2020 Financial Services and Insurance Industry Threat Report

INTRODUCTION

The global pandemic has forced many financial services and insurance (FSI) firms to accelerate digitalization efforts. These efforts have had many positive results: more streamlined everyday remote customer journeys, a scaled-up infrastructure to facilitate an expanding perimeter and accommodations for rapidly changing communication and compliance needs. While these changes have helped bankers, wealth advisors, traders and agents manage markets and financial flows, they have also opened up more opportunities for threat actors.

Threat actors quickly take advantage of every societal crisis and COVID-19 is no exception. As the FSI industry moves beyond the network perimeter, so do attackers. But threats don't just move—they take on new forms and targets. Every person in your firm represents a different security level or compliance risk because of the data they have access to and how they use technology to do their job.

To help FSI leaders better understand the evolving threat landscape, we analyzed a year of data, focusing on the first half of 2020. Proofpoint Threat Research studied thousands of campaign threats across millions of messages. This report outlines our findings, providing data, real-world examples and insights to shed light on threats that target the FSI industry.

Audience and objective

This report is intended for leadership and security executives in FSI. It aims to help reduce the risk FSI organizations face to personally identifiable information (PII), financial data, intellectual property (IP), non-public information, third-party FSI ecosystems and fraud. The report is also designed to help educate FSI workers for better security awareness, safety and security.

Research methodology

This body of research analyzed a combination of Proofpoint data across threat actors, campaigns, business email compromise (BEC) and Very Attacked People™ (VAPs) in Q4 2019 and the first half of 2020. In some cases, we used open source information to address security topics that we are researching but not directly observed in Proofpoint-sourced data.

Table of Contents

Executive Summary

The Financial Services and Insurance (FSI) sector is a consistent target for nefarious actors, regardless of whether the motive is fiduciary, hacktivism or terrorism. The key takeaways from this report are:

People, not technologies, are the most frequent attack vector.

According to Proofpoint Threat Intelligence, over 96% of all attacks start with social engineering, pretexting, phishing and insider threats, while many organizations spend the majority of budgets on technology-based solutions.

Based on Proofpoint's analysis of indicators of compromise (IoCs) and tactics, techniques and procedures (TTPs), a list of VAPs can be deduced from the overall attacked population, allowing security fidelity to be customized to those targeted threats.

Threat actors respond quickly to evolving environmental conditions.

The 2020 Verizon Data Breach Incident Report highlighted that cloud-based attacks have doubled in the past year, in line with the increase in remote workers.

Threat actors in financial services are laser-focused on their strategies, exceedingly methodical in their tactics and well-versed on their targets.

Supply chain risks have limited controllability beyond the second tier.

The financial services supply chain is globally economically volatile—more than any other industry—as it includes exchanges, settlement/clearinghouses and central banks with international reach.

Be diligent but cognizant of the nuances with supply chain security requirements. Forcing compliance to security measures with first- and second-tier suppliers by blindly pushing down your organization's internal requirements may create security gaps for that supplier or prevent that supplier from properly servicing your organization.

Each subsector has nuances specific to their threat landscape.

Proofpoint Threat Intelligence data, as well as independent reports illustrate variations in IoCs and TTPs with each subsector, so the defense should be customized for subsectors.

Cryptocurrencies are just around the corner.

The Office of the Comptroller of the Currency (OCC) has recently published a statement to allow banking institutions to hold digital keys for cryptocurrency wallets.

If banks are allowed to legally hold digital assets for their clients, the legal liabilities and cybersecurity risks of those cryptocurrencies are transferred to those holding banks.

Financial services and insurance security and threat metrics

The financial services industry has several semi-unique characteristics that attracts threat actors like bees to honey:

HIGH REWARD

The ROI for breaching a financial services firm is higher than other industries because that's where the money is.

IMPACTFUL

Any size breach can be news-worthy and can affect market reaction, and scaffolding effects can extrapolate from individual businesses to global economies.

REGULATED

Having to comply to well-defined regulatory processes and procedures reduces the target-specific reconnaissance efforts needed by an adversary.

LEGACY TECHNOLOGY

Heavily reliant on vintage IT, the security risk is introduced with abandoned manufacturer support and proprietary systems accumulated from mergers and acquisitions, systems deemed "too critical to update", or loss of legacy expertise.

INFRASTRUCTURE JUNGLE

A historically active mergers and acquisitions sector, this introduces complexity and opaqueness. Loosely coupled integrations between disparate systems create a bifurcated infrastructure that offers more significant areas of attack and increases the stress on security monitoring and defense resources.

CLOUD / CONTAINER TECHNOLOGY

Uplifting legacy applications to the cloud (or containers) can result in the exposure of previously unknown vulnerabilities or the introduction of new ones due to the deployment paradigm. Engaging new SaaS vendors to offload non-critical systems can open a new attack surface where the capability to manage incidents is severely limited.

AUTOMATION EVERYWHERE

FSI organizations increasingly seek automation to reduce costs and modernize legacy systems. However, the sprawl of commoditized automation promotes fragility when they are dependent on that legacy system, introduce new business logic complexity or go undocumented.

There are some significant statistics unique to the FSI sector in regard to security prevention, emerging threats and persistent attacks:

Security awareness training

The financial services and insurance population is slightly more aware of the insider threats and account authentication threats than other industries.

- Financial services has a 20% failure rate compared to the 22% population average.
- Financial services is better in "Identify and Prevent Insider Threats" and "Account Authentication."
- Financial services is worse only in "Protect Against Physical Risks" and "Avoid Ransomware Attacks."

Email threats

URL threats were consistently higher than attachment threats.

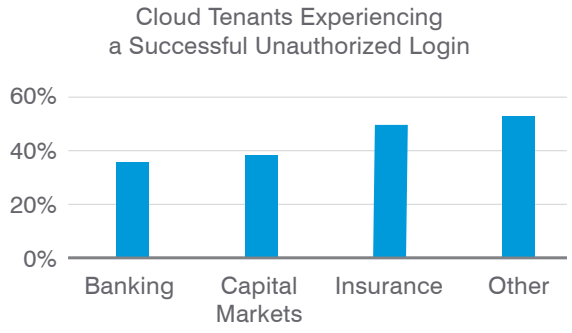
- 82% of malicious messages contained URLs across the financial services industry.
- 72% of attacks were malware-based.

Cloud access

Social engineering tactics against cloud access boasts an impressive *75% success rate*, while brute force worked only around 9.7% of the time. Clearly, people-centric attacks show the most promising ROI for a threat actor.

Insurance experienced more successful unauthorized logins than banking and capital markets.

- 72% were targeted with brute-force methods, but only 7% were successfully compromised using a brute-force method.
- 28% were targeted with social engineering methods. 21% were successfully compromised using a phishing method.



Data loss prevention (DLP) and insider threats

Each subsector of the FSI industry has its own insider threat rates. In a study of insider incidents from 1996 through 2018, banking was by far the most culpable.[1]

Segment	Group(s)	Insider Threat Risk(s)	# Insider Incidents[2]
Banking	Savings, Credit, Finance	PII, Account Takeover	190
Capital Markets	Investment Banking, Asset Management	IP, Mergers and Acquisitions, Insider Trading	no data available
Insurance	Underwriting, Property and Casualty	PII, Insurance Fraud	14
Ecosystem	Exchanges, Settlement, Market Data, Cloud/SaaS, Supply Chain	AML, Counterparty, SWIFT, ACH, Market Manipulation	33

TTPs used in financial services insider incidents

CERT in collaboration with DHS and USSS researched insider incidents between 2005 and 2012 to answer the question: "What are the observable technical and behavioral precursors of insider fraud in the financial sector and what mitigation strategies should be considered as a result?"[3] Among their top findings were:

The "low and slow" approach accomplished more damage and escaped detection for longer.

Anomaly-driven technology solutions were not only ineffective, but counterproductive, because these long-term malicious activities became part of the user baseline.

Insiders' means were not technically sophisticated.

The lack of sophistication means that existing sensor data can feed into an insider threat program. The magic, of course, is in the behavioral analysis.

Fraud by managers differs substantially from fraud by non-managers by damage and duration.

Managers have the ability to alter business processes, sometimes by manipulating subordinate employees, to profit financially. Non-managers are often customer service representatives who alter accounts or steal customer PII to their benefit.

Most incidents were detected through an audit, customer complaint or coworker suspicion.

This is an important finding: whereas an external breach has a trail of anomalous breadcrumbs, the insider threat is fueled by sentiment, motivations and mindset—factors not easily detected by technology.

The fox guarding the henhouse

Sometimes the insider threat is involved with the agency designated to deter and investigate insider threats. In 2019, a former SEC Securities Compliance Examiner was charged for accessing information pertaining to a pending investigation into a private equity firm and used that knowledge to attain a position of Chief Compliance Officer at that very firm.[4] The fact that the subject came from—and moved to—a position of compliance is not only ironic, but demonstrates that no area of morality is off-limits to an insider threat.

[1] Miller & Trotman (2018), "*Insider Threats in Finance and Insurance (Part 4 of 9: Insider Threats Across Industry Sectors)*," CMU SEI

[2] Ibid.

[3] Cummings, Lewellen, McIntire, Moore & Trzeciak (2012), "*Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector*," CMU SEI, DHS S&T, USSS and CERT Insider Threat Center

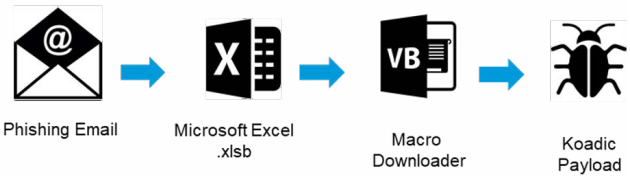
[4] Godoy & Lorenzo (2019), "Ex-SEC Compliance Expert Denies Pilfering Info For PE Firm," Law360

Prevalent Tactics in FSI Industry Attacks

Proofpoint Threat Intelligence has seen growth in several specific tactics used by threat actors:

VBA stomping

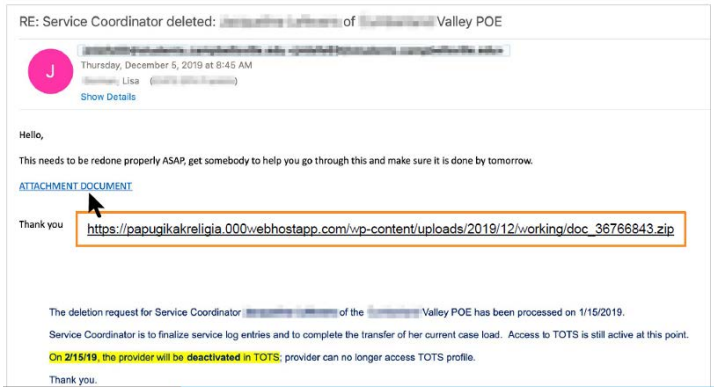
This malicious attachment technique presents different VBA (executable) code to security analysis engines than what is actually executed; thereby bypassing many code signature and heuristic detection tools.



Thread-hijacking

This BEC (business email compromise) technique captures many victims by injecting false email content (i.e. malicious URLs) into an existing email thread. When seeing an existing email thread, there is a level of inherent trust; thus many victims are more willing to open it and click on links.

Another tactic used by this technique is to embed malicious URLs in the "original email" section of the email, where many email security tools stop parsing; again bypassing many heuristic detection tools.


RE: Service Coordinator deleted: [redacted] of [redacted] Valley POE

J

Thursday, December 5, 2019 at 8:45 AM

[redacted], Lisa ([redacted])

Show Details

Hello,

This needs to be redone properly ASAP, get somebody to help you go through this and make sure it is done by tomorrow.

ATTACHMENT DOCUMENT

Thank you https://papugikakreligia.000webhostapp.com/wp-content/uploads/2019/12/working/doc_36766843.zip

The deletion request for Service Coordinator [redacted] of the [redacted] Valley POE has been processed on 1/15/2019.

Service Coordinator is to finalize service log entries and to complete the transfer of her current case load. Access to TOTS is still active at this point.

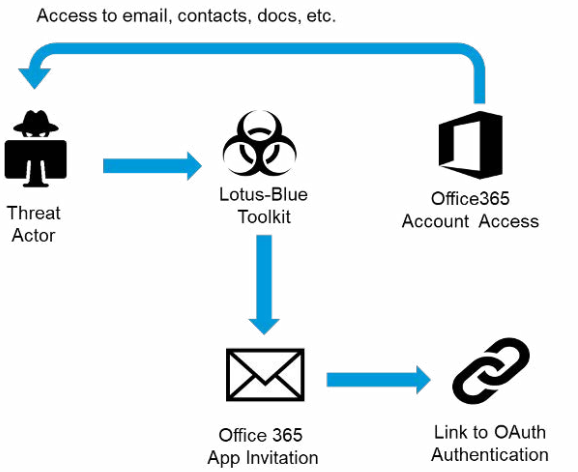
On **2/15/19**, the provider will be **deactivated** in TOTS; provider can no longer access TOTS profile.

Thank you.

In the case of the most prolific malware of the last two years, Emotet, the actors have actually automated the templating process to perform this technique at incredible scale where typically it involves some direct analysis and customization by the threat actors.

Weaponized 3rd party authentication (3PA)

This ATO (account takeover) technique uses typical DNS twisting to lure users into providing SAML-based token permissions to a user's cloud applications (such as O365, GSuite, et al). Typically this starts as BEC and quickly advances to EAC (email account compromise). With material access to a user's email account, password resets to other applications becomes possible, leading to full-fledged ATO.



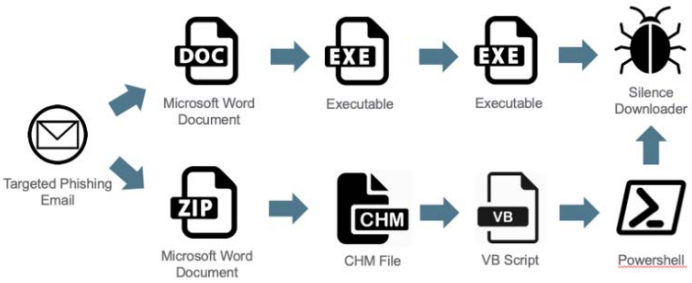
What makes this type of ATO more nefarious than others is that once an account has been permissioned, changing your password or MFA makes no difference. The only way to remove a threat actor's access is to explicitly remove the token permissions—a process which most end users are oblivious to.

Multi-layered file-share attack

This file-share technique presents a hosted document which in turn points to layers of document URLs hosted on many different file shares, which eventually traces down to a malware-laden payload.

The prevalence of financial services using cloud-based file shares (and 3PA) has created increased usage of this technique.

For example, a payload (a VB script which loads an embedded banking trojan, Ursnif) is password protected (encrypted) with the password presented in the message body of the e-mail.



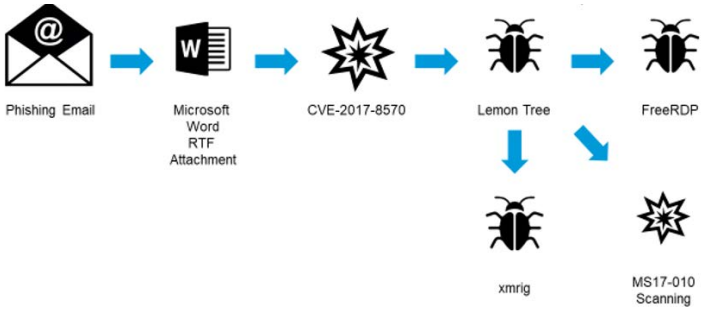
On one hand, adding steps like forcing the intended victim to enter a password seems counter-intuitive, as the more steps required the higher the likelihood that someone performs a step wrong or gives up before completing all the steps.

On the other hand, this prevents straightforward scanning of the attachment and solutions have had to implement techniques that involve either a growing dictionary of commonly used passwords (actors want to keep them simple for the above-mentioned reason and don't change them every campaign) or scanning and parsing message bodies (which is hard to do at scale).

There are some cases we've seen where the password has actually been an image rather than text and so this latter method of scanning for text passwords would not work.

"Living-Off-the-Land" (fileless/serverless) attacks

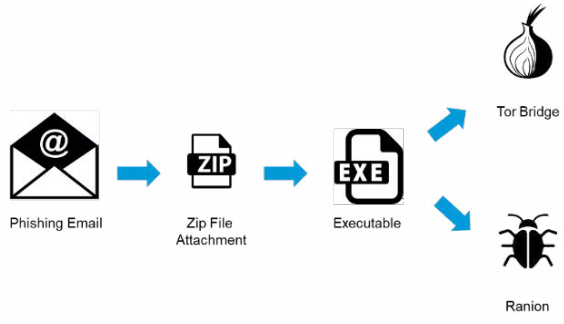
This attack technique uses existing capabilities within the target's operating systems—such as PowerShell—to execute its payload. The payload itself is not binary; therefore can evade both signature and heuristic detection methods.



Ransomware-as-a-Service (RaaS)

Ransomware platforms have been commoditized much like many other attack platforms.

Ransomware platform providers have moved to a subscription service and no longer take a percentage of the payout; not only does this make the RaaS more attractive than other attack platforms, but it also distances the RaaS providers from undue direct culpability in criminal acts. (Imagine the culpability lawsuits on gun manufacturers if they collected a fee on every bullet that was fired.)



Newer iterations of this service include automatic installation of TOR clients on the victims' computers, making it easier for victims to pay ransom.

Financial Services Industry Insights

Banking

The banking sector has seen the most innovation and progress in recent years, from the advent of mobile transactions to applications programming interface (API)-enabled services to the use of artificial intelligence (AI)-based processing. With new technologies come new methods of attack, but the motivations and targets for banking by threat actors is consistent. In fact, Accenture estimates $347 billion USD is at risk for the banking sector.[5]

QUICK VIEW: SPECIFIC TO THE BANKING SECTOR	
VAPs:	**Broad Phishing**: • Technology Team • Executive **Targeted Business Email Compromise (BEC) Attacks:** • Relationship Manager • Investor Relations/Financial Advisors • Business Development
Targets:	• Clients (direct) • Employees (direct) • Clients (indirect): Workforce with access to client data/systems • Employees (indirect): Workforce with access to human resources (HR) data/systems
Objectives:	• Client Financial Loss

Banking: Targeted attacks

Proofpoint Threat Intelligence has identified attacks targeting a single banking role or firm, which implies a laser-focused objective using firm-specific reconnaissance.

Large banking institution

Analyst comments: A Fortune 100 banking institution received 12 (100%) messages that used a novel WhiteShadow[6] technique to deploy an unknown set of malware. This is interesting for a couple of reasons.

The fact that the malware is unidentified could indicate this firm is simply a test subject for a wider systemic attack.

WhiteShadow is often used to deploy Crimson, a remote access Trojan (RAT) first identified in 2016 as a payload used by a Pakistani nexus advanced persistent threat (APT) actor dubbed "Transparent Tribe."[7] Since that time, Crimson RAT has been commoditized by a number of crime-oriented actors, but Proofpoint Threat Intelligence has received multiple inquiries from banking institutions regarding whether the WhiteShadow to Crimson attack chain could still be state-sponsored activity.

Instances of the WhiteShadow technique dropping additional malware beyond Crimson from an infrastructure not explicitly associated with the Pakistani network helps highlight and add confidence to the idea of widening adoption of the technique and associated payloads.

Credit union: Supply chain attack

Analyst comments: A credit union received 67 messages (87%) while several regional accounting firms received the same messages. Any relationship between the credit union and these firms may indicate a side-channel/supply-chain attack.

The intended payload chain of GuLoader QuasarRAT is mostly unremarkable but is exemplary of a large scale TTP shift across the entire threat landscape in the last two years which is to just establish a foothold to deploy additional payloads. Further, QuasarRAT, as open source, provides sophisticated actors a way to muddy attribution—for example, if a threat actor can get a foothold on a system with a generic/widespread piece of software, it's much harder to figure out who is actually the one initiating the attack. In the case of a successful breach, this technique still allows the actor to deploy a follow-up payload after some reconnaissance.

[5] Accenture (2020), "The State of Cybercrime in Banking and Capital Markets"

[6] https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware

[7] https://www.proofpoint.com/us/threat-insight/post/Operation-Transparent-Tribe

Banking: Threat analytics and trends

Over a six-month period, from 2019/Q4 through 2020/Q2, Proofpoint Threat Intelligence has tracked the threats shown in Figure 1 consistently targeting the banking subsector.

Wire money transfer

Analyst comments: This is a case where commercial banking receives nearly twice as many messages as the next highest vertical and going down the line. Although customers from financial investing, financial transaction services and finance ecosystem all receive messages. The messaging is spread out somewhat evenly across many institutions and regions rather than being largely concentrated on one customer with a handful of messages to like customers. The lure itself is spoofing a Western Union money transfer with the intention of dropping a RAT and the subject references compliance.

Other notable campaigns

TeamViewer Bot (MINEBRIDGE) | Word Documents | "Indeed Application: Full Time Teller"
Broad targeting of financial services verticals with a lure that purports to be "Full Time Teller" job applications from a fake recruitment company.

GuLoader / Parallax "warii" | Attachments | "MAJ Code Banques"
Messages contain Microsoft Office attachments that contain macros that, if enabled, download and execute GuLoader which, in turn, downloads and installs Parallax. Banking and services companies were the primary targets.

jSocket "88.150.189[.]98" | URLs | "Tax return"
These messages contain URLs leading to a compressed Java file. Nearly all messages were sent to a banking company.

Get2 / SDBbot | Excel Documents
Emails containing Microsoft Excel attachments include macros that, if enabled, execute an embedded DLL ("Get2" loader malware). Get2 downloads SDBbot and unknown malware. Banking was the primary target. Seventy-six percent of messages in this campaign went to the financial services industry. This campaign was found targeting banking companies in December 2018 and January 2019. Banking companies continued to be frequent targets.

URLs | Word Documents | PDFs
The U.S. is being targeted with emails that contain URLs, Word documents or PDFs. The PDFs are abusing the brands of many Fortune 100 banks. A payment-themed message lures target financial services, abusing a retail company's brand.

CobInt | Cobalt Group | URLs
The messages contain links to a PDF file hosted on Microsoft OneDrive. The PDF contains links that lead to the download of "Documents.rtf". The document contains exploits that, if successful, will download CobInt. In the U.S., several employees were targeted by CobInt malware, which is part of the backdoor and downloader families. This attack came from a tracked threat actor who primarily focuses on attacking those in banking/lending, as well as those in the media and entertainment industry. In this case, over 50% of the emails were sent to employees in the financial services industry, making this group the largest target.

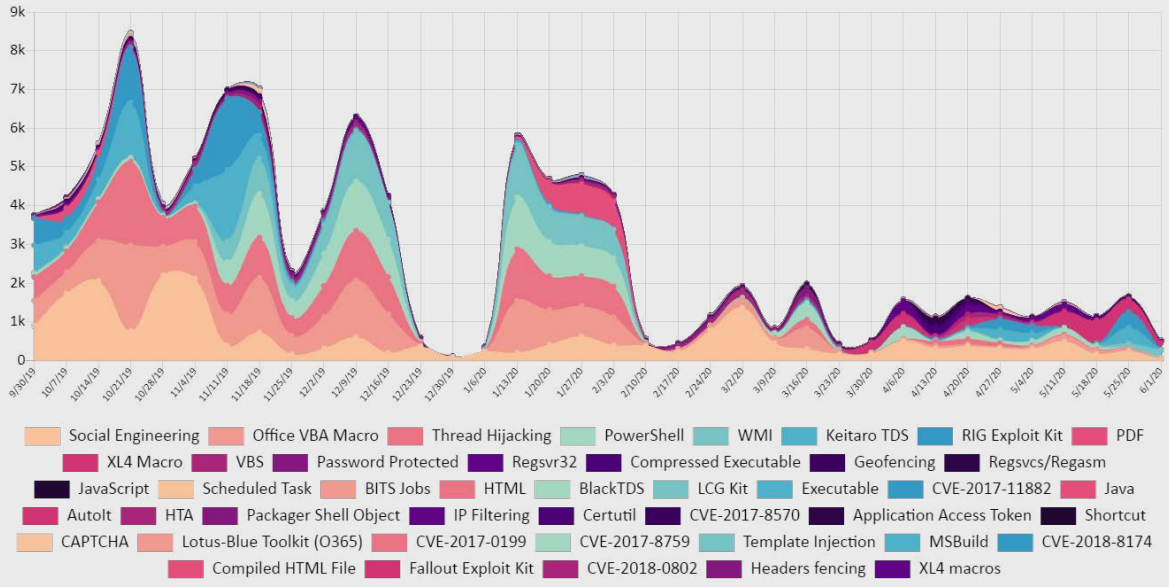


Figure 1: Savings institutions—Targeted exploits (Source: Proofpoint).

Capital markets

Accenture estimates $47 billion USD is at risk for capital markets due to cyberattacks.[8]

QUICK VIEW: SPECIFIC TO THE CAPITAL MARKETS SECTOR	
VAPs:	**Broad Phishing**: • Technology Team • Executive/Managing Partner **Targeted BEC Attacks:** • Financial Advisors/Analysts • Fund Manager/Portfolio Manager • Research Director
Targets:	• Money/Assets (direct): Workforce with access to assets • Clients (indirect): Workforce with access to client data/system
Objectives:	• Sector Disruption • Market/Economic Disruption

Capital markets: Targeted attacks

Proofpoint Threat Intelligence has identified attacks targeting a single capital market role or firm which implies a laser-focused objective using firm-specific reconnaissance.

Obscure payload might actually be ahead of the curve

Although these particular attacks were using unassuming lures, such as shipping invoices, package tracking and IRS subjects, what was novel here is the payload that relies on NodeJS to execute. NodeJS is an execution platform popular on servers and web hosts, so it would be logical to conclude that the payload would not execute when downloaded to a local endpoint.

Here's where it gets interesting: there are several application development frameworks that utilize local NodeJS deployment.[9] Although the majority of the financial applications built on these platforms are geared towards cryptocurrency, there are various open source and freeware applications for stock tracking notification, financial data analytics and open trading platforms (most likely used by the targeted brokerage firms).[10]

Capital markets: Threat analytics and trends

Financial Investing is the most targeted vertical at 31% of messages and 23% of customers. Note that there is some overlap with commercial banking.

Over a six-month period, from 2019/Q4 through 2020/Q2, Proofpoint Threat Intelligence has tracked the following threats consistently targeting the capital markets subsector. (See Figure 2)

[8] Accenture (2020), "The State of Cybercrime in Banking and Capital Markets"
[9] https://brainhub.eu/blog/javascript-frameworks-for-desktop-apps/
[10] https://www.electronjs.org/apps?category=finance

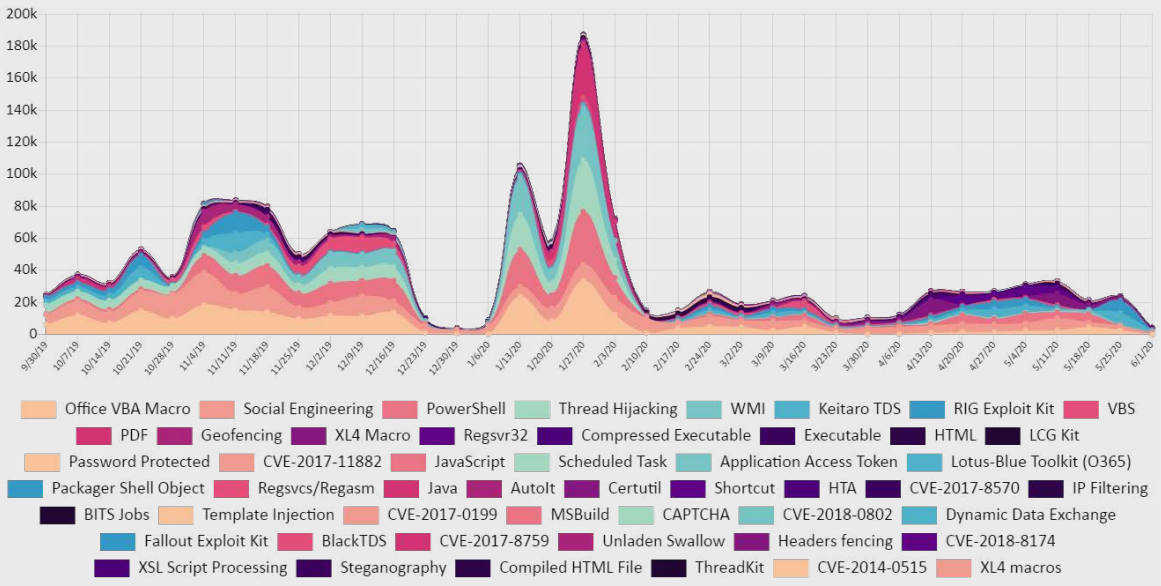


Figure 2: Securities brokerage—Targeted exploits (Source: Proofpoint).

Region-specific attack trend

Analyst comments: Inspecting the top 20 global investment banks—while headquartered in the U.S. and where you would expect a majority of employees to be in London or New York—nearly every firm's top 50 VAPs were located in Singapore, China or Japan.

This may be due to the uptick of APAC-based new hires specifically to respond to the renewed investment interests in APAC-countries. "Bankers see Chinese state-owned companies playing a major role in deal-making in 2020 and expect large floats… to buoy capital markets activity."[11]

Other notable campaigns

QuasarRAT | HTML | "IRS correspondence Notices"

Emails with the subject "IRS correspondence Notices" contain a zipped HTML attachment. The attachment, if opened, drops an embedded Word document. The document uses macros to download a VBscript which in turn downloads QuasarRAT. Capital markets (investments and securities) was the only target of this campaign.

Insurance

Insurance is categorized as a financial services industry sub-sector, as it relies on fiduciary management of funds that must be made available in the event of a disaster. The insurance industry, however, is quite different from the other sub-sectors because its main risks come from external events.

Given this abundance of potential malicious objectives, it is important to pay as much attention to who in your organization is being targeted as much as why they are being targeted.

QUICK VIEW: SPECIFIC TO THE INSURANCE SECTOR	
VAPs:	**Broad Phishing**: • Technology Team • Executive • HR/Recruiter **Targeted BEC Attacks:** • Insurance Agent/Account Manager • Program/Plan Manager (retirement plans, group benefits and more)

In addition, Proofpoint Threat Intelligence reporting shows the insurance sub-sector experienced more successful unauthorized cloud tenant logins than Banking and Capital Markets.

This may be the result of Insurance companies utilizing more big data and AI technologies,[12] which can only be cost-effective through cloud deployments.[13] Or, it can also be the continuous cost optimization of operations through the utilization of robotic process automation (RPA), outsourcing commoditized operations or shifting data and operations to the cloud.[14]

[11] Chatterjee, Murdoch (2020), "Exclusive: Bank of America to hire 50 bankers for Asia dealmaking team in 2020—sources," Reuters

[12] Oliver (2019), "Insurance sector prepares for disruption," Financial Times

[13] Thomson (2020), "Are Insurers' Confidence in their Cyber Defense Exposing Them to Revenue Losses?" Accenture

[14] Deloitte (2020), "Deloitte Insights—2020 Insurance Outlook"

Insurance: Targeted attacks

Proofpoint Threat Intelligence has identified attacks targeting a single insurance role or firm which implies a laser-focused objective using firm-specific reconnaissance.

The Trickbot franchise

Analyst comments: Generally speaking, the larger a campaign is from both the standpoints of overall message volume and number of recipient customers (spread), the less likely that campaign is to be targeted. With the insurance sector specifically, we are seeing some very high concentrations of customer grouping within a single campaign.

In this case, 21 of 26 (81%) recipient organizations are insurance affiliated, and 96% of all messages went to an insurance customer. The majority of the messages go to one particular insurance firm specifically. But it's no accident that another 25 customers receiving fewer messages all belong to the same vertical. Typically, the distribution of recipient verticals is more diversified, but insurance is routinely included in about 10% to 13% of cases, where the top targeted vertical might only see 16% to 18% of messaging.

The malware payload itself is one of the highest-profile banking Trojans—the operators run their botnet using an affiliate model. To understand how commoditized TTPs have become, let's look at how this threat works. A threat actor becomes a client of the Trickbot operators and is assigned a "group tag" differentiator, in this case "yas24," where the three-letter code denotes which campaign/sub-group/affiliate is responsible for infection. The number tends to be iterative as that group continues distributing the malware.

Insurance: Threat analytics and trends

Over a six-month period, from 2019/Q4 through 2020/Q2, Proofpoint Threat Intelligence has tracked the threats consistently targeting the insurance subsector. (See Figure 3)

AZORult | "daffy"

Emails with the subject "Mail Report From support@WellsFargo.com" contain a Microsoft Word document attachment named "purchase order nl5753637.doc" and exploiting CVE-2017-8570. The attachment, if opened, downloads and executes AZORult (aka "daffy.exe"). The insurance vertical receives 85% of messages and comprises 18% of customers.

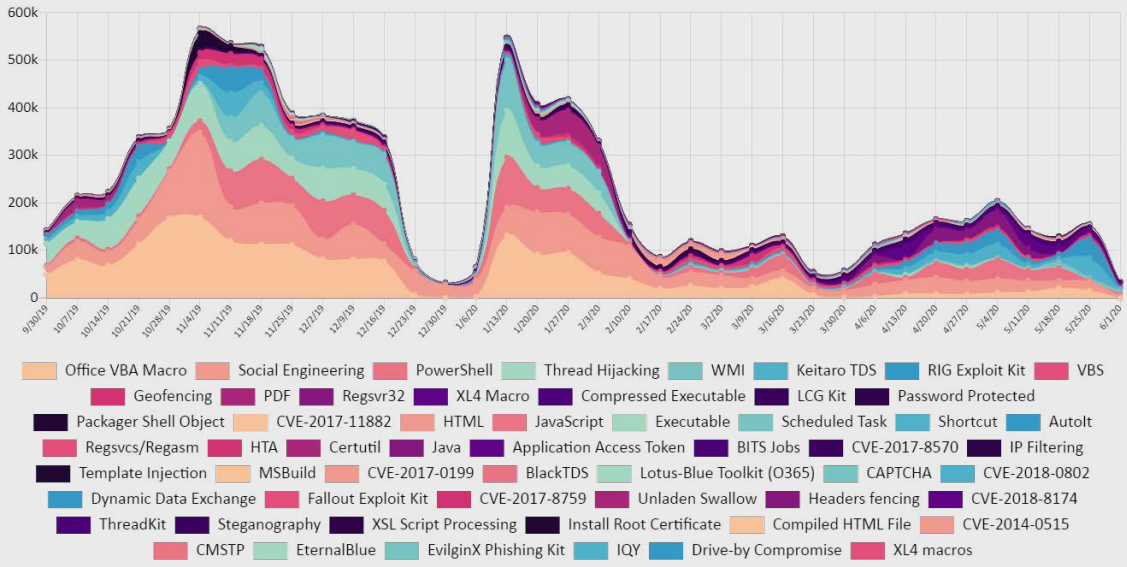


Figure 3: Insurance—Targeted exploits (Source: Proofpoint).

Conclusions and Recommendations

Cybersecurity in the FSI sector must consider not only external attack surfaces, but also security gaps created by internal efforts to optimize processes and technologies. Today's attacks target people, not just technology. They exploit the "human factor" of modern FSI: a desire to help clients achieve their goals and be the engine of opportunity. The global pandemic has forced many financial services and insurance organizations to accelerate digitalization to improve client omnichannel relationship management, solution service and selling. While simultaneously trying to secure and enhance efficiencies for remote staff, keeping information secure and compliant has never been more complex—or more critical. Today's FSI threats and compliance risks require a new, people-centered approach.

We have these recommendations for FSI organizations:

- **Adopt a people-centered security posture.** Attackers do not view the world in terms of a network diagram. They seek out people. Deploy a solution that gives you visibility into who in your organization is being attacked, how they are being attacked and whether they clicked on a malicious link. Consider the individual risk each user represents. A people-centric solution will tell you how your users are targeted, what data they have access to and whether they are prone to falling for attackers' tricks.
- **Use the data from your people-centric program to plan and receive funding for your security programs.** This data will help explain to executive management and the board your priorities and programs to reduce the company's risk profile. Also, use the data to explain to fellow employees across the company the reasons for your program and empower them to defend themselves and the company.
- **Train users to spot and report malicious emails.** Regular training and simulated attacks can reduce risk in two key ways. First, they equip users to stop many attacks. Second, they help reveal users who may be especially vulnerable. The best simulations mimic real-world attack techniques. Consider solutions that address current FSI attack trends and incorporate the latest threat intelligence. When users report suspicious emails, automation can help verify and resolve true threats.
- **At the same time, assume that users will eventually click a link.** Attackers will always find new ways to exploit human nature. Find a solution that spots and blocks inbound email threats targeting users before they reach the inbox. Stop outside threats that use your domain to target customers. Having effective email data loss prevention (DLP) help keep data secure and accessible. Look for a solution that accurately classifies sensitive and critical information and ensures that this data is accessed by the right people.
- **Build a robust business email compromise defense.** Impostor emails can be hard to detect with conventional security tools. Invest in a solution that can manage email based on custom quarantine and blocking policies. Because attackers may use compromised accounts to trick users within the same organization, your solution should analyze both external and internal email. Deploy domain-based message authentication, reporting and conformance (DMARC) email authentication to stop spoofed email—before it defrauds employees, clinical staff and outside business associates.
- **Take a Zero Trust approach to remote access.** Today's FSI organizations store and process more data than ever before. They manage a larger digital footprint. And they operate with more widely dispersed workforces. It all adds up to a new opening for cyber criminals. Additionally, traditional VPN technology just hasn't kept up. Invest in a Zero Trust solution that can quickly and securely connect employees and outside business associates and customers to your data center and cloud
- **Isolate risky websites and URLs.** Keep risky web content out of your environment. Web isolation technology can assess suspicious web pages and unverified URLs in a protected container within a users' normal web browser. This approach can be a critical safeguard for shared email accounts, which are difficult to secure with multi-factor authentication. The same technology can isolate users' personal web browsing and web-based email services. With isolation, you can give users more freedom and privacy without exposing your organization to more risk.

- **Secure Microsoft 365 and other cloud platforms.** As FSI organizations move more data and applications to the cloud, you need to see cloud activity as it unfolds. A cloud access security broker (CASB) can help you scan and act quickly on potential cloud-based email policy violations across the continuum of care.
- **Identify and stop insider threats.** Protect against data loss, sabotage and brand damage that stems from malicious, negligent or compromised insiders. Adopt an insider threat management solution that correlates activity and data movements to help you connect the dots between user behavior and intent. Empower security teams to identify user risk, detect and respond to insider data breaches and speed up incident response.
- **Reduce compliance risk.** FSI compliance regulations are always evolving. Organizations face more audits, bigger fines and the regulatory headaches of outside business associates. Find an archiving and compliance solution that can quickly detect and mitigate insider data leaks, whether malicious or accidental. And identify and stop fraudulent hospital business practices such as billing and kickbacks.
- **Partner with a threat intelligence vendor.** Focused, targeted attacks call for advanced threat intelligence. Use a solution that combines static and dynamic techniques to detect new attack tools, tactics and targets—and then learns from them.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0400-003-01-01 1/21