade the imposed sanctions.



23 https://home.treasury.gov/news/press-releases/sm845

5.5. TA505

TA505 is the name given to one of the more prolific financially motivated threat actors in recent years that targets companies worldwide. A particular characteristic of the group is the extraordinary volume of messages they send on their campaigns, surpassing most other APTs. This malicious group is responsible for some of the largest spam campaigns ever observed.

TA505 was highly active in 2019, launching multiple campaigns against several objectives in multiple countries, such as China, Germany, India and Italy. Their first campaign of 2019's second quarter started in April, when TA505 targeted financial enterprises using LOLBins and a new variant of the sophisticated backdoor ServHelper. This advanced operation combined targeted phishing attacks against a small number of specific accounts within the companies, infecting them with reconnaissance malware with the objective of gathering intel about the victim's environment. Moreover, they used a signed and verified malicious code as an extra precaution to avoid detection. An interesting and unusual particularity is the selective persistence mechanism used by some of the tools in this campaign. Usually, malware will attempt to gain persistence whenever possible, but in this case, they decided whether to establish persistence on the infected hosts or not, only after evaluating each one of them using the information from their reconnaissance malware.

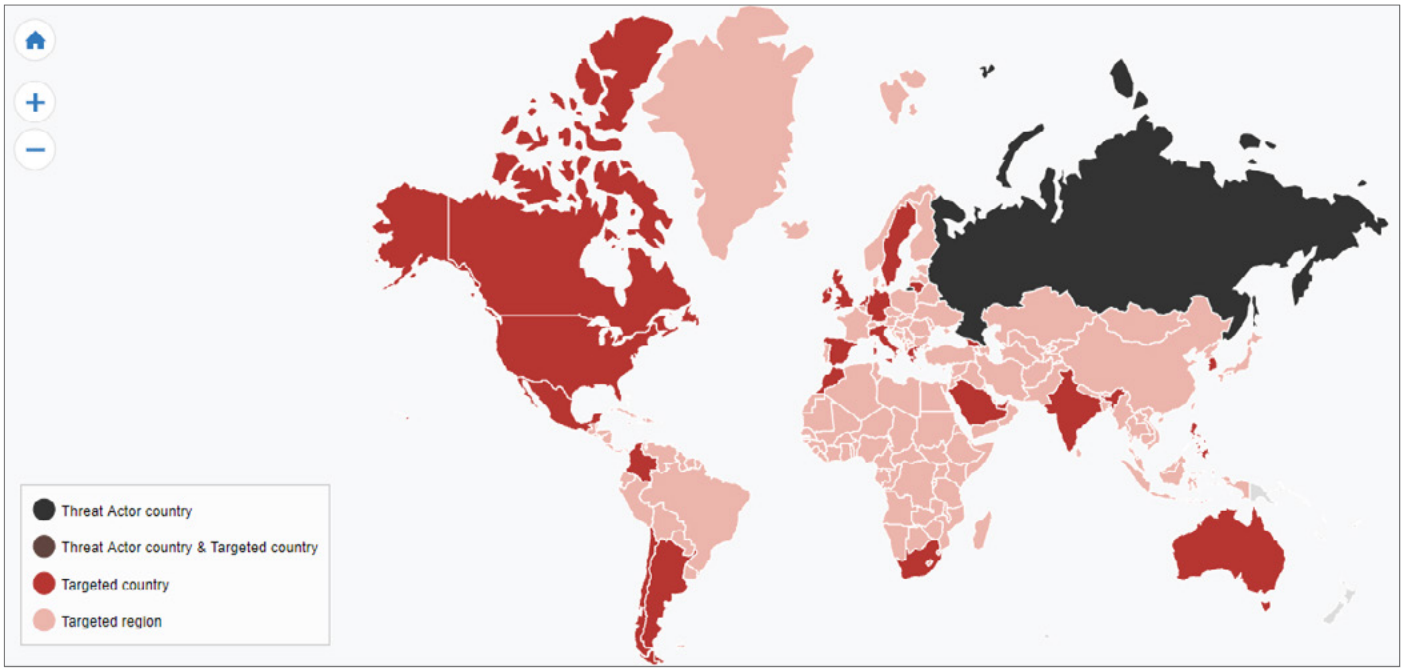
In May of 2019, researchers detected another campaign. In this case, it was not targeted at all, but distributed globally without a specific objective. As in most of their campaigns, TA505 started sending malspam with a malicious excel doc. Right after the opening of the malicious attachment, a remote access tool (RAT) named FlawedAmmy was downloaded and installed on the victim's device. This RAT implemented common backdoor features like file management, remote control, and capture the screen among others. After installing the RAT, the attackers downloaded another executable from a remote server. This signed executable was identified to be an email stealer with the sole purpose of stealing emails and credentials for Outlook and Thunderbird accounts found on the host machine. This information was gathered and sent back to a C2 server in an unencrypted JSON format. A batch script was then executed to delete all traces of the infection, including the stealer and the batch script itself.

At the end of May the same year, researchers reported an email attack against an Italian organization. The malicious email contained a highly suspicious sample which prompted the researchers to investigate its capabilities and its possible attribution, discovering a potential expansion to other industries from TA505.

The intercepted attack started with a spear phishing email embedding a spreadsheet. The document contained a malicious macro code that activated when the user opened it to see its content. The attacker used a couple of Self Extracting Archives (SFX) stages to deploy the Remote Manipulator System (RMS) software. The tool was able to grant remote access and full direct control of the infected machine to the group. It has been possible to observe multiple coincidences in the TTPs of this campaign with those of TA505 during the investigation. The fact that this recent attack hit a company not strictly related to the Banking or Retail sector suggests that the group could be potentially widening their current operations.

Throughout the COVID-19 pandemic, the group switched up its tactics to take advantage of the turbulent and vulnerable healthcare industry, using Locky ransomware and the Dridex banking trojan, complete with a coronavirus lure as part of a downloader campaign. As well as U.S. healthcare, the group used this to target the manufacturing and pharmaceuticals industries.

This change in tactics does not mean that the group has abandoned the financial industry. One of the indications that the financial sector is still a rather relevant target for the group is the observation of the MirrorBlast campaign, conducted by TA505 since at least September 2021. The campaign targets the financial sector in North America (Canada and US), Europe, Hong Kong, and other targets. In this campaign, two initial attack vectors are observed. The first one is phishing emails with a weaponized Excel file attached. Alternatively, the threat actors might send phishing email using the Google feedproxy URL with SharePoint and OneDrive lure, posing as a file share request. When the victim clicks the URL, the landing page is a fake OneDrive or SharePoint page that distributes the weaponized Excel file. This file is weaponized with lightweight macro code (aimed at anti-sandboxing evasion). In the sequence, the attack uses Windows Installer XML Toolset (WiX) that, upon execution, drops files, one being a malicious script. Finally, this malicious script communicates with the attackers' command-and-control structure, which then provides further instruction.



5.6. Shathak

Shathak (aka TA551) is a threat group tied to malware used in the Russian-speaking underground that has been active since at least 2018. The threat group has targeted the energy, healthcare, finance, manufacturing, and insurance sectors in North America, South America, Europe, and Japan.

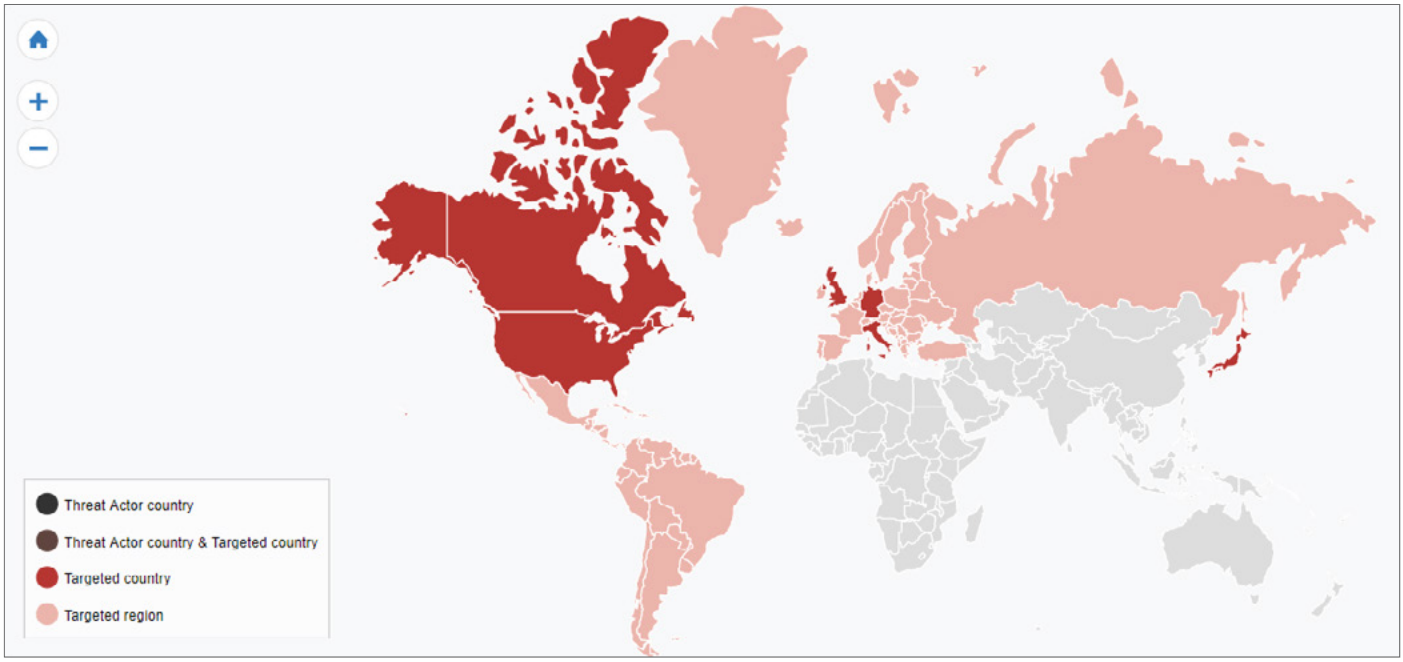
Shathak has carried out malspam campaigns consisting of emails with an attached password-protected zip file. The zip file contained a Microsoft Word document targeting English-, Italian-, German- or Japanese-speaking recipients with macros to install malware. The macros mostly generated a URL ending in a .cab file used to install malware.

The attackers often leverage mailbox data retrieved from previously infected Windows hosts to conduct further spam campaigns, sending the email chain to original senders and recipients, plus an additional comment added to the most recent message providing the ZIP archive password. Until April 2020, Shathak deployed Ursnif malware, before they switched to Valak, an information stealer and malware loader. The threat group often uses Valak as a

loader to install IcedID or Ursnif and to conduct further malicious activities, likely with the objective of profiting financially.

Shathak's IcedID implants were also observed installing ransomware such as Maze and Egregor, leading researchers to speculate Shathak might be partnering with ransomware gangs as an initial access facilitator.

By June 2021, researchers observed Shathak stopped using IcedID in favor of TrickBot, and only a month after shifted to BazarLoader. BazarLoader is spread in maldocs distributed via spam campaigns to infect targeted devices and install follow-up malware, mostly Cobalt Strike.



6. How FSIs can manage their cyber-risk

Despite having a more advanced security posture than organizations in most other sectors, there will always be gaps for FSIs. According to PwC, there are two kinds of financial services firms: those that have faced a cyberattack and those that will.[24]

Organizations must put in place proactive security measures that help them prioritize detection and response, enabling them to react quickly to incidents. This section covers a number of strategies and mechanisms designed to help companies in the financial industry, from SMBs to enterprise-size, to manage their cyber-risk and reduce the impact from cyberattacks which are all but inevitable.

24 https://www.pwc.com/us/en/industries/financial-services/research-institute/top-issues/cybersecurity.html

6.1. Executive level engagement

A cybersecurity strategy needs the full involvement and support from the C-suite and board. Senior leaders are not entrenched in day-to-day security operations and may not always fully understand some of the risks the firm has taken on, whether explicit or implicit. Executives must be more involved in making sure that their business plan has a cybersecurity component and adopt the mindset that it is not complete without one.[25]

6.2. Effective fraud prevention

The financial services sector is understandably ahead of many other industries in terms of prevention and detection of economic crime. However, there is certainly more that can be done by FSI organizations to close cybersecurity gaps. Of particular concern are weak spots in some organizations' fraud risk assessments, whistleblowing mechanisms and overall awareness.[26]

According to a Global Economic Crime Survey by PwC, there are a few things that organizations can do to mitigate fraudulent activities. First, ensure that 'Know Your Customer' (KYC) procedures and Anti-Money Laundering processes are operating effectively across a 'single customer view' – essentially ensuring that all relevant systems and records are paired up for consistency of data. Second, resolve any legacy IT issues. This will help to keep pace with new regulations and new methods of money laundering syndicates.[27]

6.3. Company-wide training and education

Organizations must heavily invest in educating their personnel against attacks and how to recognize them. Good 'cybersecurity hygiene' means implementing proper and robust employee training. Often, companies are so focused on strengthening their cybersecurity technology that they fail to look inward. Employees can be a company's biggest potential vulnerability. In fact, the three leading causes of breaches are often caused by employees, according to a recent report.[28]

Education is therefore a major issue. Businesses need to address these areas by ensuring employees are sufficiently informed and educated about processes and procedures for identifying a threat, correctly responding to any perceived threat and maintaining company-wide compliance.

As a business, understandably, one eye will always be trained on the ROI aspect. Investing in employee education has a significant return on investment. The Ponemon Institute calculated the effectiveness of anti-phishing training programs and found that the average-performing program resulted in a 37-fold return on investment, even taking into account the "loss of productivity" during the time the employees spent in training.

6.4. Incident response readiness

An IBM and Ponemon study found that 49% of the respondents said they did not have a formal cybersecurity incident response plan across their organization. Correspondingly, around half of those who responded overall expressed confidence in their organization's ability to prevent, detect, contain and respond to an attack.[29]

25 https://www.pwc.com/us/en/industries/financial-services/research-institute/top-issues/cybersecurity.html
26 https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf
27 https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf
28 https://www.ibm.com/downloads/cas/GAVGOVNV
29 https://www.ibm.com/downloads/cas/GAVGOVNV

Having established that cyberattacks are inevitable, no matter the organization, there is virtually no excuse to not have a data breach response playbook in place. In an ideal world this should be combined with automated threat intelligence. Automation prevents expensive and overworked security analysts from endless admin that keeps them from delivering true value. Playbooks enable a ready-made response to recognized threat scenarios, ensuring best practice is applied and resources optimized. If the latter become too static, playbooks are also at the behest of a rapidly changing threat landscape and emerging forms of attack. The last thing you want is to act upon irrelevant or out-of-date information. Blueliv's Threat Context solution can give your security teams the toolbox to accelerate their response in front of incidents.

6.5. Continuous monitoring

Continuous monitoring, such as those intelligence services provided by Blueliv or the vulnerability management provided by Outpost24, means that organizational risks are assessed in close to real-time, so that security decision-makers can adequately protect their organization's integrity. In terms of threat intelligence, this means monitoring external threats and leaked confidential assets, as well as all networks, systems and applications. Organizations of all sizes can strengthen their security posture and accelerate security decision-making processes through acting on real-time results. With a smarter and more targeted response to cyberthreats, organizations can allocate security resource more efficiently, proactively getting ahead of future attacks and raising the barrier to entry for cybercriminals intent on breaking in.

6.6. Third party security management

Third parties are essential to the value chain. A financial organization can have hundreds of vendors, depending on its size. Flowing through that value chain are business processes, IT bandwidth and application functionality and data. With this in mind, it is important to make the following distinction: you can outsource systems and services, but you cannot outsource your risk associated with that data and how it is managed.[30]

In the event of a breach, is also important to determine whether or not your organization is prepared to quickly and effectively respond to and communicate with external stakeholders. If a cybersecurity incident occurs, you will need to issue statements and updates to customers, partners, the media, and other interested parties. It is no longer enough to meet baseline technical requirements for post-incident response and communications with regulators and consumers.

6.7. Regulation and Legislation

Generally speaking, financial services organizations worldwide are subject to a considerable amount of cybersecurity compliance regulation. This legislation not only considers data privacy for consumers, but also places obligation on companies themselves. The EU GDPR, for example, enforces that companies should "implement appropriate technical and organizational measures to ensure a level of security appropriate to risk."[31] Given that FSIs have a high level of risk, there is a significant onus on them to invest in cybersecurity tools and solutions to minimize the impact of cyberattacks on the enterprise that could affect their business and customers.

In May 2018, the European Central Bank released the framework for Threat Intelligence-Based Ethical Red

30 https://blog.riskrecon.com/you-cant-outsource-risk
31 http://www.privacy-regulation.eu/en/article-32-security-of-processing-GDPR.htm

Teaming (TIBER-EU)[32]. Following TIBER-EU guidelines, financial institutions can create simulations of cyber-attacks that closely resemble those in the real world, managing cyber risk and improving cyber resilience.

It is clear that in recent years a greater understanding of cyber-risk has forced relevant regulatory bodies to take affirmative action. Though compliance requires significant investment, responding to these challenges encourages a greater understanding of cyber risk and a more effective approach. For more detail on how threat intelligence can mitigate the impact of GDPR, see our special whitepaper here.

7. The role of threat intelligence

Threat intelligence is actionable information, delivered in an automated way so that organizations can detect threats both inside and outside their network, and prioritize their responses. The reason it is so important is that it allows security teams of all sizes to focus their resources – which are often limited – on the most crucial threats targeting their networks and infrastructure. Organizations need to know how to utilize threat intelligence to level the playing field.

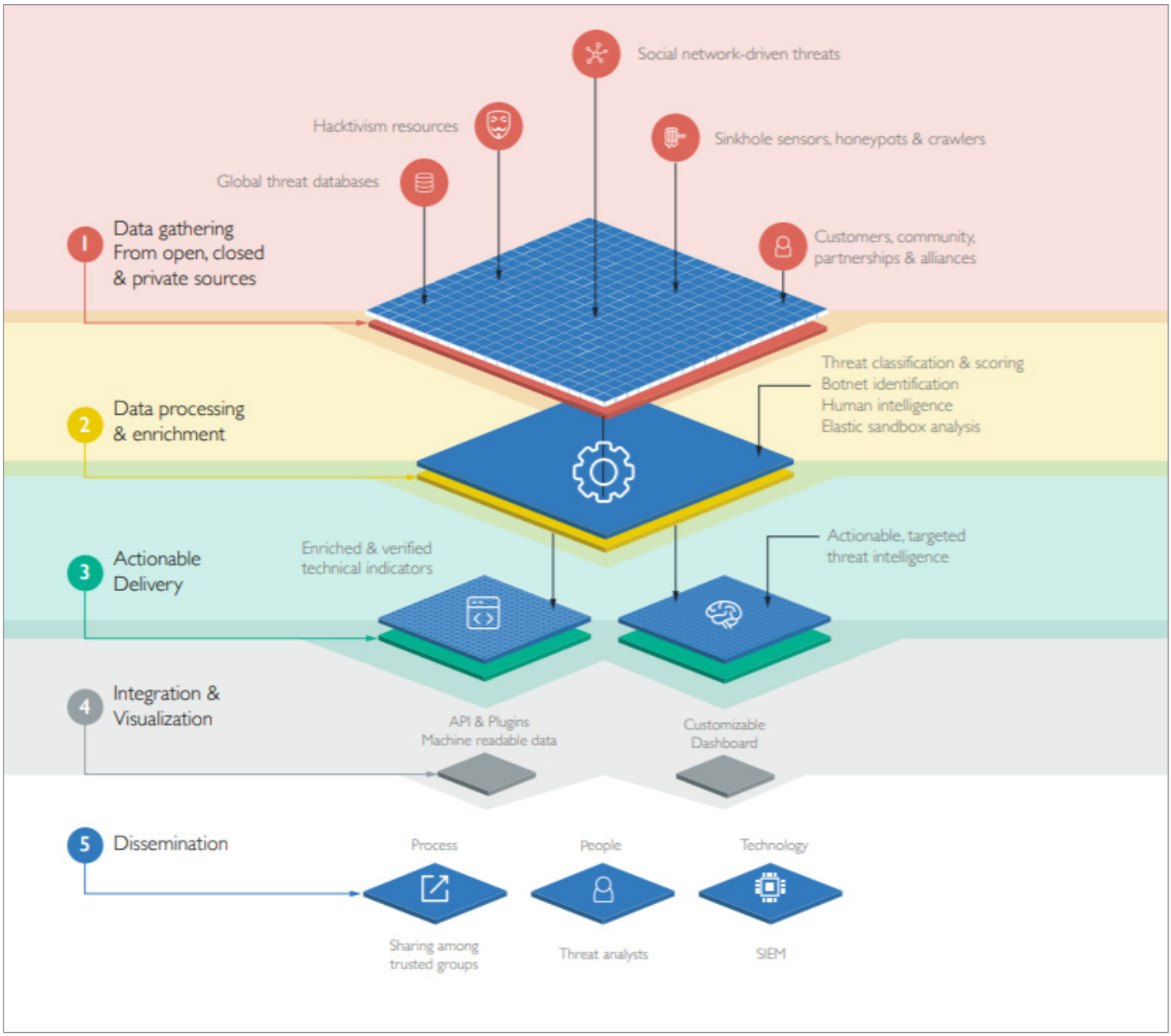
It is true that financial institutions generally spend far more resources on security than organizations in other industries - both time and money. However, it is impossible for them to invest in every single available security technology or hire an endless string of skilled security experts to keep their data and assets safe. Even the world's largest banks, investment funds, and financial services organizations find that certain gaps appear in their security infrastructure.

Security professionals are swamped, now more than ever, but threat intelligence helps prioritize these alerts and implement a more robust defense strategy, being a core element of every cybersecurity strategy

32 https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

7.1. The benefits of real-time, dynamic threat intelligence

As discussed, high quality threat intelligence helps accelerate threat and fraud detection, prioritization and incident response capabilities. By focusing scarce cybersecurity resource where it is needed most, financial entities can mitigate the impact of cyberattacks and minimize their risk of future attacks and fraud attempts imore efficiently.



Graphic: How Blueliv gathers and process data from millions of sources in the open, deep and dark web, extracting what is relevant to you.

Targeted cyberthreat intelligence should be viewed as a strategic weapon which obliges security teams to rethink their approach and overall strategy. Real-time threat intelligence ensures that you maintain visibility of the threat landscape so that your security infrastructure is able to respond to the latest threats and fraud attempts. This includes detecting fraud and malicious activity already inside your network, analyzing it and helping your security

team understand the attackers' objectives.

Most vendors push a one-size-fits-all approach – you either buy or you do not – and heavily featured service offerings: a manually-generated, report centric service which uses human analysts to identify specific threats.

Blueliv's modular architecture allows organizations in the banking and financial services sector to address individual use cases, breaking down the broad problem of external threats into more addressable projects. Automation provides speed and scale, so customers get fresh information, not aged reports.

The clear benefit of cyberthreat intelligence delivered through modules is that it works by a pay-as-you-need model. Financial sector organizations are able to select modules which are most relevant to their business and plug the gaps in their cybersecurity infrastructure.

Below, we describe several cases which could utilize threat intelligence modules.

7.1.1. Fraud prevention

A recurring problem that banks must work with other vendors on is fraud detection and mitigation. Threat intelligence services can focus on this issue delivering, for example, real-time notifications for stolen credit cards and compromised customer accounts. Generally, most threat intelligence vendors focus around detecting and retrieving cards that have been leaked or dumped on darknet sites or underground forums, or credentials available from old leaks from third parties. At this stage, it is often too late to prevent fraud from occurring.

However, there are services which can help prevent fraud in real time, using a network of crawlers, honeypots and other techniques that enable clients to often intercept cards and credentials before they are sold on the black market and therefore reduce this risk of fraud. Given that one of the most common sources of compromise is through infected PoS devices and computers, threat intelligence should be able to provide relevant, actionable trend information derived from these infected devices which can prevent credit card theft before it is too late.

7.1.2. Compromised credentials as a vector for data breaches and ransomware attacks

A successful 2021 campaign dubbed BazaCall. The Trickbot Group sent emails trying to lure the victim into calling a provided phone number to renew an expired trial subscription. If the victim called the fake call center, the scammer guided the victim into downloading the BazarLoader malware from a phishing website. Then, the malware was used to steal credentials from LSASS, use Cobalt Strike to move to high-value targets, compress documents using 7-zip and exfiltrate using Rclone, copy Active Directory database, and in some cases deploy the Ryuk or Conti ransomware.

Accessing LSASS memory dump files is one of the most effective techniques to extract credentials, which can be used for lateral movement, privilege escalation, and conduct very damaging attacks like ransomware.

It is therefore important that leaked, stolen and sold user credentials are detected in real-time. Further, any intelligence offering should be crawling the open, deep and dark web, along with information about relevant malware used to steal credentials. For instance, the MITRE ATT&CK technique T1078 - Valid Accounts is widely used by ransomware groups, either compromising the credentials themselves or purchasing them from a third-party. Attackers can employ stolen or leaked credentials to bypass access controls within a targeted network,

enabling a threat actor to gain initial access to a network, escalate privileges, move laterally and/or establish persistence.

Financial services can use a combination of sinkholes, honeypots, crawlers and sensors continuously searching for compromised credentials – the sooner these are identified, the sooner they can be retrieved, and the impact mitigated. Crucially, this includes the identification of stolen credentials of customers and partners of a company, i.e. individuals outside the network.

Complementarily, it is also important to handle another vector used by cybercriminals to gather valid credentials: phishing campaigns associated to fraudulent domains. For this, intelligence managing proactive detection is necessary, so that the entity in question can deploy effective countermeasures in time. Notably the intelligence also functions to protect and prepare corporate VIPs against phishing and social engineering attacks, since they tend to be the biggest targets.

Whether Trickbot, BazarLoader or any other malware outlined earlier in this whitepaper, malware attacks are increasingly sophisticated, targeted and much harder to detect than before. FSIs must detect malware seeking to steal sensitive information, deploy ransomware or commit fraud, including those which are successfully targeting other companies in the financial services sector.

7.1.3. The consequences of a data leak

There is a variety of ways in which data leakages can occur. For example, data may be stored on poorly secured servers and then exfiltrated to a dark web marketplace or posted in an underground forum, or compromised by ransomware that "exports" the encrypted information. If a dump contains Personal Identifiable Information (PII), including bank details and associated personal addresses, the reputational damage, in addition to massive regulatory penalties, can severely damage an FSI's standing.

FSIs would do better to boost their awareness of what is going on in the underground, observe malicious activities targeting their organization and proactively prevent future attacks. By becoming better informed about criminals targeting their organization and customers, FSIs can proactively prepare countermeasures, and find already-compromised data before the impact is too severe. To find out more about the value of using threat intelligence to mitigate the impact of PII breaches for FSIs.

Click here to download our whitepaper.

7.1.4. Eroding customer trust and non-compliance

Fake websites pose a real risk to financial entities. The surge in businesses taking their services online presents new opportunities for cybercriminals to exploit. The broader the service offering, the higher the risk, since the institution will necessarily have a greater number of URLs which can be impersonated. If, for example, an FSI offers services which nominally use the brand, then their exposure is greater as customers may trust the site without questioning the authenticity of the page.

For example, a carefully crafted spoof site for an FSI adopted the design of the target site, logos, fonts, tone of voice and had a similar URL – one that looked legitimate enough to convince the visitor that the site was safe. The replica site may be used for a variety of purposes, including advanced phishing campaigns, spreading malware and capturing visitor information which can later be used for malicious purposes. The level of potential fraud, through

illegitimate credit card usage or bank transfer, is also high. It is important to increase resilience both internally and externally, by investigating potential site impersonations through threat intelligence and taking them down as soon as possible to protect the brand.

7.1.5. Increasing efficiency, enriching intelligence

Many banks and financial institutions have a more robust security posture than organizations in other verticals. As such, some only desire additional, complementary feeds to integrate with their SIEM and SOAR systems. Security teams are already plagued by information overload and the challenge of employing further internal resources is incredibly difficult with budgets under pressure and cyberskills in short supply. Machine-readable threat intelligence feeds do not turn data into more data; they produce targeted, relevant intelligence that helps CISOs, and others make better informed security decisions.

There are frequent occasions where these analysts are seeking to gather deeper information in order to identify certain attack patterns. In these cases our Threat Context enrichment module includes advanced search capabilities to find and map Indicators of Actor activity. This means users are able to hunt for campaigns and malware distributed by an actor, even if the attack pattern is not well-known. Saving meta-datasets such as PDB path, network information or registry keys mean that it can later be correlated to discover new attack patterns belonging to 'unknown actors.'

Adding this context means that teams can enhance incident triage and post-incident forensics by approaching investigations from any point on the kill-chain. Blocking a spam email containing malware is not the same as knowing that particular spam email is related to the Dridex Gang and that the group is trying to infiltrate the network. It means that FSIs can distinguish between targeted attacks and spam campaigns and delivers value well beyond 'basic' threat intelligence.

Most importantly it is accessible to any level, from CISO to analyst, who necessarily approach investigations with varying levels of detail. The CISO can use this to find an updated catalog of Threat Actors, Campaigns, TTPs and their targets which help prioritize defenses and make budget decisions in line with the kind of attackers who might possibly target the organization. Not all threat actors will attack FSIs, but Threat Context helps to filter for these organizations based on geography, sector and other characteristics.

8. Conclusion

In order to maintain a deeper level of defense, financial institutions need to take stock of their current cybersecurity posture and prepare their organizations to adapt, making cybersecurity a core part of not just their business strategy, but also their culture. Reliable and fresh Threat Intelligence is a key component of this cybersecurity strategy, feeding the security teams and tools with relevant information to make them more effective and efficient.

This whitepaper has delivered an overview of those threats that FSIs should be aware of, with a focus on specific threat actors which can be found on our Threat Context enrichment module.

Blueliv has been working with a number of high-profile entities in the financial sector since our inception a decade ago. We have a deep understanding of their strategic cybersecurity needs and the industry-specific

threats they face. While cybersecurity strategies within the banking and finance sector are maturing, there are still many improvements that can be made. Investment efficiency, combined with an understanding of the importance of security from the top down, should drive the right allocation of funding depending on requirements.

Proactive threat detection and monitoring through threat intelligence should be supplemented by a process of continuous cyber-hygiene within the organization. This can help prevent attacks, as well as mitigate their impact when one happens.

Cybersecurity is everybody's job – not just the remit of the IT team. By establishing and promoting an appetite for cyber-risk management, FSIs will find themselves better protected. Indeed, the best way to fight cybercrime is to operate in much the same way as the bad guys. Where they build communities to exchange information and TTPs, so must we.

Blueliv hosts a global community of thousands of cybersecurity experts and encourages them to share news, views, IOCs and more – the Blueliv Threat Exchange Network. It gives members access to our free proprietary elastic sandbox, a close-to real-time cyberthreat map and it encourages information sharing. The growing global community is free to join – the fight against cybercrime is an ongoing and collaborative effort.

9. References

Share of account takeover incidents increased by 20 percentage points compared to 2019

Automatic Cybercrime with Sentry MBA

Account Takeover Fraud: What It Is And How To Stop it

Why Preventing Financial Account Takeover Attacks is Important for Banks and Fintechs

Get started with actionable threat intelligence

About Blueliv

Blueliv is Europe's leading cyberthreat intelligence provider, headquartered in Barcelona, Spain. We look beyond your perimeter, scouring the open, deep and dark web to deliver fresh, automated and actionable threat intelligence to protect the enterprise and manage your digital risk.

Covering the broadest range of threats on the market, a pay-as-you-need modular architecture means customers receive streamlined, cost-effective intelligence delivered in real-time, backed by our world-class in-house analyst team.

Intelligence modules are scalable, easy to deploy and easy to use, maximizing security resource while accelerating threat detection, incident response performance and forensic investigations.

Blueliv is recognized across the industry by analysts including Gartner and Forrester, and has earned multiple awards for its technology and services including 'Security Company of the Year 2019' by Red Seguridad, Enterprise Security and Enterprise Threat Detection 2018 category winners by Computing.co.uk, in addition to holding affiliate membership of FS-ISAC for several years.

blueliv.com

info@blueliv.com

twitter.com/blueliv

linkedin.com/company/blueliv

computing Security Excellence Awards 2018
Winner
Enterprise Threat Detection Award

computing Security Excellence Awards 2018
Winner
Enterprise Security Award

CYBERSECURITY BREAKTHROUGH AWARD 2018