Trustwave SpiderLabs

Financial Services
Deep Dive

Insider Threat

Contents

Overview

Insider threats are an often-overlooked aspect of the overall security posture of an organization. News outlets consistently report on ransomware reports and data leaks, while often leaving out the potential dangers an employee presents. When these attacks are reported, the attacker is often presented as malicious and intentional, but this is not always the case.

Insider threats fall into two main categories, unintentional and intentional. Unintentional insider threats can come in the form of either negligent or accidental. Negligent insider threats are realized through an employee's carelessness, such as ignoring messages to install patches. An accidental insider threat occurs by mistake, such as mistyping an email address or unknowingly opening a phishing email.

Average cost of an insider threat is $5 million (USD)

The other category of insider threat is far more nefarious: intentional insider threats come in two categories, malicious and collusive. Malicious insider threats work to actively harm the organization where they work. This is often done for personal benefit or personal grievance. A malicious insider may delete critical organizational databases to create operational problems to get back at the company if they feel they have been wronged. Alternatively, a collusive insider threat is when an individual works with a threat actor or group to compromise an organization. Utilizing collusive insider threats is one of the main ways LAPSUS$ gains an initial foothold in an organization. They have offered monetary gain to attract insiders to give them VPN access to organizational assets.

While there are unique types of insider threats, insider threat attacks have become more frequent over the past 12 months, with 40% of organizations reporting more frequent insider threat attacks compared to previous years. Additionally, organizations are facing more than just one instance of an insider threat. Over the past 12 months, 45% of organizations report that more than five instances have occurred.

While the amount of insider threats seems to be increasing, the cost associated with these types of incidents also increases. With an average cost of $5 million (USD) per insider threat, these employees can have major fiscal consequences.

Typically, insider threats, whether they are intentionally malicious or accidental, will fly under the radar and behaviors of personnel are baselined as “normal.” This presents a challenge in detecting insider threats and why modern threat adversaries will do their best to mimic everyday personnel behavior.

The Malicious Insider Threat

The financial services sector is navigating an increasingly complex and dangerous cyber threat landscape. Among the various risks, malicious insiders have become a significant concern. These individuals, who possess authorized access to sensitive systems and data, can exploit their positions to cause severe harm. Unlike external attackers, insiders already have the keys to the gate, making it easier for them to bypass traditional security measures. The motives of these insiders can range from financial gain to grievances or coercion by external threat actors.

Despite the adoption of new technologies, payment systems, and innovations, malicious actors seem to prefer addressing ongoing issues not by exploiting system weaknesses or hacking financial institutions, but by taking a relatively easier route: leveraging malicious insiders.

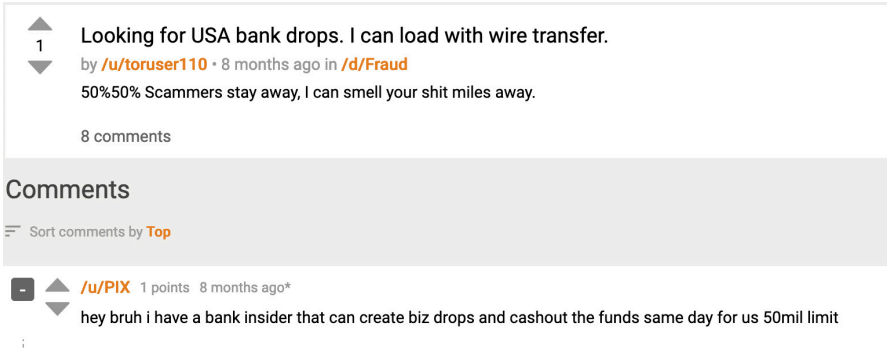

Figure 1: The actor on the Dark Web conversation board is looking for cooperation to withdraw money

The collaboration between insiders in banks and financial institutions poses a significant threat to end users. Bank insiders can provide sensitive financial information, while telecom insiders can offer access to personal communication data. This synergy enables malicious actors to execute highly sophisticated attacks, such as identity theft, unauthorized transactions, and comprehensive surveillance.

The consequences for victims include financial loss, privacy invasion, and potential blackmail. If this collaboration becomes a widespread practice, it could open a “gate to hell,” leading to an era of unprecedented cybercrime where personal and financial data security is severely compromised. This normalization could erode trust in both financial and telecommunication systems, making it difficult for consumers to feel secure in their interactions with these essential services.

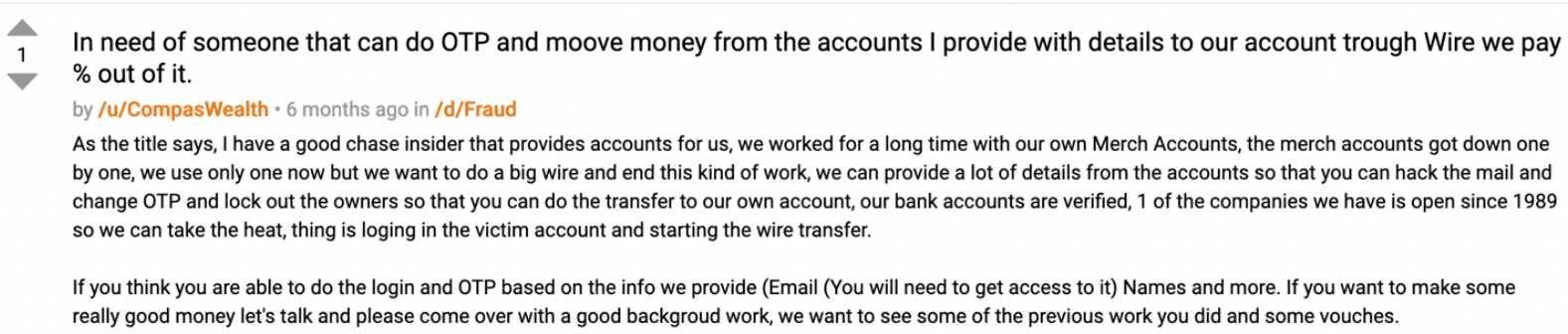

Figure 2: The actor is looking for cooperation in moving serious amounts of money from accounts provided by a malicious insider

The extent of insider infiltration is difficult to imagine and indicates a significant level of intrusion. This approach allows cybercriminals to bypass many security measures, gaining direct access to sensitive information and systems with less effort compared to traditional hacking techniques.

The Demand for Malicious Insiders

Malicious insiders are sought after by cybercriminals due to their ability to combine insider knowledge with external malicious capabilities.

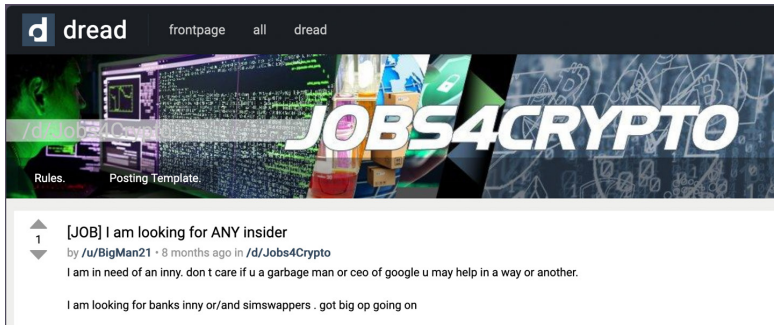

Figure 3: The actor is looking for a malicious insider from any position

Closed, dedicated Telegram channels often feature requests for connections with malicious insiders, highlighting the growing demand for their services. This collaboration between insiders and external hackers amplifies the threat, leading to substantial financial losses and long-term reputational damage for financial institutions.

12/06/2024, 0:25:26
any bank teller innys/workers in NJ, PA, MD, OR OH areas?

12/06/2024, 0:27:30
That's what I'm looking for Chase/TD inny

03/07/2024, 16:04:18
looking for a cb inny for an simple task dm me big $

Figure 4: Quotes from Cyber Group's Telegram Channels

Why Insiders Become Malicious

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

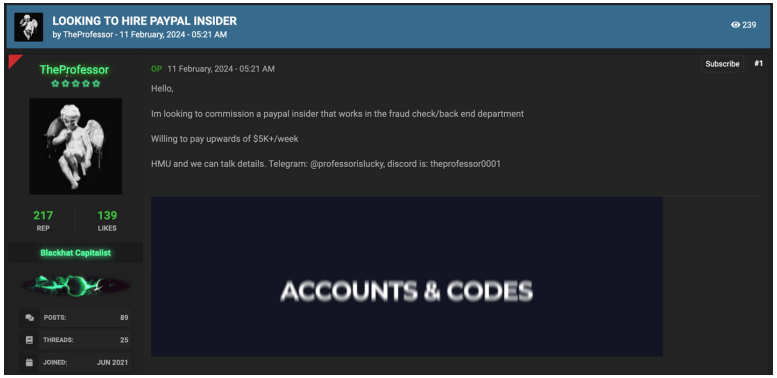

Figure 5: The actor offers a high salary for PayPal's insider services

The actor offering additional payment to the PayPal employee is serious and knowledgeable, offering such a salary. This actor 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 indicate that they are a high-level, possibly paid account with an escrow deposit, signifying their trustworthiness and influence within the forum.

External actors sometimes coerce insiders through blackmail or other means, compelling them to exploit their access. Additionally, some insiders are motivated by ideological beliefs, seeking to advance political or social agendas. The allure of easy money and the perceived low risk of getting caught further contribute to the rise in insider threats.

Recruiting Malicious Insiders

Recruitment of malicious insiders in financial institutions varies by region. In the US, recruitment often involves exploiting financial difficulties or personal grievances. Cybercriminals might target employees through social engineering, offering substantial financial incentives, or leveraging blackmail. Online forums, darknet marketplaces, and closed communication channels are common platforms for these recruitment efforts.

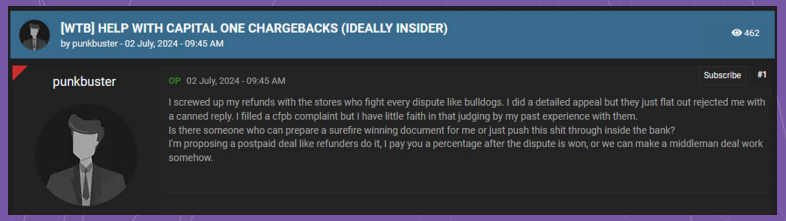

Figure 6: The actor offers compensation for insider to solve its bank issue

In Russia, the recruitment process may involve a mix of coercion and enticement. Insiders might be approached through underground networks or corrupt intermediaries, high-ranking malicious insiders that are already present in the system. Additionally, patriotic, or political motivations can play a role, with some individuals cooperating to support nationalistic agendas. Both US and Russian malicious insiders use of encrypted communication channels and covert operations to avoid detection and maintain secrecy.

Malicious insider recruitment in Dark Web platforms is mostly addressed not to end users but a physical provider who established or know already someone who would be happy to gain some good money in addition to their salary. The Russian malicious insider's cooperation advertisements are mostly bulk fields since initially these advertisements were done by an organization that retrieves information about people and claims to be able to solve issues in different fields.

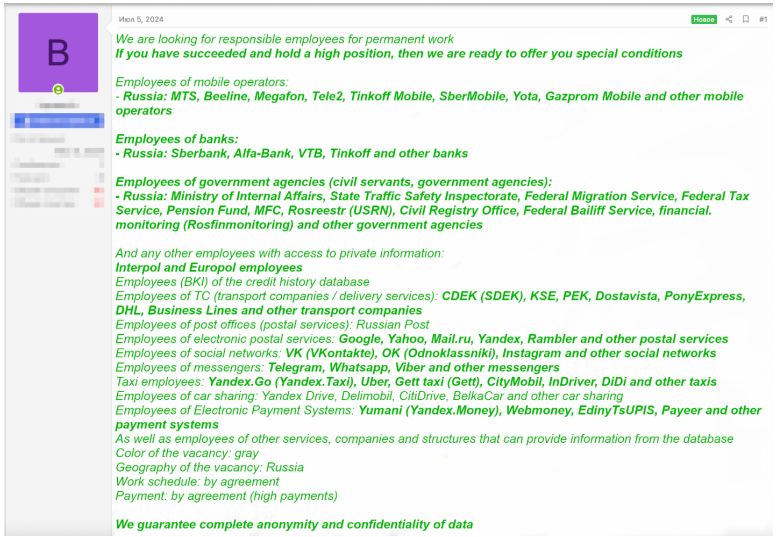

Figure 7: Actor on the Dark Web advertises cybergroup's needs in insider from a variety of organizations (note: Translated from Russian)

Sanctions have undoubtedly impacted operations, networking, and business expansion, often leading to the breaking of old relations and the formation of new ones. Recent recruitment advertisements on Russian Dark Web forums now target not only local services but also representatives from global corporations like Google, Yahoo, Telegram, and WhatsApp. This shift indicates an attempt to broaden their operational scope and enhance their reach.

These insiders could assist hackers in various malicious activities, including unauthorized data access, which could lead to extensive personal information breaches. Hackers could use this information for identity theft, social engineering attacks, and targeted phishing campaigns, closing eyes on abuses or forcing account termination.

Additionally, these insiders could facilitate the bypassing of security measures, allowing hackers to plant malware or conduct espionage. In the realm of money laundering, insiders could manipulate account verifications or transaction records to obscure the origins of illicit funds, making it easier to launder money through legitimate platforms.

By recruiting from global corporations, malicious actors aim to expand their influence, improve their techniques, and gain access to more valuable and diverse information. This strategy reflects a long-term plan to bolster their capabilities and adapt to an evolving cyber landscape.

Consequences and Mitigations for Malicious Insiders

The consequences of insider threats in the financial sector can be dire, including unauthorized access to customer data, intellectual property theft, and significant financial losses. Regulatory penalties and loss of customer trust exacerbate the impact. If sophisticated threat actors leverage malicious insiders, catastrophic breaches could undermine global financial stability.

To combat these threats, financial institutions must adopt proactive and comprehensive insider threat management strategies. Deploying advanced monitoring tools, conducting regular security audits, and fostering a culture of security awareness among employees are crucial steps. By enhancing insider threat detection and mitigation, organizations can safeguard their operations and maintain customer trust in an increasingly hostile cyber environment.

To combat the threat of malicious insiders, financial service companies can implement several strategies:

- **Enhanced Vetting Processes:** Strengthen background checks during the hiring process to identify potential risks.
- **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.
- **Security Training:** Conduct regular security awareness training to educate employees about the risks and signs of insider threats.
- **Incident Response Plans:** Develop and regularly update incident response plans specifically tailored to address insider threats.
- **Anonymity and Reporting:** Create anonymous reporting mechanisms for employees to report suspicious activities without fear of retribution.

By implementing these measures, financial institutions can better protect themselves against the growing threat of malicious insiders.

The Unintentional Insider Threat

Unintentional insider threats can come in the form of either negligent or accidental. Negligent insider threats are realized through an employee's carelessness, such as ignoring messages to install patches. An accidental insider threat occurs by mistake, such as mistyping an email address or unknowingly opening a phishing email.

Our Trustwave SpiderLabs team modeled a threat hunt with the following Tactics, Techniques, and Procedures (TTPs) of the MITRE ATT&CK framework:

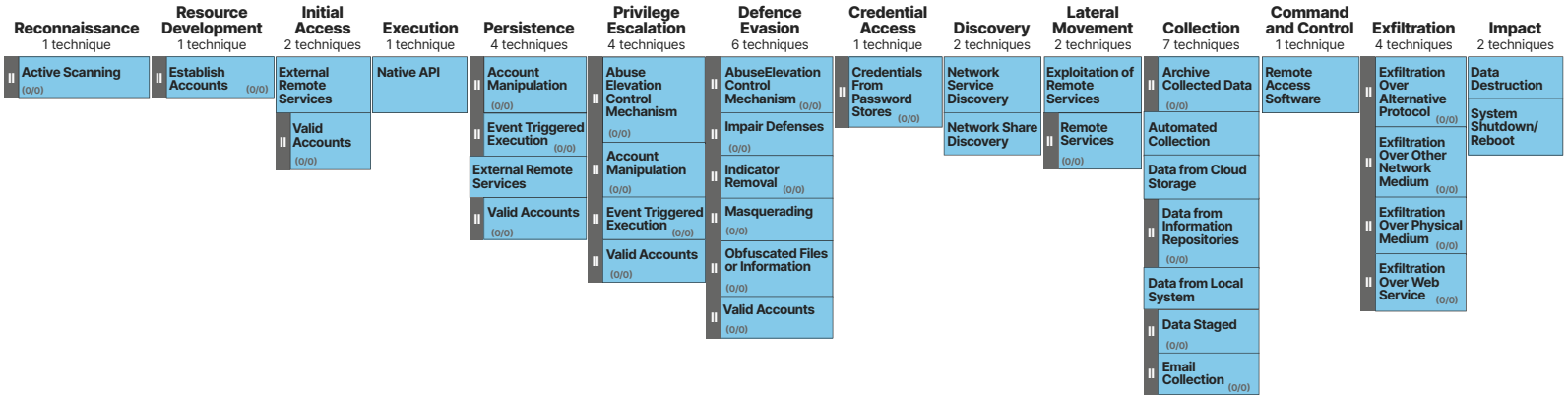

Figure 8: The MITRE ATT&CK framework with the specific TTPs the Trustwave SpiderLabs Threat Hunt team uses to hunt for unintentional insider threats

These TTPs represent areas where threat actors trigger, coerce or take advantage of negligent or accidental mistakes made by an authorized user. In this section we will be focused on Remote Monitoring and Management (RMM) Tools, personal VPN Software, Sneakers, and USB Drives.

Based on our global threat hunt, we learned that there are many opportunities in the financial services sector to curb the abuse of these services and devices. **A staggering 48% of our risk-based findings came from hunting for T1219 Remote Access Software and T1572 Protocol Tunneling.** Another threat vector that we witnessed in this hunt campaign was T1052 Exfiltration over Physical Medium with the sub-technique Exfiltration over USB.

Remote Monitoring and Management (RMM) Tools

During the hunt, our goal was to identify misuse or negligent behavior. As we analyzed our leads, we found in many cases multiple RMM tools across an organization. At the worst, we found four RMM tools in use on one system. Typical tools that we come across are LogMeIn, TeamViewer, AnyDesk, Bomgar, SecureLinkCM, ScreenConnect, and Zoho Assist. Each one of these tools is considered legitimate and non-malicious; however, when there are many of these tools running or active in the environment, it increases the chances of an attacker using them maliciously or bringing their own under the radar.

RMM as a RAT (Remote Access Trojan)

These techniques are not unique to industry or threat group, but ransomware-as-a-service (RAAS) groups (e.g., Lockbit, BlackCat, BlackBasta, Akira, etc.) along with their affiliates and Initial Access Brokers use these tools quite frequently in their operations.

A recent article from Microsoft describes an attack scenario whereby BlackBasta ransomware group ran a successful social engineering attack which led to remote access, lateral movement, and successful deployment of ransomware.

In that attack, they began with a vishing campaign to convince the victim they were the IT staff and had the end-user use Microsoft's Quick Assist to give them remote access. Once the adversary had access to the system, they ran several curl commands to download and install the tools they needed to login remotely (outside of Quick Assist) and maintain persistence. In those attacks, ScreenConnect, NetSupport Manager, and Cobalt Strike were the tools of choice, but it is important to know, any RMM tool would work.

Where organizations have allowed any RMM tools and there are many deployed in the environment, this attack looks like business as usual to an EDR or other security technology. Reducing the authorized RMM tools to one coupled with detection rules \ blocks or alerts on any other tool installed could help to minimize this type of threat.

Mitigations for RMM Tools

- Reduce RMM usage to one tool and enforce restrictions on which authorized accounts can use it and the locations they can use it from.
- Create detection rules to identify usage of rogue RMM tools or non-authorized accounts.
- Uninstall after use, any one-time or special use RMM tools that third-party vendors may require. These may be left in a “listening” mode increasing attack surface after the vendor no longer requires it.
- Enforce Multi-Factor Authentication where remote access is required.

Personal VPN Software

Our findings related to T1572 Protocol Tunneling are similar to the Remote Access Software risks. We found many cases where personal VPN software was installed on one or two machines in a given environment whereby there is already a corporate standard VPN solution in place. Typical VPN applications we are seeing are Wireguard, NordVPN, Windscribe, and ExpressVPN. Again, while these are not malicious by themselves, they bring greater risk to the company.

Sneakers

In using these technologies, personnel may be evading web access controls to keep their internet usage private. While there may be business needs to allow personal VPN software, there is added risk in allowing anonymous activity, including unmonitored exfiltration of data, and the potential introduction of malware from compromised sites (drive-by downloads). In 2021, Justice.gov reported on a case whereby an employee stole confidential company information and extorted the company for approximately $2 million while working to “remediate” the issue. It was discovered that he was able to secretly exfiltrate data hiding behind Surfshark, a personal VPN service, used to mask his IP address while conducting unauthorized access to AWS and GitHub.

In addition to malicious insider threats or accidental insider threats causing risk, threat actors may use this software to evade detection and exfiltrate data. If it already exists or is authorized in the network, this becomes an easier path to evade detections.

Mitigations for Personal VPN Software

- Authorize only one VPN solution.
- Create detection rules to identify usage of any non-authorized VPN software.
- Enforce Multi-Factor Authentication for authorized VPN.
- Implement a data loss prevention (DLP) tool to detect unauthorized data transfers.

USB Drives

Lastly, with our findings on T1052 Exfiltration over Physical Medium, this presents a two-sided risk. In this part of the hunt, we looked for obvious signs of large data being moved to USB drives. This could be an indicator of a disgruntled employee, corporate espionage, or simply someone backing up their work. Whether the activity is deemed work-appropriate or malicious, the risk of data leaking is very high.

Malware Injection

The other side of the USB device problem is the introduction of malware. With no USB policies in place, any end-user staff can bring in any USB device regardless of where it came from, plug it in, and use it. Recently, there have been outbreaks of USB-based trojans and worms such as Raspberry Robin and PlugX.

Raspberry Robin is considered a USB worm because the initial delivery mechanism is typically from an infected USB drive. It is unclear how these drives get infected at this time. This malware, when executed, connects to infected QNAP servers, downloads a malicious .dll file, and establishes persistence via the Registry. Raspberry Robin has been observed being used as an Initial Access Broker and distributing final payloads linked to various ransomware groups.

PlugX is a RAT (Remote Access Trojan) attributed to Mustang Panda, a Chinese APT group. This malware is designed for espionage. It supports commands to exfiltrate files, perform keylogging operations, backdoor remote access, and can download additional plugins or additional malware as needed. PlugX can establish initial access via spearphishing campaigns, other trojanized malware, or via infected USB which has been spotted in the wild during our hunts. It is unknown how the USB became infected.

Mitigations for USB Drives

A clear policy on authorized usage should be established and for the risk averse, disabling USB altogether may be the best solution. Where USB devices are allowed due to business need, there are many ways (some expensive) in controlling the data flow. Some of those might be:

- Enforce encryption on USB devices.
- DLP solution to monitor data leaving the environment.
- Enforce on-demand USB access.
- Enforce USB policies that allow USB devices provided by the company to be permitted.
- Enforce data classification and only allow non-critical data to be exported.

Summary

Insider threats will always be a problem for any organization to stay on top of. The goal is to reduce the potential for Unintentional insider threat and have strong detection and response measures for the Malicious type. Using EDR telemetry to conduct behavior-based hunting can provide a lot of insight into the operations of end-users across an organization. Based on our latest insider threat hunt campaign in the financial services sector, T1219 Remote Access Software, T1572 Protocol Tunneling, and T1052 Exfiltration over Physical Medium were the top three categories of findings, but we also had findings in:

- Resource Development
- Reconnaissance
- Initial Access
- Credential Access
- Defense Evasion
- Collection

Finding open risks such as an overabundance of RMM tools, multiple VPN technologies, and USB usage can empower your governance teams to make strategic decisions about risk mitigation. Putting policies and controls in place in these three areas is one way to conduct a low-cost security exercise with high-value outcomes. Continual threat hunting operations are critical for using rich telemetry to discover malicious behaviors in the environment that may be Malicious or Unintentional insider threats. Stay vigilant.

For all of Trustwave SpiderLabs' research on the Financial Services sector, please see the full series here.


Trustwave
SpiderLabs