North Korea’s Fraudulent IT Employment Scheme: A Cybersecurity Threat

recordedfuture.com/research/inside-the-scam-north-koreas-it-worker-threat

Research (Insikt)

Inside the Scam: North Korea’s IT Worker Threat

Posted: 13th February 2025

By: Insikt Group®

cation for Employment
ns for persons with disabilities in the hiring
and we will provide assistance.
Date of Application
Name
Education

·|¦|· Insikt Group®

Executive Summary

In an era in which remote work has become the norm, North Korea has seized the opportunity to manipulate hiring processes, using fraudulent information technology (IT) employment to generate revenue for the regime. North Korean IT workers infiltrate international companies and secure remote positions under false identities. These operatives not only violate international sanctions but also pose severe cybersecurity threats, engaging in fraud and data theft and potentially disrupting business operations.

Beyond financial fraud, these IT workers have been linked to cyber espionage. Insikt Group tracks PurpleBravo (formerly Threat Activity Group 120 [TAG-120]), a North Korean-linked cluster that overlaps with the “Contagious Interview” campaign, which primarily targets software developers in the cryptocurrency industry. The campaign employs malware such as

BeaverTail, an infostealer that gathers sensitive information; InvisibleFerret, a cross-platform Python backdoor; and OtterCookie, a tool used to establish persistent access on compromised systems. At least three organizations in the broader cryptocurrency space were targeted by PurpleBravo between October and November 2024: a market-making company, an online casino, and a software development company.

The findings also highlight North Korea’s expansion into other areas of fraud, with the establishment of front companies that mimic legitimate IT firms. TAG-121, a separate cluster of activity, has been identified as operating a network of these companies across China. Each front company spoofs a different legitimate organization by copying large parts of their website. These entities create an added layer of deniability and make detection more challenging, allowing North Korean actors to further embed themselves in global IT supply chains.

The implications of this threat are far-reaching. Organizations that unknowingly hire North Korean IT workers may be in violation of international sanctions, exposing themselves to legal and financial repercussions. More critically, these workers almost certainly act as insider threats, stealing proprietary information, introducing backdoors, or facilitating larger cyber operations. Given North Korea’s history of financial theft, the risks extend beyond individual companies to the broader global financial system and national security interests.

To mitigate these threats, organizations must adopt stringent identity verification measures, ensuring that remote hires undergo thorough screening. This includes requiring video interviews, notarized identification documents, and continuous monitoring of remote workers for anomalies. Employers should also implement technical controls to detect unauthorized access, restrict data exposure, and flag suspicious remote connections. Awareness and training for human resources (HR) teams and IT security personnel are essential in preventing these actors from infiltrating critical business operations.

While the threat posed by North Korean IT workers is a fraud issue, it is also a key component of a sophisticated cyber strategy that financially sustains an internationally sanctioned regime. As these operations continue to evolve, businesses, governments, and cybersecurity organizations must work together to close the gaps that enable North Korea to exploit the remote work environment.

Key Findings

- North Korea’s use of IT workers to secure fraudulent employment and execute coordinated cyber campaigns highlights its evolving tactics to fund its military programs while undermining global intellectual property security.
- Insikt Group assesses that PurpleBravo has targeted at least seven entities, three of which are in the cryptocurrency sector, including a market-making firm, an online casino, and a software company.

- Insikt Group found evidence that PurpleBravo uses Astrill VPN to manage its command-and-control (C2) servers.
- PurpleBravo was found posting job advertisements on at least three hiring websites, Telegram, and GitHub.
- Insikt Group identified at least seven suspected North Korean-linked front companies operating in China spoofing legitimate IT firms in China, India, Pakistan, Ukraine, and the United States (US).
- Organizations should implement robust technical safeguards, such as, where feasible, disabling remote desktop software, conducting regular checks of open ports across networks, deploying insider threat monitoring, and geolocating devices.
- Insikt Group expects to continue to see groups like PurpleBravo and TAG-121 exploit the remote work environment, threatening global IT supply chains and intellectual property.
- North Korea's shift toward fraudulent remote employment and front companies will likely outpace traditional hiring protocol checks, driving organizations and governments to adopt more rigorous identity verification, enhanced remote work security, and robust international intelligence-sharing to counter this expanding threat.

Background

On January 23, 2025, the US Department of Justice (US DOJ) indicted two North Korean nationals and three facilitators for remote worker fraud that enriched the North Korean regime. In the indictment, the US DOJ described a six-year scheme in which two US citizens and one Mexican national conspired with North Korean IT workers to remotely work for at least 64 US companies. Payments from ten companies generated at least $866,255 in revenue that was laundered through a Chinese bank account. In addition to the indictment, stories of organizations and individuals that have come across North Korean IT workers can be regularly found in open sources (1, 2, 3). Besides sanctions violations, the threat from these workers, whether stealing sensitive data or installing malware on internal systems, presents unique challenges to organizations, especially in remote work environments.

North Korea remains highly isolated from the outside world due to the regime's strict control over goods, people, and information, as well as international sanctions placed upon the country. Despite this, Pyongyang's leadership is well-versed in exploiting emerging technologies to fund its operations. As sanctions have tightened, the regime adapted by escalating illicit activities, including smuggling and cybercrime. In recent years, the regime has achieved significant success in stealing from traditional financial institutions and digital assets like cryptocurrency. Between 2020 and 2024, the rise of remote work created new opportunities for North Korea to deploy skilled IT workers who infiltrate global companies under false identities. Their activities directly support the regime's military programs while posing a significant threat to industries reliant on intellectual property.

Research into North Korean IT workers has focused on the following aspects of the threat: North Korean IT workers gaining fraudulent employment through proxies; North Korean front companies, often in the software development space, imitating legitimate organizations; and fake employment opportunities targeting software developers in cryptocurrency and AI, among other industries. Other research has established links between IT workers and ongoing malicious campaigns by North Korean threat actors.

Threat Analysis

PurpleBravo

The Contagious Interview campaign, first documented in November 2023, targeted software developers primarily in the cryptocurrency space and was attributed to North Korea. The campaign used the JavaScript infostealer BeaverTail, the cross-platform Python backdoor InvisibleFerret, and most recently OtterCookie, a new backdoor identified in December 2024. The group responsible for this activity is known as CL-STA-0240, Famous Chollima, and Tenacious Pungsan in open sources. Insikt Group has given this cluster of activity the designation PurpleBravo (formerly TAG-120).

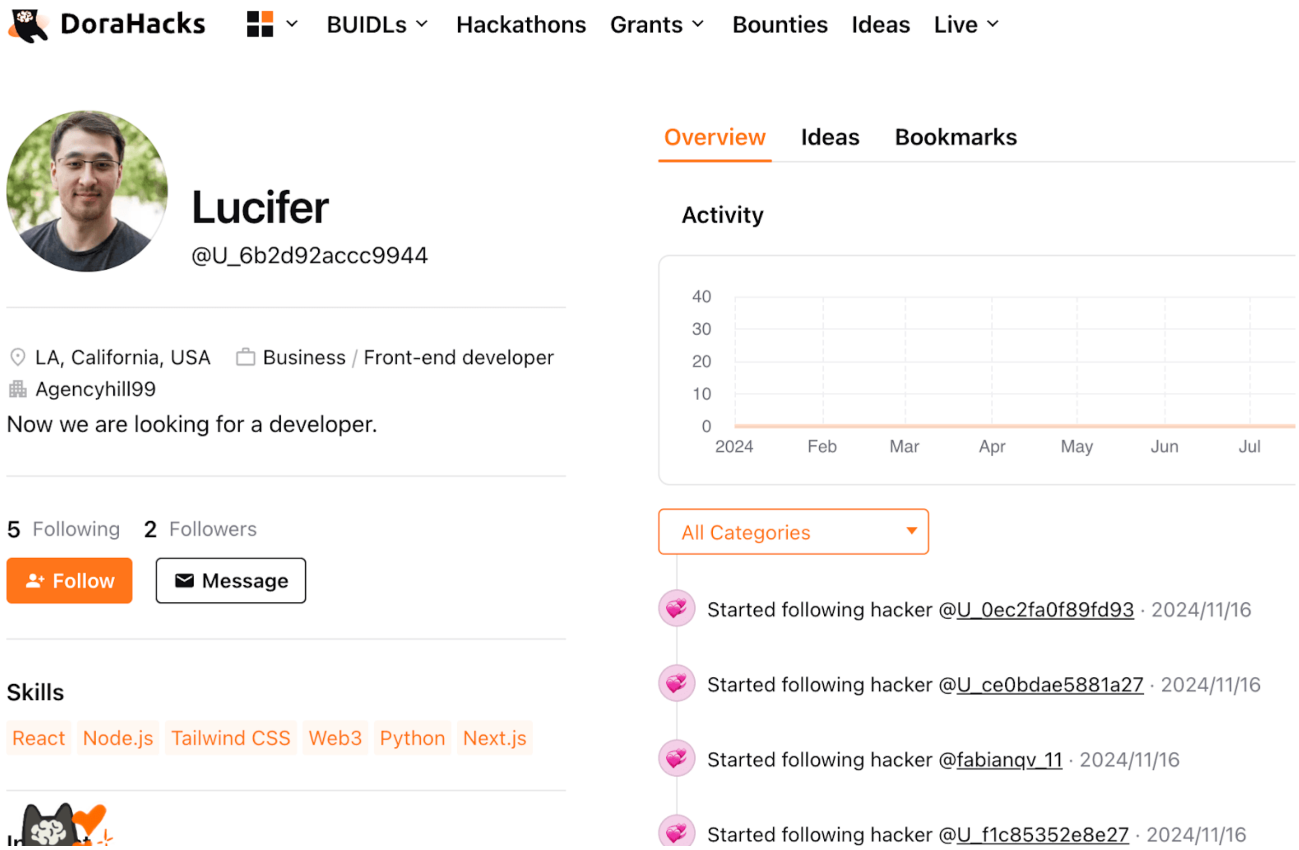
PurpleBravo's Fraudulent Profiles

On December 3, 2024, a developer posted a blog about their experience with a suspected PurpleBravo operator. An individual claiming to be a recruiter contacted them about a job offer and then followed up with an interview. During the interview, the interviewer asked the developer to download a coding challenge from a repository. The developer realized there was a malicious function in the file and ended the interview. While the developer does not attribute the malware or actor, Insikt Group assesses with high confidence the file is a BeaverTail infostealer.

The interviewer used a LinkedIn account with the name Javier Fiesco, who describes themself as the CTO of AgencyHill99. Further investigation into Javier Fiesco uncovered an individual with the same name available for work on remote3, a Web3 development job board. The website *agencyhill99[.]com* was registered on Hostinger on September 13, 2024. As of early February 2025, this website no longer resolved, but it previously displayed a Hostinger landing page. Research into AgencyHill99 uncovered a job posting seeking a developer with blockchain knowledge on *levels[.]fyi*, with the following contact info:

- Contact us: *alexander@agencyhill99[.]com*
- Recruiter: *vision.founder1004@gmail[.]com*

Pivoting on the text in the job description returned two private job postings on Upwork (1, 2). Additionally, a profile with the name of Lucifer, and what appears to be an AI-generated headshot, who works for AgencyHill99 was observed on the website DoraHacks, which is a hackathon, bounty, and grant organization. The profile on DoraHacks states that AgencyHill99 is looking to hire a developer. Insikt Group also discovered a company with the name Agencyhill99 on the website Intch, a part-time and remote job platform. The company posted a “Part-Time IT Developer Opportunity” by an individual with the name Newton Curtis, who is a recruiter at AgencyHill99.



Lucifer
@U_6b2d92accc9944

LA, California, USA
Business / Front-end developer
Agencyhill99
Now we are looking for a developer.

5 Following 2 Followers

Skills
React Node.js Tailwind CSS Web3 Python Next.js

Activity

Started following hacker @U_0ec2fa0f89fd93 · 2024/11/16

Started following hacker @U_ce0bdae5881a27 · 2024/11/16

Started following hacker @fabianqv_11 · 2024/11/16

Started following hacker @U_f1c85352e8e27 · 2024/11/16

Figure 1*: PurpleBravo operator’s account on DoraHacks (Source: DoraHacks)*

Insikt Group found several posts in Telegram channels from individuals with *@agencyhill99[.]com* email addresses advertising jobs. Below is a summary of the posts:

- On September 16, 2024, an account with the username Dale_V and email address *ayat@agencyhill99[.]com* posted in the Telegram channel “freelancerclients” that they were looking to hire a developer.
- On September 26, 2024, an account with the username jaxtonhol and email address *ysai@agencyhill99[.]com* posted in the Telegram channel “indeedemploijobeur” that they were looking to hire a developer. On the same day, the account Dale_V using the email *ysai@agencyhill99[.]com* posted in the Telegram channel “cryptolux_b” that they were looking to hire a blockchain developer. They posted the same message in the “itkita”, “andexzuxiaomichat”, and “usvacancy” channels. On September 27, 2024, Dale_V posted the same message in the “crypto_brazil” and “cryptolux_br” channels.
- On October 2, 2024, Dale_V posted the same message with a new email address, *sam@agencyhill99[.]com*, in the “fortifiedx_chat”, “family_indonesia_uae_ph”, “cryptolux_br”, and “freelancerclients” channels.

- On October 3, 2024, a user in an Indonesian-language Telegram channel posted a screenshot of an email message they received from PurpleBravo operators.
- On October 9, 2024, Dale_V posted job advertisements in the “andexzuxiaomichat”, “family_indonesia_uae_ph”, “cryptolux_br”, “crypto_brazil”, and “freelancerclients” channels.
- On October 22, 2024, Dale_V posted in the Telegram channel “hiringofm” seeking individuals to help maintain a game called Destiny War, and added the X link, *hxxps://twitter[.]com/destinywarnft*. It is unclear if the actor controls this X account or game.
- On November 13, 2024, the Telegram user jaxtonhol posted in the Telegram channel “near_jobs” seeking blockchain engineers. The same user posted again on December 7, 2024, in the same channel with the email address *ysai@agencyhill99[.]com*.
- On November 30, 2024, a Telegram user posted asking if a job offer on LinkedIn from the account mentioned above, Javier Feisco associated with Agencyhill99, was legitimate and shared a screenshot of the message.

GitHub Repository

Insikt Group discovered a GitHub repository named agencyhill99 with the email address *admin@agencyhill99[.]com*. A GitHub user, dev-astro-star, made several commits to the repository between October 9 and 19, 2024. Based on the commits, it appears the website used Firebase, a Google backend service for web applications. The user added a button to download a file at the Google Drive link *https://drive.google[.]com/uc?id=166zcmpqj-C7NPltm4iwRolz8XuxqZIXt*, which is no longer accessible. The email address *admin@agencyhill99[.]com* was also added to the repository, along with the Telegram channel *hxxps://t[.]me/+2AurfGZWxZo0MDgx*, which is also no longer live. The user also added a download link to *hxxp://65.108.20[.]73/BattleTank[.]exe*, which is no longer live and was later updated to *hxxp://65.108.20[.]73[:]3000/BattleTank[.]exe*. Port 3000 was open from October 20, 2024, to November 22, 2024, on *65.108.20[.]73*. The link was then updated to *hxxp://locahost[:]3000/BattleTank[.]rar*.

PurpleBravo Malware and Infrastructure

PurpleBravo uses the malware families BeaverTail, InvisibleFerret, and OtterCookie. BeaverTail is a malware family initially distributed via NPM packages as a JavaScript payload and later as executables and downloaders targeting Windows and macOS environments. BeaverTail also acts as an infostealer, gathering cryptocurrency wallet and browser information. InvisibleFerret is a collection of post-compromise payloads that collectively act as a backdoor in victim environments. InvisibleFerret introduces additional malicious payloads into victim environments, performs information stealing and fingerprinting actions within the victim environment, and leverages legitimate protocols and software for C2 communications. Like InvisibleFerret, OtterCookie is a post-compromise malware family used as a backdoor, which establishes C2 connectivity via Socket[.]IO, receives and executes shell commands from C2 servers, and exfiltrates sensitive victim data.

Insikt Group analyzed BeaverTail, InvisibleFerret, and OtterCookie malware samples (See **Appendix B** for related file hashes). The BeaverTail samples were identified as PE variants targeting Windows environments. These samples included URLs linked to *freeconference[.]com*, a legitimate conferencing website, which aligns with Unit42's findings of Contagious Interview payloads posing as FreeConference executables. The OtterCookie samples were two separate versions of the malware family; however, static analysis of these samples included strings that demonstrated both samples' ability to gather and send system fingerprinting information to attacker C2 servers, including strings that indicated OtterCookie is capable of identifying cryptocurrency assets and sensitive information found in specific file types by using regex patterns, including executables, photos, and config and env files, among others.

The InvisibleFerret samples analyzed were Python scripts with the following functionalities:

- Determining victim device location via local IP address lookup
- Fingerprinting device details (user and hostname)
- Connecting to a Base64-encoded C2 address via HTTP POST requests
- Performing local directory discovery using hard-coded strings
- Creating a reverse shell for SSH session management and data exfiltration
- Copying clipboard data, keylogging, and tracking mouse movements.

Previous samples of InvisibleFerret were analyzed by Zscaler, which described a two-part infection chain in which the initial reconnaissance took place over HTTP traffic and FTP was used for data exfiltration, as shown in **Figure 2**.

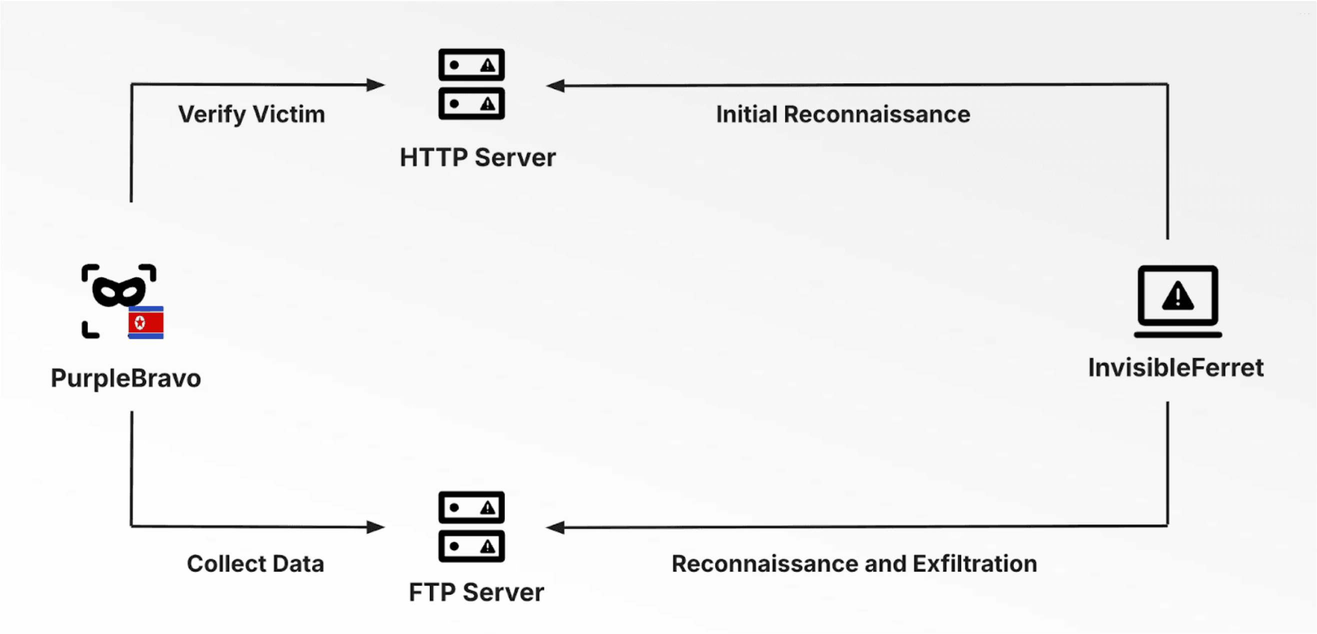


***Figure 2**: InvisibleFerret Infection chain (Source: Recorded Future and Zscaler)*

Insikt Group identified 21 PurpleBravo servers between August 2024 and February 2025 (see **Appendix B** for the complete list). The majority of servers use Tier[.]Net hosting, with Majestic Hosting, Stark Industries, Leaseweb Singapore, and Kaopu Cloud HK also being used in this campaign. Insikt Group has previously observed other North Korean threat groups favor many of these hosting providers. In addition to the C2 servers, using Recorded Future Network Intelligence, Insikt Group observed at least seven suspected victims between September 2024 and February 13, 2025. The victims are located in at least six countries, including the United Arab Emirates, Costa Rica, India, Vietnam, Türkiye, and South Korea. Open-source research identified Astrill VPN as a favored service by North Korean IT workers, with evidence that they use the service with remote administration tools. Insikt Group also observed network traffic between known Astrill VPN endpoints and PurpleBravo servers, corroborating this connection.

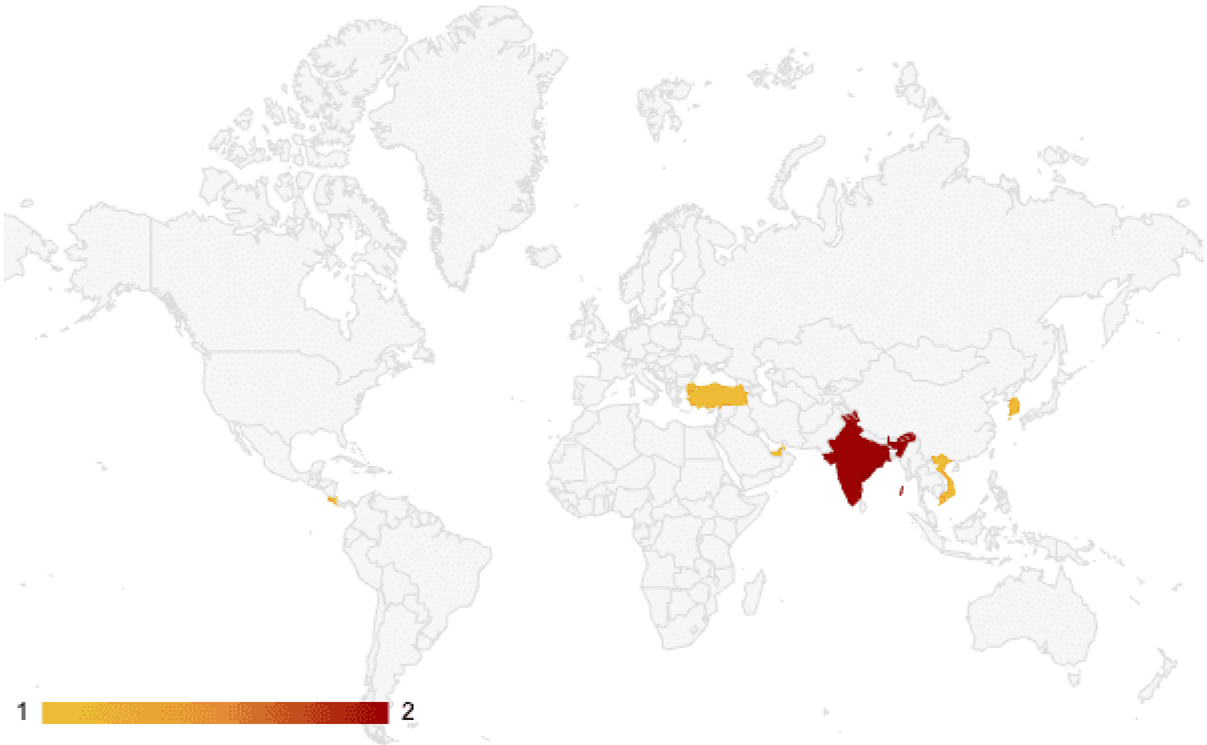


Figure 3*: Location of PurpleBravo victims (Source: Recorded Future)*

At least three victims in the cryptocurrency space were identified in the findings summarized below:

- On October 3, 2024, Insikt Group observed likely reconnaissance traffic between a BeaverTail C2 and a market-making company in the cryptocurrency space based in the United Arab Emirates. Shortly after the reconnaissance traffic, we observed likely exfiltration FTP traffic between the same IP addresses.
- On October 15, 2024, Insikt Group observed likely reconnaissance traffic between a BeaverTail C2 and a gambling company that offers online games and sells slot machines in the cryptocurrency space. The company is registered in Costa Rica. Reconnaissance traffic followed by FTP exfiltration traffic was observed between the C2 and the company's infrastructure on November 25 and 26, 2024.
- On October 2, 2024, Insikt Group observed potential FTP exfiltration traffic between a BeaverTail C2 and a software development company based in India that builds blockchain, AI, and mobile, among other applications.

To read the entire analysis, click here to download the report as a PDF.