NISOS

Marketing Research

The Insider Threat Digital Recruitment Marketplace

January 2025

Executive Summary

Nisos routinely monitors mainstream and alternative social media platforms, as well as cloud-based messaging applications and dark web forums to identify individuals and networks advertising insider access or recruiting insiders at companies. This effort revealed a rapid increase in the number of insider threat activities from 2019 to 2024.

Our findings in Q4 2024 illuminated an insider threat digital recruitment marketplace available across multiple digital realms (cloud-based messaging apps, dark web forums) in which threat actors seek insiders and offer their services for targeting companies in the telecommunications, sales and e-commerce industries.

Identifying insider threat activities prior to a leak of sensitive information is an important part of a security team's ability to mitigate risk and is something many security teams are not staffed or equipped to handle on their own for a number of reasons. Our clients are better equipped to reduce their risk of insider threats when they are aware that threat actors are targeting them.

Insider Threat Risks and Recruitment

Nisos and other companies specializing in human risk intelligence and security research have noted a steady rise in the number of insider threat attacks over the last five years. Employees with authorized access to an organization's systems or data perpetrate these attacks, often causing serious financial and reputational harm to their organizations.[1] According to data from PwC, 57% of fraud is committed by company insiders or a combination of insiders and outsiders.[2] Moreover, according to Cybersecurity Insiders' 2024 Insider Threat Report, 83% of organizations reported at least one insider attack in the last year - which was an increase of five times over the amount in 2023. Insider threats pose unique challenges for organizations, as they can emerge from trusted individuals with legitimate access to sensitive systems and data.[3] From 2019 to 2024, the number of organizations reporting insider attacks increased from 66% to 76%.[4]

Nisos saw an equally rapid increase in the number of insider threat intelligence investigations we conducted to help protect organizations and safeguard against financial losses, reputational damage, and operational risks. As part of our investigations, Nisos frequently monitors mainstream and alternative social media platforms, as well as cloud-based messaging applications and dark web forums to identify individuals and networks advertising insider access or recruiting insiders at companies. A review of posts on cloud-based messaging applications and on dark web forums revealed numerous newly posted advertisements for insider access and recruitment pitches for insiders during Q4 of 2024 alone.

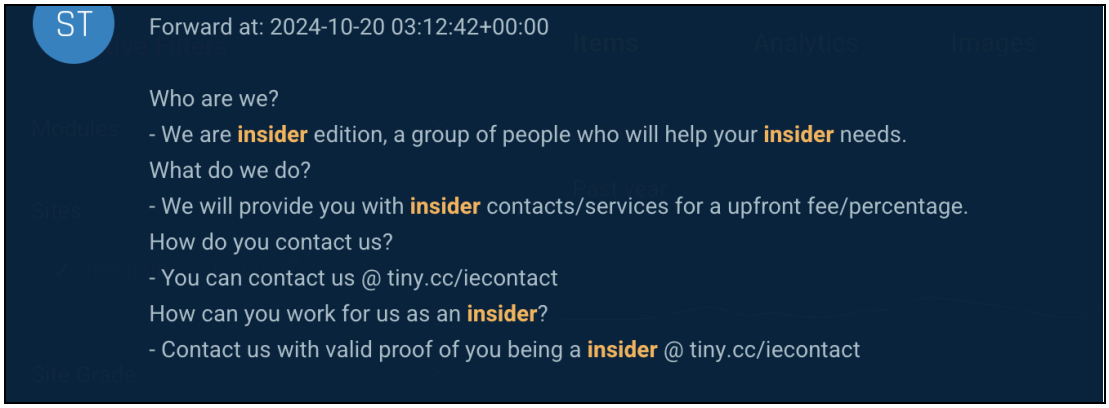
[1] https://www.cisa[.]gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats
[2] https://www.barclayscorporate[.]com/insights/fraud-protection/internal-fraud/
[3] https://securityintelligence[.]com/articles/83-percent-organizations-reported-insider-threats-2024
[4] https://www.securonix[.]com/wp-content/uploads/2024/01/2024-Insider-Threat-Report-Securonix-final.pdf

Cloud-Based Messaging Applications

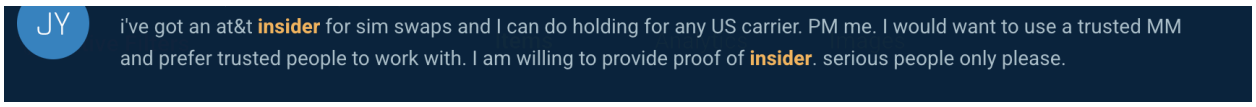
Using appropriate tradecraft and following legal guidance, Nisos monitored private discussion groups and channels on cloud-based messaging applications where threat actors discussed insider threat activities. Nisos found that the discussions over the last three months focused on general insider services, recruitments for insiders at specific companies, and the ability to offer refunds at companies via insiders.

General Insider Services

Nisos identified threat actors advertising their services to connect buyers with insiders. They used the same advertisements to recruit insiders as well. These actors frequently direct users to connect on other platforms or connect via trusted middle men.



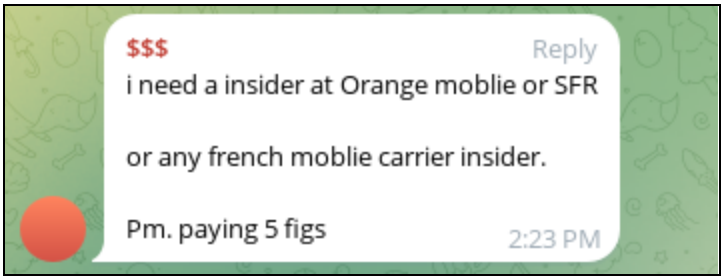
Graphic 1: Example of an insider recruitment and services post on Telegram.



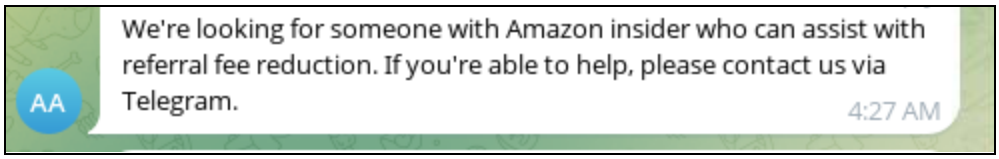
Graphic 2: Example of an insider threat advertisement on Telegram.

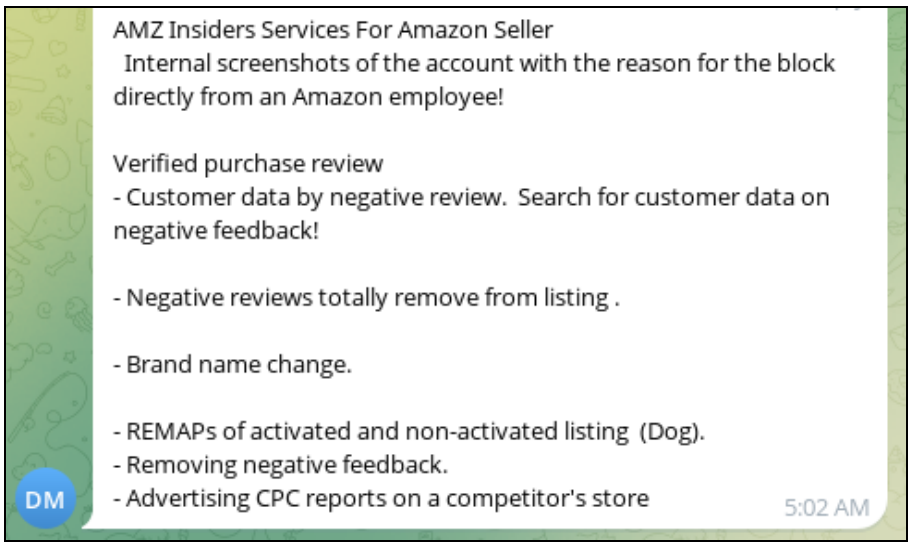
Insider Recruitment

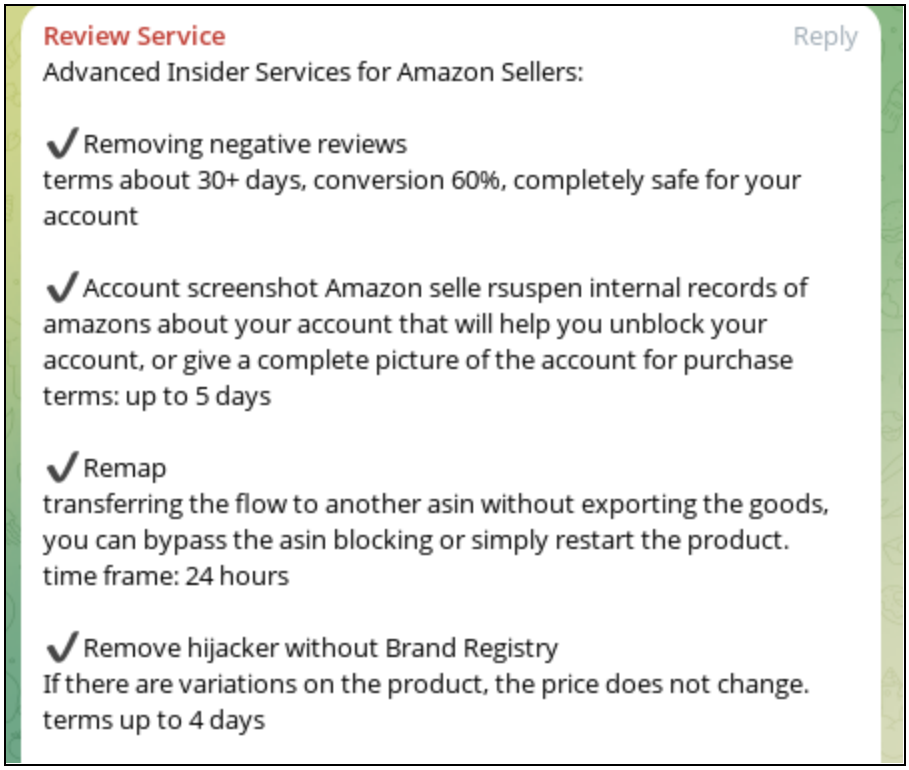
Nisos identified threat actors requesting insider services at phone companies and at Amazon. These messages typically promise large payouts for insider access and list the types of services the threat actors are looking to access.



Graphic 3: Example of a Telegram post requesting insider access at French mobile carriers.



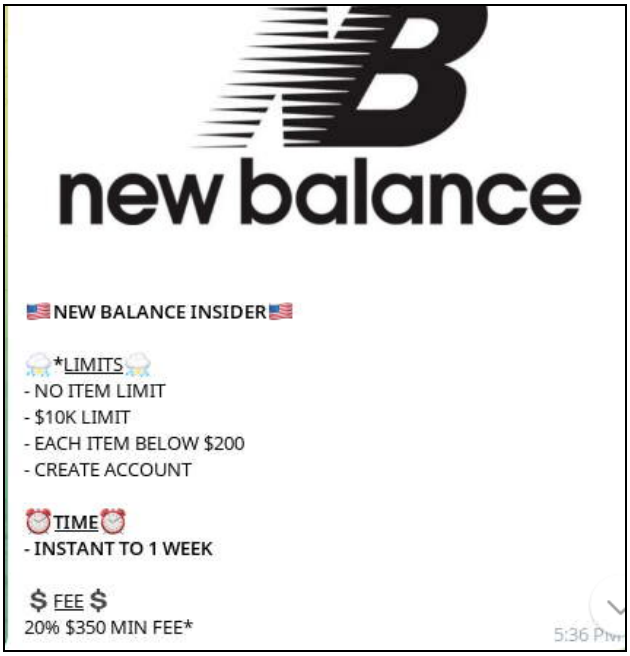




Graphic 4-6: Examples of Telegram posts requesting insider access at Amazon.

Insiders for Refund Services

Nisos identified threat actors advertising insider services at companies to process refunds. These posts typically list the capabilities of the insiders and their fees for insider services.



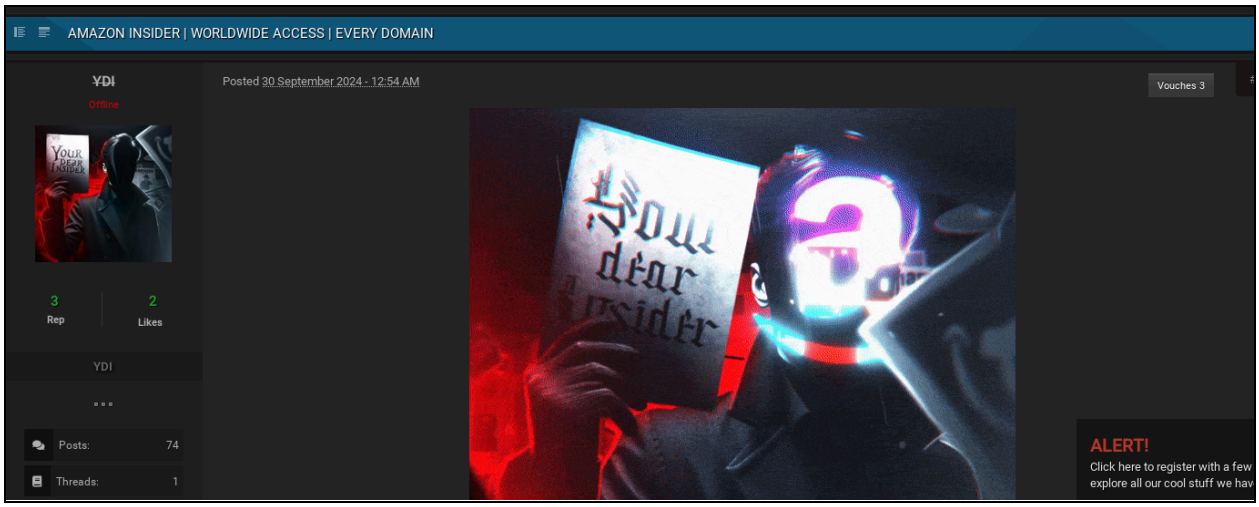
Graphic 7-9: Examples of Telegram posts advertising insider services to process refunds.

Dark Web Forums

Using appropriate tradecraft and following legal guidance, Nisos monitored dark web forums where threat actors discussed insider threats. Nisos found that the discussions over the last three months focused on selling insider services and recruiting insiders.

Insider Threat Services

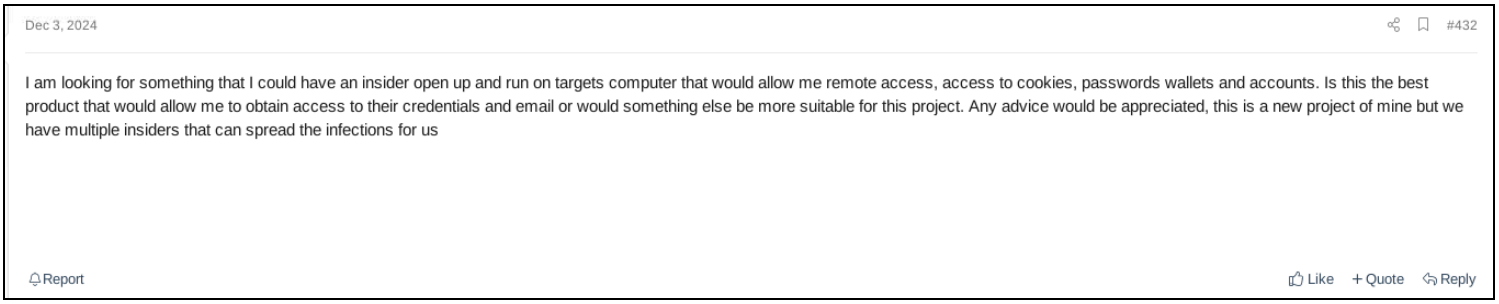
Nisos found dark web forums where users advertised insider access for a fee. In one example, the threat actors posted that they would connect buyers to an insider working at Amazon, who could perform services for a fee. The threat actors clarified that they were not the insider, but had access to one.

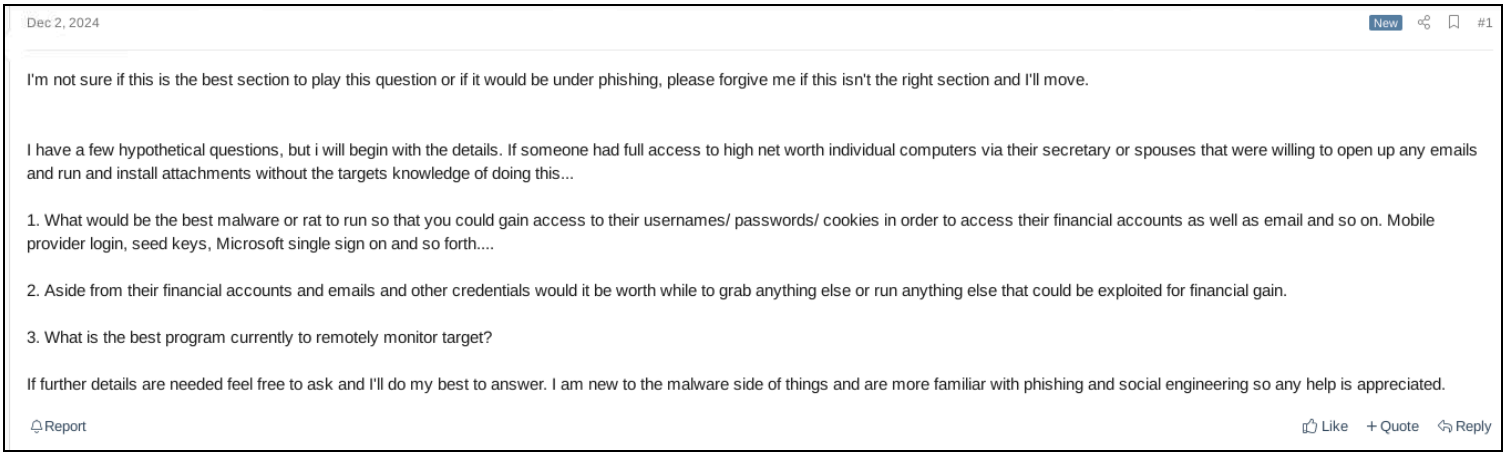


Graphic 10: Example of a dark web post advertising insider services.

Insider Recruitment

Nisos found dark web forums where users sought to recruit insiders. They also requested insights on how to infiltrate an organization and the computers of high-networth individuals to remotely obtain sensitive information.





Graphic 11-12: Examples of posts on dark web forums seeking insider services.

Human Risk Intelligence and Insider Threats

Insiders can cause significant harm to organizations, resulting in financial costs, data loss, operational disruptions, legal issues, and reputational damage.[5] Nisos helps enterprise security teams identify, investigate, and prevent insider threats - both prior to an incident and support client investigations following an incident - through investigations and monitoring. Threat actors' efforts to recruit enterprise insiders are pervasive, evolving, and present across the digital realm. Human risk intelligence can make a real difference in successfully combatting insider threats. Enterprises are better equipped to reduce their risk of insider threats when they are aware that threat actors are targeting them and recruiting insiders, and when they understand the tactics used and the profile of sought-after individuals. Security, human resource, and legal teams are better able to focus their insider threat efforts on the departments likely to be recruited and know what indicators to look for. Combining outside-the-firewall insights such as online recruitment intelligence with internal telemetry is a best-practice approach to combatting insider threats.

[5] https://www.teramind[.]co/blog/consequences-of-insider-threat