
Blueliv.
FOLLOW THE MONEY
Cyberthreat intelligence for Banking
& Financial services

Contents

Cybercriminals are becoming **increasingly more sophisticated** in their tactics, techniques and procedures

$18m
per firm

Banking and financial services entities remain at **the forefront of digital risk**

Cyberattacks **cost more in damages and recovery** than any other sector

(Source: Accenture)

Why is financial sector targeted?

Financial institutions manage money - lots of it

Pushing political or personal agendas

Cybercriminals crave recognition

Top threats targeting the sector

Credential theft

Malware infection

Data leakage

Third party exposure

Banking Trojans

Webinjects

Ransomware

Point of Sale

ATM

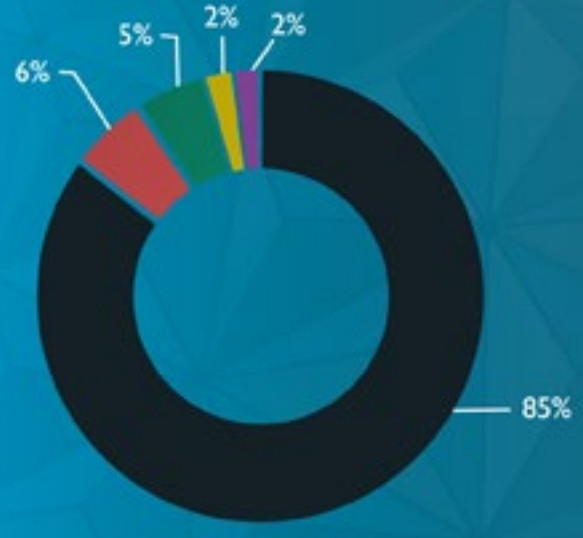
Pharming

Mobile apps

283%
increase in Trickbot botnets

130%
increase in Dridex botnets

Top 5 credential stealers targeting the financial sector



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.

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.

The risk of cyberattacks on financial services firms cannot be overstated. Attacks and breaches hit and disrupt financial services firms hard and often costing them more in damages and recovery than firms in any other sector at $18 million per firm (vs. $12 million for firms across all industries)[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.

Cyberattacks on financial services firms cost more in damages and recovery than any other sector

In an industry 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 generally 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 cyberdefense 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.

According to Gartner, traditional banks are highly focused on risk and compliance and use traditional mechanisms to fight fraud. They continue to embrace new security innovations in order to minimize the window of opportunity for attackers.

This report sets out the cyberthreat landscape for financial services institutions, including proactive steps that FSIs can take to manage their cyber-risk

The following pages set out some elements in a very broad cyberthreat landscape for financial services institutions (FSIs). As a threat intelligence provider, we seek to offer insight around trends and encourage the development and continuation of proactive steps that FSIs can take to help manage their cyber-risk.

This report does not discuss the immense levels of regulation that FSIs are subject to on a global scale, though we do cover the value of using threat intelligence to mitigate the impact of GDPR in a separate whitepaper – this can be downloaded by following the link.

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. Cyberattacks can undermine the integrity of a financial organization's underlying infrastructures as well as the systems that drive its operations. High profile attacks in recent years have demonstrated this, with attacks that were more persistent, elaborate and far-reaching. The end game varies - the attackers' objective may be to cause reputational damage, to cause a political stir or to extort profit from their victims.

Whatever the case, in order to begin to strengthen the financial institution's cybersecurity posture, it is important to gain insight into attacker motivations.

Attackers' objectives vary, from simply making money from FSIs, to pursuing a political or personal agenda, to achieving recognition

Financial institutions manage money - lots of it

This is the obvious one. 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, manipulating payment information and many more methods outlines below.

Pushing political or personal agendas

Many cybercriminals, from APTs down to script-kiddies, tend to view finance sector as a key target due to its importance across the global economy. Some attackers seek to target particular organizations as a way of drawing attention to their agendas. Take, for example, the Cayman National Bank and Trust banking network hit in November 2019 – "Phineas Fisher," a notorious hacktivist published a manifesto following the attack on a bank of the global ultra-elite. At a lower level, attackers might be disgruntled current or former employees of an organization seeking to cause damage. At a higher level, many attacks can be attributed to nation states who are acting on a political agenda.[3]

Cybercriminals crave recognition

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

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 many organizations approach the management and mitigation of cyber-risk. 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.

A recent Ponemon report "The State of Software Security in the Financial Services Industry" states that 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 keep up 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 integration with third parties, 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

Though the industry is aware of the threats railed against it, FSIs acknowledge they are not doing enough to protect systems, network or data

A robust cybersecurity posture should go well beyond protecting sensitive information and systems from malicious external attack

Recent attacks

We have established that the potential value of the information within financial institutions' IT systems makes them frequent targets of cybercriminals. It is important to study recent attacks that have occurred in the financial services sector to aid cybersecurity programs that meet and exceed regulatory requirements and keep information and property safe and secure.

Capital One

In July 2019, US financial services organization Capital One, one of the nation's largest issuers of credit cards, revealed a breach affecting 106 million customers in North America. Cybercriminals accessed the personal information of Capital One credit card holders or credit card applicants in the US and Canada, resulting in the disclosure of a massive data breach.

Capital One suffered one of the largest breaches to a financial institution on record when 106 million customers in North America were impacted

Among the information obtained by the cybercriminal were 140,000 Social Security numbers and approximately 80,000 bank account numbers for US consumers, and roughly 1 million Social Insurance Numbers (SINs) for Canadian credit card customers. In a statement, Capital One said that no credit card account numbers or log-in credentials were compromised, and over 99% of Social Security numbers were not compromised. The breach is among the largest of a major US financial institution on record.[5]

Desjardins Group

Back in June of 2019, a breach hit Canada's Desjardins Group, a Canadian cooperative that is the largest federation of credit unions in North America. The attack affected all of the financial cooperative's 4.2 million members, prompting government reforms to protect personal information in the Canadian province of Quebec. Quebec Finance Minister Eric Girard said the province would take steps to improve cybersecurity and the protection of personal information in the wake of the data breach, a classic after-the-fact move.

The breach was a result of an employee improperly collecting information about customers and sharing it with a third party outside the financial institution. The leaked information included names, addresses, birth dates, social insurance numbers (SINs), email addresses and detailed information about transaction habits. Passwords, security questions and personal identification numbers weren't compromised, according to Desjardins. Desjardins flagged a suspicious transaction to Laval police December 2018, but it was acknowledged that there was a significant delay in discovering and acting on the data theft.[6]

A robust cybersecurity posture should go well beyond protecting sensitive information and systems from malicious external attack

UniCredit

Italian financial services giant UniCredit, which has more than 8,500 branches in 18 different countries, was attacked in October 2019. It was discovered that a single file dating back to 2015 had been compromised. Roughly three million records were exposed, revealing the names, telephone numbers, email addresses, and cities where clients were registered.

UniCredit was quick to emphasize that the data leak did not include any financial information or the credentials required to access client accounts, but rather valuable PII. This news

Over three million UniCredit clients' details were exposed in an attack dating back to a compromise in 2015

came during a time when Italian banking had seen a surge in cyberdefense spending. The attack demonstrates that simply throwing money into cyber defense is not enough to protect an organization from data breaches.

HSBC

Cybercriminals successfully carried out credential stuffing again HSBC customers, compromising valuable PII

In October 2018, multinational bank HSBC reported a cyberattack in which cybercriminals gained unauthorized access to accounts for some of its US customers. Compromised information included customer's full names, addresses, phone numbers, email addresses, birthdates, account numbers, account types, account balances, payee account information and transaction history.

HSBC said the breach was the result of a credential stuffing attack. This is an increasingly common means of compromise, whereby attackers discover a cache of credentials and use them multiple times to log in to different services. An attack tool which is becoming increasingly prevalent is the use of account checkers, which take lists of already-compromised login credentials and tests them against certain targeted sites.

Cybercriminals were able to gain access to personal information from other sources that ultimately allowed them to gain unauthorized access to HSBC accounts. Credential stuffing can happen in cases where a customer uses the same password on multiple sites, including the same password for online banking.

HSBC responded to the incident by fortifying its log-on and authentication processes and implementing additional layers of security for digital and mobile access to all personal and business banking accounts.[7]

Scottrade Bank

In 2017, Scottrade Bank, the banking arm of Scottrade Financial Services, reported that a third-party data breach had inadvertently exposed 20,000 of its customers' non-public information. This particular breach highlights third-party vendor risk, which we go into detail about later in this whitepaper.

What's interesting to note about this breach is that it originated through a third party as a result of careless employee behavior. A security researcher had noticed a cache of unencrypted consumer information from Scottrade on publicly accessible servers, which contained sensitive personal information, such as names, addresses, and social security numbers, as well as usernames and passwords for various employee accounts. The data had been uploaded in error by a third-party vendor, a professional services firm called Genpact.

Genpact took full responsibility for the breach, calling it a one-time mistake, but it points to a potential lack of effective cybersecurity training and overall knowledge within the organization, as well as a hole in proper controls. Notable here is that effective vendor risk management should be a mandatory component of any financial services firm's cybersecurity efforts.[8]

Scottrade inadvertently exposed thousands of clients' PII. A cache of unencrypted consumer information was discovered on publicly accessible servers

The takeaway here is that financial services firms must protect their own IT systems at all costs. Security programs should be as robust as possible and exceed regulatory requirements. However, this alone may not be enough. Firms must not only focus on internal security, but comprehensive financial services risk management programs should also focus on third parties who have access to sensitive information, or resources and the risk they pose to the organization.[9]

It is recommended that organizations invest in threat intelligence, whether they be plug-in feeds for their existing setup or standalone modules to respond to the specific requirements of the organization. Good intelligence is like having eyes on the internet to monitor, detect and prevent attacks from any vector.

Cyberthreats targeting the finance sector

Which cyberthreats should financial institutions be on the lookout for? This section will outline some, but not all, cyberthreats which are actively targeting the financial services sector, supported by to 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.

Credential theft

Credential theft is often the initial part 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.

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 following profiles on social networks.

These account takeovers can also lead to blackmail. With access to accounts or systems, sensitive and confidential

All it takes is a single good credential to gain access to an organization and cause havoc

There are a variety of ways cybercriminals can turn a profit from credential theft from using phishing techniques to exploiting vulnerabilities to using malware

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 organizations 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.

Phishing

Phishing remains one of the most effective attack vectors for cybercriminals, and is normally used together with social engineering techniques

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 attackers 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 ROI.

BEC

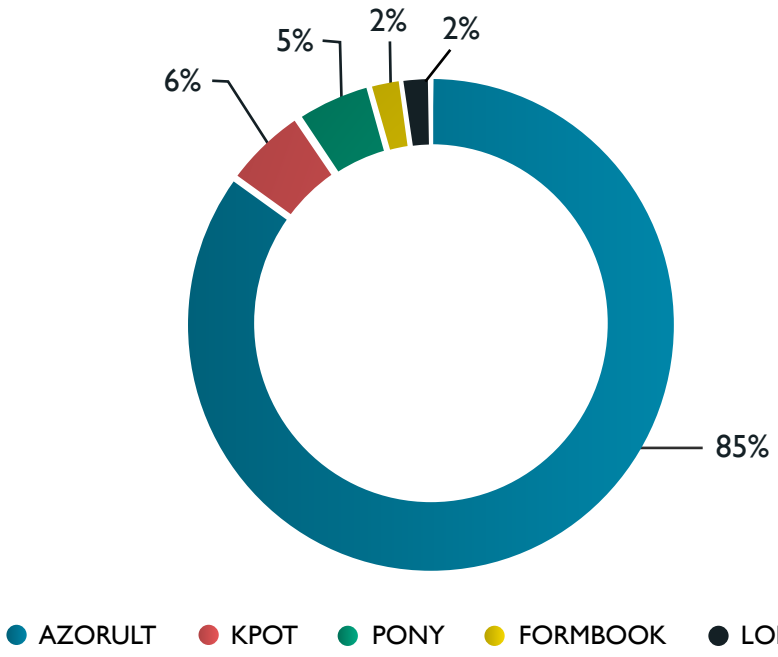
A business email compromise (BEC) attack is a type of exploitative hack in which malicious actors obtain access to a business email account and imitate the owner's identity, or use a spoofing email address to look like the legitimate email address. Its objective is to defraud the company and its employees, customers or partners. In this way, BEC attackers are able gain access to critical data and infiltrate all sorts of company systems and networks. 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.

BEC attacks are where malicious actors obtain access to a business email account and imitate the owner's identity

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 November 2019 are expressed in the chart below.

Top 5 credential stealers targeting the financial sector



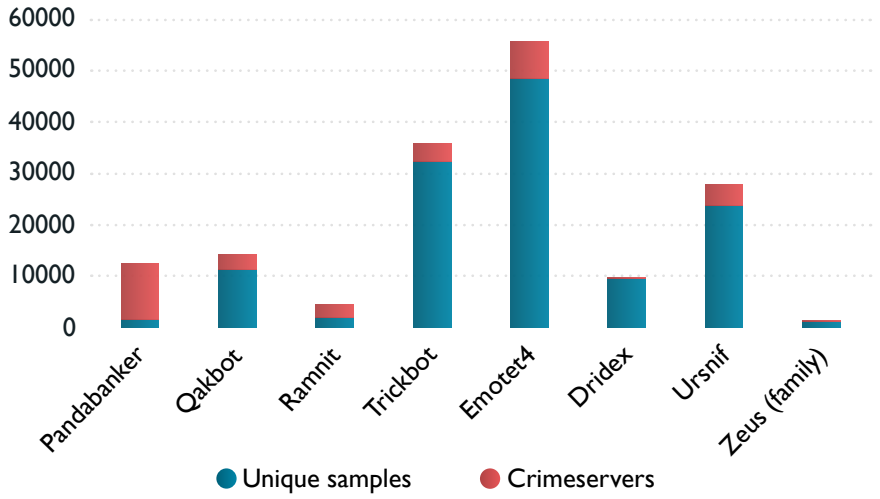
Banking Trojans may use form-grabbing, code injection and specific stealer modules dropped in the infected machines to harvest sensitive information

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 Trojan botnets targeting the financial sector since the beginning of 2019.



The 'Zeus' entry in the charts represents the Zeus (or Zbot) malware family, encompassing Zeus, Citadel and Atmos, and may include other Trojans derived from the original Zeus banking malware. This is due to the release of the Zeus source code on criminal underground marketplaces, which laid the foundations for the emergence of many new banking Trojans based on it.

The most distributed Trojan during this period was Emotet, owing to the large number of samples and crime servers that have been detected compared to the rest of botnets. It is important to consider that different Trojans use different network architectures. Emotet in particular started out as a banking Trojan and now is a customizable modular package used to deploy additional payloads and other malware families.

Following this, it is interesting to note that over the past two quarters (Q2 and Q3 2019), we have observed a 283% increase in botnets relating to Trickbot, and 130% relating to Dridex. This is in line with an increased effort by cybercriminals to deploy these two malware families. It is also interesting to note that both are used as an entry point to compromise specific targets and deploy targeted ransomware like BitPaymer (Dridex) and Ryuk (Trickbot), discussed later in the report.

To help readers understand the technicalities of a banking Trojan campaign, Blueliv has recently observed 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 stage 1 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.

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

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.

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.

There is 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 should trust. Once they are clicked on, downloaded and opened, they can take over the victim's computer. Some other, more aggressive forms of ransomware, like NotPetya, exploit security holes to infect computers without needing to trick users.[11]

Many researchers have asserted that many 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.

A webinject is a tool used to intercept data after it is decrypted from SSL but prior to its display in the browser

There are many ways organizations can fall prey to ransomware, including phishing spam and criminals gaining access to a poorly-secured RDP server

All employees should be trained in cybersecurity to lower the chance of human error as an infection vector

Financial services 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.

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,"[12] and have functionalities that include credential theft as well as stealing funds from mobile users' bank accounts.

Mobile banking Trojans one of the most rapidly developing, flexible and dangerous types of malware

Research from 2019 highlighted a year over year increase of 50% in cyberattackers targeting smartphones, in part due to an increased use of mobile banking applications. 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 doesn't detect movement, the malware will not deploy its payload in case it is in a sandbox environment. 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.

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 (and unrelated to malware, in some circumstances criminals attach a physical device to a PoS system to collect card data, called skimming.

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.

In recent years, malware affecting PoS systems has gained popularity among cybercriminals

In recent years, malware affecting PoS systems has gained popularity among cybercriminals

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.[15]

Some malware families modify legitimate DNS responses to return malicious IPs rather than the legitimate website IP – known as pharming

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.

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.

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.

Digital skimmers are scripts designed to steal data entered into online payment forms

Magecart groups were first identified in 2015, attacking the e-commerce platform Magento outlined above. Later in 2016, they hacked numerous e-commerce websites. 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.

Last year saw a number of Magecart megabreaches, including breaches at Ticketmaster, British Airways, and Newegg – the consequences of these hacks are still being felt. Customers are inconvenienced, maybe defrauded but certainly losing trust and goodwill. The companies meanwhile must face not only high rates of attrition after such incidents, but also massive financial penalties. For example, in the UK the Information Commissioner's Office has hit BA with an all-time record fine

DDoS attacks

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

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. 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.

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.

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 Tbps and include more ransom demands to increase the financial benefit.

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 stock markets 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 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 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.[17]

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.

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

Data leakage

The damage caused to any organization through data leakage can be extremely difficult for them to dig themselves out of both on a technical and regulatory level

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. Data leakage can happen all too easily in banks and financial services. The damage caused to any organization can be extremely difficult for them to dig themselves out of both on a technical and regulatory level. The below diagram illustrates the costs associated with a breach.

Immediate costs

These are the largely unavoidable costs that include the immediate business and media impact, plus the cost of restoring the confidentiallity, integrity and availability of data and systems.

Immediate costs include:

- Forensic investigation costs
- Legal costs
- Customer notification costs
- Credit monitoring for customers
- Potential business interruption costs
- Public relations expenses
- Fraud costs
- Extortion costs
- Physical damage costs
- IT/business remediation costs

Slow-burn costs

These vary according to the type and severity of the event, and how it is handled, but typically include the long-term business impact and costs incurred by reimbursing victims, as well as reparation and the payment of penalties for failure to meet obligations.

Slow burns costs include:

- Third-party litigation expenses
- Customer churn from reputational damage
- Regulatory fines and penalties
- Share price impact
- Loss of management focus
- Loss of competitive advantage
- Loss of revenue

Time from event discovery

This graphic from KPMG illustrates the impact of a successful cyberattack on a business.[18]

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.

56% 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 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 process.[19]

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.

Your risk management program must look beyond your own organization to properly scrutinize and vet the third and fourth-party vendors

Hacktivism

The financial services sector is particularly vulnerable to hacktivism

With the heightened sense of political awareness across society in recent years, criminals regularly engage in agenda-driven attacks as opposed to taking down websites or 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.[20] In the current climate the financial services sector is particularly vulnerable to this type of cyberthreat.

Threat Actors

Certain threat actors are responsible for most of 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 remove even governments.

In this section, there is an explanation of some 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.

Lazarus Group

Lazarus Group has been linked to some of the most notorious cyberattacks in recent memory, 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 has been linked to some of the most notorious attacks on financial services in recent memory

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 memory, 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, with the collective beginning to pursue financial gain for the first time.
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 cybercriminals due to their use of crimeware products such as Hermes ransomware.

Some analysts suggest this APT may interact with Russian-speaking cybercriminals due to their shared use of certain crimeware products

Money Taker

MoneyTaker is a skilled adversary targeting financial institutions, studying how their internal systems and networks function in order to penetrate the systems for financial gain. The group has successfully stolen over $11M USD from banks since they were first identified in 2016. They mostly target financial institutions from the US and Russia, with a focus on stealth and using both self-developed and publicly available tools.

MoneyTaker studies internal systems and network functionality to penetrate financial institutions' systems

The first malicious activity attributed to MoneyTaker dates back to May 2016, when they were seen stealing from a US bank. The money was stolen after the group had gained access to First Data's STAR card processing system. From September of the same year to June 2017 they targeted 17 institutions

(financial providers, law firms, software and service providers, and banks) from the US and the UK and two banks from Russia. From the US and UK entities they stole SWIFT documentation and were able to deploy banking and PoS Trojans.

On July 3, 2018, the MoneyTaker hacking group stole about $1M USD from the PIR Bank in Russia through the AWS CBR (Automated Work Station Client of the Russian Central Bank), a Russian interbank fund transfer system similar to SWIFT. They transferred the money to 17 mule accounts at major Russian banks and cashed out. After that, they tried to ensure persistence in the bank's network, but they were detected and removed. The fraudulent transactions were not detected until the next day.

It appears that the attack started in late May 2018, when the group used a compromised router from one of the bank's regional branches (support for the router's software ended in 2016). From there, they gained access to the main network where they managed to compromise the AWS CBR. It seems that they automated some of these processes using PowerShell scripts. After the attack, they wiped the OS logs on numerous computers and left several reverse shells connected to the C&C server.

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 a 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 the arrest, the Cobalt Gang continues to be active. Some researchers have theorized that the Cobalt Gang may have experienced a split in the aftermath of its leader's arrest, leading to a Cobalt Gang 1.0 and 2.0.

This financially motivated cybercrime group is primarily known for their theft of payment cards but has targeted major companies

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 elects 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 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.

FIN10

FIN10 is not known to have attacked financial institutions, but the sophistication level and the potential impact in the targeted company makes it an adversary to keep in mind for any large company worldwide. FIN10 was first identified by FireEye in 2017, following a number of attacks in the previous three years. They specialize in extortion. After compromising their victims' networks and stealing sensitive information and uploading malicious scripts, they contact the executives of the affected company and demand that they pay large sums of money in Bitcoin. If the ransom is not paid in time, the group threatens to release the compromised information and destroy their victims' systems. When the victims do not comply, the information is released through online paste services such as pastebin[.]com or justpaste[.]it, torrent sites like Thepiratebay or cloud file sharing/storing solutions like Dropbox. Also, Windows systems of the company are damaged.

After compromising their victims' networks FIN10 contacts their victim demanding Bitcoin

They have tried to disguise them as Russian-speakers, saying that the attacks were in response to Canadian economic sanctions on Russia, but the quality of the Russian-language posts they

made suggested that FIN10 used an automatic translation tool to write them. They also have named themselves as "Tesla Team," "Angels of Truth," and "Anonymous Threat Agent" trying to achieve this same objective.

Dridex Gang

The Dridex Gang is primarily focused on developing, distributing, and profiting from banking Trojans and ransomware

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 lead 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.

Dridex Gang continues to use the Dridex banking Trojan to commit financial crimes and has even updated the Trojan to target cryptocurrency exchanges

EmpireMonkey

EmpireMonkey is an advanced financially motivated cybercriminal gang. The group gained notoriety for a heist they conducted in February 2019 against the Maltese Bank of Valletta, which initially resulted in roughly €13 million in losses, though much of this was subsequently recovered or frozen.
While a thorough post-mortem of the Bank of Valletta attack has yet to be made public, it is highly likely that the threat actors sent malicious spear phishing emails to employees at Bank of Valletta and other European financial institutions. In October 2018, HSBC Malta reported receiving phishing emails that bore hallmarks of the subsequent EmpireMonkey attack against Bank of Valletta.

TA505

TA505 is the name given to one of the more prolific financially motivated threat actors in recent years that targets companies worldwide

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.

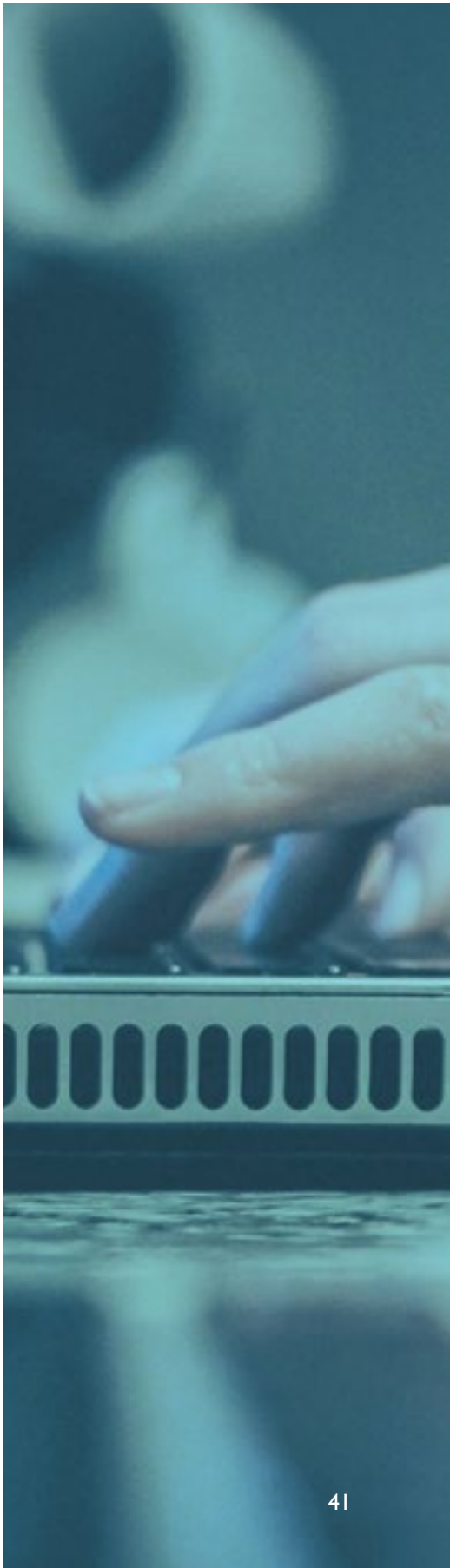
TTA505 has been highly active in 2019, launching multiple campaigns against several objectives in multiple countries, such as China, Germany, India and Italy. Their first campaign of 2019's second quarter started in April, when TA505 targeted financial enterprises using LOLBins and a new variant of the 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 if they should establish persistence on the infected hosts or not after evaluating each one of them using the information from their reconnaissance malware.

In May of the same quarter, researchers detected another campaign. In this case, it was not targeted at all, but actually 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, researchers reported identified 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 it opened 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 the Banking or Retail sector suggests that the group could be potentially widening their current operations.



How organizations in financial services can manage their cyber-risk

Organizations must put in place proactive security measures that help them prioritize detection and response, enabling them to react quickly to incidents

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.[21]

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 protect themselves from cyberattacks which are all but inevitable.

Executive level engagement

A cybersecurity strategy needs the full involvement and support from the C-suite and board

A cybersecurity strategy needs the full involvement and support from the C-suite and board. Senior leaders aren't 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's not complete without one.[22]

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 FS organizations to close cybersecurity gaps. Of particular concern are weak spots in some organizations' fraud risk assessments, whistleblowing mechanisms and overall awareness.[23]

According to a recent Global Economic Crime Survey by PwC, there are a few things that organizations can do to. 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.[24]

FSIs should seek to resolve as many legacy IT issues as they can, as regularly as they can

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.[25]

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.

Good 'cybersecurity hygiene' means implementing proper and robust employee training

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.[26]

Incident response readiness

A recent IBM and Ponemon study found that 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.[27]

Combine playbooks with automated threat intelligence

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.

Continuous monitoring

Continuous monitoring, such as those intelligence services provided by Blueliv, mean 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. 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.

Continuous monitoring means that organization risks are assessed in close to real-time

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 and outsource your risk associated with that data and how it's managed.[28]

You can outsource systems and services, but you cannot and outsource your risk associated with that data and how it's managed

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's no longer enough to meet baseline technical requirements for post-incident response and communications with regulators and consumers.

Regulation and Legislation

Generally speaking, financial services organizations worldwide are subject to a considerable amount of cybersecurity compliance regulation. This legislation not only regards data privacy for consumers, but also places obligation on companies themselves. The EU GDPR, for example, enforces that companies should "implement appropriate technical

There is a significant onus on FSIs to invest in cybersecurity tools and solutions to minimize the impact of cyberattacks

and organizational measures to ensure a level of security appropriate to risk." 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.

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.

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.

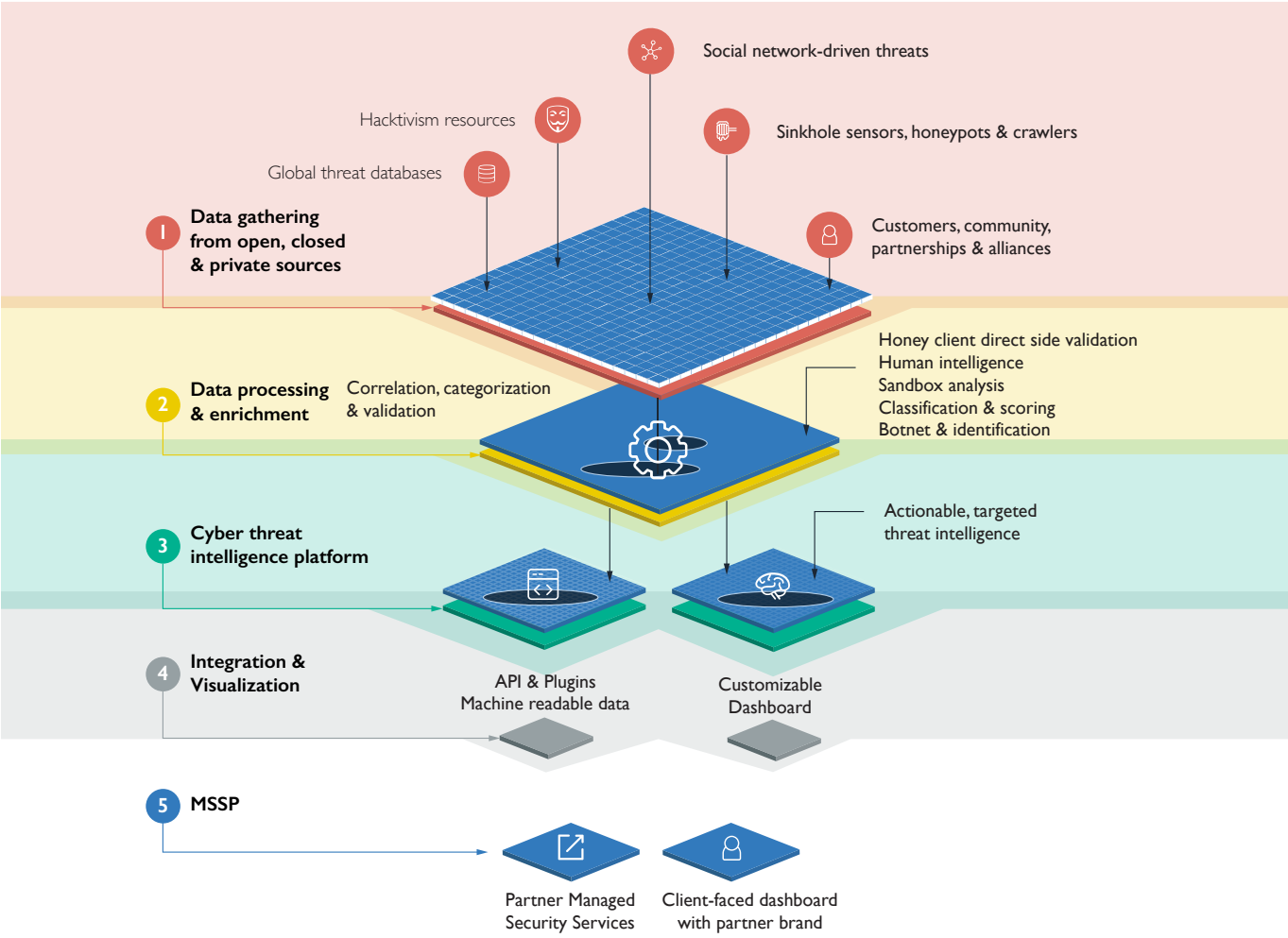
It's true that financial institutions generally spend far more resources on security than organizations in other industries - both time and money. However, it is impossible for them to invest in every single available security technology or hire an endless string of skilled security experts to keep their 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.

Threat intel helps organizations can detect threats both inside and outside their network, and prioritize their responses

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.



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.

Targeted threat intelligence should be viewed as a strategic weapon which obliges security teams to rethink their approach and overall strategy

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

However, fully modular and automated intelligence is available, using customer information to identify closely targeted 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 to 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.

Modular means FSIs select modules most relevant to their business and plug the gaps in infrastructure

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

Fraud prevention

Fraud can be reduced using a network of crawlers, honeypots and other techniques to intercept cards and other leaked or stolen information

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. Generally, most threat intelligence vendors focus around detecting and retrieving cards that have been leaked or dumped on darknet sites or underground forums. 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 enable clients to often intercept cards 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, threat intelligence should be able to provide relevant, actionable trend information derived from infected PoS which can prevent credit card theft before it is too late.

Spam campaign deployed against corporate emails

It is important that leaked, stolen and sold user credentials are detected in real-time, along with relevant malware used to steal them.

A successful campaign last year delivered Trickbot, a banking Trojan which had the capability to harvest user credentials by exploiting a known vulnerability. These credentials were the gateway to the organization's infrastructure and could potentially have been used for account takeovers and further attacks (such as deploying Ryuk ransomware), so business risks associated with their initial compromise were extremely high.

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.

Meanwhile, in this case it is also important to handle the initial phishing campaign and associated 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 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 or commit fraud, including those which are successfully targeting other companies in the financial services sector.

Boosting awareness of what's going on in the underground can limit business, reputational and regulatory costs

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. If a dump contains 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's going on in the underground, observe malicious activities targeting their organization and proactively prevent future attacks. These module delivers a serious advantage to security teams by putting a spy in the enemy camp: FSIs become better informed about criminals targeting their organization and customers, can proactively prepare countermeasures, and find already-compromised data before the impact is too severe.

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.

Increase resilience both internally and externally by investigating site impersonations and taking them down as soon as possible

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.

Brand protection: VIPs at high risk of attack

A spike in chatter on several dark web forums about several executives from a major bank in Northern Europe occurred earlier this year. This was enough to ring some alarm bells, but it also coincided with negative social media and media coverage against this entity, and it transpired that a group was seeking to cause considerable reputational damage to this institution.

The *modus operandi* of this APT was likely to have been to deploy a highly targeted spearphishing attack, dropping malware which was intended to harvest VIPs' credentials. From there, it was expected that they might carry out BEC attacks on employees, or even a 'pump & dump' scheme. These schemes often see cybercriminals impersonate VIPs (sometimes even on social media) to take actions or make misleading statements which end up artificially manipulating the price of stocks so cybercriminals can benefit from their change in value.

VIPs are at high risk of attack from account takeovers to other forms of fraud

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.

MRTI feeds produce targeted, relevant intelligence that helps CISOs make better informed security decisions

Threat Context enriches threat information to find and map indicators, well beyond basic intelligence

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 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 that particular spam email is related to 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.

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.

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.

FSIs are establishing and promoting an appetite for cyber-risk management, but there is still work to be done

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.

References

1 - https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

2 - https://www.ey.com/en_us/innovation-financial-services/cybersecurity

3 - https://www.safesystems.com/blog/2018/03/three-reasons-cybercriminals-attack/

4 - https://www.ey.com/en_gl/advisory/how-financial-services-organizations-can-manage-cyber-risk

5 - https://abc7news.com/finance/capital-one-breach-106m-people-compromised-woman-charged/5430934/

6 - https://www.nasdaq.com/articles/desjardins-group-data-breach-hit-all-4.2-million-members-quebec-finance-minister-2019-11

7 - https://thehill.com/policy/cybersecurity/415556-hsbc-bank-confirms-some-us-customers-affected-in-data-breach

8 - https://www.bitsight.com/blog/lessons-learned-from-3-major-financial-services-data-breaches

9 - https://www.bitsight.com/blog/lessons-learned-from-3-major-financial-services-data-breaches

10 - https://www.techopedia.com/definition/33769/business-email-compromise-bec

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

12 - https://www.finextra.com/pressarticle/78517/kaspersky-reports-rise-on-mobile-banking-malware

13 - https://www.zdnet.com/article/mobile-malware-attacks-are-booming-in-2019-these-are-the-most-common-threats/

14 - https://www.zdnet.com/article/these-malicious-android-apps-will-only-strike-when-you-move-your-smartphone/

15 - https://www.cyber.nj.gov/threat-profiles/atm-malware

16 - https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html

17 - https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html

18 - KPMG July 2017, Closing The Gap: Cyber security for the Insurance Sector, p.5

19 - https://www.upguard.com/articles/five-things-to-know-about-third-party-risk

20 - https://www.itpro.co.uk/hacking/30203/what-is-hacktivism

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

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

23 - https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf

24 - https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf

25 - https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_Generali_The-Impact-of-Cybersecurity-Incidents-on-Financial-Institutions-2018.pdf

26 - https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_Generali_The-Impact-of-Cybersecurity-Incidents-on-Financial-Institutions-2018.pdf

27 - https://www.ibm.com/downloads/cas/GAVGOVNV

28 - https://blog.riskrecon.com/you-cant-outsource-risk

29 - http://www.privacy-regulation.eu/en/article-32-security-of-processing-GDPR.htm

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

twitter.com/blueliv

info@blueliv.com

linkedin.com/company/blueliv