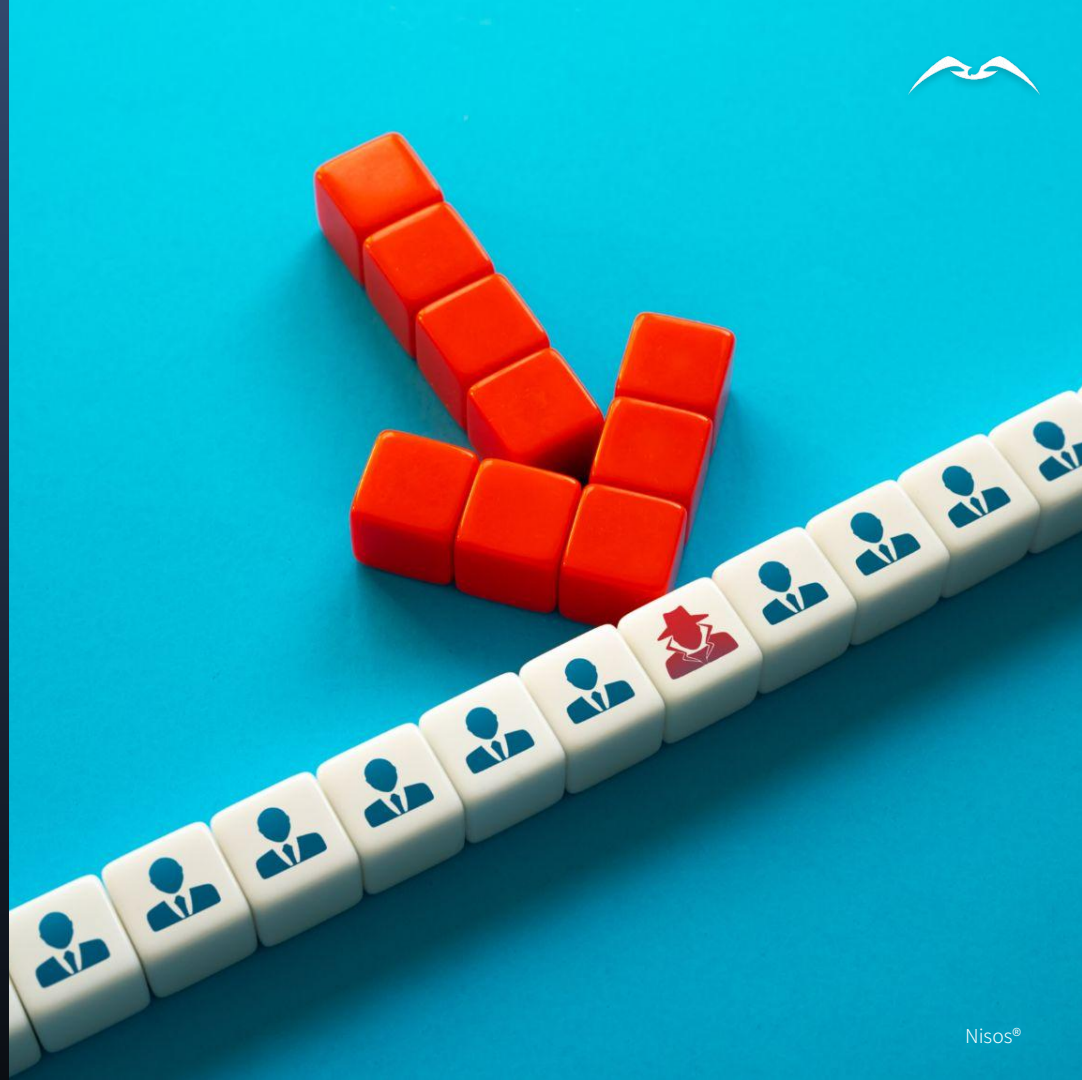
Case Study

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.

Let's **Connect**

Nisos the Managed Intelligence Company®, is a trusted digital investigations partner specializing in unmasking human risk. We operate as an extension of security, risk, legal, people strategy, and trust and safety teams to protect their people and their business. Our open source intelligence services help enterprise teams mitigate risk, make critical decisions, and impose real world consequences.
For more information, visit **nisos.com**.

For more information:

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