Case Study

Employment Shield

Investigating Nation-state Employment Fraud

Nisos **uncovers North Korean state actors gaining employment** at major tech platform company

SITUATION

Employment fraud presents significant risks to businesses, leading to financial loss, security breaches, and damaged reputations. Fraudulent employees accessing sensitive information can undermine organizational trust, especially in remote work environments where vetting processes can be more challenging.

North Korean IT workers have been known to pose as non-North Korean nationals to infiltrate businesses, funneling funds to the DPRK's economic and security efforts. In 2022, the U.S. government issued warnings about North Korean IT workers using fake identities to secure jobs and fund illicit activities.

Fearing an insider threat, a Client and their legal counsel engaged Nisos to investigate several former employees who provided false documentation to obtain employment and exhibited suspicious behavior during their time with the company. Nisos was tasked to investigate the former employees to uncover any relationship with criminal or nation-state organizations.

Client counsel engaged Nisos to investigate potential links to criminal or nation-state actors and to provide guidance on responding to a security incident.

A team of Nisos experts analyzed the information provided by the Client, including background logs, email addresses, IP addresses, and social media accounts related to the subjects.

- **Nisos found the subjects used falsified identity documents,** and copied specific language from the resume of another, unrelated individual.
- Several application IDs connected to the subjects' email addresses and IP addresses used at login have **also been used by North Korean threat actors.**
- Despite claiming extensive work histories, **there is only a limited online presence for the subjects**, including a LinkedIn account, two GitHub accounts, and a Slack community.
- Nisos investigators **attributed two individuals** who were likely associated with the person of interest based on social media and US-based address association.

The individuals discovered are part of a growing effort by the DPRK to exploit remote work to fund the DPRK's weapons development programs, as well as steal intellectual property (IP) and other sensitive information on behalf the regime.

- **Legal and Law Enforcement Action**: The investigation resulted in actionable intelligence that supported law enforcement efforts to pursue legal action against the individuals involved.
- **Enhanced Security Response**: By working alongside legal counsel and law enforcement, Nisos supported the Client in reinforcing their security posture against future exploitation attempts.
- **Compliance:** By terminating the employment of the fraudulent employees, Nisos helped the Client to avoid sanctions and regulatory fines.

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