Case Study

Insider Threat

Monitoring and Identification of Insider Threats

Nisos identifies potential insider threats brought to light through **posts on social media during ongoing monitoring**

SITUATION

Insider threats can severely damage companies by exposing sensitive information, disrupting operations, and undermining trust. These risks, whether intentional or accidental, can lead to financial losses, reputational harm, and compromised security.

Nisos alerted an existing Client of elevated risks identified during our ongoing monitoring service. Our team of expert researchers continuously monitored for emerging threats that could compromise the Client's security.

During our investigation, Nisos discovered a post on X (formerly known as Twitter), in which an individual claimed to have leaked sensitive internal information about the Client to prominent news outlets.

INVESTIGATION

The discovery of the X (formerly Twitter) post triggered an in-depth investigation to assess the credibility of the threat and to uncover the identity of the potential insider.

Through a combination of open source intelligence, proprietary tools, and third-party vendor solutions, Nisos was able to gather crucial details that ultimately helped the Client address the situation and protect their data.

- **Employment History:** The individual likely worked for the Client following their acquisition of another company, until a certain period thereafter.
- **Leaking Propensity:** In the same post, the individual also offered to expose sensitive information about another former employer, indicating a tendency to leak employer information.
- **Disparaging Posts:** The individual had posted multiple disparaging tweets about the Client and its personnel, which were later deleted.

IMPACT

Nisos identified a major risk to the Client by carefully monitoring insider threats. Nisos' comprehensive approach provided a clear path for the Client to safeguard their sensitive information and address the risk effectively.

- Nisos utilized publicly available, open source information to gather insights about the individual behind the X account. By analyzing their digital footprint and online behavior, Nisos was able to track the individual's activities and identify connections that provided valuable context for the threat.

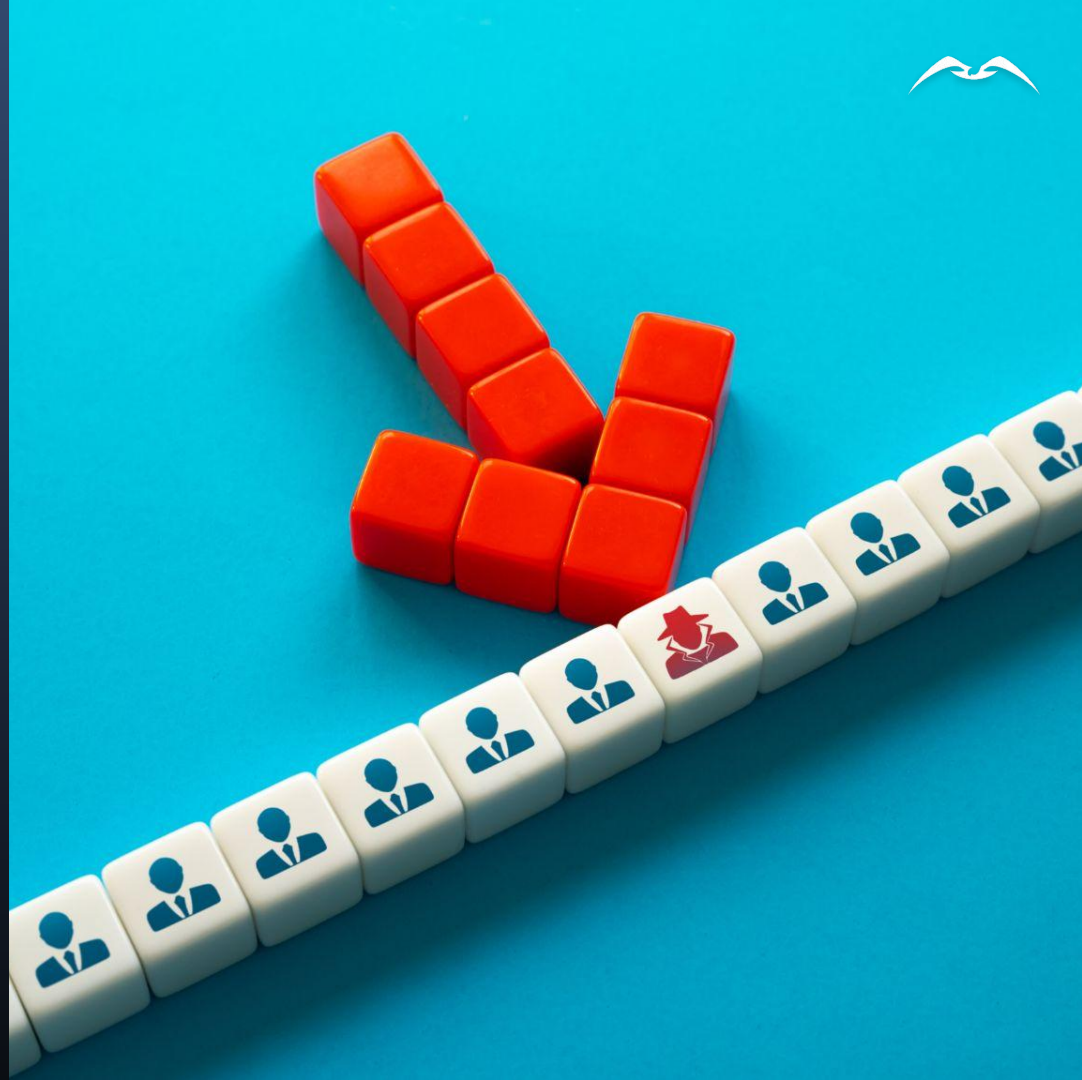
- Our team of researchers assessed the individual's behavior, past actions, and potential motives to determine the level of threat posed to the Client. This analysis gave the Client a clear understanding of the severity of the situation and informed their decision-making process.

Case Study

Insider Threat

Exposing Insider Threats via Dark Web Attribution

Nisos **uncovers identities behind dark web threats** helping a Client neutralize insider threats



SITUATION

Organizations face an increasing array of digital threats, with malicious actors using the dark web to sell sensitive access credentials, such as Remote Desktop Protocol (RDP) credentials, that can compromise networks. The anonymity of the dark web and the complexity of tracking criminals make it increasingly difficult for businesses to identify and neutralize these threats before they cause significant harm.

A Client received an alert from law enforcement that two personas on the dark web were selling RDP access credentials. Concerned about potential compromise, the Client sought Nisos' expertise to attribute the dark web handles and determine the nature of involvement of their third-party contractor.

Initial analysis suggested the attempted sale might involve the third-party contractor. Nisos was tasked with identifying the individuals behind the dark web personas, determining their roles, and uncovering whether the contractor was involved in or victimized by the breach.

INVESTIGATION

How Nisos investigated:

- **Identifying the Seller:** Using a username provided by law enforcement, Nisos engaged the seller, confirming their role as a broker. Through controlled interactions, the seller revealed the username of the operator, the source of the credentials.
- **Attributing the Seller:** Analysis linked the seller's username to breached accounts and unique identifiers. Cross-referencing this data with open source information revealed their identity through a developer conference attendee list. Further online activity confirmed the Seller lacked the technical skills to conduct hacking, aligning with their role as a broker.
- **Tracing the Operator:** The operator’s forum activity showed advanced hacking skills. Linking reused passwords to open source data revealed their real identity and role as the source of the credentials.
- **Internal Investigation:** The client confirmed the operator exploited a single-factor RDP account via password spraying. The contractor was cleared of complicity, and no data was accessed or leaked.

IMPACT

Within three days, Nisos identified both the seller and operator and provided their real names and detailed their methods. Nisos' rapid and precise investigation not only unmasked the threat actors but also ensured the Client could address vulnerabilities, safeguard critical assets, and maintain trust in their contractor relationships.

Nisos actionable intelligence allowed the Client to:

- Bolster security controls by enforcing mandatory two-factor authentication for contractors and subsidiaries.
- Confirm that no sensitive data was accessed or exfiltrated, mitigating broader risk.
- Strengthen defenses against future threats through informed policy changes.

Case Study

Insider Threat

Uncovering Insider Threats in Gig Economy Platforms

Nisos helps gig economy platform **trace and eliminate malicious bot activity**

SITUATION

Malicious activities within gig economy platforms have become a growing concern for tech companies. As the gig economy expands, the potential for exploitation and system manipulation increases, posing significant risks to both platform integrity and user trust. These issues can erode customer satisfaction, lead to financial losses, and damage a company's reputation.

A gig-economy tech company faced a surge in malicious activity on its platform. Bad actors were selling bots designed to automate interactions, providing buyers with unfair advantages and violating the platform's Terms of Service. These bots not only compromised the platform's integrity but also mirrored the legitimate application, creating security risks and causing financial harm to rule-abiding users.

The bots enabled users to "game the system," leading to frustration and anger among legitimate users who suffered financial disadvantages. This activity resulted in reputational damage and security vulnerabilities for the Client. The Client sought to mitigate these threats and restore user trust. The company engaged Nisos to investigate and address the issue.

INVESTIGATION

Nisos played a crucial role in helping the Client navigate this complex challenge, using our deep expertise in technical application analysis and threat detection. Our team quickly began a thorough evaluation of the platform's infrastructure to assess the extent of the malicious bot activity. Additionally, we conducted open source research to identify other indicators of compromise, which helped us understand how the bots were exploiting the system.

Our approach included:

- Pinpointing vulnerabilities within the platform
- Tracing the origin of the malicious activity
- Uncovering the entities behind the bots
- Providing actionable insights for stronger defenses

IMPACT

Following our comprehensive 3-month investigation, Nisos provided the Client with critical insights and actionable recommendations to address the malicious activity on their platform and take decisive action.

- **Enhanced Security Posture:** Nisos delivered tailored recommendations for improving platform security, complicating attempts to duplicate the legitimate application or bypass controls.
- **Disruption of Malicious Activities:** The Client successfully revoked the fraudulent developer's platform certificate, halting their ability to create and update bots.
- **Legal Action:** The Client issued cease-and-desist orders and prepared civil suits against bot developers using Nisos' attribution findings.
- **Internal Accountability:** Using our research, the Client uncovered and addressed an employee's role in damaging the platform's reputation.
- **Restored Trust:** The Client was able to address user grievances and ensure proactive measures were being taken to protect the platform and its users.

Case Study

Insider Threat

Insider Data Leaks to Unauthorized Third-Parties

Safeguarding the tech industry **from insider data leaks to unauthorized third-parties**

SITUATION

Insiders leaking sensitive information to third-parties can severely impact organizations. When employees with authorized access misuse their privileges to share sensitive information, it exposes the organization to financial losses, potential legal repercussions, and operational disruptions. Because of these risks, it is essential for organizations to implement robust security measures to detect and prevent insider threats.

A technology company discovered that proprietary information was being leaked to unauthorized third-parties. The leak threatened the company's competitive position and raised serious concerns about potential ongoing breaches. Suspicion soon centered on a disgruntled employee with access to the compromised data.

To address these risks, the Client sought assistance from Nisos to confirm whether this individual was responsible for the leaks and to explore solutions for preventing future incidents. The Client required a thorough investigation and effective mitigation controls to protect their sensitive information and secure their internal environment.

INVESTIGATION

This investigation began with a targeted review of leaked content and Human Resource (HR) records to identify potential suspects. A review of firewall and VPN logs identified one individual who used their personal third-party file share to violate corporate policy, exfiltrate the sensitive data, and provide unauthorized access to a third-party.

Nisos worked with the Client's IT team to implement a device check at the suspect's work location, allowing us to isolate the employee's device for forensic analysis.

Our findings provided conclusive evidence of collusion with external parties. In coordination with physical security, we matched digital logs to surveillance footage, confirming that the employee had been taking photos of sensitive data on their phone and sending it through encrypted chat to unauthorized third-parties.

IMPACT

Our investigation empowered the Client to act decisively by collaborating with their HR and legal teams to terminate the insider without further incident. In addition to identifying and addressing the leak, Nisos provided strategic guidance to strengthen the Client's security posture, including configuring monitoring systems to detect unauthorized file-sharing activity and refining bring your own device (BYOD) policies to enforce device security.

The Client acknowledged that Nisos' intervention not only prevented additional leaks, saving significant resources, but also laid the groundwork for a robust insider threat program that involves engineering, legal, and HR in a coordinated defense against internal risks.

Nisos brought a multifaceted approach to the investigation, seamlessly blending digital forensics with discrete physical security data-gathering techniques that allowed us to collect evidence without alerting the employee.

Let's **Connect**

Nisos is the Managed Intelligence Company®. Our services enable security, intelligence, and trust and safety teams to leverage a world-class intelligence capability tailored to their needs. We fuse robust data collection with a deep understanding of the adversarial mindset, delivering smarter defense and more effective response against advanced cyber attacks, disinformation, and abuse of digital platforms.
Learn more at **nisos.com**.

For more information:

visit: www.nisos.com
email: info@nisos.com
call: +1-703-382-8400
follow: LinkedIn