Trustwave SpiderLabs

2024 Trustwave Risk Radar Report

Financial Services Sector

Trustwave®

2024 Trustwave Risk Radar Report: **Financial Services Sector**

Contents

In 2023, Trustwave released its Financial Services Threat Intelligence Briefing that analyzed the attack flow specific to the financial services sector, offering insight on specific threat actors, actionable intelligence, and recommended mitigations for each stage.

In our 2024 report, the Trustwave SpiderLabs team highlights the unique factors at play in financial services, the significant trends currently affecting the industry, and an overview of the threat actor techniques by attack stage. Additionally, Trustwave SpiderLabs created two complementary deep-dive writeups containing extensive research and analysis on two looming threats: phishing-as-a-service and insider threats.

Recent research by the Ponemon Institute identifies malicious insiders as the costliest type of data breach, with phishing as the second most expensive and the most prevalent. Our in-depth analysis explores why these threats are particularly pervasive in the financial services sector.

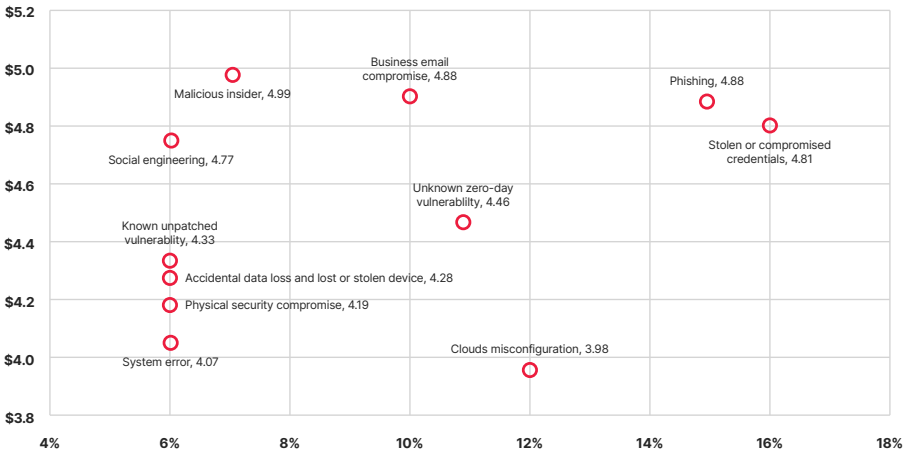

Figure 1: Cost and frequency of a data breach by initial attack vector; measured in USD millions; percentage of all breaches. Source: Ponemon Institute.

Financial services organizations are a goldmine for cybercriminals. With their abundance of sensitive financial data and large sums of money, these institutions are highly attractive to attackers. Cyberattacks on this sector have surged, as threat actors exploit vulnerabilities to extort, steal, and defraud financial institutions and their customers. The potential for substantial financial gain drives a relentless pursuit of these lucrative targets. According to Ponemon research, the cost of a breach in the financial services sector is $6.08 million, making it the second most expensive sector, just behind healthcare.

Key Report Findings for the Financial Services Sector

24%
of ransomware attacks were ALPHV

65%
of ransomware attacks were in the US

49%
of attacks originated from phishing

37%
of phishing emails contain HTML attachments

20%
of ransomware attacks were against banking institutions

73%
of credentials access techniques were brute-force attempts

Financial Services' Unique Threat Landscape

Expanded Regulatory Requirements

- The European Union's Digital Operational Resilience Act (DORA) represents a significant shift in how financial institutions are expected to manage and respond to cyber threats. This regulation mandates that organizations must not only implement robust cybersecurity measures but also continuously test their resilience to cyber incidents.
- DORA, along with other regulations like the GDPR and PCI-DSS, requires financial institutions to maintain comprehensive cybersecurity frameworks, conduct regular audits, and demonstrate their preparedness for potential cyberattacks. Compliance with these regulations ensures that financial institutions maintain high standards of security and operational resilience, directly influencing their cybersecurity strategies.
- The regulatory landscape extends beyond Europe. Jurisdictions like the United States and Australia have also introduced stringent cybersecurity requirements for financial institutions. In the US, regulations such as the Gramm-Leach-Bliley Act (GLBA) and the Cybersecurity Framework (CSF) impose specific obligations on financial firms. Similarly, Australia's Privacy Act and the Security of Critical Infrastructure Act (SOCI) mandate robust cybersecurity practices.
- Complying with multiple overlapping regulations, often with varying requirements and enforcement mechanisms, is extraordinarily intricate in nature.

Cryptocurrency Evolution

- As cryptocurrencies gain legitimacy and integration into traditional banking systems increases, the financial services industry faces new cybersecurity challenges. The rise of digital wallets and crypto transactions introduces potential targets for cybercriminals, such as infostealers that focus on capturing private keys and wallet credentials.
- Financial institutions must adapt by developing robust protection mechanisms for digital assets and ensuring the security of their customers' cryptocurrency holdings. This includes implementing advanced security protocols for wallet protection, monitoring for suspicious activities, and educating consumers about best practices in managing their digital assets.

Jersey Financial Regulator Leaks Private Documents in Second Data Breach of 2024

July 2024, **Financial Times**

Consumer Protection Considerations

- The financial services industry is a prime target for various forms of cyber threats aimed at stealing sensitive consumer information. Banking trojans, for instance, can capture login credentials and facilitate unauthorized transfers of funds. Phishing attacks continue to evolve, targeting individuals with sophisticated schemes designed to extract personal and financial information. Additionally, Magecart attacks, which involve injecting malicious code into e-commerce sites to capture credit card data, pose a significant risk.
- Financial institutions must implement advanced threat detection and response systems, educate their customers on recognizing and avoiding scams, and ensure robust mechanisms are in place to protect consumer data.

Heightened Risk Aversion

- Financial institutions operate under a high level of risk aversion due to the potential impact of security breaches on their operations, reputation, and regulatory compliance. This heightened risk sensitivity drives a proactive approach to cybersecurity, with organizations investing in advanced technologies and dedicated teams to preemptively address vulnerabilities.
- The financial sector's emphasis on minimizing risks results in stringent security protocols, frequent updates to security measures, and a focus on incident response and recovery planning.

Franchise Model

- The franchise model in the financial services industry introduces variability in cybersecurity practices across different branches and entities. With different franchisers and franchisees adopting diverse business models, there can be significant disparities in the consistency and effectiveness of cybersecurity policies and their implementation.
- This fragmentation can lead to uneven protection levels and potential vulnerabilities. Standardizing cybersecurity practices across franchises and ensuring uniform adherence to industry best practices are crucial for maintaining a cohesive and resilient security posture throughout the organization.
- Ensuring compliance with regulatory requirements across a franchise network can be complex, especially when dealing with different jurisdictions and varying local regulations. This requires a coordinated approach to maintain consistent security and compliance.

Trustwave SpiderLabs

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 200,000 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 10k per day that are uniquely identified by Trustwave SpiderLabs. Our diverse coverage of infosec disciplines, including Advanced Continuous Threat Hunting, Digital 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 examines the myriads of threats facing the financial services industry. In addition to supplemental reports focused on insider threats and phishing-as-a-service, Trustwave SpiderLabs will offer recommendations to help financial institutions mitigate risks and safeguard their customers and data.

Notable & Prominent Trends in Financial Services

Growing Risk of Insider Threats

The Threat

We explore insider threats in-depth in our accompanying report. At a high level, here are some key points to consider:

Insider threats are often overlooked in an organization's overall security posture. While news outlets frequently highlight ransomware attacks and data breaches, they often neglect the potential dangers posed by employees.

Unlike external attackers, insiders already have access to critical systems, making it easier for them to bypass traditional security measures. Insider motives can vary widely, including financial gain, personal grievances, or coercion by external threat actors.

Insider threats generally fall into two main categories: unintentional and intentional.

Unintentional Insider Threats:

- Unintentional insider threats can result from negligence or accidents. Negligent threats occur when employees are careless, such as by ignoring updates or security patches.
- Accidental threats arise from genuine mistakes, such as sending sensitive information to the wrong email address or inadvertently opening a phishing email.

Intentional Insider Threats:

- Intentional insider threats are categorized as malicious or collusive. Malicious insiders actively seek to harm the organization, often for personal benefit or out of grievance.
- For instance, they might delete critical databases to create operational issues if they feel wronged. Collusive insider threats involve individuals who collaborate with external threat actors or groups to compromise the organization.

What Trustwave Is Seeing

The Trustwave SpiderLabs team conducted a threat hunt to identify behaviors indicative of insider threats. They discovered that 48% of the risky findings were related to **T1219 Remote Access Software and T1572 Protocol Tunneling**.

Another notable threat vector observed during this campaign was **T1052 Exfiltration over Physical Medium**, specifically the sub-technique **Exfiltration over USB**.

Then, the Trustwave SpiderLabs team took to the Dark Web to analyze the demand for malicious insiders, why insiders become malicious, and how threat actors are recruiting.

Several factors drive individuals to become malicious insiders. Financial gain is a primary motivator, as insiders may sell sensitive information or facilitate breaches for profit. Personal grievances, such as dissatisfaction with their employer, can also lead insiders to engage in malicious activities.

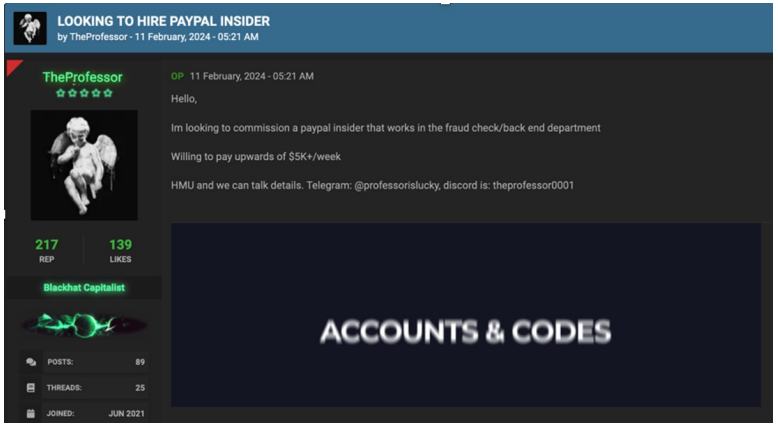

Figure 2: Threat actor offers a high salary for PayPal's insider services

The above threat actor offering additional payment to the PayPal employee is both serious and knowledgeable, as evidenced by their salary offer. This individual is a respected forum user with a high reputation score of 217, 139 likes, and 89 posts. The golden highlights on their nickname, status, and rate suggest that they are a high-level, possibly paid account with an escrow deposit, indicating their trustworthiness and influence within the forum.

Mitigations to Reduce Risk

- **Access and Usage Controls:** Reduce RMM (Remote Monitoring and Management) usage to one tool, enforcing restrictions on authorized accounts and their locations.
- **Continuous Monitoring:** Implement continuous monitoring of employee activities to detect unusual behavior or access patterns.
- **Access Controls:** Enforce strict access controls and the principle of least privilege to limit access to sensitive information.
- **Enhanced Vetting Processes:** Strengthen background checks during the hiring process to identify potential risks.
- **Anonymity and Reporting:** Create anonymous reporting mechanisms for employees to report suspicious activities without fear of retribution.

More Than 450K hit by JPMorgan Breach

May 2024, **SC Media**

Phishing-as-a-Service Goes Mainstream

The Threat

We cover phishing-as-a-service in-depth in our accompanying report. At a high level, here are some key points to consider:

Phishing-as-a-Service (PaaS) has emerged as a major cybersecurity threat to the financial sector. This "Cybercrime-as-a-Service" model offers sophisticated phishing tools and services that can be accessed through underground forums and Telegram marketplaces.

Today, many phishing emails targeting corporate networks are part of campaigns driven by PaaS platforms.

What Trustwave Is Seeing

The accompanying report provides an in-depth analysis of how PaaS operates, its features, and various platforms, including a detailed case study of Tycoon PaaS.

Attackers have increasingly adopted HTML and PDF attachments to transport, hide, and obfuscate phishing URLs. These attachment types are common and often bypass email scanning gateways.

- HTML attachments can serve as self-contained phishing pages, redirectors to phishing sites, or use HTML smuggling techniques to deploy malware.
- PDF attachments may include links that redirect to phishing pages or malware downloads, or they might contain QR codes leading to malicious content.

Malicious Email Attachments

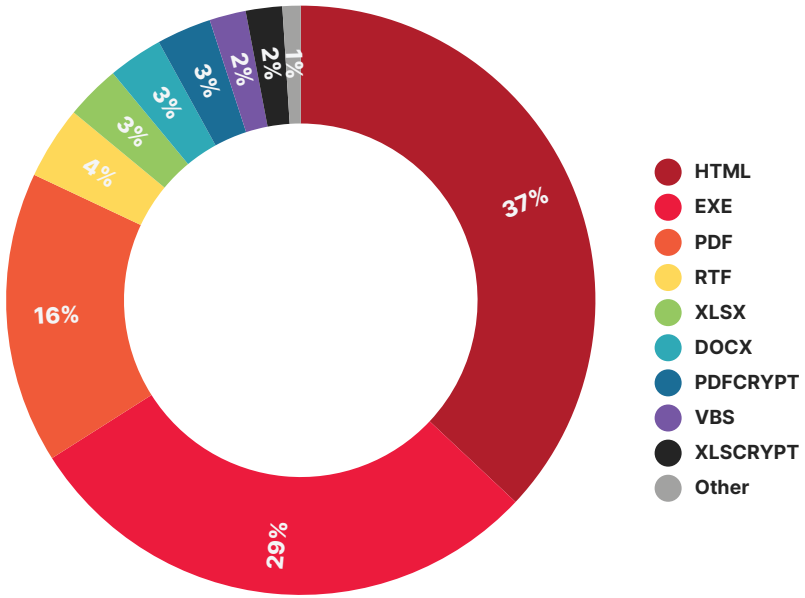

Figure 3: Malicious email attachment types; June 2024

Mitigations to Reduce Risk

- **Advanced Training and Awareness Programs:** Continuously update training to educate employees on the latest phishing tactics and prevention methods.
- **Layered Email Security:** Tools like Trustwave MailMarshal provide layered protection against email-based threats, capturing all forms of threats to protect an environment and reduce the burden on security teams.
- **Email Filtering and Analysis:** Use advanced email filters with machine learning to detect anomalies, analyze headers, and assess sender reputation.
- **Regular Audits and Simulations:** Perform regular security audits and phishing simulations to evaluate and improve organizational readiness against phishing attacks.
- **Collaboration and Intelligence Sharing:** Engage in industry collaborations to stay updated on emerging phishing trends and share critical security insights.
- **Hardware-based Authentication:** Implement FIDO2 authentication with cryptographic keys stored on hardware devices to prevent MFA bypass attacks and ensure secure authentication.

Ransomware Groups Continue to Target Financial Services

Threat

Ransomware poses a significant and escalating threat to financial institutions and the broader financial services sector. As these organizations handle vast amounts of sensitive data and financial transactions, they are prime targets for cybercriminals seeking to disrupt operations and extract large ransoms. The impact of a ransomware attack on a financial institution can be catastrophic, leading to operational paralysis, substantial financial losses, and severe reputational damage. Attackers often deploy sophisticated encryption methods to lock access to critical systems and data, demanding hefty ransoms in cryptocurrency, which further complicates recovery efforts and legal responses.

The financial services sector is particularly vulnerable due to its interconnected nature and the reliance on complex IT infrastructures. Institutions such as banks, investment firms, and insurance companies manage intricate networks of information systems that, if compromised, can have ripple effects across the entire economy. The downtime caused by ransomware attacks can disrupt not only daily operations but also critical financial transactions, affecting everything from individual bank accounts to international market stability. Moreover, the regulatory environment around financial institutions requires them to adhere to stringent data protection and reporting standards, adding layers of complexity to their response and recovery strategies.

In addition to the direct financial costs and operational disruptions, ransomware attacks on financial institutions can lead to a loss of customer trust and regulatory scrutiny. Customers expect high levels of security and reliability from their financial service providers, and any breach can erode confidence and drive customers to seek more secure alternatives. Regulatory bodies may impose hefty fines and mandate enhanced security measures, further straining the resources of affected institutions.

What Trustwave Is Seeing

Trustwave SpiderLabs analyzed ransomware incidents targeting the financial services sector and identified AlphV and LockBit as the predominant groups operating in this space. Last year, AlphV accounted for 10% of attacks, but this year their share has increased to 24%. Similarly, LockBit's share was 24% last year, compared to 23% this year.

Though threat actors target companies worldwide, the majority of reported breaches involve organizations from the US, with Brazil and Canada coming in second and third, respectively. The proportion of breaches affecting US companies has increased from 51% last year to 65% this year.

Top Ransomware Groups

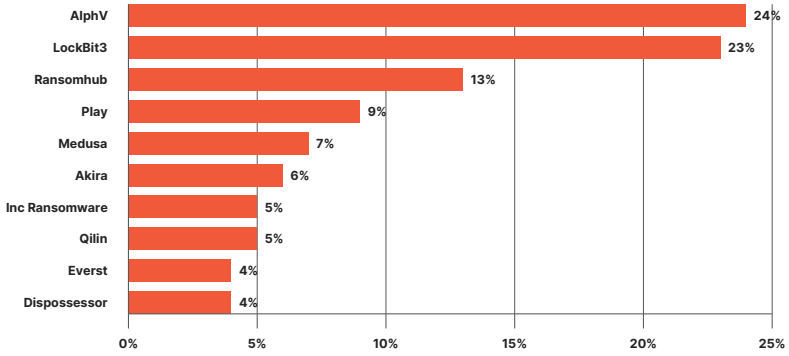

Figure 4: Top ransomware groups targeting financial services

Top Countries Impacted

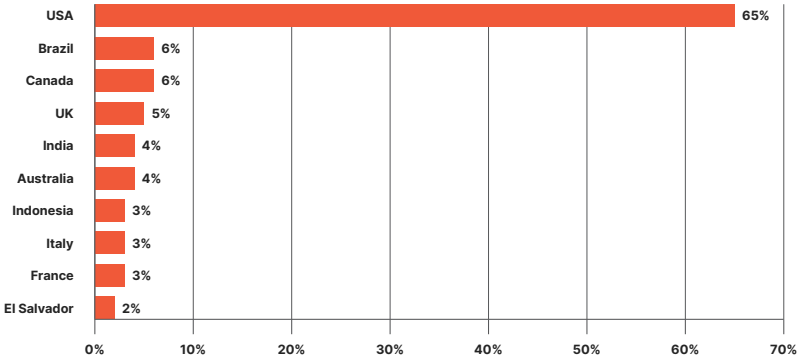

Figure 5: Financial services organizations affected by ransomware by country

Data Breach Affects 57,000 Bank of America Accounts

February 2024, **American Banker**

Perhaps unsurprisingly, banking is the top target for ransomware attacks, accounting for 20% of incidents, followed closely by the insurance sector at 18%. It's important to note that no subsector is immune from these attacks. Credit unions are targeted 8% of the time, while loan and legal services, as well as wealth management firms, each face a 6% attack rate. This distribution underscores the need for robust cybersecurity measures across all financial services sectors.

Top Industry Types Impacted

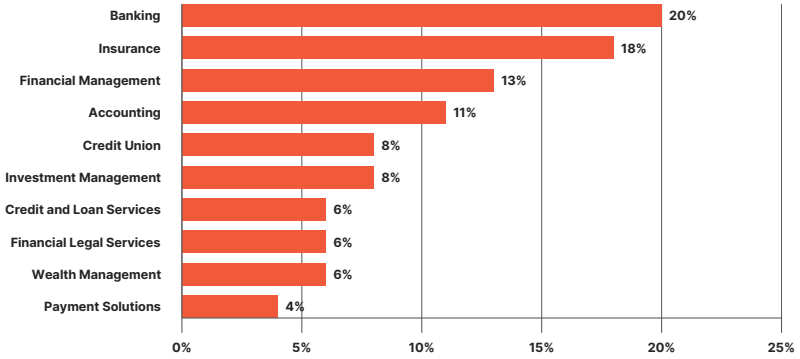

Figure 6: Ransomware attacks by financial services type

Mitigations to Reduce Risk

- **Use Host-Based Anti-Malware Tools:** Deploy anti-malware tools on individual hosts to identify and quarantine specific malware. Be aware that these tools have limitations and may be circumvented by custom malware packages.
- **Enable and Audit System Logs:** Activate logging on valuable systems and workstations. Implement network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels. These logs are crucial for identifying potential compromises.
- **Active Monitoring of Logs:** Regularly monitor logs to detect abnormal behavior or traffic. Establish a baseline of normal activity to make deviations more noticeable, as merely enabling logs without active monitoring diminishes their effectiveness.
- **Establish a Formal Incident Response Process:** Develop and routinely practice a formal incident response plan to ensure a swift and coordinated reaction to ransomware attacks.
- **Ongoing Underground and Dark Web Monitoring:** Continuously monitor the underground and dark web for information leakage that might have been overlooked. This can provide early warnings about potential threats or data exposure.

Prudential Financial Data Breach Impacts 2.5 Million

February 2024, **SecurityWeek**

Evolution of Emerging Technology: Cryptocurrency and Deepfakes

Threat

As emerging technologies advance rapidly, they bring both transformative opportunities and new challenges, particularly in cybersecurity.

For the financial services sector, the evolution of cryptocurrencies and the rise of deepfake technology represents a double-edged sword. While these innovations offer enhanced efficiency and new avenues for growth, they also introduce significant security risks that require proactive and sophisticated responses.

Cryptocurrency, once a niche financial product, has become a mainstream asset class, increasingly integrated into traditional financial systems. This integration opens up new attack vectors, including the theft of digital assets and hacking of cryptocurrency exchanges. The EU's Markets in Crypto-Assets Regulation (MiCA) aims to mitigate these risks by establishing a comprehensive regulatory framework for the crypto-asset market.

Deepfake technology, meanwhile, presents an emerging threat in the form of highly convincing but fabricated digital content. These synthetic media can be used to deceive individuals and organizations, undermining trust and facilitating fraud.

Earlier this year, a finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call.

What Trustwave Is Seeing

Cryptocurrency Risks: The surge in cryptocurrency adoption has created several new security challenges:

- **Wallet Theft:** Digital wallets, essential for storing cryptocurrencies, are prime targets for cybercriminals. Successful attacks can result in the irreversible loss of funds.
- **Exchange Hacks:** Cryptocurrency exchanges, where users trade digital assets, are increasingly targeted by hackers seeking to exploit vulnerabilities and steal assets on a large scale.
- **Cryptojacking:** Malicious actors may use infected systems to mine cryptocurrencies without the user's consent, leading to significant operational disruptions and financial losses.

In February 2024, Trustwave SpiderLabs discovered Ov3r_Stealer, a malware designed to steal credentials and crypto wallets through Facebook job advertisements.

The observed Ov3r_Stealer malware is designed to collect and exfiltrate the following data:

Data Type	Location
Crypto Wallets	C:\Users\IEUser\AppData\Roaming\wallet.dat
	C:\Users\IEUser\AppData\Roaming\Coinomi\Coinomi\wallets
	C:\Users\IEUser\AppData\Roaming\bytecoin
	C:\Users\IEUser\AppData\Roaming\Electrum\wallets
	C:\Users\IEUser\AppData\Roaming\Exodus\exodus.wallet
	C:\Users\IEUser\AppData\Roaming\com.liberty.jaxx\IndexedDB\file_0.indexeddb.leveldb
	C:\Users\IEUser\AppData\Roaming\Guarda\Local Storage\leveldb

Figure 7: Types of cryptowallets the Ov3r_Stealer malware is designed to exfiltrate

Deepfake Threats: The proliferation of deepfake technology has introduced several cybersecurity concerns:

- **Identity Fraud:** Deepfakes can be used to impersonate individuals, potentially leading to fraudulent transactions or unauthorized access to sensitive information.
- **Phishing Scams:** Cybercriminals can leverage deepfakes to create convincing videos or audio recordings that trick individuals into disclosing personal or financial information.
- **Reputation Damage:** Financial institutions may face significant reputational damage if deepfakes are used to spread false information or manipulate public perception.

Recently, Trustwave was asked to create a fake video of a client's CEO using nothing but publicly accessible tools. The video would be shown during a company town hall on the dangers of social engineering. Trustwave SpiderLabs researchers wrote about the experiment and how easy a deepfake was to create.

A notable mention here is also biometrics. Trustwave SpiderLabs frequently employs AI to crack complex passwords during penetration testing and Red Team engagements. If security professionals use these tactics, it's reasonable to assume that malicious actors do as well. While biometrics represent a significant advancement beyond traditional usernames and passwords, they are not a cure-all. Organizations must remain vigilant and continue to strengthen their security measures.

Mitigations to Reduce Risk

- **Enhanced Wallet Security:** Implement advanced encryption and multi-factor authentication (MFA) for digital wallets to protect against unauthorized access and theft.
- **Secure Exchanges:** Ensure that cryptocurrency exchanges utilize robust security protocols, including regular security audits, penetration testing, and real-time monitoring to detect and respond to breaches.
- **User Education:** Educate customers on best practices for managing and securing their cryptocurrency assets, including recognizing phishing attempts and securing their private keys.
- **Advanced Detection Technologies:** Invest in technologies capable of detecting deepfakes and other forms of synthetic media. This can include machine learning algorithms and forensic analysis tools designed to identify inconsistencies and anomalies.
- **Verify Identities:** Implement multi-layered authentication processes to verify identities before authorizing transactions or providing access to sensitive information. This may involve combining biometric verification with traditional methods.
- **Employee Training:** Train employees to recognize and respond to potential deepfake attacks, including verifying the authenticity of communications and reports.
- **Incident Response Planning:** Develop and regularly update incident response plans to address potential breaches related to cryptocurrencies and deepfakes, ensuring swift and coordinated action.
- **Industry Collaboration:** Participate in industry forums and information-sharing networks, like FS-ISAC, to stay informed about emerging threats and collaborate on developing effective countermeasures.
- **Regulatory Compliance:** Ensure adherence to regulatory requirements related to cybersecurity and data protection, adapting policies as necessary to address new challenges posed by emerging technologies.

Data Breach Confirmed by Toyota Financial Services

December 2023, **SC Media**

China's ICBC, the World's Biggest Bank, Hit by Ransomware Attack that Reportedly Disrupted Treasury Markets

November 2023, **CNBC**

Threat Actor Techniques by Attack Stage

Data breaches and compromises come in many forms, but they often follow a similar pattern. Attackers gain access, escalate privileges, establish a foothold, steal, or destroy data, and then vanish. Trustwave SpiderLabs analyzed data from Fusion to understand the path that threat actors take within financial services and the techniques they deploy at each stage.

Initial Access Techniques

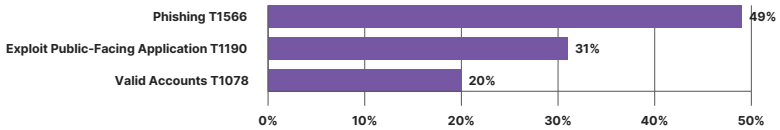

Figure 8: Initial access techniques used by attackers of financial services

Almost half of all initial access techniques used by threat actors to gain entry to financial services entities were phishing (49%). Following that, threat actors exploited public-facing applications, including vulnerabilities such as Apache Log4J, SQL injection, and potential ZeroLogon attempts.

Execution Techniques

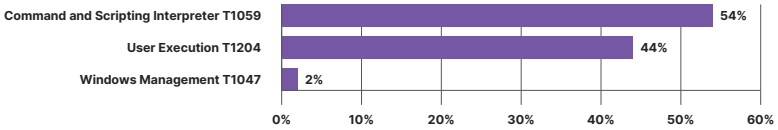

Figure 9: Execution techniques used by attackers of financial services

In financial services security incidents, execution techniques predominantly involve command and scripting interpreters (54%), such as PowerShell, and User Execution (44%) of malicious files and links. Attackers commonly use PowerShell to execute commands and scripts on compromised systems, as well as to download and run malicious payloads. Another prevalent technique involves social engineering to persuade users to open malicious files, leading to code execution.

Credential Access Techniques

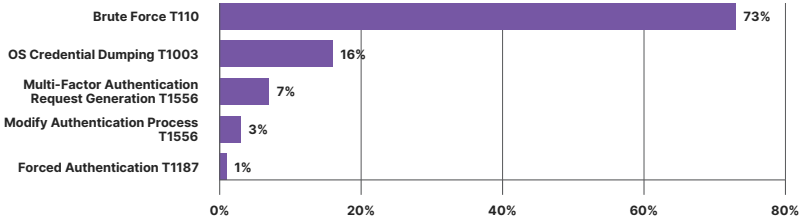

Figure 10: Credential access techniques used by attackers of financial services

Credential access techniques observed in attacks against financial services organizations predominantly involved password brute-force attempts (73%). Additionally, OS credential dumping using Mimikatz (16%) and MFA fatigue attacks (7%) were also observed.

Lateral Movement Techniques

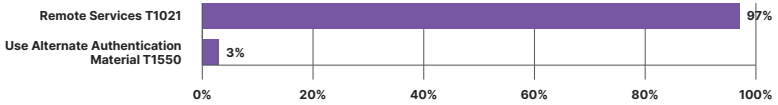

Figure 11: Lateral movement techniques used by attackers of financial services

To move laterally within financial services organizations, attackers almost always used remote services (97%). These remote services predominantly include Remote Desktop Protocol (RDP) and SMB/Windows admin shares.

Persistence Techniques

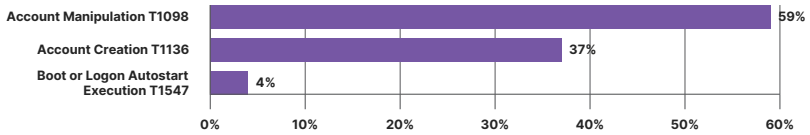

Figure 12: Persistence techniques used by attackers of financial services

Lastly, the persistence techniques observed were account manipulation (59%) and account creation (37%). Account manipulation involves modifying existing accounts to either maintain access or escalate privileges. For example, an attacker might change account permissions or add their own credentials to an existing user account to retain access. Account creation refers to the creation of new user accounts by attackers. These new accounts are often used to maintain access or to disguise their activities as legitimate users.

Fidelity National Financial Subsidiary Says 1.3M Affected by November Cyberattack

November 2023, **Cybersecurity Dive**

Conclusion & Key Takeaways

The 2024 Trustwave Risk Radar Report underscores the escalating cyber threats faced by the financial services sector. As the industry continues to be a prime target for cybercriminals, the need for comprehensive and proactive security measures has never been greater. This report highlights the sophisticated nature of current threats, including phishing-as-a-service and insider threats, and provides a detailed analysis of how these issues impact financial institutions.

The financial services sector remains highly attractive to attackers due to its valuable assets and sensitive data. Recent incidents reveal a disturbing trend in the rise of cyberattacks, with phishing, ransomware, and insider threats emerging as significant concerns. The implementation of robust security measures, adherence to regulatory requirements, and continuous vigilance are essential to mitigating these risks.

Trustwave SpiderLabs' extensive research and insights offer actionable recommendations for financial institutions to enhance their cybersecurity posture. By adopting advanced training programs, implementing layered security solutions, and engaging in industry collaboration, organizations can better protect themselves and their customers from emerging threats.

Key Takeaways

1. **Heightened Threat Landscape:** Financial services are increasingly targeted by sophisticated cyberattacks, including phishing-as-a-service and ransomware. The sector's substantial financial and data assets make it a prime target for cybercriminals.
2. **Costly Insider Threats:** Malicious insiders pose a significant risk, being the most expensive type of data breach according to recent research. Both unintentional and intentional insider threats require targeted mitigation strategies.
3. **Regulatory Pressures:** Compliance with evolving regulations like the EU's DORA and other international standards is crucial for managing cybersecurity risks. Adherence to these regulations ensures robust security and operational resilience.
4. **Emerging Technology Risks:** The rise of cryptocurrencies and deepfake technology introduces new security challenges. Financial institutions must develop advanced protection mechanisms for digital assets and implement measures to detect and counteract deepfakes.
5. **Phishing-as-a-Service:** The proliferation of phishing-as-a-service platforms has made phishing attacks more accessible and prevalent. Financial institutions should enhance their email security and training programs to address this growing threat.
6. **Proactive Measures:** Implementing continuous monitoring, enforcing strict access controls, and strengthening background checks are critical steps in reducing risk. Regular security audits and phishing simulations are also essential for maintaining readiness.
7. **Ransomware Resilience:** Ransomware attacks remain a major threat, with notable groups like AlphV and LockBit targeting the financial sector. Regular data backups, securing remote desktop services, and updating security patches are key defenses against ransomware.

By addressing these key areas, financial institutions can improve their resilience against cyber threats and safeguard their operations and customer data more effectively.


Trustwave®