Case Study

Disrupting Nation-State Recruiting and Disinformation Efforts on Job Site Platform

The Challenge

A job recruiting platform approached Nisos to determine the severity and authenticity of an affiliate recruiting company that appeared to be involved with disinformation and foreign nation state espionage efforts. The foreign nation state was suspected of targeted recruiting of individuals in sensitive US government positions using sockpuppet accounts.

Why Nisos

After receiving an allegation that the affiliate was using their platform to advance these efforts, the client asked Nisos to perform a digital investigation and use high operational security tradecraft to determine the extent of the operation and make recommendations on how to address the issue. Options included:

1. Removing the recruiting company from the platform,
2. Continuing to monitor, and/or
3. Informing law enforcement.

Preparation

Nisos was provided with minimal information consisting only of the name of the recruiting company. Nisos was not provided with any data regarding the details of the client's organization or internal telemetry.

Execution

The affiliate company appeared to be a typical startup venture. However, upon further investigation, their obfuscation of ownership information and use of sophisticated persona operations strongly suggested the hand of a sophisticated threat actor. Sophisticated persona operations included planting disinformation in media outlets, the use of sock puppets, platform modifications to ensure an ongoing presence on social media outlets, and the direct targeting of US-based individuals in sensitive government positions.

Execution Continued...

Nisos identified several supposed employees of the recruiting company but was unable to link any of the employees to real individuals. This included searches across social media platforms and data aggregators. The majority of the employee personas were young females located in US locations. Nisos determined that these personas were a marketing strategy meant to increase traffic to the recruiting company's website. Coupled with the sophistication of the executive's profile and the disinformation that was being disseminated through high-profile news publications, we assessed sophisticated threat actors' involvement.

Impact

The client used Nisos' investigation results and the detailed analysis and reporting provided as the basis for additional investigations into the recruiting company. It was decided to report Nisos' findings to law enforcement. Ultimately, the client determined the affiliate was in violation of their terms of service agreement and removed them from the platform to prevent any further abuse.

About Nisos

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.

For additional information, visit www.nisos.com or contact info@nisos.com.