Marketing Research

Shielded on All Sides:
How Company Executives Can Mitigate Virtual Kidnapping Schemes

December 2024

Table of Contents

Introduction

Virtual kidnapping, or virtual kidnapping for ransom, is a coercive telephonic scheme used to extort ransom payments from victims. Victims are contacted, via telephone, and tricked into believing their loved one has been kidnapped, is at risk of being kidnapped, or is in imminent danger.[1] The Federal Bureau of Investigation (FBI) cautioned in October 2024 that recent instances of virtual kidnapping have grown more sophisticated by using AI technology to simulate a loved one's voice.[2] While virtual kidnapping scams target the public indiscriminately, high-wealth individuals and individuals with access to critical company information, such as company executives in chief executive officer (CEO) and chief information security officer (CISO) roles, are at higher risk. Media reporting shows that these scams have been targeting high-networth individuals and company executives since at least 2022, however instances of virtual kidnappings have been reported as early as 2000.[3] [4]

Social media accounts often provide scammers with the information they need to approach and target their victim.[5] Nisos partners with corporate security and executive protection teams to evaluate online vulnerabilities, including on social media, that pose a risk to executives and their family members. Through our detailed Executive Vulnerability Assessment, we identify content revealing personally identifiable information (PII) and pattern-of-life details that can enable scammers to build a profile to assist virtual kidnapping scams.

2023 Cyber Crime Statistics

According to the FBI Internet Crime Complaint Center's (IC3) 2023 annual report the number of complaints and financial losses related to cyber crimes increased between 2022 and 2023. IC3 reported that they received 880,418 complaints in 2023, a record number, with potential losses exceeding $12.5 billion. This represents a nearly 10% increase in total number of complaints received, and a 22% increase in losses suffered, compared to 2022. IC3 also reported that the total number of complaints for extortions, which likely includes virtual kidnapping scams, increased in 2023 compared to 2022. This increase is the second highest year-over-year increase compared to all other crime types IC3 tracks, which include phishing, employment fraud, tech support, and business email compromise. The total loss reported due to extortions increased by $20 million between 2022 and 2023.[6]

[1]https://www.colorado.edu/isss/sites/default/files/attached-files/slicksheet_-_virtual_kidnapping-english_version[.]pdf
[2]https://www.kulr8.com/news/fbi-cautions-citizens-about-a-i-ransom-scams/article_f133106c-8821-11ef-bbe1-3752337cb54a[.]html
[3]https://www.rollingstone[.]com/culture/culture-news/virtual-kidnappings-wealthy-elite-entertainment-1392918/
[4]https://pmc.ncbi.nlm.nih[.]gov/articles/PMC10256574/#Sec8
[5]https://www.fbi[.]gov/contact-us/field-offices/chicago/news/press-releases/fbi-chicago-warns-public-about-virtual-kidnapping-scams
[6]https://www.ic3[.]gov/AnnualReport/Reports/2023_IC3Report.pdf

Executive Protection Overview

The executive protection work we do for clients involves manual, analyst-driven **social media review and analysis** for cyber-fraud protection - such as victims and targets of virtual kidnapping scams, identity theft, and romance scams. We also provide threat monitoring and alerting to mitigate digital vulnerabilities that can enable digital and even physical attacks. An analyst's coordination with and understanding of an individual's life helps identify unique, dated-yet-relevant, or nuanced data that automated services likely miss.

Social Media Review and Analysis

Effective protection against scammers requires more than only identifying personal information on deep/dark web marketplaces, public records sites, and data breaches. According to the FBI: "Virtual kidnappers scour the Internet for targets by searching for social media posts by international travelers. Scammers then contact the target's loved ones claiming to have taken the target hostage."[7] Posting about travel in real time and allowing public access to friends lists gives threat actors insight that enables virtual kidnapping scams. The same scammers are also looking for additional personal information about the victims, their family members, and estimated net worth to make their scams more believable.

- Nisos was tasked to investigate a virtual kidnapping event, in which scammers claimed that the sibling of a family member was kidnapped. The scammers asked the victim to send close to $100,000 via a wire transfer within two hours. Nisos found that the victim's social media posts identified their sibling by name and revealed an approximate $100,000 windfall within the last two weeks. Additionally, Nisos identified that the sibling traveled overseas for vacation, via the sibling's social media accounts, which is why the victim was unable to contact their sibling. Nisos' Executive Shield services are designed to highlight and mitigate vulnerabilities this threat actor exploited.

- Nisos was tasked to help protect a senior executive at a large company. Nisos found a number of social media posts that included location and pattern-of-life information for the client's children, which threat actors could exploit. We highlighted these risks to the client, and with continuous monitoring, we help ensure that similar information is not exposed online.

- Many executive protection services do not focus on social media risks for their clients and rely on the identification and automated removal of personal information from deep and dark web marketplaces, public records sites, and data breaches. These services can help mitigate instances of identity theft, but they fall short of mitigating cyber crimes, such as virtual kidnapping scams, that became more prevalent in 2023.

[7]https://www.fbi[.]gov/contact-us/field-offices/chicago/news/press-releases/fbi-chicago-warns-public-about-virtual-kidnapping-scams

Executive Protection Threat Monitoring

Executive protection services are most effective when social media analysis is combined with ongoing monitoring. PII removals from people search sites, data marketers, data brokers, ancestry sites, residence listings, telephone lookups, and business records are only effective if sensitive data is not otherwise available to threat actors, including on social media. Social media posting habits can negatively impact an individual's online footprint.

- The most effective monitoring solutions provide consistent, personalized recommendations to support individuals in reducing publicly available information, adopting new practices on social media, and alerting them to how threat actors can act on or exploit seemingly benign information.

- The FBI reported that in 2023 extortion crimes resulted in circa $74 million loss for individuals. A large percentage of complaints and losses due to cyber-crime scams affected people between the ages of 40 and 60+. This age range is typical for executives, such as company CEOs and CISOs, suggesting they are a more likely target for cyber scammers.[8]

Conclusion

Nisos' Executive Shield service offers a proactive approach to mitigating threats—preparing for the worst while eliminating nefarious actors' access to information that can enable attacks. Combining effective social media analysis with ongoing monitoring and vulnerability mitigation efforts protects our clients from ever increasing threats. Nisos recognizes that individuals and companies place a significant level of trust in our partnership and capabilities when undergoing this level of monitoring and proactive protection. Through this trust and relationship, Nisos can help protect an individual's family, assets, and reputation and mitigate vulnerabilities.

[8]https://www.ic3[.]gov/AnnualReport/Reports/2023_IC3Report.pdf