Case Study

# Investigating Nation-State Espionage and Theft of Intellectual Property

## The Challenge

A technology company approached Nisos after it appeared some of their source code and intellectual property was leaked. The client discovered the issue after identifying a series of emails that had been sent to one of their engineers from a foreign competitor. The client was understandably alarmed and wanted to understand if competitors or nation-states were targeting their employees in an attempt to access and exploit proprietary intellectual property.

## Why Nisos

The client needed a partner with capabilities that extended beyond traditional incident response. They needed a partner with the ability to help them monitor employee devices, establish placement and access in web forums, and use technical internet data to help them determine the severity of any exfiltration of intellectual property.

## Preparation

Nisos was provided with access necessary to connect internal forensic data to the external threat hunting we needed to conduct.

## Execution

After conducting the forensic device analysis and merging the findings with our external internet data, we uncovered a significant coordinated effort to infiltrate our client's engineering department. Indications were the attack was being conducted by a competitor backed by a foreign nation-state.

This nation-state recruited engineers and sent them to the United States on student and work visas. They were directed to secure employment in the client's engineering department. The nation-state provided financial backing to intermediaries connected to one of the client's competitors. Upon a short period of employment, the intermediaries would approach their targets and make an offer on behalf of the competitor to hire the engineers for substantially more money. Prior to leaving our client's employ, the engineers would secure proprietary source code on removable media and transfer it to the competitor.

As part of our investigation, we developed custom technology that allowed us to ingest, translate, and categorize hundreds of thousands of foreign language messages. These messages provided the necessary intelligence in close to real time. During the associated forensic examination process of chat logs and browser history, it was clear the engineers had limited skill sets and were unqualified to be conducting the work for which they were hired. Their sole purpose was to exfiltrate information.

## Outcome

Our actions helped the client stop the infiltration and limit losses. In coordination with the client's legal team, our research was provided to the Federal Bureau of Investigation. After law enforcement became involved, the client continued to monitor the attempted espionage for an ongoing period of time and was able to take action, including termination of the employees as well as filing civil suits against the individuals involved.

## 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.