Case Study

Mitigating Advanced Threat Actors: Acquiring and Analyzing Malicious Tools to Stop Fraud

The Challenge

Malicious foreign actors were creating automated tools to abuse an e-commerce client's platform. Using that automated process the threat actors were able to mass create and bulk manage accounts, run advertisements, and use credit cards. With those credit cards, they were able to make purchases through the client's site, and the client's customers and third party service providers.

Why Nisos

The client needed help infiltrating closed groups where automated tools were discussed in a local language dialect to determine how customers were being defrauded.

Preparation

Nisos researchers analyzed open-source reporting and utilized technical tools and niche datasets to provide assessments on the fraud ring and their operations. We did not need access to any internal Client data.

Execution

We started with the fraudsters' selectors and online digital activities to gain access to closed groups that were discussing how the fraud was being perpetrated. We interacted with administrators of the group who provided us with a tool that was designed to spam the client's platform.

Using the tool, users had the ability to perform fake engagement and benefit monetarily. Upon running the tool, we monitored communications with the threat actor's server, which passed our registration key in cleartext to the server. This was done to ensure tool registration was complete before allowing full access to all the features.

After gaining full access to the features, we used the tool and followed-up with its creators to understand the spam tool's full functionality.

Impact

The client was able to use the specific TTP information we provided about the tool to write code and prevent the tool from working on its platform in the future. Further, thanks to the detailed attribution we conducted, the client's legal team was able to take direct action against the threat actors, preventing them from moving on to their next potential fraud scheme against the client's platform.

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.