Research

People, Process, Personas: Nisos Exposes the Human Risk in DPRK Employment Fraud Schemes

June 2026

Dear Reader -

Nisos has been helping our clients uncover fraudulent North Korean remote workers in their employee ranks for over four years, so imagine our surprise in the summer of 2025 when one of these scammers applied for a role with us!

A lot has been written about the North Korean regime and the cyber lengths they go to in order to evade sanctions and fund their government with the illicit gains of ransomware, cryptofraud, and payroll laundering. We have benefited from the great research published by our peers in the cyber intelligence community, our partners in law enforcement, and even other companies victimized by this scheme. It truly is a community committed to keeping our economy safe.

With this research paper, we build on our existing body of work by shedding light on some of the unique human dynamics we uncovered with the unwitting help of our candidate. Once we confirmed our suspicions that Joe was not who he purported to be, we consulted with law enforcement and decided to run Joe as an operation to see what we could learn. What followed from July through October of 2025 was a fascinating look inside the day to day of our source (who spent a LOT of time applying for other jobs) as well as shining a light into the organization to which he belonged; their motivations, metrics, and mannerisms; their roles and interplay; the raft of US companies they had victimized; and even the failures that led to their ability to improve.

As we were notifying victim companies, and working with the FBI, even more anecdotes came out about how companies are trying to address this issue. One lesson we learned from the pandemic was that remote work is here to stay - it's one of the best ways for companies to get access to a global workforce of scarce talent. It's also one of the new favorite ways for North Korea to get access to funds that move quickly to non-State currencies and evade sanctions and roadblocks to funding the regime. So no matter your size, from a small community based app developer to a Fortune 50 (both ends of this spectrum fell victim to the cell we encountered), you are being targeted for the $50-200k/year your roles may pay.

We are sharing the observations and learnings, the lexicon, the dynamics, and the human stories from the cell we encountered in the hopes that Security teams, Hiring teams, Operations and Risk Teams, and others can get an appreciation for the sheer scale of what we are up against. Train your HR and hiring managers on what to look for, build detection into your hiring processes and tools, and look for ways to weed out candidates earlier in the process to avoid a flooded pipeline and to find that right candidate for the role.

Got a story to share or indicators that can help the community? We'd love to hear from you at info@nisos.com.

Thanks for having a read,
Ryan LaSalle
CEO, Nisos

Table of Contents

Executive Summary

Nisos assesses with high confidence that a Democratic People's Republic of Korea (DPRK) state-sponsored cell conducted industrial-scale employment fraud against US companies, submitting more than 170,000 job applications that yielded 76 employment offers across 22 operatives between December 2024 and September 2025, utilizing appropriated identities, AI-driven interview assistance, and US-based facilitators to infiltrate UScompanies primarily in the technology sector. The cell—which Nisos identified and has tracked since mid-2025—possesses the same technical indicators, operational patterns, and tactics that align with documented North Korean employment fraud campaigns designed to generate income for the regime.[1]

- Some operatives likely operated from Taraksan, North Korea and other international locations.
- Technical analysis revealed tactics, techniques, and procedures (TTPs) consistent with known DPRK tactics, including use of Astrill VPN, PiKVM devices for remote access, and cryptocurrency payments.
- The cell focused on revenue generation through actual employment rather than traditional cybercrime, providing high-confidence attribution to DPRK's systemic campaign to generate funds through fraudulent IT employment.

Overview

The cell maintained a hierarchical structure with an administrator, administrative manager, team leads, and operatives who managed one to four personas each. Each operative was responsible for completing the job duties of their respective personas, either through their own efforts or through outsourcing to a third party they referred to as a "bidder."

These roles are further defined in Appendix A.

- The cell employed facilitators, known internally as "natives," who managed US-based laptop farms that served as controlled technical entry points for operatives to remotely conduct fraudulent activities.
- The cell used a Discord server for internal communication among operatives and a Vercel dashboard (cloud-hosted web management tool) to track the cell's performance.
- The DPRK operative cell maintained strict operational security to conceal identities, limit discoverability, and segment communications.

Pre-Employment

[1] https://www.ic3.gov/PSA/2025/PSA250723-4

Operatives built personas using appropriated or purchased information associated with real people, but usually with new email and LinkedIn accounts the operatives controlled, to aid in passing initial background checks during the onboarding process.

- Operatives conducted some vetting of the identity information, such as checking the validity of the social security number (SSN) on www.ssn-verify[.]com, verifying whether the identity is registered for Selective Service on www.sss[.]gov/verify, and searching the individual in TruthFinder.
- Operatives purchased identity packages and accounts from bespoke brokers (i.e. - one on Telegram) to build personas, paying between $20 and $200 per item.
- Operatives obtained likely Department of Motor Vehicles (DMV)-issued but fraudulently obtained driver's licenses through state DMV websites, routed physical documents through US-based "natives," then digitally manipulated the photographs to match operatives or natives conducting interview/drug tests, verifying accuracy using Dynamsoft barcode readers.
- Operatives created a closed-loop reference validation system where operatives provided mutual employment verifications and reference checks for each other through their established personas.
- Operatives recruited US-based individuals, or natives, to serve as front-facing employees and to manage laptop operations. Operatives paid natives via ERC20 cryptocurrency.
- Operatives established a website for a fictitious company to potentially verify false employment history when needed, though we did not identify any active use of this fictitious company during our investigation.

Application, Interview, and Onboarding

Analysis of DPRK activity across application, interview, and onboarding phases highlight how the cell executes industrial-scale employment fraud with discipline, precision, and coordinated tradecraft. Investigation origins are detailed in Appendix B.

- In the application phase, team leads set priorities, enforce exclusions, and push volume through resume generators and shared dashboards, driving thousands of tailored submissions across mainstream hiring platforms.
- The interview phase shows reliance on AI-enabled coaching, accent training, and remote access overlays that allow operatives to inject technical responses while operatives or "natives" support the personas' presence within the United States.
- The onboarding phase leverages forged documentation, metadata scrubbing, and employer-issued hardware to establish persistence and integrate accounts into the broader operation.

On the Job

Upon employment, DPRK operatives executed work through at least three distinct models: A native as front-facing employee with the operative performing work (likely 50/50 compensation split); an operative as both front-facing employee and worker; and an operative as front-facing employee with a bidder who performs work.

DPRK Attribution Analysis

The fraudulent employment scheme Nisos detected employs tactics consistent with documented North Korean activities, including appropriating legitimate biographical information from US citizens to pass pre-employment verification, systemically requesting hardware shipment to addresses different from personas' listed residences, and utilizing certain personas to serve as employment references and emergency contacts for multiple candidates in the pre-hire and post-offer stages.

- Nisos assesses with moderate confidence that at least some operatives were physically co-located in Taraksan, North Korea, while others operated from multiple locations outside the US. Discord direct messages revealed at least three operatives explicitly referencing the location of Tarak in their discussions, likely a reference to Taraksan, North Korea. Taraksan, also known as Mount Tarak, which has a sparse population density. Discord messages also showed a reliance on Google Meet, Zoom, and Microsoft Teams for communication and infrastructure testing, suggesting a dispersed operational structure rather than full co-location.
- Technical analysis of the operative who applied to Nisos revealed TTPs consistent with DPRK IT workers: use of Astrill VPN (IP addresses 167.88.61.250 and 167.88.61.117); deployment of PiKVM devices for undetectable remote access to corporate laptops; and use of Tailscale mesh VPN to create encrypted networks across distributed laptop farms.
- The cell's operational security (OPSEC) practices—including the use of AI-generated resumes that mirror job descriptions and VoIP phone numbers from services like Hushed—align with FBI and Treasury warnings about DPRK IT workers.[2] [3]
- The cell's structure reveals a high level of coordination: a formal hierarchy with administrators, managers, and team leads overseeing up to 22 operatives who submitted at least 166,893 job applications in roughly 9 months, resulting in at least 76 employment offers.
- The cell focused on revenue generation through actual employment rather than traditional cybercrime, demonstrated avoidance of cybersecurity roles that might expose their activities, and used cryptocurrency payments for payments to and from the group.

Operational Overview

The DPRK employment fraud cell demonstrated organizational capabilities through three operational components that enabled systematic infiltration of US companies: hierarchical structure, coordinated communication systems, and large-volume execution. The cell maintained a hierarchical structure with

[2] https://www.ic3[.]gov/PSA/2025/PSA250723-4
[3] https://ofac.treasury[.]gov/media/923126/download?inline

specific roles and responsibilities. Internal coordination occurred through Discord and a custom Vercel dashboard, allowing real-time communication and performance tracking across operatives. The cell's activities generated measurable results at industrial scale with up to 22 operatives submitting at least 166,893 applications that yielded 76 confirmed employment offers by US companies during the observed operational period.

Framework of the Cell

The DPRK employment fraud cell operated with a hierarchy and defined responsibilities. An administrator oversaw all activities and likely received a portion of the entire cell's revenue. The cell divided operatives into three to four groups led by team leads; however, the whole cell shared certain administrative resources, such as sharing paid accounts or coordinating identity management resources through the administrative manager.

Each DPRK operative maintained between one and four personas, tied to employment seeking. Operatives managed these personas throughout the entire employment lifecycle, from application through job performance, ensuring each identity remained consistent and believable to potential employers.

When companies hired operatives' personas, operatives connected the personas directly to employer-issued laptops located in laptop farms that "natives" established and maintained. These laptop farms served as the physical infrastructure that enabled operatives to appear as if they were working from legitimate US-based locations.

When operatives secured multiple jobs simultaneously, they managed each active persona across separate devices within the laptop farm. This device segregation prevented operational overlap between different employer accounts and maintained the illusion that each persona represented a distinct individual working for only one company.

Each operative, regardless of position, was responsible for completing the job duties of their respective personas. The operatives likely had discretion to complete the job themselves, which potentially enabled them to retain the most money, or outsource the responsibilities to a bidder who reported directly to the operative who contracted them, which would enable the operative to scale employment efforts.

Operatives relied on "natives" to anchor personas inside US-based companies through their management of laptop farms. The cell provided "natives" with laptops that served as controlled technical entry points to the United States. In-country infrastructure enabled operatives to appear as though they were located in the United States while conducting fraudulent activities through remote access. "Natives" sometimes acted as front-facing employees by attending interviews remotely and completing onboarding requirements such as drug tests. "Natives" also received, configured, and operated employer-issued laptops for remote DPRK use. "Natives" assisted operatives in creating bank accounts in the persona's name and in transferring employers' salaries to the operatives.

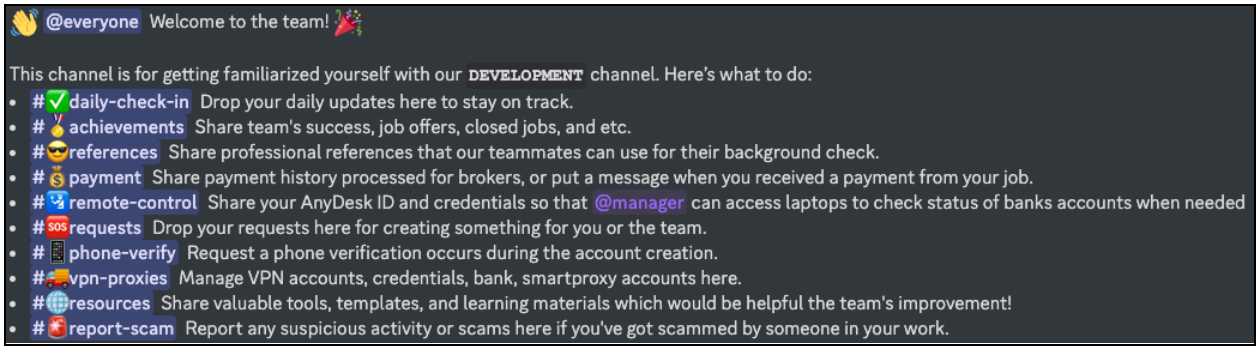
Individual operatives recorded metrics such as applications submitted, interviews conducted, and offers received. Automations enabled the cell to easily track performance data in the Vercel-hosted

productivity dashboard. The entire cell maintained visibility of each others' performance data and they often shared and implemented lessons learned from their successes and failures.

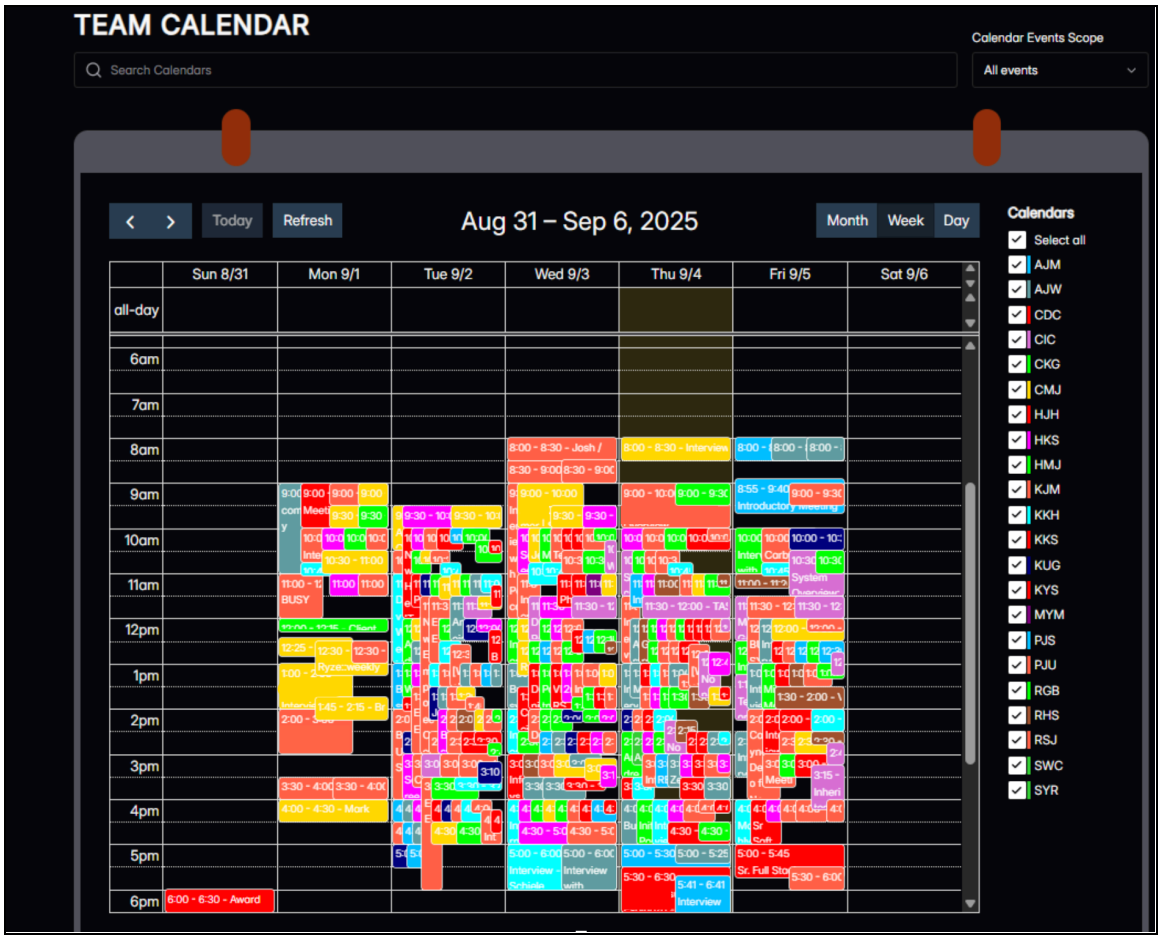
Internal Coordination

Starting in late February 2025, the cell began using Discord as a platform to communicate team updates and highlights. Every member of the Discord server was a DPRK operative, including a designated administrator, two managers, and three team leads. The administrators created channels for all members to post daily interview statistics, alert one another about reference checks, provide updates or requests for "natives," and to report scams.

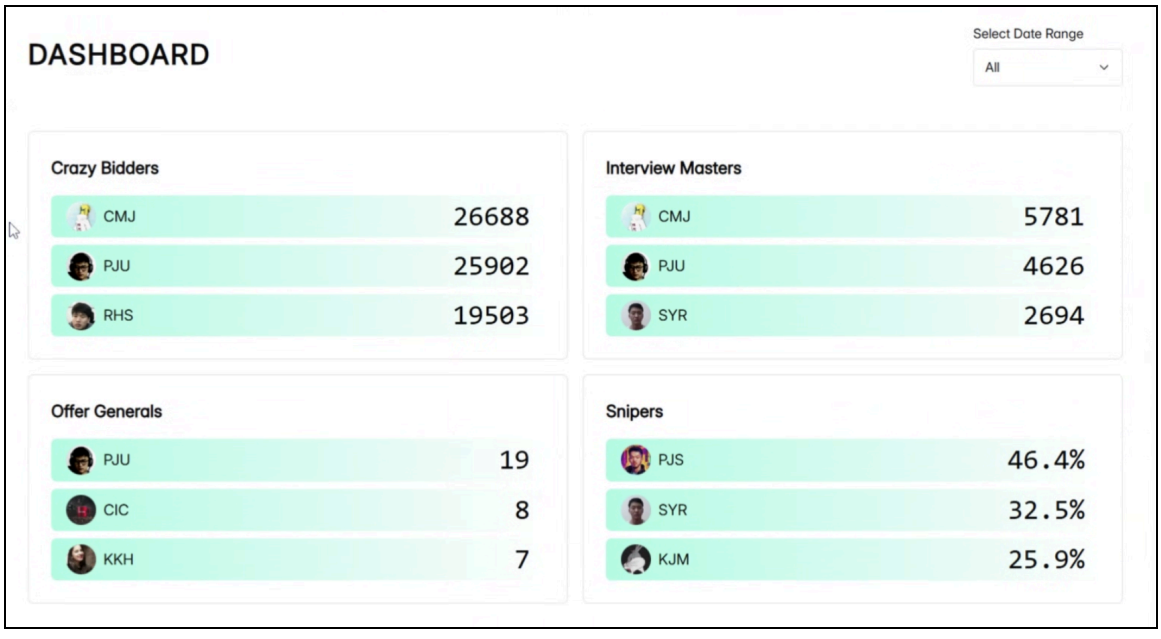
Starting in late May 2025, the cell used a new dashboard on vercel[.]app, which served as a separate repository for information, although they still sent updates to the Discord server's Jobs page channel. The Vercel dashboard provided more statistical information of the cell's performance and tracked the number of applications, interviews, and jobs for each operative as well as all of the personas' calendars in a single view. The operatives likely used the aggregated calendar to identify times when an operative required assistance from others to manage overlapping appointments, which included meetings for current employers and interviews for new jobs.



Graphic 1: Overview of channels in the Discord server and their stated purposes.



Graphic 2: Team calendar view from the Vercel dashboard.



Graphic 3: Cell leaderboard on the Vercel dashboard, tracking number of job applications, interviews, offers, and percentage of interviews from applications.

Operational Security (OPSEC)

The DPRK operative cell maintained strict operational security to conceal identities, limit discoverability, and segment communications. Operatives discussed the need to avoid posting sensitive messages in public channels and adhered to the following OPSEC measures:

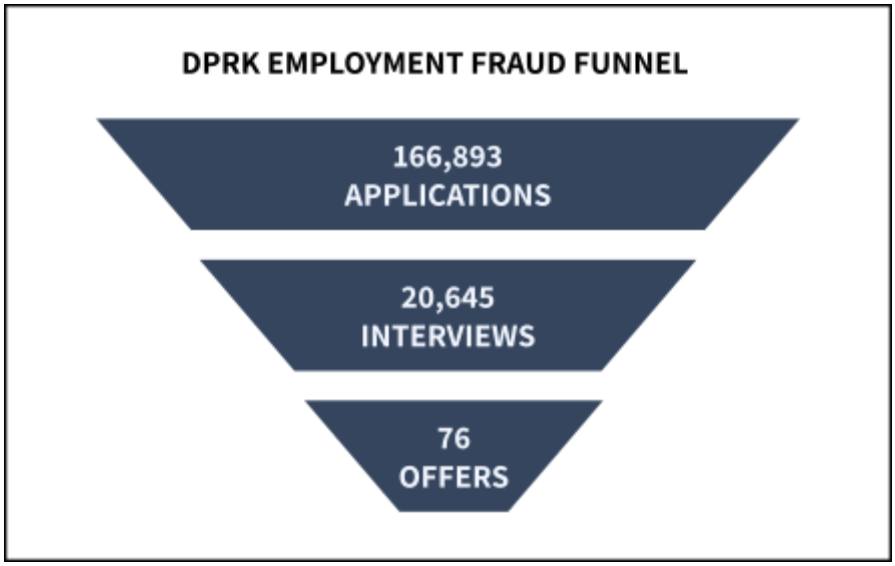
- Operatives used 3-letter initials instead of full names in Discord and the productivity dashboard to obscure real-world identities.
- Operatives deliberately avoided registering public domains or linking identifiable web properties to their Vercel dashboard to prevent discovery.
- Operatives restricted Discord server visibility and relied on invite-only channels so the server remained hard to find.
- Operatives compartmented communications with those outside the cell. For example, operatives used Discord for internal coordination, while they communicated with brokers and "natives" over Telegram and WhatsApp, and occasional Discord direct messages connected operatives with potential "natives" and bidders.
- Operatives used avatars for Discord profile images to obfuscate their real-world identities and prevent attribution.
- Operatives communicated exclusively in English, avoiding their native language.

Breakdown of Targeted Industries and Positions

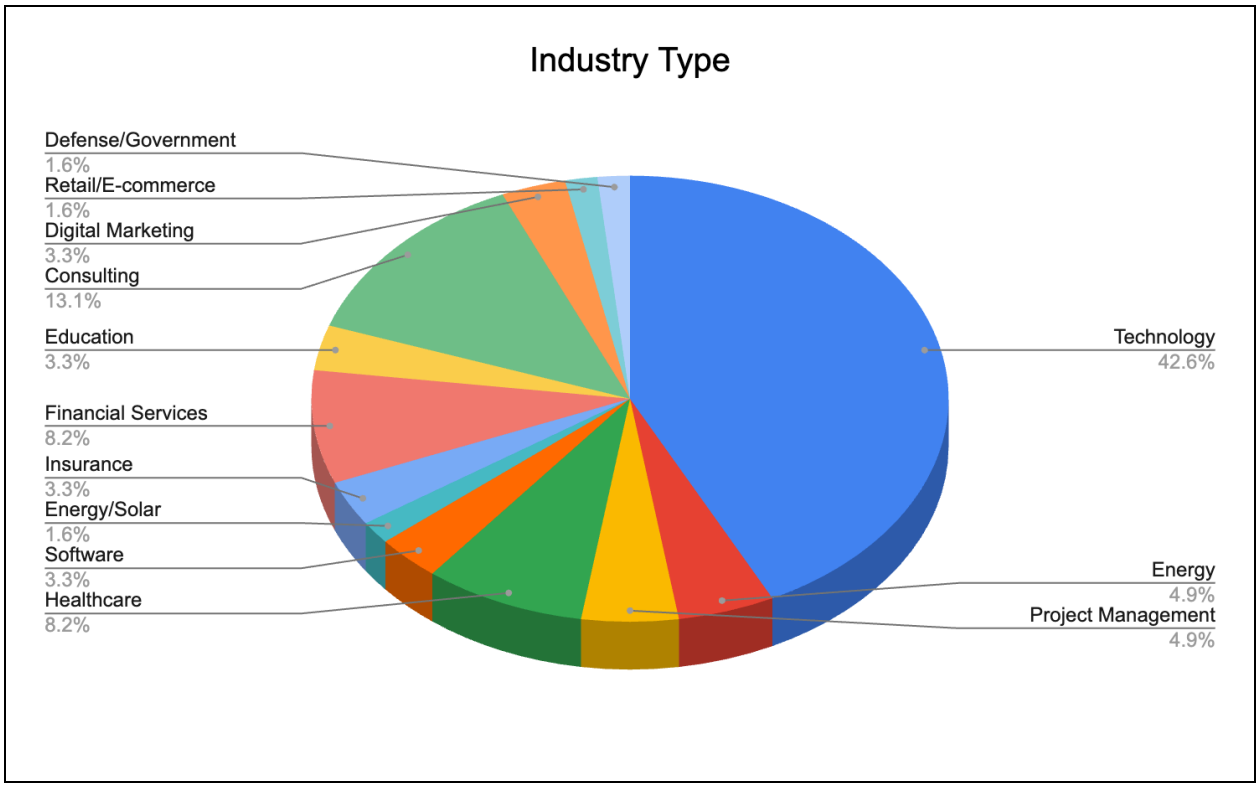
The DPRK employment fraud cell operated at scale, with 22 operatives submitting at least 166,893 applications that generated at least 21,645 interviews since mid April 2025. The cell reported at least 76 confirmed job offers between December 2024 and September 2025. This equates to a 13% interview rate but only a 0.35% success rate from application to offer.

Technology companies comprised 42.6% of all employers that offered the cell positions, followed by consulting firms (13.1%), healthcare organizations (8.2%), and financial services (8.2%). This heavy technology sector focus reflect the technical capabilities of DPRK operatives, the need for technical talent, and the prevalence of remote work arrangements within this particular sector. Defense and government positions represented only 1.6% of targets despite potentially offering valuable access, likely indicating that operatives deliberately avoided sectors with enhanced security screening that could expose their fraudulent identities or their operation.

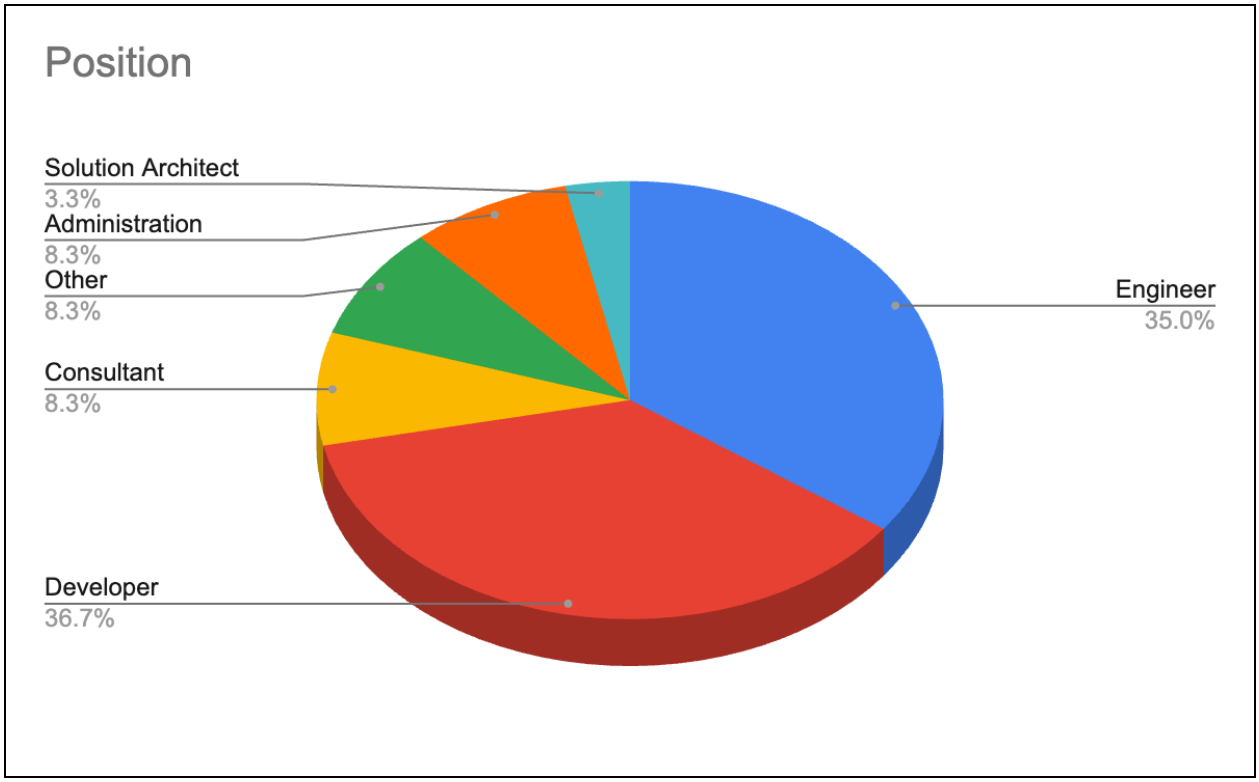
The cell very likely targeted specific job roles for employment, with developers (36.7%) and engineers (35%) comprising 71.7% of all pursued roles. These positions offer ideal characteristics for DPRK operations: high average salaries, established remote work culture, technical interview processes that can be gamed with AI assistance, and limited requirements for security clearances or in-person collaboration. The DPRK cell pursued positions ranging from entry-level positions at $55,000 to senior roles up to $230,000.



Graphic 4: DPRK employment fraud cell displaying the conversion rates through the employment fraud process.



Graphic 5: The cell's job offers by employer industry.



Graphic 6: The cell's job offers by position title.

Pre-Employment

The DPRK employment fraud cell's pre-employment operations constitute a sophisticated identity laundering system that enables industrial-scale infiltration of US companies. Operatives execute at least three independent operational phases to backstop a persona before initiating job applications.

- First, operatives acquire appropriated US identities through Telegram brokers that include government IDs, Social Security numbers, and biometric data.
- Second, the cell coordinates mutual employment verifications, effectively creating a closed-loop validation system.
- Third, the cell recruits US-based natives through platforms including Reddit, Chaturbate, and Discord, offering 50% salary splits and $300 drug test payments to secure physical presence requirements.
- Additionally, operatives established a website for a fictitious company, possibly to provide employment history verification for the cell, although we did not observe operatives using this company during our investigation.

Persona Creation

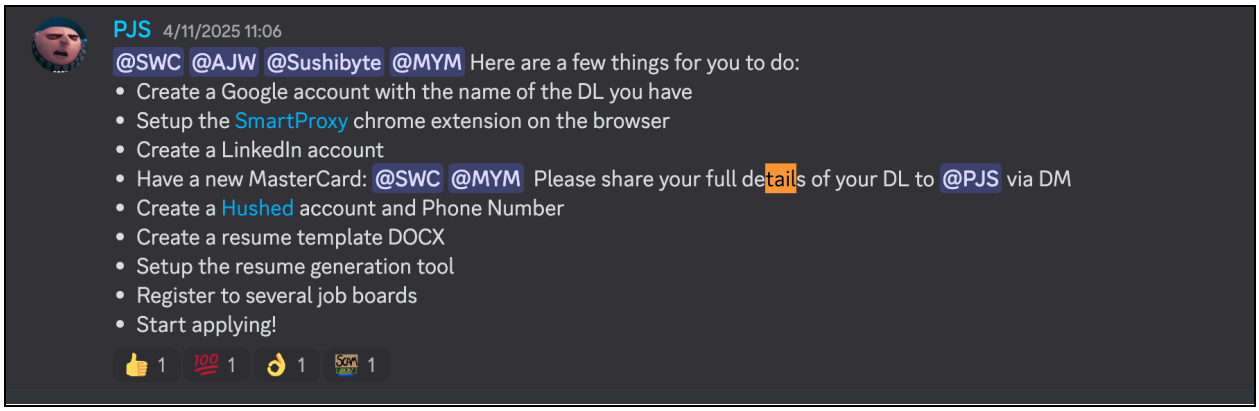
A crucial part of the scheme is the operatives' use of US-based personas to apply to and obtain positions. Operatives build personas using appropriated or purchased information associated with real people to apply for and obtain employment. Each operative is likely responsible for securing their own personas for use in the scheme. Operatives construct these false identities specifically to pass initial background checks during the onboarding process.

Operatives obtain identity information such as a name, address, date of birth, and drivers license number and/or SSN, likely through a broker, purchased on the dark web, or in data breaches. Operatives typically create new email addresses and LinkedIn accounts under the appropriated identities to maintain direct control over persona communications.

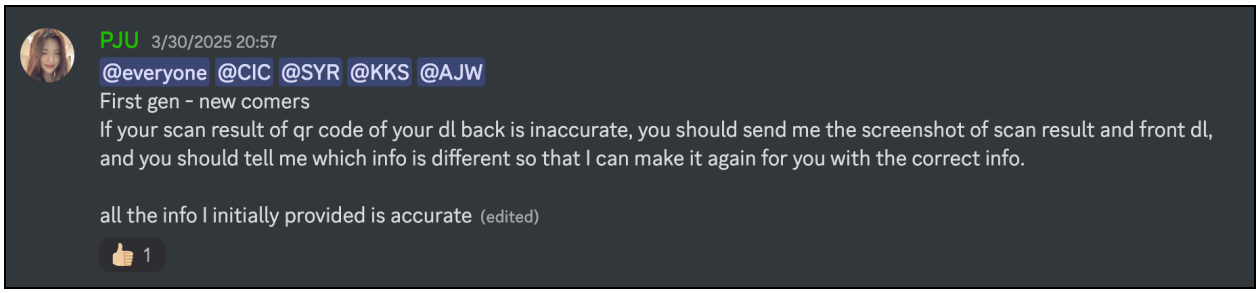
Operatives conduct some vetting of the identity information, such as checking the validity of the SSN on www.ssn-verify[.]com, verifying whether the identity is registered for Selective Service on www.sss[.]gov/verify, and searching the individual in TruthFinder. From this point, the operative either works with a designated operative to either create fraudulent documents for backstopping the persona or purchasing them from a broker.

- One such broker, Telegram user @accountproviderforyou, claimed to offer identity packages, ranging from a real US ID card, SSN, and selfie for $120, fraudulent ID card, bank statements for $50-70, payment accounts such as Mastercard, Payoneer, Paypal, and Wise for $50-300, and Discord accounts for less than $20 (accounts with more longevity cost more). A likely team leader noted that this broker provided most of the services the cell needed. Separately, operatives referenced purchasing a LinkedIn profile for $75 and another unspecified profile for $200, although we did not identify where the accounts were being offered for sale.

- Additionally, operatives have manipulated likely legitimate driver's licenses for their use in this scheme. Operatives have visited state DMV websites, likely in an effort to obtain reprints of legitimate licenses for the appropriated identities. The real driver's license likely is sent to a native, who sends a photograph of it to their handler, who then uses digital tools to manipulate the image for further use, including changing the photograph to match either the operative who is interviewing for a job or the native who is taking a drug test for a persona. Operatives verify that persona drivers licenses have been created with the correct data for their persona by scanning the license barcode using Dynamsoft's reader to extract all the data.[4]
- Once the operative has established the persona's identity, they then created a Google account in the name of the persona, set up the SmartProxy extension on their Chrome browser, created a LinkedIn account in the name of the persona, created a new credit card, created a Hushed account and phone number, created a resume template, set up the resume generation tool, registered for several job boards, and started applying for jobs. The operatives then used Hushed to create temporary, disposable VOIP phone numbers that they had the ability to access from multiple devices.[5]



Graphic 7: Cell operatives instructions for full persona creation.



Graphic 8: Cell operative instructions for persona drivers license verification.

Closed-Loop Validation System For Employment References

The DPRK operatives' Discord server included a channel dedicated to employment references. The channel included a list of all available personas, including email addresses and phone numbers, which

[4] https://demo.dynamsoft[.]com/barcode-reader-js/driver-license
[5] https://hushed[.]com/features/

the cell could use for their employment references. Operatives then used other channels to deconflict responses for reference requests, and informed each other what role and employer each reference would need to represent, and sometimes provided sample text about what the reference should say about the persona, if contacted.

Recruitment of Natives

DPRK operatives in this cell recruited at least three United States-based individuals to serve as front-facing employees and to manage laptop operations. Operatives utilized Reddit, PeopleGPT, Chaturbate, Discord, and Telegram to find potential natives. In some cases, operatives specifically sought out people who expressed financial difficulties; in other cases operatives advertised opportunities for quick income or flexible remote work. Operatives sometimes direct messaged prospective natives on Discord for further engagement and vetting. However, operatives generally used WhatsApp and Telegram for continued coordination with natives.

Operatives vetted potential natives through multiple steps, including basic background checks, likely using truthfinder[.]com. The cell required prospects to hold government-issued ID cards on camera and to provide video verification of their home environment. In some cases, operatives offered to purchase laptops for prospective natives to establish new or alternative accounts in the native's name, allowing operatives to work under the native's identity if needed.

Once operatives gained employment, employers unknowingly shipped work laptops to the native's address under the operative's persona. Natives primarily ran the laptop farm; however, some attended interviews. In some cases, natives performed a portion of the employee duties for a 50/50 split of the employer's salary. In the instances where natives served as front-facing employees or performed job duties, operatives could actively monitor and coach them using transparent ChatGPT overlays, AnyDesk, and other remote access tools.

Some natives received compensation via ERC20 cryptocurrency. The cell paid natives weekly for standard tasks and on a per-task basis for specific activities, such as $300 for completing drug screenings. Operatives oversaw disbursement to maintain financial control and operational continuity.

Backstopping Companies

Additionally, DPRK operatives in this cell almost certainly established a website for a fictitious business, 710TECH LI, which claims to deliver innovative technology solutions that empower businesses to grow and succeed. The company claims to be located in Plano, Texas; however the address and phone number are associated with other entities, suggesting the entire company is fictitious, including the individuals listed on the website. The company website, which is created on the Vercel[.]app platform, lists three cell operative personas as their employees.[6] Cell operatives very likely created the website to backstop a fake previous employer for persona resumes, but we did not find evidence that the cell referenced 710TECH LI in any way on any LinkedIn account or resume we discovered in our investigation.

- Carlos Salcedo is listed as Chief Executive Officer

[6] https://www.tech710[.]com/

- Dominic Zambrano is listed as a Senior Software Engineer
- Jordan Rinehart is listed as a Project Manager

Graphic 9: Screenshot of Vercel[.]app website for DPRK fictitious created company to provide backstopping.

Application, Interview, and Onboarding

Analysis of DPRK activity across application, interview, and onboarding phases highlight how the cell executes industrial-scale employment fraud with discipline, precision, and coordinated tradecraft. These insights reflect only part of a broader scheme but demonstrate the methods the cell used to convert applications into employment. In the application phase, team leads set priorities, enforce exclusions, and push volume through resume generators and shared dashboards, driving thousands of tailored submissions across platforms. In the interview phase operatives relied on AI-enabled coaching, accent training, and remote access overlays that allowed operatives to inject technical responses while either operatives or natives maintained the personas' presence. In the onboarding phase, operatives leveraged forged documentations, metadata scrubbing, and employer-issued hardware to establish persistence and integrate accounts into the broader operation. Together, these phases reveal a structured system that blends automation, deception, and tradecraft, reflecting very likely state-level direction and resourcing.

Application

Team leads provided guidance on the target jobs, which are primarily remote full stack software engineer roles. Other keywords include:

- senior react
- senior .net
- data engineer
- senior angular
- senior next
- senior node
- senior python
- senior ruby

- power bi
- ab initio
- software developer, engineer, fullstack
- data engineer, scientist

Team leads specifically instructed operatives not to apply for positions titled cybersecurity, embedded engineer, architecture, manager, staff, principal, or VP. Each operative was responsible for applying to jobs, either by submitting applications themselves or by outsourcing the task to a bidder. They applied to multiple positions a day, and they appeared to independently decide which job search platforms or strategies to employ. One operative claimed to have applied to jobs on LinkedIn, Indeed, Google, Slack, ZipRecruiter, Monster, Dice, Otta, Discord, JsJobbs, YCombinator, Adzuna, Jora, and Jobot and reported the most success (not further defined) with JsJobbs, Slack, and Discord. A team leader also recommended applying during 4am-7am CST and 11am-1pm CST, purportedly to align with the time of a typical US workday.[7]

Operatives used a SwiftCV resume generator repository on GitHub to create unique resumes for each position for which they apply. The tool, which the user ran locally on their machine, allows the user to easily customize a resume based on selected text from the job posting, easily switch between different profiles tailored to individual browsers, exclude job postings that require security clearances, are on-site positions, or to which the user had previously applied. The resume generator is also connected to the aforementioned Vercel dashboard to track the number of applications.

Interview

DPRK operatives used technical support, AI tools, and accent training to maximize interview success while maintaining operational security. Natives sometimes attended interviews as the front-facing employee, while operatives provided technical answers and guidance as needed. Operatives and natives leveraged ChatGPT (sometimes with shared accounts) to rehearse answers, in an effort to make responses sound conversational and consistent with the adopted persona. Additionally, operatives performed accent testing and voice training through tools such as BoldVoice Accent Oracle and vocalimage[.]app, though the frequency of practice per interview is unknown. Cell operatives demonstrated persona awareness, using local weather details, university nicknames, and other localized knowledge to pass interviews and vetting checks.

Operatives focused interview preparation on rehearsing conversational answers rather than following structured scripts. The cell maintained application and interview quotas and required some operatives to apply to jobs at least twice daily, while requiring others to attend five interviews per day.

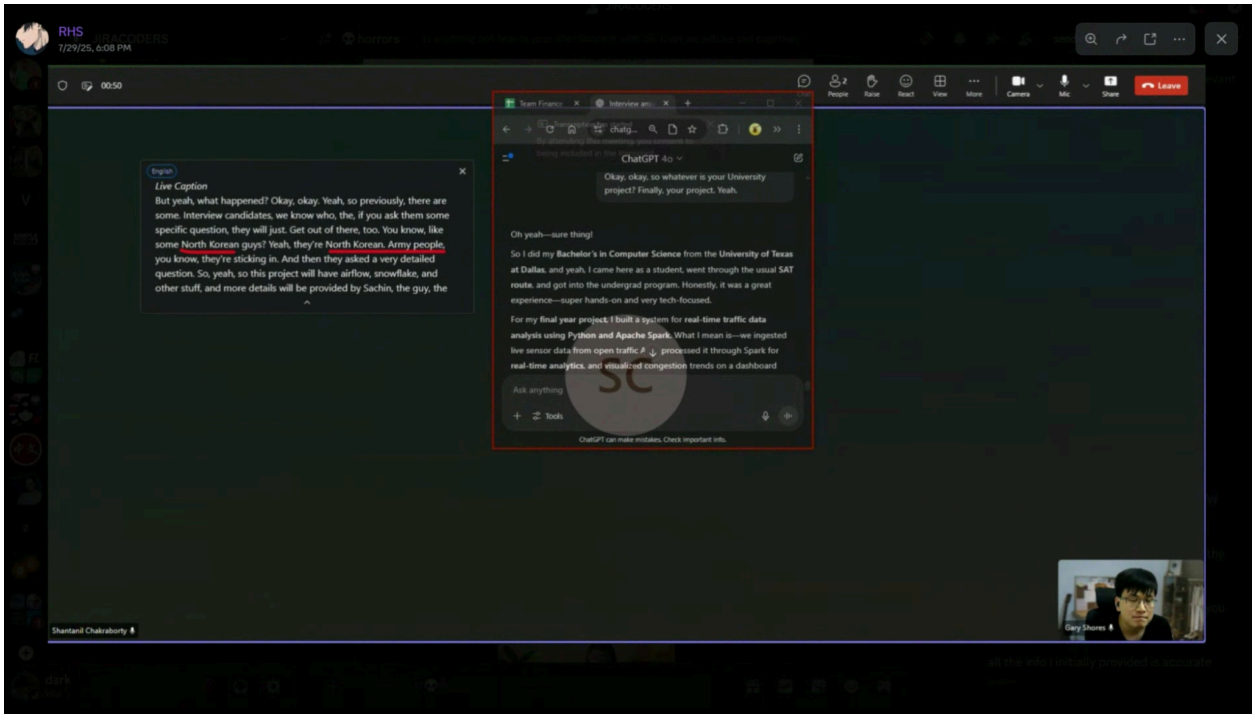
Operatives and natives employed VPNs, including Astrill and Tailscale, in an attempt to protect their operational security during interviews. However, this security measure backfired in at least one instance when the hiring organization detected the operative's VPN usage and ended the interview.

[7] These hours do not match US business schedules and the reason for these misaligned times is unknown.

AI-driven Interview Assistance

During interviews, DPRK operatives used two primary methods to blend AI assistance with human participation.

- **Method One: Native front-facing, operative supporting:** In some cases, the native attended the interview as the employee while the operative, connected via PiKVM to a cheap Windows laptop at a US laptop farm, provided technical answers. The operative ran ChatGPT locally to craft responses, then injected them into the native's laptop through the KVM session. The native's laptop generated the live audio, video, and captions, while the operative's local machine generated the ChatGPT content that displayed on the native's laptop. This setup increased the apparent authenticity of the interview, with the native handling general interaction and the operative supplying precise technical knowledge.
- **Method Two: Operative front-facing, ChatGPT assisting:** In other cases, the operative acted directly as the persona. Here, ChatGPT support occurred in two possible ways. One method involved another operative playing the supporting role, mirroring the process they used with natives by listening in, generating ChatGPT-crafted answers, and injecting them to the front-facing operative. In the other method, the operative used transparent ChatGPT windows overlaid on the video feed of the interviewer. In this configuration, ChatGPT live-listened through transcription features on the farm laptop, generated draft responses, and displayed them in real time on the operative's local machine. The operative then verbally delivered the AI-assisted answers reducing reliance on manual input while keeping eye contact consistent.



Graphic 10: Example of front-facing operative's screen while in an interview.

Onboarding

Operatives shared templates for creating fraudulent W-2 forms and paystubs, almost certainly to use as proof of previous employment as listed on their persona's resumes. Operatives used Adobe Photoshop to manipulate images in the templates; further, operatives instructed each other to use an online metadata remover on the file, suggesting the operatives' awareness of vulnerabilities from document metadata.

On the Job

DPRK operatives in this cell developed at least three distinct employment execution models that balance operational security, profit maximization, and scalability requirements. The three models we observed include the native as the front-facing employee with the DPRK operative performing job tasks, the operative as both the front-facing employee and performing job tasks, and the operative as the front-facing employee but outsourcing the job tasks to a bidder. These models present differing risk distributions among cell members, salary allocation structures, and the cell's capacity to manage multiple simultaneous employment roles. Bidders, natives, and operatives primarily communicated on Telegram and WhatsApp to coordinate and assign tasks. Operatives used tools including PiKVM, AnyDesk, Astrill VPN, shell services, Tailscale, and virtual machines to monitor natives, outsource to bidders, and maintain control of employment accounts. The cell logged successful employment offers into a shared dashboard for collective visibility, which allowed Nisos to observe such activity.[8] The

[8] Nisos attempted to contact every victim company that employed one of the DPRK operatives to facilitate protective measures.

DPRK operative acting as both the front-facing employee and performing the job tasks is likely the maximum profit method, while the operative acting as the front-facing employee but outsourcing the work to a bidder is likely their preferred method when job volume exceeds operative bandwidth.

1. Native as front-facing employee; operative performs work (50/50 split)
    a. The native completes onboarding tasks, which may include drug tests, setup of employer-issued computers, providing right-to-work documents and verification, and acting as the public-facing employee.
    b. The operative performs all technical work remotely almost certainly from outside the US.
    c. Profits are split evenly between the native and operative.
    d. Risk distribution: Shared between the native, who faces employer scrutiny, and the operative, who executes the work.
2. Operative as both front-facing employee and worker
    a. The native completes some of the onboarding tasks, which may include drug test and setup of employer-issued computer.
    b. The native remains involved for physical access to employer-issued devices in the US.
    c. The operative retains the majority of the salary and pays the native a modest administrative fee for maintaining the employer-issued computer and one-time fees for tasks such as a drug test.
    d. Risk distribution: Concentrated primarily on the operative, who carries full responsibility for the persona and work performance.
3. Operative as front-facing employee; bidder performs work
    a. The native completes some of the onboarding tasks, which may include drug test and setup of employer-issued computer.
    b. The operative secures employment under a persona, while a bidder almost certainly outside the US executes the technical tasks remotely. This cell's operatives discussed employing bidders from India, Kenya, and Nigeria to perform the actual work.
    c. The operative pays the bidder a portion of the salary.
    d. Risk distribution: Shared with bidders, whose errors or underperformance could expose the persona, while the native retains physical exposure.
    e. Bidding oversight: Operatives watch bidders work via AnyDesk.

Appendix A: Definition of Roles

The roles below reflect terminology used among the operatives, except where noted.

- **Administrator.** The senior DPRK operative who maintained overall control of cell operations. The administrator created and managed communication channels, such as the Discord server and Vercel dashboard, and set operational policies. We only identified one administrator in the cell hierarchy.
- **Administrative Manager.** An operative who managed and corresponded with "natives" and brokers, and facilitated the transfer of persona information between brokers and operatives. The administrative manager also applied to and worked jobs like the other operatives. We only identified one administrative manager in the cell hierarchy. Nisos uses this term to describe this role, based on our observations of how the cell operates.
- **Bidder.** An outsourced worker who performed technical tasks and, in some cases, applied for jobs under the direction of DPRK operatives. Bidders supported the cell by executing work as the DPRK operative's persona, enabling operatives to scale their activity and maintain multiple employment pipelines simultaneously. DPRK operatives also referred to themselves as bidders, as the term broadly applies to anyone who is applying for a job.
- **Broker.** An intermediary who supplied DPRK operatives with pre-created persona accounts or access to personal information such as government-issued IDs. Brokers interacted directly with operatives to provide resources for persona creation, but were not involved in ongoing operational tasks.
- **Laptop Farm.** A collection of computers that "natives" configured, housed, and managed for and at the direction of DPRK operatives to support multiple employment personas simultaneously. DPRK operatives or their bidders accessed these devices remotely with the assistance of the native. Operatives and bidders used the devices to run applications, facilitate technical tasks, and for other employment purposes. Nisos uses this term to describe this activity, but never observed operatives using this term.
- **Native.** A US-based individual DPRK operatives recruited to act as the front-facing employee, attend interviews, complete drug tests, and/or maintain and run laptops for operative use. Natives may operate multiple devices simultaneously, but operatives retain control of the personas and technical tasks. Nisos and the FBI previously referred to "natives" as facilitators to describe the same operational role. However, we will use the term "natives" as this is the specific nomenclature employed by the cell in their communications.
- **Operative/Member.** A DPRK-affiliated individual who participates in the employment fraud operation, creates and manages personas, supervises natives and bidders, and performs job duties when their persona obtains employment. Operatives use their three-letter initials to identify themselves in Discord and Vercel.
- **Persona.** A fabricated identity DPRK operatives constructed using appropriated or purchased information from legitimate US residents. Each persona features a full professional profile, including resume(s), LinkedIn account, email address, phone number, and corroborating references. Nisos uses this term to describe this concept, but never observed operatives using this term.

- **Team Lead.** A DPRK operative responsible for managing several operatives, tracking metrics such as applications submitted, interviews conducted, and offers received, and guiding the team's operational strategy.

Appendix B: Investigation Origins

In June 2025, Nisos began hiring for a remote lead artificial intelligence (AI) architect role with our company. We detected suspicious activity from one of the applicants and performed a pre-employment diligence investigation and used targeted interview questions to determine that the applicant exhibited characteristics consistent with DPRK operatives. The operative unsuccessfully used appropriated personally identifiable information (PII), a newly created email, and an AI-created resume to pose as a Florida-based lead AI architect and senior full stack developer.

We led the applicant to believe we had selected him for a fictitious contractor position and sent the actor a laptop to his requested location in Florida. Our analysis of the activity on the laptop, combined with open source research, revealed the identity of the Florida-based facilitator and uncovered a DPRK employment fraud cell. The actors established the main communication and coordination in or around December 2024 and over time its size fluctuated, at times reaching up to 22 operatives who each used multiple persona accounts to pursue employment with US companies. We did not hire the operative, did not pay the operative, and did not give the operative access to any internal communications, data, or our network. We used misattributable infrastructure for every step of the investigative process. We analyzed the technical indicators, operational patterns, and communications obtained through this investigation to assess the cell's state sponsorship and national attribution.

Appendix C: Definitions of Probability and Confidence

Nisos Use of Probabilistic Analytic Language

Nisos uses terms such as “likely” and “probably” to convey analytic judgments. The table below shows the spectrum of how those terms correlate with percentages of likelihood.

Assessment Language	Almost no chance	Very unlikely	Unlikely/ Improbably	Possibly	Likely/ Probably	Very likely	Almost certainly
Percentages	<5%	6-20%	21-45%	46-55%	56-80%	81-95%	96-99%

Nisos Use of Confidence Levels

Where helpful, we also include confidence levels that highlight the quality of information underpinning an analytic judgment.

- **Low confidence** usually indicates that the information is too fragmentary or questionable to make solid analytic judgments.
- **Moderate confidence** means the pieces of information are credibly sourced and plausible but not highly corroborated.
- **High confidence** is associated with high-quality information and data that is corroborated by other credible information.

