eBook

Legal Case Studies

White Glove Digital Investigations

How Nisos helps legal counsel **protect value, reduce risk, deter adversaries, and pursue criminals.**

Proprietary and Confidential Information - Copyright© 2024 - All Rights Reserved - Nisos®

Trusted Digital Investigators

Protecting legal rights, intellectual property, and assets, as adversaries continuously innovate, is a challenge for every business. The digital realm amplifies threats to data, and introduces new risks to transactions, physical assets, and people.

Nisos provides an unparalleled digital investigations capability for:

- Cybersecurity & Privacy,
- IP & Technology,
- National Security, and
- White Collar Defense practice groups

Nisos extracts and enriches surface, deep, and dark web data to develop deeper insights into your clients' unique threats and digital exposure. By providing greater visibility, expertise, and guidance you can help your clients become more proactive and systematic in risk management.

In this eBook, we explore three examples of how Nisos has helped law firms and their clients overcome security challenges.

Case Studies:

- Navigating Vulnerability Disclosure Negotiations
- Uncovering Copycat Apps and Bots
- Investigating Nation-state IT Employment Fraud

Proprietary and Confidential Information - Copyright© 2024 - All Rights Reserved - Nisos®

“In just a few weeks, your analysts have generated numerous promising leads the FBI, US Marshals and Interpol could not uncover, despite having a three-year head start.”

Top Attorney for the Defense of the Victims
In Pursuit of an International Fugitive

Proprietary and Confidential Information - Copyright© 2024 - All Rights Reserved - Nisos®

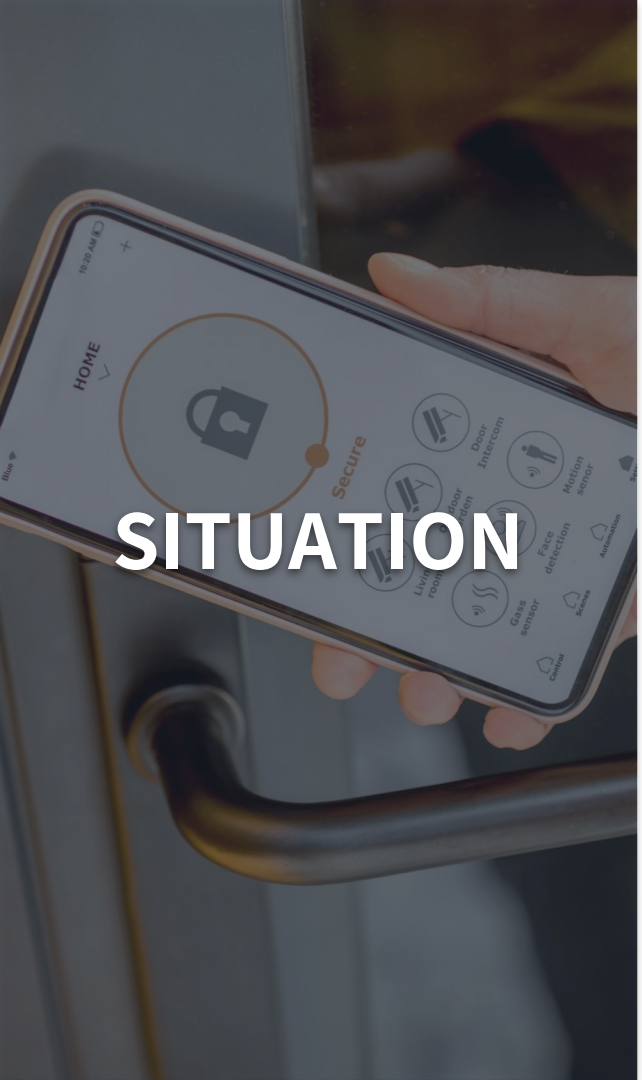
Case Study

Cybersecurity and Privacy

Navigating Vulnerability Disclosure Negotiations

Nisos investigates security researchers and uncovers an NDA violation **for a global technology brand**

Proprietary and Confidential Information - Copyright© 2024 - All Rights Reserved - Nisos®

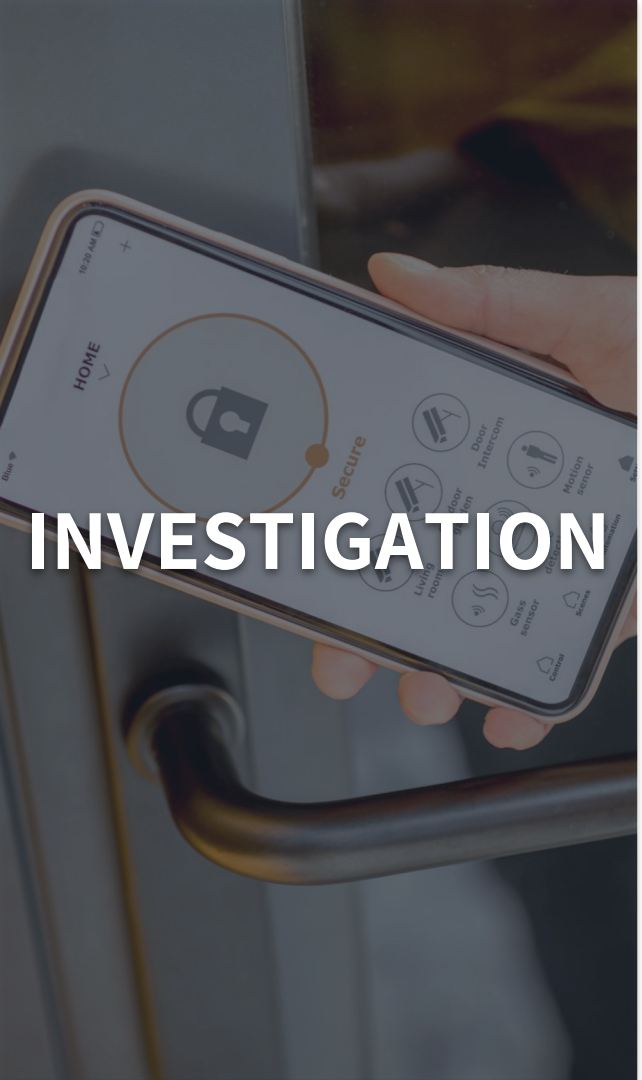


SITUATION

Technology companies are often approached by 'white hat' security experts who have discovered security flaws in their products, and demand a bounty payment for the find. While bug bounty requests are a normal part of a healthy technology community, they can also be exploited by ill-intentioned parties looking to make a buck or embarrass the brand.

When a smart device company was approached by security researchers who had discovered vulnerabilities in their products, they turned to Nisos to provide critical context.

While in-house and third-party cyber experts investigated and remediated the vulnerabilities, Nisos investigated the researchers behind the discovery to ensure they weren't threat actors, and were likely to adhere to the terms of an NDA signed as part of a disclosure reward.



INVESTIGATION

Nisos was retained by counsel to conduct a background investigation of all security researchers. The Client engaged a Nisos team of Open Source and Cyber threat analysts, with specialists in attribution and closed group monitoring.

The task was to validate the individual identities of the researchers, and rule out any association with criminal or sanctioned groups. Nisos was also asked to monitor the open and dark web to ensure information about the vulnerabilities hadn't leaked, and researchers adhered to the Non-Disclosure Agreement (NDA) signed during the course of negotiations.

Nisos confirmed the **identities of five security researchers** and monitored their online presence to ensure no public disclosure of the vulnerabilities occurred.

During monitoring, it was discovered that, while the researchers hadn't discussed the vulnerabilities publicly, they had **ongoing discussions about the vulnerabilities** in private Discord channels.

Knowledge of these discussions and a full understanding of the researcher's background **allowed counsel to posture for negotiating leverage** for the bounty payment.

IMPACT

While Nisos validated that the security researchers were above board, and hadn't leaked anything sensitive publically, knowledge of ongoing discussions of the vulnerabilities in Private Discord channels gave general counsel leverage in bounty negotiations.

As a result of our work:

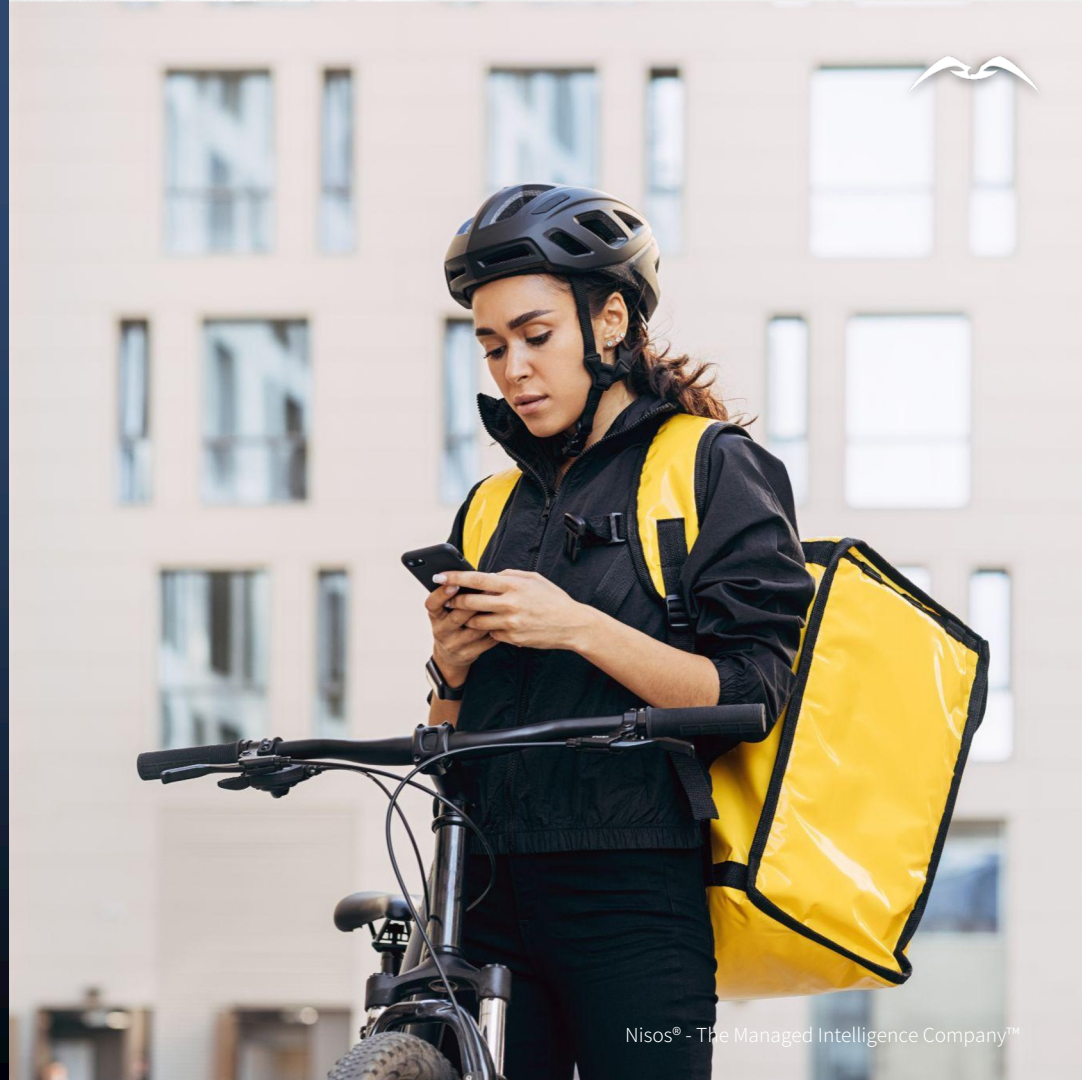
- Legal counsel had critical context to navigate bounty payment negotiations
- The eventual bounty payout to security researchers was reduced significantly
- The technology company was confident they were able to remediate the issue before public vulnerability disclosures were issued

Case Study

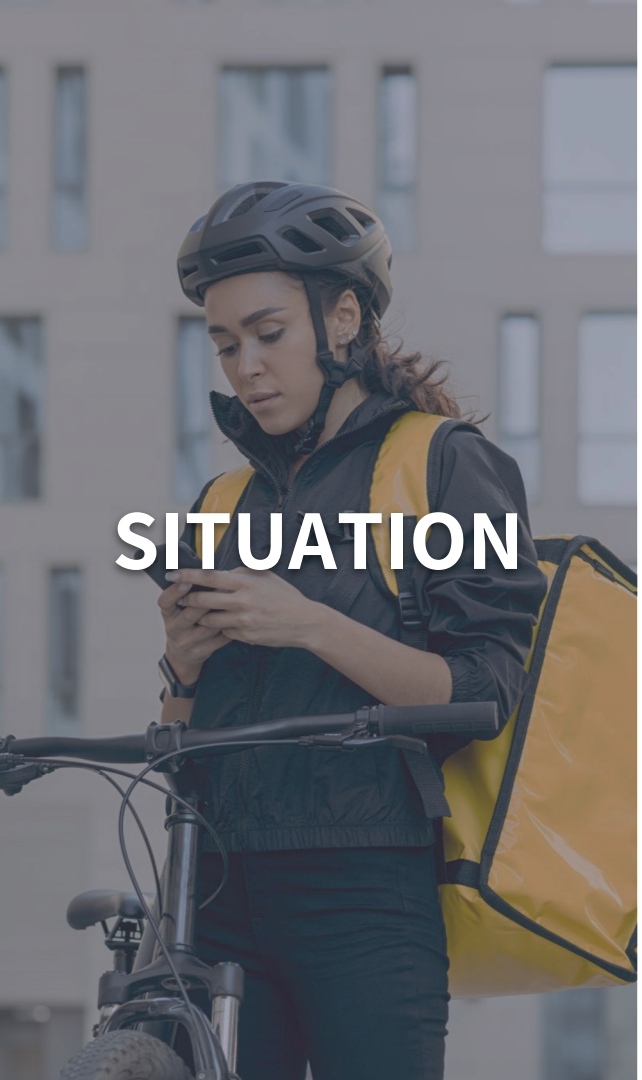
Legal - Intellectual Property & Fraud

Uncovering Copycat Apps and Bots

Nisos investigates threat actors behind fake apps impersonating **a major gig economy platform**



Proprietary and Confidential Information - Copyright© 2024 - All Rights Reserved - Nisos®



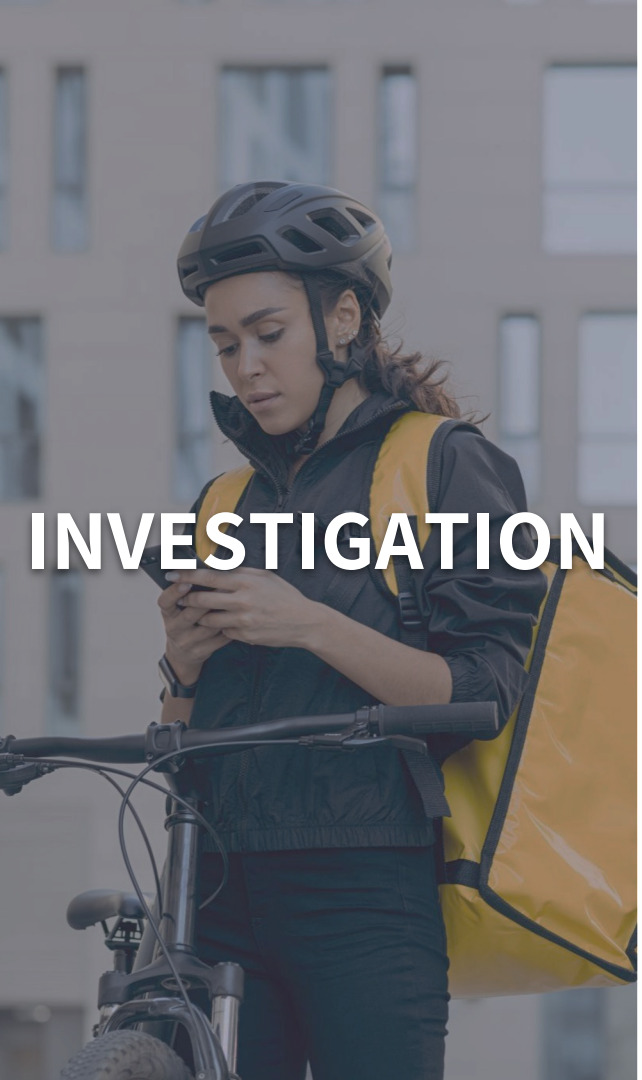
SITUATION

Online platforms are a prime target for fraud actors to exploit users and game systems to their advantage. Bots and look-alike applications are an acute challenge, especially when they threaten a key revenue stream for the business.

When a technology company noticed an increase in malicious activity on their platform, they discovered unknown individuals selling bots designed to game their systems. The bots were part of a scheme that allowed gig-workers to use a special app to jump the line, and gain priority access to the most lucrative gigs available at the time.

The fraudulent app appeared like a legitimate application, and was available for purchase on popular app stores. Gig Workers who lost out on tasks were rightly frustrated, and turned their anger on the client.

Legal counsel for the Client enlisted Nisos to determine how the bots were able take advantage of the platform, provide recommendations on how to counter them, and – if possible – identify the actors behind the scheme.



INVESTIGATION

Nisos was tasked to investigate the wider threat of bots and fraudulent applications to their platform, and identify additional fake applications where possible.

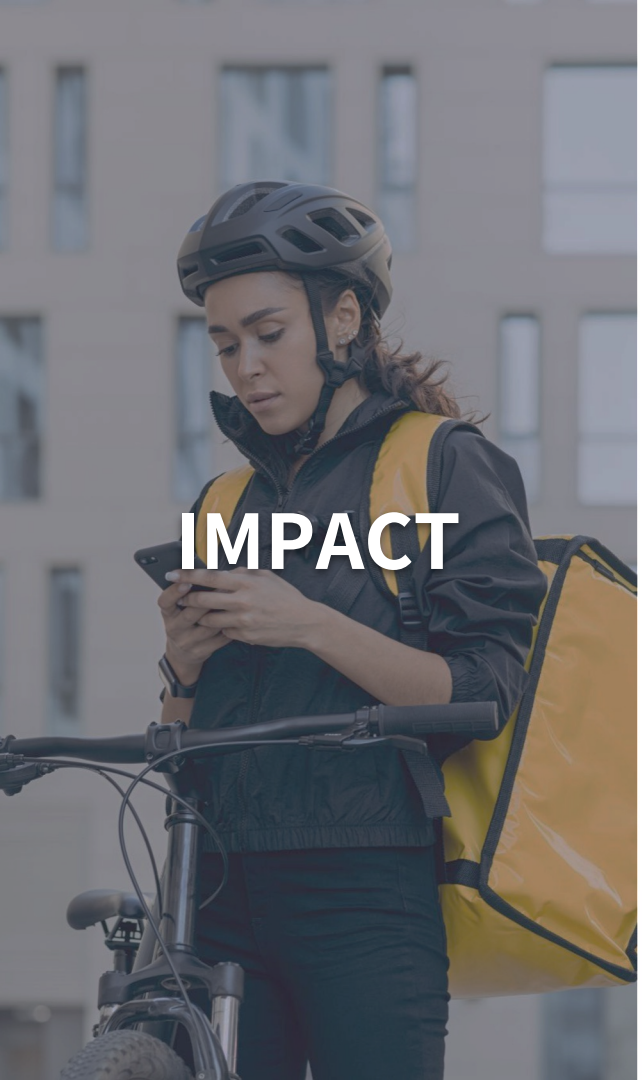
As a first step, a Nisos team of experts in technical and OSINT investigations purchased the most concerning apps listed on common app stores, and reverse engineers the software to understand how it functioned at the code level.

Our assessment concluded that **threat actors** acquired the binary from a device and **altered the official client application with their own malicious code**, in violation of the Terms of Service.

A deeper look **revealed details about the infrastructure** behind the scheme, including an IP address for a Virtual Private Server hosted in Japan.

Nisos connected the malicious bot domains with several truncated email addresses, and a telegram account with a partially named online persona.

Using these selectors, our proprietary breach data sets, and external telemetry, we **identified a Contractor employed by the Client as the author of the malicious bot.**



IMPACT

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.

The client used our findings to successfully request removal of the fraudulent application 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.

In addition to supporting the efforts of legal counsel, 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.

Case Study

Legal - National Security

Investigating Nation-state IT Employment Fraud

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

Proprietary and Confidential Information - Copyright© 2024 - All Rights Reserved - Nisos®

SITUATION

Fraudulent IT workers provide a critical stream of revenue that help fund the Democratic People's Republic of Korea's (DPRK) regime's highest economic and security priorities. On 16th May 2022, the US Department of State, Department of the Treasury, and the Federal Bureau of Investigation (FBI) warned of attempts by North Korean IT workers to obtain employment while posing as non-North Korean nationals.

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 tenure with the company.

Nisos was tasked to investigate the former employees (subjects) to uncover any relationship with criminal or nation-state organizations in anticipation of litigation or regulatory investigation.

INVESTIGATION

Client Counsel requested Nisos uncover any links to criminal or nation-state actors and provide legal advice with respect to responding to the security incident.

A Nisos team of experts in technical and OSINT investigations 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 subject's 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**, comprising a LinkedIn account, two GitHub accounts, and a Slack community.

Nisos investigators **attributed two individuals** who were likely associated with Subject based on social media and US-based address association.

IMPACT

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

Our investigation revealed several critical findings that lead to law enforcement action, including identifying named individuals involved in the scheme. Nisos attributed both threat actors using social media and US-based address association, and Nisos worked with legal counsel and law enforcement agencies as they pursued legal action.

Meet the Nisos **Legal Investigations** Team

Landon Winkelvoss
Co-Founder and VP of Legal and Intelligence Advisory

Landon Winkelvoss co-founded Nisos in 2015 and serves as its VP of Legal and Intelligence Advisory. He leads Nisos legal go-to-market where his team is directly involved in sales, demand generation marketing efforts, law firm partnership acquisition, product management, and project sales conversion to annual recurring revenue. He also sits on the Board of Directors and is involved in the strategic direction of Nisos with Columbia Capital, Paladin Capital Group, and Skylab Capital. His vision as a founder was to engineer digital investigations at scale using AI to deliver intelligence community-level insights to blue-chip companies and the national security sector.

Prior to founding Nisos, he spent 10 years as a Technical Targeting Officer for the U.S. Intelligence Community, including multiple warzone deployments and overseas postings. Landon is a regular contributor to numerous publications on cyber intelligence and investigations, including Security Week, Dark Reading, and SC Magazine.

Jennifer DeTrani
General Counsel

Jennifer DeTrani is General Counsel, SVP Legal, and Corporate Secretary. Prior to Nisos, she co-founded a secure messaging company, Wickr, ran a solo law practice, practiced corporate law in BigLaw and served as a federal prosecutor at the Department of Justice. She is a visiting fellow at the National Security Institute at George Mason School of Law, serves on the Executive Leadership team of SunLaw, a non-profit organization dedicated to the advancement of women in-house counsel, and is a member of TechGC.

In addition to advancing diversity and promoting equality in the legal profession, she is passionate about helping companies devise an informed response to advanced cyberattacks, e-crime, IP theft, disinformation, threats to executives and physical assets, state-sponsored actors, and abuse of digital platforms.

Nisos is The Managed Intelligence Company®. Our analyst-led intel investigations, assessments, and monitoring services empower your security, intelligence and trust and safety teams. We provide accurate, customized intelligence that guides your security and risk decisions – protecting your organization, assets, and people.

Let's **Connect**

Proprietary and Confidential Information - Copyright© 2024 - All Rights Reserved - Nisos®