Case Study

Identifying and Disrupting Platform Abuse in the Gig-Economy

The Challenge

A technology company noticed a disturbing increase in malicious activity across their platform. Unknown individuals were selling bots that claimed to automate interactions with their platform and provide those that purchased the app an advantage over other users. This use of the app was a clear violation of the client's Terms of Service. In other words - the bots would "game the system" to the financial disadvantage of normal conforming users - leading to frustration and anger directed at the client. To make matters worse, the bots mirrored the legitimate client application, presenting additional security threats.

The client enlisted Nisos with three primary objectives:

1. Determine how the bots were able to subvert client controls and take advantage of the platform.
2. Provide recommendations on how the client could improve their security posture and counter the illegitimate activity of the bots.
3. Identify the actors making the bots, enabling the client to properly attribute the crime and take legal action.

Why Nisos

Nisos' ability to help the client was rooted in our ability to deliver high-quality technical application analysis combined with open source research and attribution.

Preparation

The Client started by providing Nisos with a detailed history of bots that they had previously uncovered. They requested Nisos identify additional bots that may be present and undiscovered. In order to accomplish this task, Nisos did not need to access the Client's network or sensitive data.

Execution

Nisos acquired the bot of most concern to the client through a common App store. We confirmed that it operated as claimed and provided an analysis of how the bot functioned at the code level. We also determined that several methods could be used to create a functional bot targeting the client's platform, and we provided recommendations to the client to remediate this risk.

Our assessment concluded that the creator of the bot took the official client application, acquired the binary from a device, and altered it with their own additional code. This additional code pulled the necessary information from the client and automated user responses.

Attribution

Nisos found that previous application bot domains were associated with truncated email addresses. In one case, Google cache inspection of application .vip revealed a telegram account associated with a partially named online persona. We acquired a license for the application and extracted the Intelligent Process Automation (IPA). We then identified that the back end server for downloading the app bot was associated with an IP address that served as a Virtual Private Server (VPS). The infrastructure was hosted in a Japanese hosting facility.

In another case, we were able to track back “old” versions of the application bots that revealed selectors. Using these selectors and cross referencing them in Nisos proprietary credential databases and other external telemetry, we attributed them to named individuals. We also determined that these selectors were being used for additional, identifiable fraudulent activity

Outcome

Nisos provided numerous recommendations to the legal, trust and safety, and engineering teams of the client. These recommendations allowed the client to improve the platform’s security and increase the difficulty of duplicating the legitimate application binary and circumventing application controls.

The client used our findings to successfully request removal of the fraudulent application’s platform developer certificate. Working with outside counsel, the client used our attribution research to issue cease and desist orders and prepare civil suits against the application bot developers.

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