TTP: Insider Threat (2022)

Fusion (FS) Strategic (ST)

August 24, 2022 12:32:21 AM, 22-00017439, Version: 1

Executive Summary

- Mandiant suggests that since mid-2020, insider threat incidents have remained relatively rare in comparison to other types of threat activity.
- Although we suggest malicious insiders remain a relatively low-frequency threat to organizations, the impact of the threat these employees pose is disproportionately high.
- While insider threats affect a wide variety of verticals and are commonly associated with several motivations, we assess with high confidence that data exfiltration with the goal of financial gain is the most common objective.

Threat Detail

With increasing amounts of information being stored on internal networks and the cloud as well as amplified storage available on portable devices, the corresponding risks associated with a well-placed insider have expanded as employees can easily access, store, and transfer vast troves of data. With regards to industrial control systems (ICS) specifically, insiders may be able to cause especially grave damage due to specialist knowledge of these systems' weak points that would be difficult or impossible for outside threat actors to discern. Additionally, the legitimate permissions granted to insiders almost certainly make some of this activity more difficult to detect. As a result, we assess with moderate confidence that the difficulty in identifying insider threats allows many incidents to go undetected and unreported. As with traditional targeted attacks by external threat actors, malicious insider operations are often carried out over time, with the insider taking steps to try to hide their malicious activity and remain undetected in the victim environment. Although malicious insiders likely remain a relatively low-frequency threat to organizations, the impact of the threat these employees pose is disproportionately high. Malicious insiders threaten all industry sectors, and data theft for financial gain is likely the most common motivation.

- In June 2022, a Canadian court approved a $200.9 million CAD settlement of a class-action lawsuit against Desjardins Bank over a data breach that occurred between 2017 and 2019. The incident exposed the data of 4.2 million people who had accounts at the bank and is one of the largest financial data breaches in Canada's history. The incident was linked to the actions of a rogue employee who was siphoning bank customer data silently for 26 months and passing it to an unknown person or persons, presumably for financial gain.

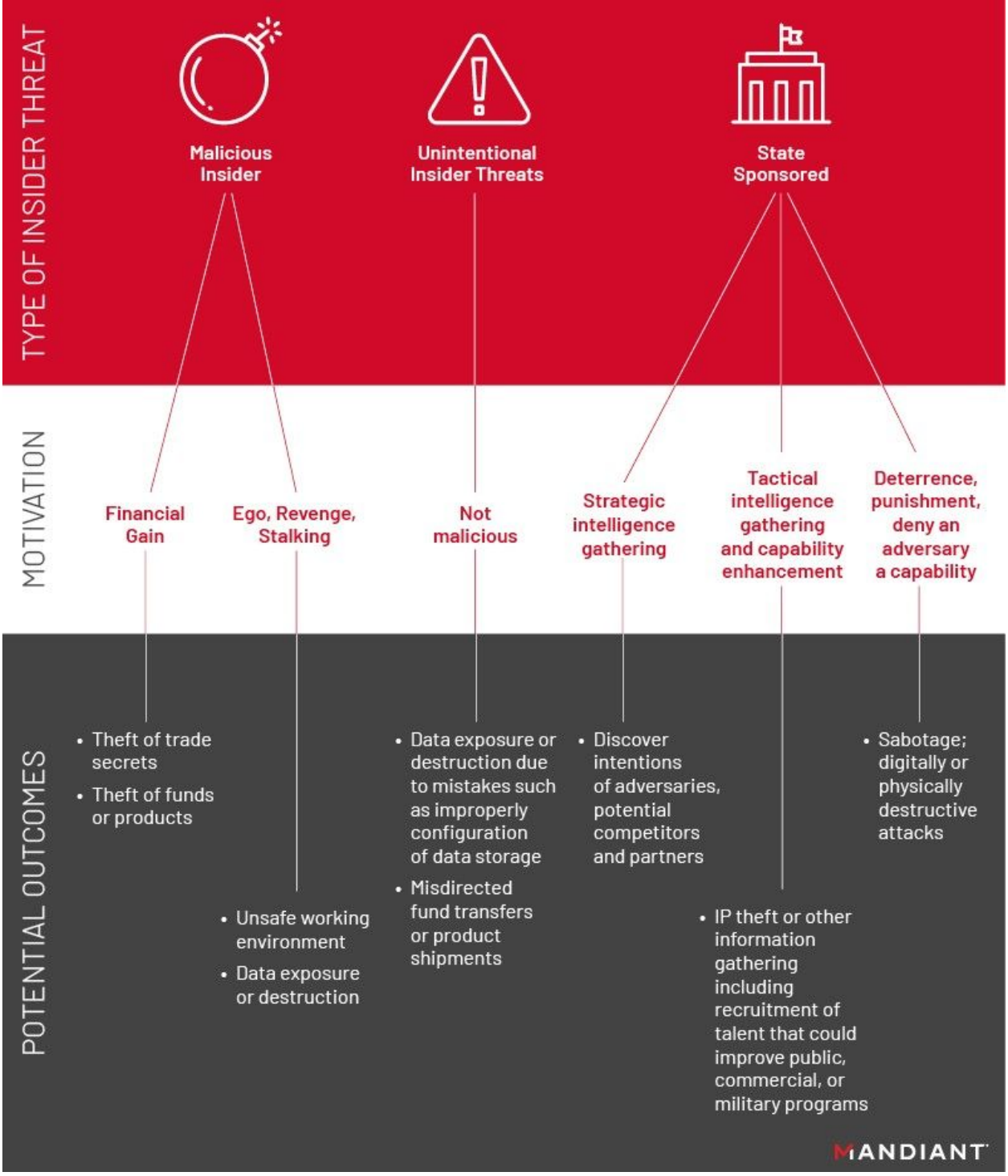

Figure 1: Types of insider threat activity

Financial gain: We assess with high confidence that data exfiltration with the goal of financial gain is the most common manifestation of intentional insider threats as evidenced by observed instances of compromised information from financial institutions, security vendors, and vehicle manufacturers. We have also observed insiders abuse legitimate accesses and privileges for financial gain that do not involve data exfiltration, such as stealing employers' funds or products. This activity has targeted a wide array of verticals, including financial services, retail, and entertainment. We anticipate that insider activity for personal and financial gain will occur for the foreseeable future.

Ego, revenge, stalking: We have also seen insider activity motivated by ego, the desire for revenge, or to stalk individuals associated with a company. We assess with moderate confidence that we will continue to see occasional examples of this activity for the foreseeable future as well.

State-sponsored use of insiders: We have observed instances of insiders leveraged to facilitate intelligence gathering operations and use of insiders to conduct industrial sabotage. We also assess with high confidence that China's talent recruitment plans incentivize the theft of intellectual property, although this activity is not directly controlled by Chinese intelligence organizations.

Unintentional threats: While the primary focus of this report is intentionally malicious insider threat activity, unintentional insider incidents are common and can cause significant damage, from accidental exposure of sensitive data on cloud resources to business email compromise (BEC) schemes (20-00008939, 18-00000257). It is worth noting that business disruptions, such as the coronavirus pandemic shifting many workers unexpectedly to remote work, can increase the probability that employees will use non-corporate approved or owned resources out of expediency.

Insider Threat Incidents Remain Relatively Rare

Based on our observations and several studies conducted since our previous insider threat report, Mandiant assesses with low confidence that insider threat incidents have remained relatively rare in comparison to other types of threat activity, such as breaches conducted via system compromise by outside threat actors.

- The 2021 edition of Mandiant's annual M-Trends report noted only one percent of intrusions investigated by Mandiant related to insider threat activity. Our 2022 M-Trends report noted this metric has remained relatively stable.
- Verizon's 2021 and 2022 Data Breach Investigations Reports both concluded that insider threat incidents remain relatively rare.

However, it is important to note that several factors undermine our ability to make this judgement with a confidence rating higher than low.

- We acknowledge some reporting by other vendors is at odds with the findings described above.
- We believe that insider-attributed incidents have likely historically been underreported by victim organizations.
- We regularly observe advertisements for illicit access or compromised databases on underground forums that claim to involve an insider, especially regarding financial institutions in Brazil and Mexico (please see the Appendix)

Risk Factors for Insider Threat Incidents

Business Disruptions May Lead to Increased Insider Threat Activity

We assess with moderate confidence that during times of significant business disruptions, insider threat events are more likely to occur and may have a greater impact (20-00005156).

- Any broad disruption to financial markets, industries, or companies, such as a recession, natural disaster, armed conflict, large-scale protests or strikes, or a government shutdown, can cause unrest among employees or divert security personnel to other priorities. These types of events—particularly when they create anxiety among workers regarding the stability of their employment and/or financial

situation—can drive increased risk of malicious insiders abusing trusted access or improperly accessing valuable or sensitive systems or data.
- Financial hardships placed on employees due to business disruptions, such as a spouse's loss of employment, can be a particularly serious driver of threat activity. These situations can open otherwise rule-abiding users to exploitation by financially motivated or state-sponsored actors.
- The threat of activity by malicious insiders is also likely significantly elevated during merger and acquisition negotiations and implementation as employees may be concerned regarding their future job prospects or how integration may change their duties, benefits, pay, and other aspects of employment (19-00009078).

Departing Employees

We assess with high confidence that there is a high risk associated with employees who abuse access to sensitive data when organizations fail to terminate the accounts of former employees. Similarly, organizations seeking to monitor insider threat risks should consider auditing the behavior of employees who are known to be planning on leaving the company.

- In late 2020, a former Cisco employee was sentenced to 24 months in prison for accessing the company's Amazon Web Services (AWS) cloud infrastructure and deploying code from his personal Google Cloud Project account that resulted in the deletion of approximately 450 virtual machines related to the Cisco Webex Team application. According to the U.S. Department of Justice (DOJ), Cisco spent approximately $1,400,000 USD in employee time to restore the damage to the application and refunded more than $1,000,000 USD to reimburse affected customers.
- In early 2021, open sources reported that former employees of a competitor provided Ticketmaster with URLs of ticketing webpages and stolen passwords that were used to unlawfully collect business intelligence by repeatedly accessing the competitor's systems without authorization (20-00026826). The employees also provided Ticketmaster with confidential financial documents belonging to the competitor. Ticketmaster's employees purportedly held a division-wide "summit" at which the stolen passwords were used to access the victim company's computers.
- Spanish authorities allege that two former employees of a contractor responsible for maintaining Spain's radioactivity alert network (RAR) accessed the network and disconnected 300 of 800 sensors from the system between March and June 2021. The individuals also purportedly attempted to delete the RAR management web application in the control center.
- Also in 2021, open sources reported a former contractor working for an unnamed contracted service provider (CSP) managed to breach Victoria, Australia, government information technology (IT) systems 260 times and steal personally identifiable information (PII) from its client relationship information system for service providers (CRISSP) for 12 months after leaving the CSP (21-00005756). The government stated the breach was partially the result of the absence of any effective secondary procedure or system for when the primary mechanism for terminating a user's access had failed.
- In early 2022, a former employee purportedly accessed the customer account information of a mobile payment service including customers' full names and brokerage account numbers associated with investment activity on the service and, for some customers, portfolio values, holdings, and possibly trading activity for one trading day (22-00008955).

Figure 2: Typical insider threat progression

Financially Motivated Insider Threat Activity

PII Harvesting

PII is regularly offered in numerous forums we monitor and is valuable to threat actors conducting a wide array of malicious operations.

- In late 2020, a South Africa-based financial services group advised customers that their ID numbers, contact details, physical addresses, and account numbers were provided to third parties by an employee (20-00024788). It is unknown how many customers were affected.
- In early 2021, Russia-based multi-national corporation Yandex disclosed that thousands of its customers' email accounts were accessed by an insider who then sold access to them for profit (21-00003800). The responsible employee was purportedly a system administrator.
- In late 2021, Canada-based eCommerce company Shopify disclosed it experienced a security breach after two rogue members of its support team accessed and attempted to collect customer transaction details and PII from Shopify shop owners. Shopify estimates that the breach may have impacted nearly 200 stores and exposed some customers' full names, email addresses, physical address, and order details.

Ransomware Deployment and Extortion

Mandiant assesses with high confidence that the incentives for threat actors to continue ransomware operations currently greatly outweigh risks that may cause the actors to stop, despite increasing pressure from law enforcement and government organizations in many countries (22-00007932). Mandiant has observed multiple extortion actors attempt to recruit insiders to deploy ransomware; however, it is not clear how successful these efforts have been.

- In early 2021 a Russian national pled guilty to attempting to bribe a Tesla employee to introduce malware to company systems to distract network administrators with a disruptive attack while

exfiltrating proprietary data. The data would then be used to extort the company by threatening to disclose the data. The man explained the group he worked with pays employees of target companies to introduce malware into the target's computer system and had conducted several "special projects" in the past.
- In mid-2021, open sources reported on LOCKBIT activity that changed the Windows wallpaper placed on encrypted devices offering "millions of dollars" to insiders willing to distribute the ransomware (21-00017395). While we judge that the insider threat will continue to be a serious, perpetual concern for organizations, the fact that LOCKBIT was not soliciting insiders until after a network is encrypted makes it less likely to be effective. However, the recruitment strategy may be to leverage media attention to reach a wider audience of potential insiders.
- UNC3661, also known as Lapsus Group or Lapsus$ Group, is a threat actor that has conducted data theft extortion operations since mid-2021. The actors behind these operations appear to be motivated by both financial gain and a desire for notoriety. Their activities are focused on exfiltrating sensitive data they can threaten to publish on their Telegram channels, which they have used to shame victims and leak information when attempts to coerce a victim are unsuccessful (22-00007945). We have observed the group seeking insiders in the telecommunications and technology sectors (22-00006229, 21-00026988). In early 2022, seven people were arrested in connection with this activity (22-00007945).
- In early 2022 English-speaking actor "EricJapier" claimed to have insiders working in several verticals, including insurance, banking, real estate, and transportation, in France (22-00002461). The actor stated they were searching for individuals with access to ransomware and insiders that have "no fear to go at the boss's computer and plug an USB stick" [sic].

Direct Theft from Financial Institutions

We have also observed several instances in which insiders have used their access to attempt to facilitate direct theft, and we anticipate this activity will continue for the foreseeable future.

- In mid-2020, a South Africa-based bank disclosed that employees stole more than ₹56 million Rand (~$3.2 million USD) from the bank after accessing the 36-digit Host Master Key (HMK) at one of its data centers in December 2018 (20-00011128). The HMK is a 36-digit encryption key that protects all the lower-level keys and allows access to the ATM PINs, home banking access codes, customer data, credit cards, and even internal systems modifications. Employees purportedly used the master key to access accounts to conduct more than 25,000 fraudulent transactions and steal funds.
- In mid-2022, Nigerian authorities stated they detained four suspects for attempting to access the networks of a Nigerian bank to steal funds. According to authorities, the group bribed an employee in the IT department to leave critical network gateways open so they could gain access to the bank network. Per data recovered from seized devices, the group was planning to use the same method on 10 other banks if the first operation was successful.

Intellectual Property Theft

Insiders who have access to intellectual property may attempt to exploit their access for financial gain, and we anticipate we will occasionally observe this activity for at least the near to mid-term

- In late 2020, Italian authorities arrested an employee of an Italian defense contractor, accusing him of exfiltrating data including human resources records, procurement information, and information regarding the design of civil aircraft components and military aircraft. The man purportedly used a USB key to install malware on workstations between 2015 to 2017. The man was a member of the firm's cybersecurity team, and an accomplice on the team also purportedly misrepresented the scope of the malfeasance and otherwise hindered the investigation.

Third-Party Threats

Third-party insiders who have access to sensitive data may not be aware of best security practices or may intentionally expose sensitive data, especially as cloud technologies and mobile devices increase in ubiquity.

- A Japanese electronics manufacturer issued an apology in August 2021 after learning that bank account information was exposed after a subcontractor downloaded a database containing more than 30,000 documents on business partners and 41,000 documents related to employees (21-00017862). Documents included information such as company names, addresses, associated names, phone numbers, email addresses, and bank account numbers belonging to business partners in Japan, China, the Philippines, Malaysia, Singapore, the U.S., and the European Union (EU), while exposed customer information was limited to China and the Philippines.
- In early 2022, a nonfungible token (NFT) marketplace stated an employee working for third-party contractor downloaded the email addresses of the firm's customers and then provided that data to an unknown third party (22-00015425).

Insider Trading

- In January 2021, Russian-speaking actor "graham" posted an advertisement on the Exploit[.]in forum seeking spammers who could email employees of U.S. businesses in various industry sectors (21-00006742). The purported goal of the spam emails would be leading potential insiders to a TOR website named "Gravy Train," which claims to offer an intermediary service between insiders and investors where insiders can provide sensitive, nonpublic company documents to traders to give them a trading advantage in exchange for a portion of any obtained profits (21-00008079).
    - Notably, according to trusted, sensitive sources, graham admitted that they do not know how successful their insider trading operation would be. The actor indicated they need insiders to provide sensitive corporate information since they could no longer rely on "hackers" because they are all currently involved in ransomware operations.

SIM Swapping

We frequently observe advertisements on underground forums either soliciting or advertising insider access to telecommunications companies to facilitate SIM swapping. For examples, please see the Appendix of this report. An attacker with access to a valid or duplicate SIM card and a subscriber's personal information may be able to perform a SIM swap and effectively transfer the subscriber's phone number and all associated communications to a phone possessed by the actor. Since many organizations have enabled multi-factor authentication (MFA) via mobile devices, this scenario could allow malicious actors to access victims' bank accounts, approve fraudulent transactions, steal cryptocurrencies, or conduct other malicious activities.

Non-Financially Motivated Threat Activity

Ego and Revenge

We regularly observe actors exfiltrating or leaking information for reasons other than financial gain, such as ego or revenge, and we assess with high confidence that we will continue to observe disgruntled or angry insiders targeting organizations for the foreseeable future. This activity has impacted multiple verticals including governments, energy and utilities, healthcare, and business and professional services.

- Recently reported open sources indicate that in 2017, a disgruntled Central Intelligence Agency Operations Support Branch developer allegedly provided the WikiLeaks organization with 34 TB of classified data that could be used to identify the agency's tactics, techniques, and procedures (TTPs) shortly before leaving the organization. It is unclear how the former employee exfiltrated the data, although he had administrative privileges during much of his tenure with the agency.
- In late 2020, a San Jose resident was sentenced to 24 months in prison for damaging his former employer's network. Following his departure from the organization, he accessed the company's AWS cloud infrastructure and deployed code from his personal Google Cloud Project account that resulted in the deletion of some 450 virtual machines related to the company's Webex Team application. The intrusion purportedly forced the company spend approximately $1,400,000 USD in employee time to restore the damage to the application and refund more than $1,000,000 USD to affected customers.
- In April 2021, a Georgia resident was charged with conducting an intrusion that disrupted and delayed a medical device packaging company's shipment of personal protective equipment (PPE). The individual had previously been employed by the company and had administrator access to the computer systems containing the company's shipping information. He allegedly leveraged a fictitious account he created before being terminated to conduct the intrusion.
- In early 2021, a Kansas resident was indicted for remotely accessing the Ellsworth County public water supply system in 2019 and shutting down processes that can affect the facility's cleaning and disinfecting procedures. The individual had previously worked at the facility and was purportedly periodically tasked with remotely logging into the Post Rock computer system to monitor the plant after hours (21-00007167).

State Use of Insiders

We assess with high confidence that insider threat incidents associated with state-sponsored actors are typically much more impactful than those associated with financially motivated actors. China has been known to leverage insiders to conduct intelligence gathering operations, while North Korea is suspected of using insiders to gather intelligence and generate revenue for the regime.

Incentivizing Industrial Espionage

We assess with high confidence that Chinese talent recruitment programs and analogous corporate policies are a component of China's overall development strategy and are a significant driver of insider-enabled physical theft of trade secrets (20-00010164). China operates more than 200 talent recruitment plans, the most prominent of which is the Thousand Talents Plan (TTP) established in 2008. Incidents associated with these programs frequently involve the exfiltration of intellectual property or simply using corporate systems to communicate with partners in China, but they have also included elements of physical theft and recruitment of additional insiders and were addressed in open sources during 2021.

- In December2021, the Foundation for Defense of Democracies released a report asserting that China is exploiting its existing relationship with U.S. universities to steal sensitive data and technology that it will ultimately use to "achieve military dominance" (21-00026275).The Foundation reported that 34 U.S. universities continue to work with Chinese Communist Party (CCP)-sponsored Confucius Institutes.

Intelligence Gathering and Revenue Generation

Mandiant investigated open-source reports of suspected North Korean personas who attempted to gain employment at a blockchain-based biopharmaceutical organization and a cryptocurrency security company in April and May 2022 (22-00012603).

- Though we cannot independently confirm that the individuals interviewing for the jobs are North Korean actors, these events appear consistent with a May 2022 U.S. government report on Democratic People's Republic of Korea (DPRK) IT worker characteristics.
- Further, North Korea has demonstrated a history of targeting cryptocurrency platforms to potentially provide the regime with direct financial gain and serve as a medium for money laundering and sanctions evasion (22-00001546).

Mitigation Strategies and Recommendations

As organizations across verticals are continuously at risk of being affected by insider threats, developing and updating security measures to combat this activity is ideally a dynamic and continuous process. As the National Insider Threat Task Force points out, "Our collective efforts to address the insider threat require constant evaluation, fresh perspectives, and updated approaches to address current and future risk."

- Education is one of the best ways to prevent and respond to a potential insider incident. This may include training and communications across the enterprise, including meetings between departments and teams to discuss the specifics of potential insider breaches to individual organizations and how best to respond to them.
    - Insights gained from meetings may assist in identifying the most valuable assets and the threats likely to affect organizations to inform decisions about the cost and deployment of countermeasures.
    - Interdepartmental communication will also likely enable organizations to develop incident response plans that lay out the steps necessary for responding to an insider breach. Testing plans regularly with tabletop exercises to identify areas of improvement is likewise recommended.
- Contacting a local or federal law enforcement agency in advance of an incident will likely identify an appropriate point of contact and establish what data may need to be collected for prosecution in the event an insider event occurs. Exercising best practices for data retention to inform post-incident forensics is essential if organizations seek to press charges against suspected insiders.
- Organizations should monitor user and device behavior and compare it to previously established baseline activity. By auditing user practices and evaluating the audits against the baseline, organizations may be able to detect individual habits that expose the company to additional risk. This may include the use of social media, working odd hours, large data transfers, or use of remote storage services and mobile access to company assets.

    - Understanding this baseline activity will likely enable administrators to build strategies that protect networks based on where (e.g., at home, during conferences), how (e.g., via mobile phones, personal devices, or software), when, and why employees typically access the corporate or agency network.
- Network administrators, policy makers, and data owners should restrict opportunities for individuals to gain or leverage unauthorized access. This means limiting access and permissions down to a need-to-know basis for all users, ideally through an access management system, and ensuring that users are not sharing credentials to access common assets. Similarly, organizations should consider restricting the use of removable storage devices and cloud storage services strictly to a business-need basis as they could be used to introduce malware and exfiltrate data.
- Establishing a policy for classifying and marking data (e.g., public, proprietary, confidential, restricted) will enable organizations to better monitor for data leaving the organization.
- Organizations should identify their "crown jewels," which are the most valuable or sensitive data such as customer information, source code, and financial data, know where it is stored, build controls around it, and ensure they are monitoring for insiders.
- Organizations should ensure that they have language in their Acceptable Use Policy (AUP) clearly outlining employee privacy expectations and allowing organizations wide latitude to monitor and investigate insiders.
- Data loss prevention (DLP) tools, while not foolproof, may identify and prevent sensitive data from leaving an organization.
- User behavior analytics (UBA) tools may be used for identifying abnormalities in user behavior, and they can be used to monitor for insiders in conjunction with DLP tools.
- Privileged access management (PAM) solutions can reduce the risk of a privileged insider accessing proprietary information. In general, privileged administrators such as IT and security administrators need to be monitored for activity outside the scope of their roles.

Appendix: Examples of Advertisements Referencing Insiders

Report Number	Report Title	Country	Industry
22-00002461	Threat Activity Alert: English-Speaking Actor 'EricJapier' Claims to Have Insiders in French Companies and Looks for Partners for Infecting Networks with Ransomware on Exploit[.]in	France	Financial Services/Insurance
21-00019000	Threat Activity Alert: English-Speaking Actor 'Magician' Advertises Insider Access at Canadian Bank on Telegram Group	Canada	Financial Services
20-00010323	Threat Activity Alert: English-Speaking Actor 'vladptn' Claims to Have Insider Information and Data of U.S. Metal Engineering and Manufacturing Company on Torum	U.S.	Manufacturing/ Construction & Engineering
22-00015602	Threat Activity Alert: English-Speaking Actor 'melclipson' Seeks Insiders at	Canada	Manufacturing/Legal & Professional Services

	Law Firms and Manufacturing Industry on Telegram Group		
22-00010427	Threat Activity Alert: Brazilian Actor 'Eduardo Maia' Advertises Insider Services at Brazilian Bank on Facebook Group	Brazil	Financial Services
22-00012489	Threat Activity Alert: Brazilian Actor 'Junior Boyzin' Advertises Access to Insider at Spanish Bank Operating in Brazil to Cash Out Compromised Accounts on Facebook Group	Brazil	Financial Services
21-00005569	Threat Activity Alert: Multiple Brazilian Actors Advertise Insider Access to Employees of Banks Operating in Brazil on Facebook Carding Group	Brazil	Financial Services
21-00011576	Brazilian Actor 'MARSH' Advertises Insider at Brazilian Bank to Cash Out High Balance Accounts on WhatsApp Carding Group	Brazil	Financial Services
21-00005679	Brazilian Actor 'Miejvinski' Advertises Insider Services at Mexican Telecom Operating in Brazil on Telegram Carding Group	Brazil	Telecommunications
22-00011568	Threat Activity Alert: Brazilian Actor 'UN' Advertises Datasets Obtained from Insider Access to Brazilian Government Entity on WhatsApp Group	Brazil	Governments
22-00015268	Threat Activity Alert: Spanish-Speaking Actor 'Rodolfo Ortiz' Advertises Access to Insider at Mexican Bank on Facebook Group	Mexico	Financial Services
22-00014524	Threat Activity Alert: Spanish-Speaking Actor 'Purple Devil' Advertises Access to Insider at Mexican Bank on Telegram Group	Mexico	Financial Services
21-00011950	Spanish-Speaking Actor 'Joss Mannu' Advertises Insider Access and Payment Card Data from Mexican Bank on Facebook Carding Group	Mexico	Financial Services
21-00008401	Spanish-Speaking Actor 'Mario Hernandez' Looks for Insider at a Bank in Mexico to Obtain Datasets of Customers on Facebook Group	Mexico	Financial Services
21-00009166	Spanish-Speaking Actor 'welldonejob60' Advertises SIM Swap	Mexico	Telecommunications

	Service for Telecom Companies Operating in Mexico on Pandora		
20-00026678	Threat Activity Alert: Spanish-Speaking Actor 'Compapollo' Advertises Payment Card Data Obtained from Mexican Insurance Companies on Carding Forum	Mexico	Insurance

Table 1: Examples of advertisements referencing insiders

Please rate this product by taking a short four question survey

First Version Publish Date

August 24, 2022 12:32:21 AM

Threat Intelligence Tags

Actors

- UNC3661
  Aliases
  - UNC 3661
  - UNC-3661
  - UNC3661

Affected Industries

- Aerospace & Defense
- Automotive
- Chemicals & Materials
- Construction & Engineering
- Education
- Energy & Utilities
- Financial Services
- Governments
- High Tech/Software/Hardware/Services
- Insurance
- Legal & Professional Services
- Manufacturing
- Media & Entertainment
- Oil & Gas
- Retail
- Technology
- Telecommunications
- Transportation

Intended Effects

- Competitive Advantage in Business or Economic Advantage
- IP or Confidential Business Information Theft
- Interference with ICS
- Disruption
- Financial Theft

- Degradation

Motivations

- Ego
- Financial or Economic

Malware Families

- LOCKBIT
  Aliases
  - LOCKBIT

Source Geographies

- Global

Tactics, Techniques And Procedures (TTPs)

- Malware Propagation and Deployment
- Insider Threat
- Ransomware
- Pen Testing
- Network Reconnaissance

Target Geographies

- Global

Targeted Information

- Intellectual Property
- Financial Data
- Customer Data
- Credentials

Version Information

Version:1, August 24, 2022 12:32:21 AM

german[.]simkin@mandiant.com