flare

IBM

# Inside the North Korean Infiltrator Threat

By Flare Research & IBM X-Force

## Research Collaboration Overview

Beginning in late 2025, Flare and IBM X-Force initiated joint research activity focused on North Korean IT workers after Flare's initial discovery of concerning worker activity. This project marked the first in what is expected to be an ongoing series of collaborative threat-research efforts between the two organizations.

IBM X-Force and Flare combined their complementary strengths, with IBM contributing its threat-intelligence expertise, language analysis capabilities, and global visibility into emerging cyber trends, while Flare leading and providing platform-driven insights into illicit online ecosystems, behavioral patterns, and activity occurring across dark-web and high-risk communities. Together, the teams integrated their findings to build a more comprehensive understanding of the tactics used by North Korean IT workers to infiltrate legitimate organizations and the broader risks they pose.

# Executive Summary

Increased federal activity, including indictments over the last year, has brought to light the growing scale and sophistication of a global threat: North Korean nationals operating as remote IT contractors and full-time technology staff within unsuspecting companies across the globe. Research conducted in collaboration between Flare and IBM X-Force details the extensive tactics and techniques employed by these North Korean IT Worker (NKITW) operatives. The North Korean regime mobilizes thousands of skilled IT professionals to infiltrate organizations across North America and Western Europe, primarily for financial gain, but also for corporate espionage and the theft of sensitive information. The report details their methodologies, offering a critical understanding of this evolving threat to the global business ecosystem.

There have been several reports about the activities of various North Korean IT worker operations, and countless incidents reported in the news related to North Korean threat actors in general. The research conducted by Flare and IBM X-Force does not focus on a specific incident or cluster of activity, but rather on gaining an intimate understanding of the way these groups work on a day-to-day basis. This research is based on proprietary threat intelligence data collected from multiple sources and analyzed through Flare's platform. To protect our methodology, we have chosen to intentionally minimize information on sources and methods.

# Key Findings Distinguishing this Report

- **Internal North Korean Infrastructure Uncovered:** Our research provides concrete evidence of internal North Korean IT management platforms like "RB Site" (assessed to be associated with Ryonbong, a sanctioned entity) and "NetkeyRegister," revealing a structured back-office operation for tracking work, managing devices, and distributing software updates to NKITWs.
- **Western Collaboration Enables Deeper Compromise and Scale:** With the help of recruited western collaborators, primarily from LinkedIn and GitHub, who, willingly or unwillingly, provide their identities for use in the IT worker fraud scheme, NKITW are able to penetrate more deeply and reliably into an organization, for a longer period of time.
- **Daily Life of an IT Worker:** The report highlights internal documentation, including "timesheets" for tracking job applications and work progress, as well as slide decks distributed to workers, giving advice on how to best land a job. We have gained an intimate understanding of the day-to-day operations of North Korean IT workers.
- **Insight into Internal Communication and Operational Security:** The widespread use of IP Messenger for decentralized internal communication on local networks, along with Google Translate logs indicating routine English-to-Korean self-validation, reveals key aspects of NKITW operational communication practices.
- **Detailed Breakdown of the NKITW Ecosystem and Roles:** Our findings delineate a clear, multi-tiered operational structure involving "Recruiters," "Facilitators," "IT Workers," and "Collaborators/Brokers," each with distinct responsibilities in the fraud lifecycle.
- **Revenue Generation is the Primary Motivation:** Although some teams of IT workers have been reported to also engage in malicious activity such as data exfiltration, extortion or financial theft, the overriding motivation of North Korean IT workers is revenue generation.

- **IT Workers are Diffuse Within the DPRK Party-State:** Despite many reports attributing NKITW to specific groups subordinate to the DPRK party-state, there is evidence that teams of IT workers are deployed by numerous government bodies, party organizations, front companies and public-private partnerships, making them a ubiquitous, diffuse presence.

## Introduction

Flare and IBM X-Force's analysts have uncovered a vast cache of intelligence detailing the tactics and indicators used by NKITW operatives. This data offers an unprecedented window into how the North Korean regime mobilizes thousands of skilled IT professionals to infiltrate organizations across North America and Western Europe—pursuing financial gain, corporate espionage, and the theft of sensitive information. This report does not focus on a specific incident or cluster of activity but rather provides an intimate look at the day-to-day lives of North Korean IT workers and their operations.

This report dives deep into the exact tactics, techniques, and procedures (TTPs) used by North Korean operatives to infiltrate and extract information and financial resources out of companies—all based on primary source material unearthed by Flare Research and IBM X-Force. Armed with this knowledge, organizations will know exactly what to look for in candidates, employees, and endpoint device logs. The information in this report is not only useful to security teams, but also human resource (HR) professionals who find themselves on the front line facing this threat. Security teams and human resource teams alike will be empowered to threat-hunt within their organization and among candidates.

## Introduction to North Korean IT Workers

The Democratic People's Republic of North Korea (DPRK), aka North Korea, is subject to international sanctions that make it difficult to generate revenue through international trade, which has led the North Korean government to employ numerous techniques to generate revenue and evade sanctions. One such technique is the deployment of remote IT workers who use false identities to apply for and work remote IT jobs worldwide. With the primary goal of funneling generated income from IT work back to the DPRK party-state to fund various weapons programs, some evidence of malicious activity suggests data exfiltration and/or cryptocurrency theft by some teams of IT workers.

## Organizational & Government Structure

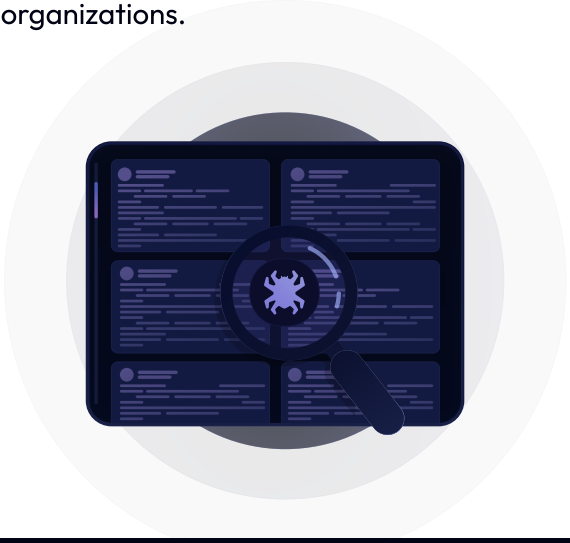
North Korean IT workers (sometimes abbreviated as NKITW, DPRKITW, or ITW) are increasingly becoming a cornerstone of North Korea's government strategy to deploy workers overseas and extract salaries for regime revenue generation. Historically, the North Korean government sent restaurant and construction workers who often worked in China and Russia to remit most of their earnings back to the government. NKITWs are a continuation of this trend, albeit earning at a much higher rate than their blue-collar counterparts. While the exact number of North Korean overseas workers is difficult to ascertain, in 2023, the United Nations Security Council Panel of Experts estimated the number to be between 3,000 to 10,000. Furthermore, a 2024 report suggests that there are over 100,000 workers spread across 40 countries working in factories such as sewing, construction sites, information technology etc., generating approximately $500 million annually. In 2022, a US Government advisory indicated that a DPRK IT worker may individually earn more than $300,000 a year.

NKITW are considered elite members of North Korean society and have become an indispensable part of the overall North Korean government's strategic objectives. These objectives include, but are not limited to, revenue generation, remote employment activity, theft of corporate and proprietary information, extortion, and providing support to other North Korean groups.

Publicly available reports from sources such as the US Treasury, sanctions watchdogs, the United Nations, and private-sector threat intelligence research teams have attributed IT worker operations to various organizations within the DPRK party-state, such as the Munitions Industry Department, the Ministry of National Defense, the Science and Education Department, and the Reconnaissance General Bureau, among others. It is difficult to confidently attribute any one IT worker to a specific department unless the worker makes serious operational security mistakes, but it is clear that IT workers are deployed across disparate government bodies; however, it is unclear whether there is systematic interdepartmental coordination between cells of IT workers at a high level.

## Known Activity and Operational Security Failures

While it is difficult to attribute specific individuals or teams of IT workers to a particular government body or subordinate corporation, we have observed opsec failures revealing the names of organizations.



One example of such a leak is a seemingly throwaway credential for testing a web service running locally, with the email kimhyok@pt.net[.]com. Another known NKITW using the email address pororo940616@pt.net[.]kp. The domain pt.net[.]kp is the domain name for a page on North Korea's geofenced Kwangmyong intranet, belonging to the Central Information and Communications Center, formerly known as the Ministry of Posts and Telecommunications. It is unclear whether the email address containing pt.net[.]com is an intentional or unintentional typo, whether a pt.net[.]com email exists, or whether an email address like this would belong to an employee or a customer.

Another DPRK-specific email that we observed was jangyi@pic.co[.]kp. The pic.co[.]kp domain is another Kwangmyong intranet address belonging to the Pyongyang Informatics Center (PIC), alternatively the Pyongyang Information Center. Possibly subordinate to, or simply renamed as, the Pyongyang Information Technology Bureau, the bureau has been under U.S. government sanction since 2016. The PIC (or PITB) is likely a subordinate organization under North Korean Workers' Party Central Committee's Science and Education Department, and is known for the development of various network hardware and software tools.

Numerous references to RB Corp and RB Site can be found in internal communications between IT workers, and will be explored later in this report. We assess with a moderate level of confidence that RB stands for Ryonbong, a reference to Korea Ryonbong General Corporation, an entity sanctioned by the US Treasury for its ties to DPRK weapons procurement and development, and known to be subordinate to the Munitions Industry Department. Regardless of whether the attribution of RB to Ryonbong is correct, RB appears to maintain an internal back-office web platform where IT workers can track work, manage hardware devices, and download software updates.

## Education – University of Sciences, Pyongyang (리과대학)

These workers, like other North Korean threat group actors, are selected at a young age for mathematical and scientific aptitude, starting at middle school, and are trained through a series of elite North Korean educational institutions up to college. Several top North Korean universities, such as Kim Il Sung University and Kim Chaek University, are often mentioned in previous publications when discussing where North Korean threat actors are trained.

The current investigation has exposed another university only mentioned in a previous article: University of Sciences (리과대학). One of the exposed NKITW used this university's name as a personal account username, suggesting a possible affiliation or operational connection.

The University of Sciences is managed by North Korea's State Academy of Sciences, the top scientific body for North Korea, and is situated on the outskirts of Pyongyang. Former students who defected, describe the university as a prestigious school that offers Pyongyang residency and a guaranteed job inside the capital. (Note: North Korean citizens are prohibited from traveling or moving within North Korea without a permit. Being able to live within Pyongyang proper is considered a status change as the government provides better provisions and privileges only reserved for the residents.)

## Associated North Korean Organizations

Our investigation also uncovered the names of two other North Korean organizations when suspected NKITW used the following two organization names as usernames for their accounts:

버들경제기술교류소
신봉기술제품개발소

The term, 버들경제기술교류소, is loosely translated as "Willow Tree Economic Technology Exchange Center," while 신봉기술제품개발소 is loosely translated as "Sinbong Technology Product Development Center." Economic Technology Exchange Centers act as a Google Play Store equivalent for mobile phones in North Korea, where users must physically visit the center to install new apps or update virus definitions. Information suggests the Technology Product Development Center is developing machinery or other related technology for businesses and consumers.

# Key Positions and Roles

While researching, analysts uncovered several documents and spreadsheets containing key information regarding the separation of jobs and duties. Based on the information found within these documents, it is highly likely that the NKITW ecosystem contains the following personnel:

Recruiters

Facilitators

IT Workers

Collaborators/ Brokers

## The Recruiter

While examining the contents of the spreadsheets and documents, there are clear statements that the DPRK IT system includes recruiters. Similar to your everyday recruiter, these recruiters are responsible for screening potential IT workers and recording initial interview sessions to send to facilitators to be accepted or denied for employment, much like a hiring manager. These interviewees have resumes, typically seeking employment in positions specializing in JavaScript, development, blockchain, etc. If the recruiter feels that the candidate is a good fit, they pass them to a facilitator. It is unclear whether these candidates realize that the job they applied for or are being recruited for is to ultimately work for the DPRK.

Interview evidence supports this: when asked about adopting a "more 'US American' name," candidates express confusion rather than acceptance—a reaction inconsistent with knowing they'd be working for the DPRK under false American identities.

**Recruitment Screening**

Recruiters appear to play an instrumental part of onboarding new participants into NKITW fraud operations. Evidence suggests professional recruiters use their skills to screen and persuade job-seeking IT workers into the role of collaborators. Recorded interviews reveal a common set of questions asked to legitimate job seekers.

In the initial job screenings analyzed by X-Force and Flare, a recruiter first states that the company they are interviewing for is an “early-stage stealth startup” with no published information about the company. The alleged company is named “C Digital LLC” and is communicated to the candidate that they are formed by several “founders” and still in the early stages of formation.

Next, the recruiter proceeds to communicate to the candidate that they will be “learning effective job-hunting strategies” and will be mentored by a team lead, as they will spend most of their day attempting to gain employment at western-based companies. The recruiter then informs the candidate that they will be given a US-based identity (or “profiles”) to use while they work to gain employment. Then they are asked if they are comfortable working US-based hours. The recruiter is clear that they are unable to offer US citizenship, but gives the notion, they may gain it in the future.

Although not an ethical practice, the embellishment or use of western-style names for foreign candidates is not unheard of. It is sometimes used by recruitment agencies when they stand to receive a larger commission for certain types of candidates. However, this practice continues to call into question the motives of the recruiter. Continuing through the process, the candidate is asked about expected compensation. They are informed that if they do gain third-party employment, their salary will be increased by C Digital LLC but will risk being replaced by another person if they fail to meet the demands of their gained third-party employment. The candidate is also told they will be tasked with mentoring junior developers and bringing them into the fold.

Job candidates appear to be caught up unwittingly in the ploy set up by the recruiter. Our joint research cannot confirm the extent to which recruiters themselves know they are playing in the fraud ecosystem. They exhibit characteristics of motivated blindness by financial gain and are willing to bend the ethical rules of normal hiring processes. Candidates often questioned these practices but were willing to continue the initial screens to the next round. It is unknown if any of the candidates were accepted as full-time employees. These findings suggest recruiters are at least likely aware they are contributing to a potentially illicit scheme.

## Facilitators and IT Workers

The organization that makes up the whole of the NKITW, contains both facilitators and IT workers, and from analyzed documentation, appear to have separate roles and duties. However, analytical attribution or delineation cannot always be precise due to the apparent overlap in work activities between facilitators and IT workers. Facilitators and IT workers may be the most important roles within the NKITW system, playing a crucial role with a myriad of responsibilities. Based on the information gleaned from internal spreadsheets and documents, our research suggests that facilitators and IT workers have the most responsibilities and are required to document their tasks in detail, performing the following daily duties:

- Persona creation
- Obtaining fulltime employment
- Onboard new hires
- Connect with collaborators

From available documentation, we assess that IT Workers and facilitators are sought out with desired experience in:

- .NET
- Blockchain development
- WordPress
- CMS development
- Full stack development, etc

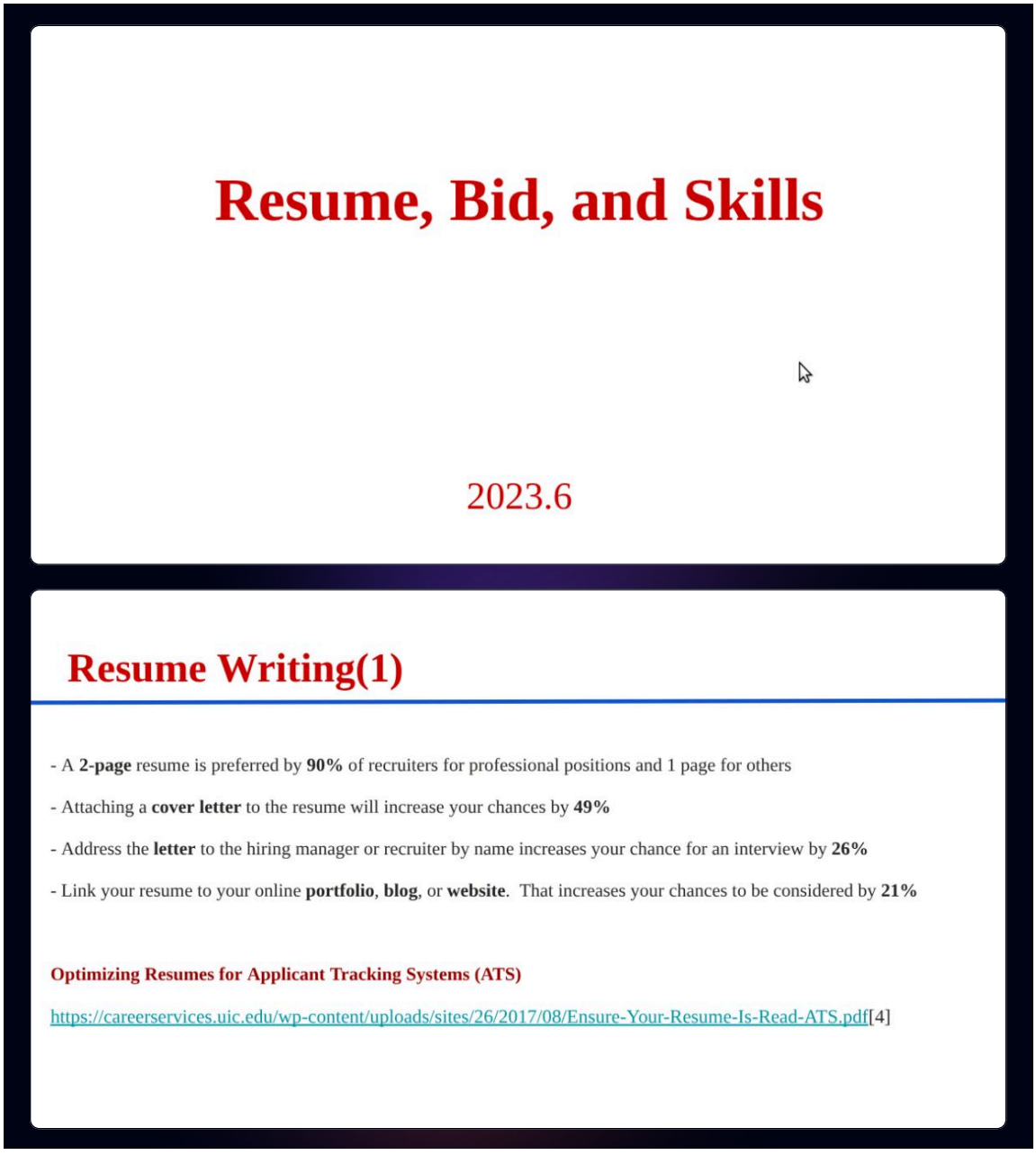
**A Dual Structure: Freelance & Full Time**

Analysts have observed that it's likely both NKITW and facilitators have been taking on large volumes of freelance work, in addition to increasingly seeking out more full-time employment in recent years.

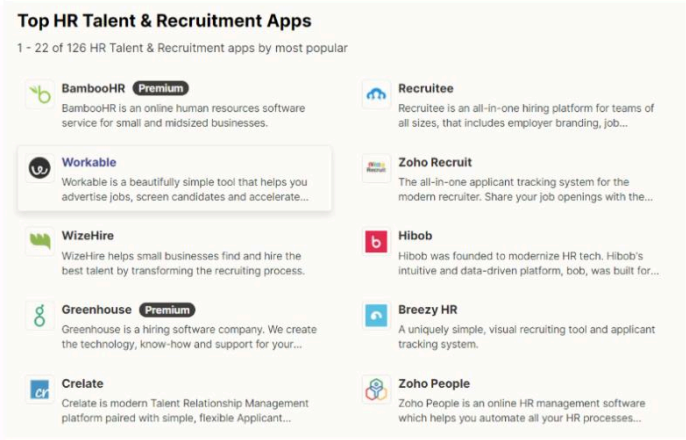
Freelance jobs may be done concurrently and in short periods of time, but web platforms facilitating contract work often require ID and bank information to verify accounts. Operationally, the requirement often causes problems at scale for NKITW who create and maintain multiple accounts for fake identities, which risk getting suspended or banned. Full-time employment is more stable and lucrative, but often requires the recruitment of western collaborators to assist with overcoming the job screening process.

### Educational Slide Decks

Research unearthed a slide deck that was shared internally to a team of North Korean IT workers, with various pieces of information and advice related to landing freelance jobs and remote full-time work, although it's unclear who assembled the presentation. The presentation included tips on what freelance platforms to use, useful Google dorks for finding work in a specific country, and advice on writing a good resume, which was clearly taken from Cardinal Staffing. Below are a few samples of the slides contained in the deck:

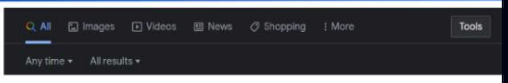


# Bid-job search-platform(3)[3]




# Bid-job search-google

site:https://*.com/careers → site:https://*.com/




site:https://careers.*.com, site:https://career.*.com

site:https://jobs.*.com, site:https://job.*.com

https://join.com/*

https://*.zohorecruit.eu https://*.zohorecruit.com

jobs.smartrecruiters.com/*

jobs.polymer.co/*

app.jobprotocol.xyz/*

*.teamtailor.com/jobs

*.freshteam.com/jobs

*.jobs.personio.com, .de

Domains

.com

.org

.xyz

.pro

.network, .net, .global

.io, .gg, .ai, .eu, .app

.de, .nl, .tech, .team

# Bid-job search-country

**UK, German, Netherlands, Polish(B2B), Ukraine…**
**Use country domain search method as much as possible.**

**"remote" and "developer" site:https://*.uk/**
**"remote" and "developer" site:https://*.de/**
**"remote" and "developer" site:https://*.nl/**
**"remote" and "developer" site:https://*.pl/**
**"remote" and "developer" site:https://*.ua/**
**"remote" and "developer" site:https://*.cy/**
**"remote" and "developer" site:https://*.fr/**
**"remote" and "developer" site:https://*.sg/**

### Time Tracking

Discovered spreadsheets and documentation include what appear to be timesheets, or “working time.” These documents helped researchers gain insights into how these workers are grouped and track their time. Based on the data within the reports, it is likely that these time sheets are used by facilitators and/or their assistants to track time worked on conducting bids and messages for freelance work.

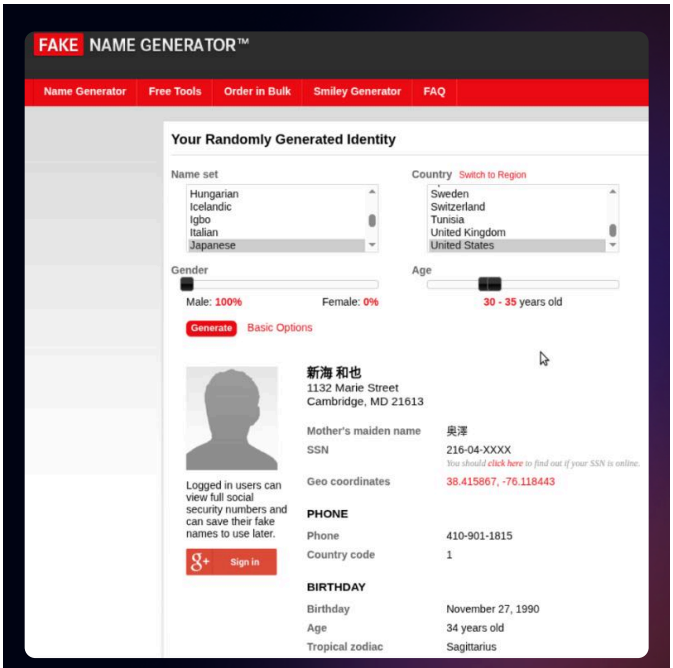
Analyzed documentation suggests that each day of the month, members log their time worked by the second “9:34:04.” Analysis of available timesheets indicate that time worked is averaged out, and groups/individuals are labelled with a number rank. For example, in Group Three, worker three might have worked an average of 14 hours, putting them in position one, while the second worker in Group Three may have averaged about 11 hours, placing them in rank position 21. Ranking may be part of North Korean life, where those at the bottom of the rank will likely face 'self-criticism' sessions amongst peers.

The timesheets include hours worked on “Bids” and “Msg.” The count of “Bids” likely represents how many bids in a day a worker made on freelancing sites such as Upwork. Msg likely refers to how many messages or connections a worker made on UpWork, LinkedIn, Freelancer, or even Nextdoor. On any given day, a worker may submit upwards of 300 bids, often only receiving confirmation on about 10 jobs. Extensive overbidding likely happens because they charge below the market value for their work but receive a low bid acceptance rate.

Analysis of the documents indicate that there are several groups consisting of likely facilitators and/or their assistants, including no less than two, and no more than three members. Each person in the group is assigned a nickname, although it is unclear how these names are established. For nicknames derived from more conventional names such as “Christian” or “Adam,” researchers assess that these nicknames are just shortened names for each profile created. Less likely assessments include names that refer to character abilities in games such as the nicknames “Phoenix,” “Calm,” and Flash.” These names may have been picked referring to the character “Phoenix” in the game Valorant, and the ability to cast a flash during curveball plays, in combination with a "calm aim" technique. Another possibility is that group members pick characters from movies, such as Disney characters including “Coco,” “Aurora,” and “Bruce,” or they just may be randomly generated.

### Setting Up the Persona

North Korean IT workers and facilitators use one or more fake identities to maliciously pursue work opportunities. Depending on the targeted role and its requirements, identities can range from simple sockpuppet accounts, all the way to verified accounts linked to human beings who, willingly or unwillingly, give the worker access.

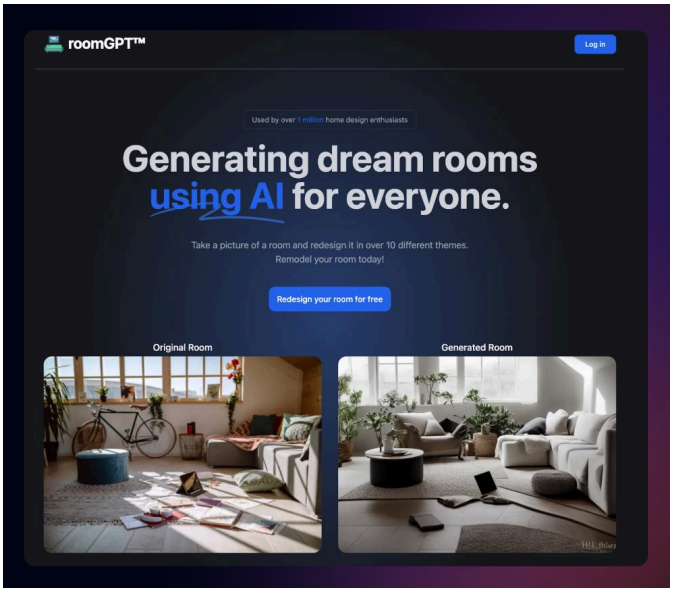


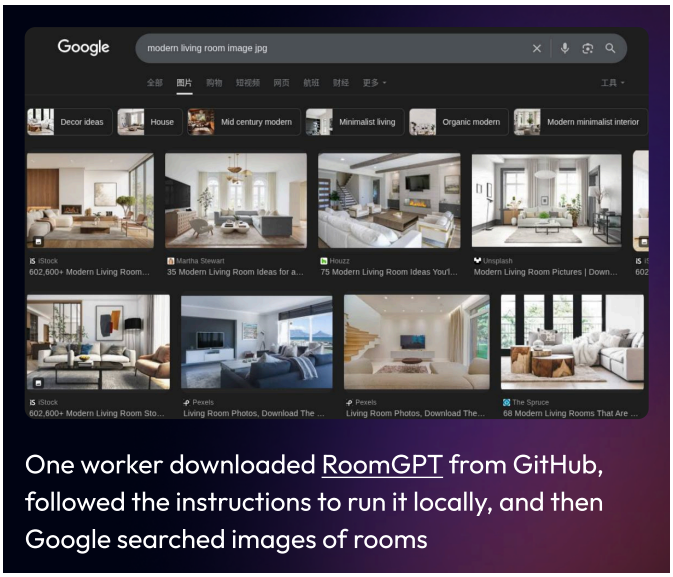

FAKE NAME GENERATOR used to create a fake Japanese identity of a person living in the US

Work is done on computers or virtual machines (VM) with IP addresses located in regions where the worker wants to appear to be from. These machines are often virtual machines hosted on a cloud provider, but could also be physical machines belonging to western collaborators, to which the worker is given remote desktop access. These machines may be used by one or more people, often managing several different fake identities at a time. A throwaway email is often created using Protonmail or some other similar provider lacking stringent verification requirements first, in order to have a second verification address for the Gmail account.

Facilitators and IT Workers will often download a photo of someone who matches their target ethnicity, and use an online AI photo editor to change the image so it can't be reverse-image searched. Sometimes they will use a real photo of themselves and remove the background with an online background remover.

Researchers also observed downloaded images of rooms used as background images, and the subsequent use of AI tools to modify the images, likely to avoid internet searchability.




One worker downloaded RoomGPT from GitHub, followed the instructions to run it locally, and then Google searched images of rooms

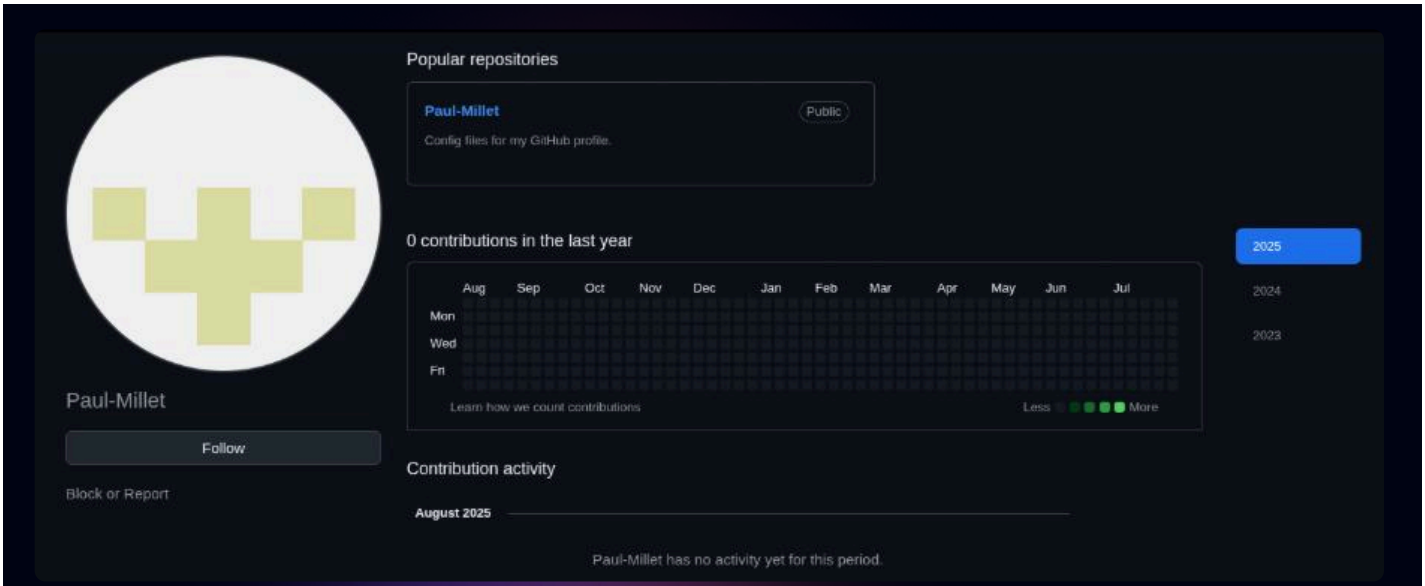
The initial setup is followed by creating accounts on numerous web services like GitHub and LinkedIn. Research found that profiles are created on LinkedIn, Upwork, and GitHub to cover several regions, including but not limited to:

| | |
|---|---|
| Iran | India |
| United States | Croatia |
| Czech Republic | Colombia |
| Ireland | Syria |
| Saudi Arabia | Japan |

Sometimes GitHub profiles are left blank, while others contain added flair with a comprehensive bio and graphics showcasing a list of technologies. Flare researchers uncovered Google searches for topics such as "how to create fake commit activity on GitHub" or "how to get fake Github badges."

A prominent feature of the GitHub profiles is the existence of repositories that are completely empty, or contain only boilerplate code, with generic-sounding names like “nextjs-app” or “flutter-app.” There are often several forked repositories to make the profile look more substantial.

GitHub profiles account for at least two different purposes. Some profiles are elaborate and designed to showcase a worker’s skillset for attracting potential clients or employers. Others are created solely to conduct daily work for employers, like working on branches and submitting pull requests on private corporate codebases. These latter profiles are usually empty and are likely not intended for attracting clients.

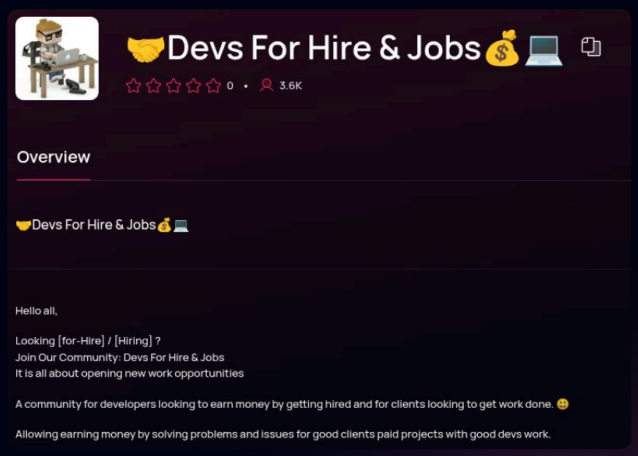



A bare-bones GitHub profile created for full-time work using the fake identity Paul Millet from France. There is nothing on the profile as the account’s purpose is not to advertise to potential clients, but conduct full-time work for an employer.

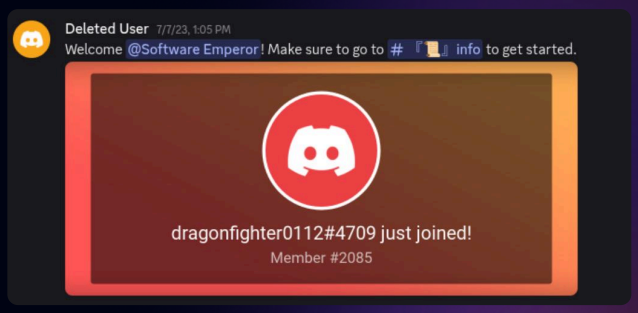
**Freelancing**

If workers are seeking freelance employment, they will create accounts on every freelancer platform they can find, often conducting Google searches for freelance job platforms specific to the country being targeted. The worker will sign up for several platforms such as Upwork, Toptal, Guru, Djinni, SimplyHired, Fiverr, Glassdoor, SmartRecruiters, RemoteBase, Jooble, dev.to and various others. Discord is another platform where NKITW look for work. There are numerous public Discord servers, not affiliated with DPRK IT worker operations, that provide a platform to match freelance and remote job seekers with job postings.

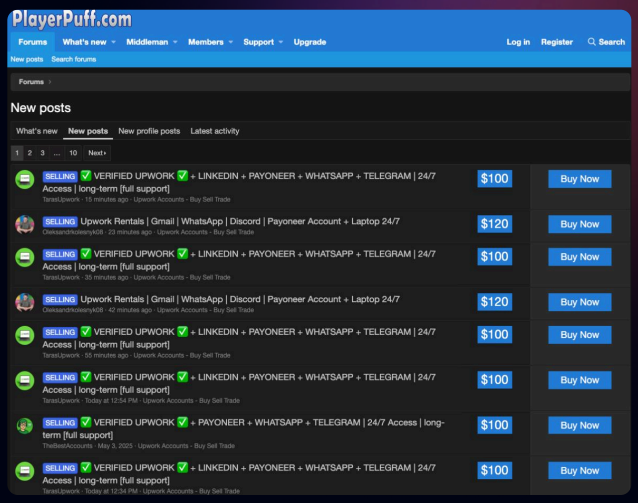
Based on available documentation, workers will bid on freelancing projects using their created profiles, bidding on anywhere from 80 to 1000 projects (such as “Blockchain project”) in one month. Often, only about 10 bids will be accepted with an average payout between $200-$1,000. Facilitators and IT workers may also hire additional help if they are unable to perform the task they were hired to do from a project bid. For example, within the available, documented task list, one worker notes, “The dev is working on the [company name] job.” This comment was noted after a worker’s bid was accepted but they could not perform the task.




Discord servers for freelance job seekers advertised on top.gg. Some DPRK freelancers search for these servers and join them en masse.



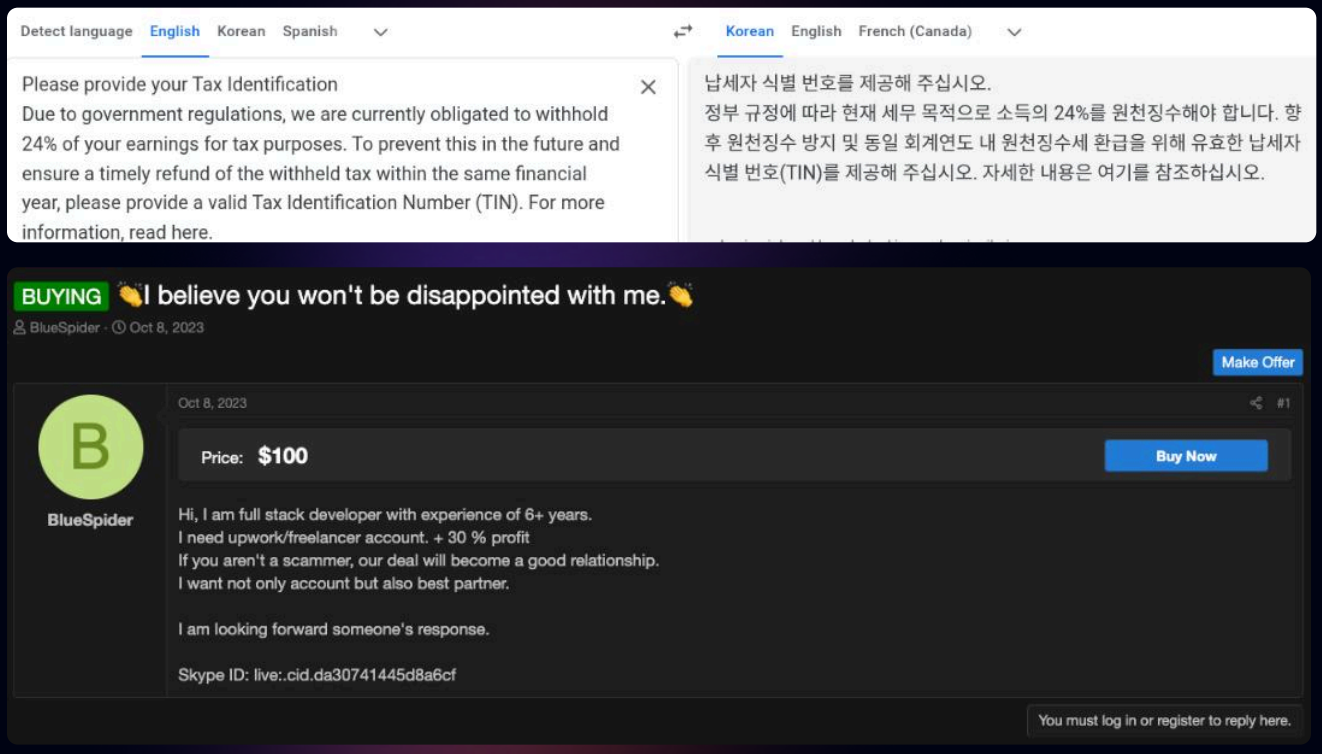

A known NKITW persona joins a job-seeker's Discord server and triggers a welcome message



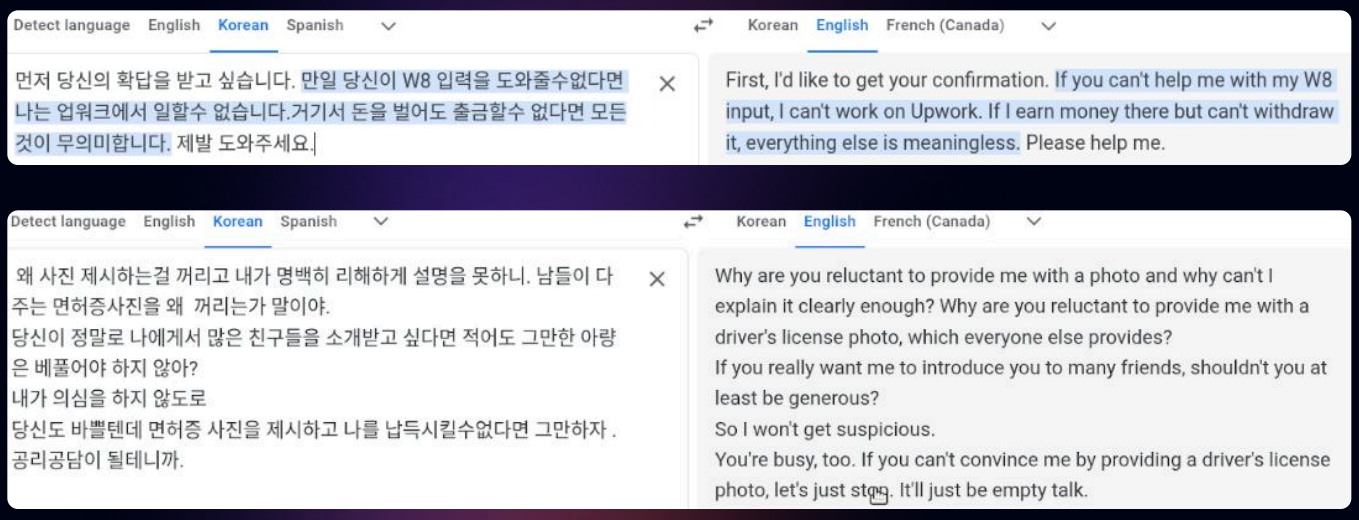

Posts on the playerpuff.com forum selling accounts on freelancer platforms, and a post from a known NKITW looking to purchase accounts with a profit-sharing agreement

Verifying accounts on freelance platforms and receiving payments is an obstacle for the NKITW where a collaborator is usually required. The worker either buys an account for the platforms from illicit forums or from individual brokers selling accounts.

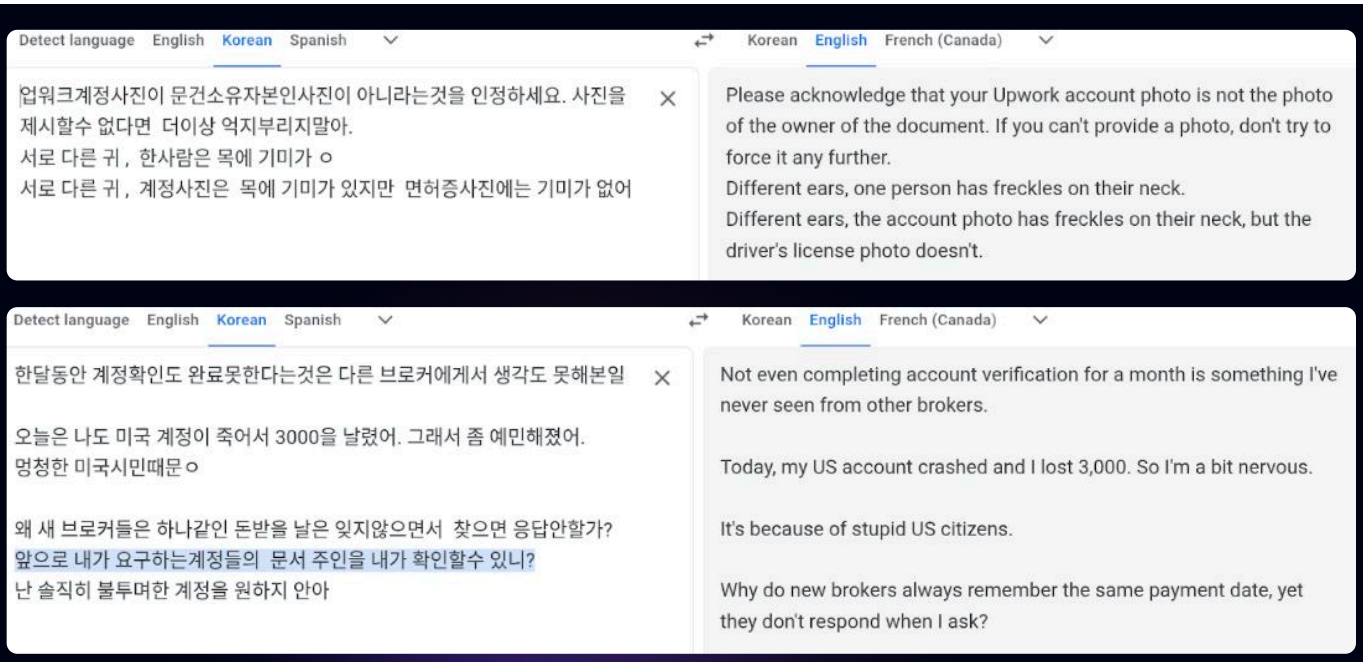
Some of the Google Translate screenshots below contain North Korean spellings for certain words, which are not evident in the English translation.



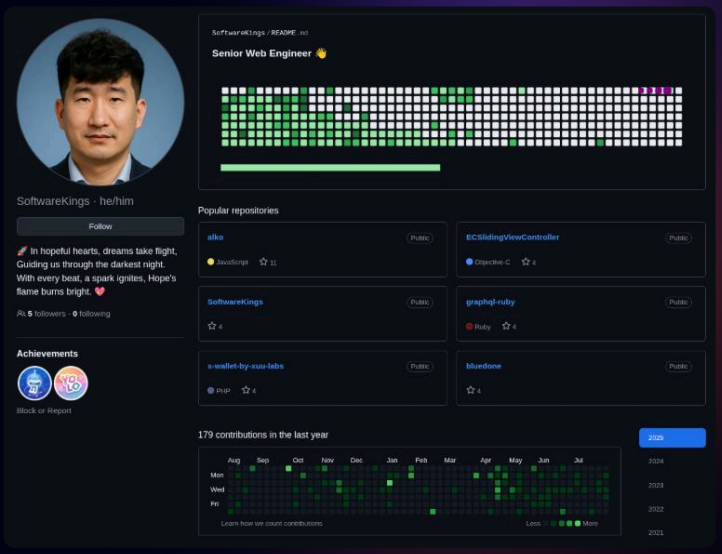

IT worker advertising for freelance work




Evidence of a dispute with an Upwork account broker over identity verification




Evidence of a dispute with an Upwork account broker over identity verification




A more fleshed-out GitHub profile with what appears to be an AI-edited profile photo, with several repos copied (not forked) from existing repos

**Full Time Employment**

Facilitators and IT workers create profiles and resumes on LinkedIn to apply for jobs; however, they also apply for full-time positions directly on company sites. Facilitators may apply to anywhere from 30 to 120+ jobs per day, but may also hire assistants to apply to jobs for them, as referenced in an internal task-tracking document:

"The assistants were applying for 400 jobs on LinkedIn, Indeed, and Dice".

LinkedIn profiles are also used to connect to people, mainly to find collaborators/brokers. These connections are made likely with the hopes of obtaining personal identities, typically willing and paid for. The facilitator's task list may include:

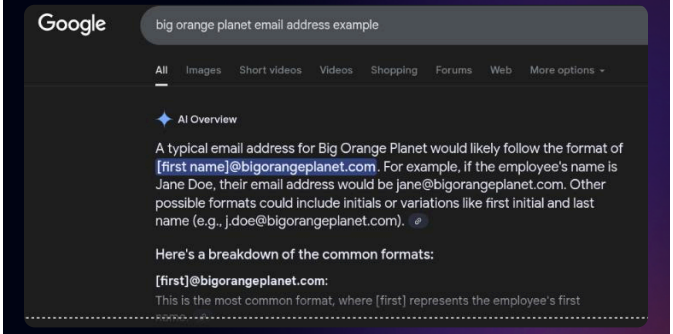
"Discuss with local person in NY to use his Identity for future job hunting".

**The Job Application Process**

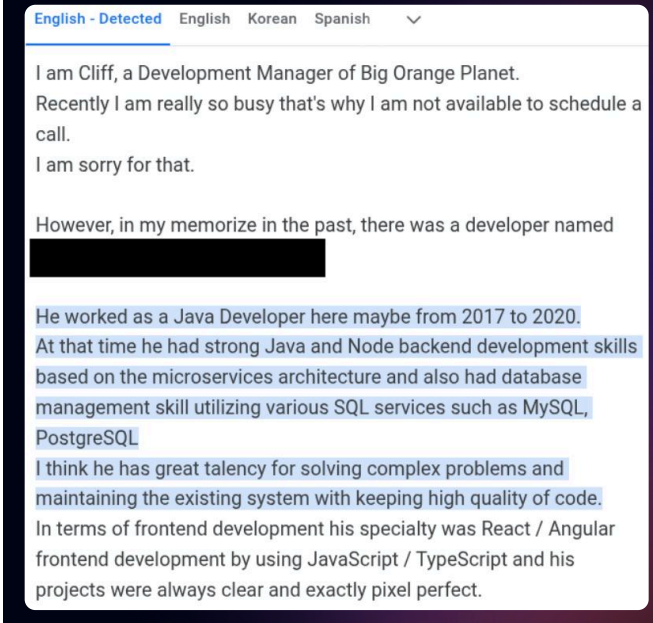
IT workers and facilitators will look for jobs in places that correspond to the profile of the fake identity or the collaborator. For example, if the worker is using a French name, they will seek jobs in France and craft a resume appropriate for a French software developer. The worker will often download packs of resume templates and edit them to fit the fake profile being cultivated. Analysis determined that workers conduct Google searches for the most popular universities and tech companies in the geographic region they are targeting, assisting them in crafting a resume specific to the place they want to work.

If during the application and interview process a facilitator or IT worker is called back from a job they applied to and is selected to conduct an interview, they will proceed with using a Google Voice account. The Google Voice will match the nationality/ethnicity of the created profile that was used to apply for the position.

If a western collaborator (or stolen identity of a real person) is involved, it appears that the resume will use the real person's name and contact information, but contain fake employment history, references, and education. They will often go as far as doing research on how certain companies construct employee email addresses so that they can write convincing, fake reference letters from fake former employers.




A Google search for a typical email address from the company Big Orange Planet, listed as a former employer in the above resume

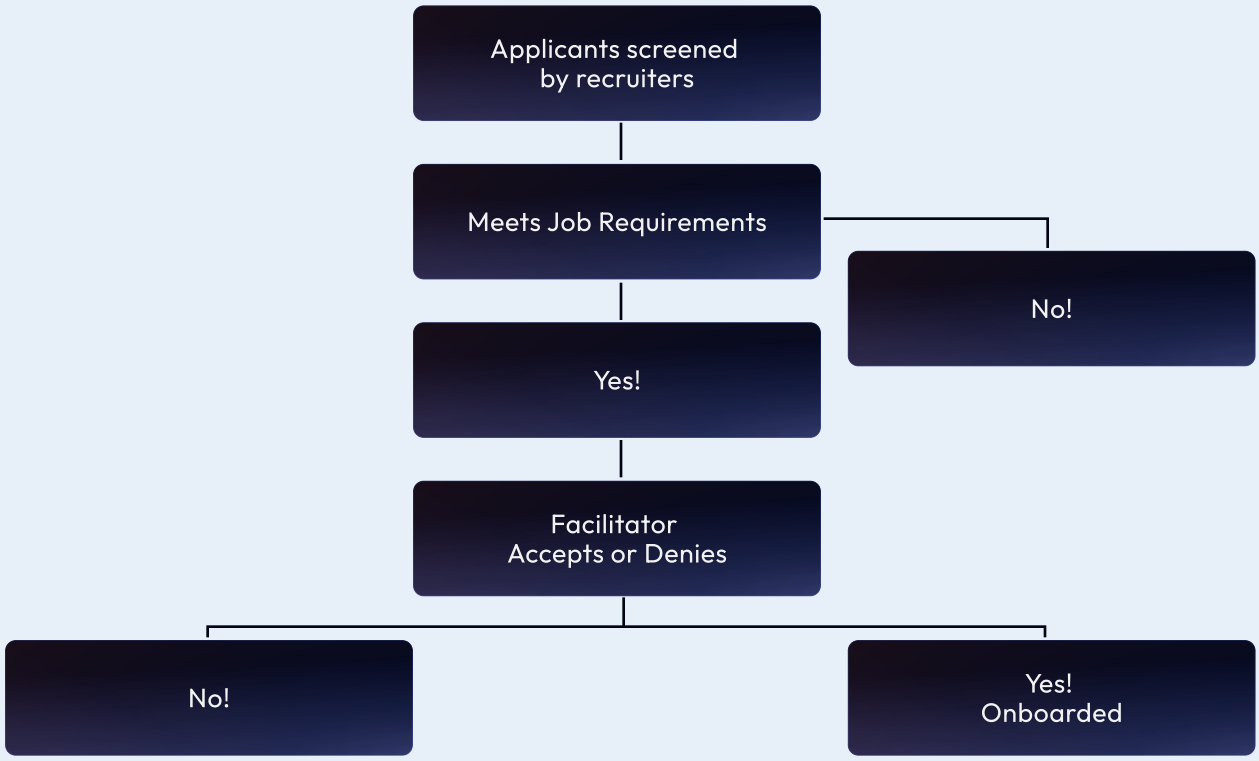



A fake reference letter from Big Orange Planet

**Onboarding New IT Worker Hires**

Another role of the facilitator, and likely IT worker as well, is onboarding new hires. Based on analyzed documentation, once recruiters have screened applicants (IT workers) and if they meet job requirements, they are pushed forward to be accepted or rejected. As referenced in analyzed documentation, some applicants are rejected solely for the reason because their English is not good enough.

“My recruiter [name] had 2 HR interviews (15 mins), and I reviewed the videos and decided to move forward with 1 guy who speaks English fluently.”




Hiring process for IT workers

Once a recruit is accepted, they join a team in which a facilitator or IT worker is then responsible for onboarding the new hire. Onboarding includes:

1. Matching and assigning new hires to profiles and Google Voice accounts, ideally representing a similar nationality/ethnicity; the new hire essentially takes over ownership of the profile.
2. IT worker updates the profiles and related resumes to match their own skillset; “[Name] has been hired to my team, and he needs to update according to his primary skills.”
3. IT worker fulfills job requirements.
4. Assisting the IT worker with upcoming interviews: “Update [first and last name] Resume for new guy's upcoming interviews.”

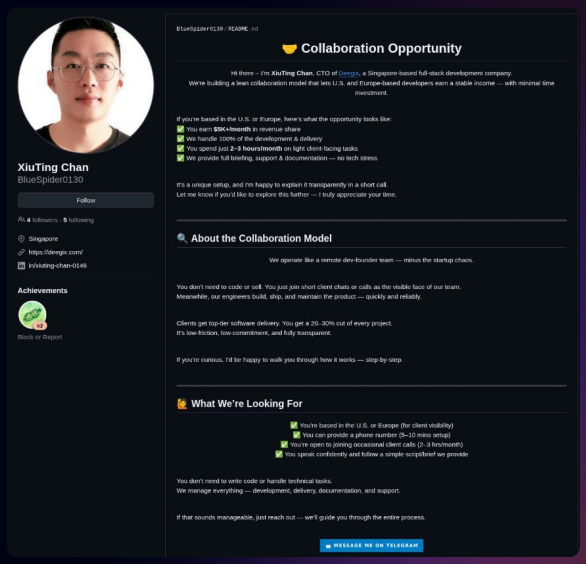
# The North Korean Collaboration Workflow

## Finding Collaborators

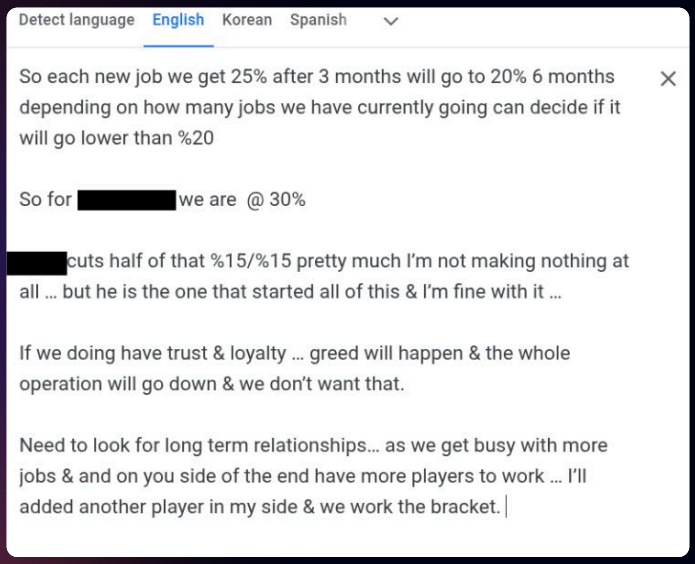
When an IT worker or facilitator seeks full-time employment, identity verification and payroll processing can be rigorous requiring additional work to be successful. The collaborator or broker is used to help complete the hiring process for a worker.

Sometimes the worker or facilitator will have a business relationship with a specific individual who agrees to donate their identity in a more comprehensive way. In some observed cases, it is unclear whether the verified identities of westerners have been stolen or willingly donated, or sold to them.

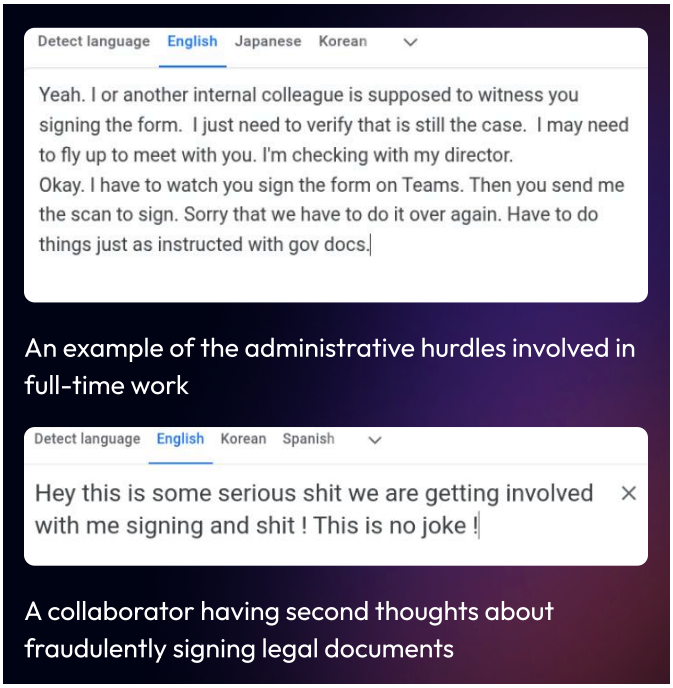
Workers use LinkedIn to make connections and to seek out potential collaborators. Sought out connections may be those who are self-employed, possibly to keep up the appearance of being self-employed, having the ability to work for foreign companies, and to avoid direct government oversight. In other instances, facilitators will use their GitHub profile to advertise that they are seeking a western collaborator. They will often claim to be from a country in Asia such as Singapore or Hong Kong, interested in finding work in the US or Europe with the help of a collaborator.




IT worker advertising for collaborators




Evidence of a profit-sharing agreement with an American collaborator, likely written by a second American collaborator. The North Korean worker is known to have been employed full-time with at least two US-based firms.




An example of the administrative hurdles involved in full-time work




A collaborator having second thoughts about fraudulently signing legal documents

Workers will ask for remote desktop access to an American computer so they can apply for more favorable jobs in the US and offer to split the salary from any employment they gain. In some cases, a successful connection leads to additional collaborators through introduction via family or friends.

Once collaborators are found and agree to sell, or donate their personal identity and/or information, they assist the IT workers by taking employment drug tests, obtaining passports and drivers licenses, passing background checks, and filling out I-9 paperwork or any other necessary employment forms. The collaborator also needs to be available at a US location, ideally a home address, to receive corporate machine deliveries, and to provide banking and tax information.

## Leaning on AI and Google to Bridge the Gap

One of the most ubiquitous and essential tools for North Korean IT workers appears to be Google Translate. Research suggests they rely on it at nearly every stage of their online activity: translating job descriptions, crafting applications and proposals, researching technical information, and even interpreting responses from tools like ChatGPT. They also use it to communicate with account sellers, brokers, and Western collaborators, pasting entire message threads through the service to bridge language gaps. In many ways, Google Translate functions as the central lifeline of their digital operations—the tool that enables them to navigate, participate in, and conceal themselves within the global online marketplace.

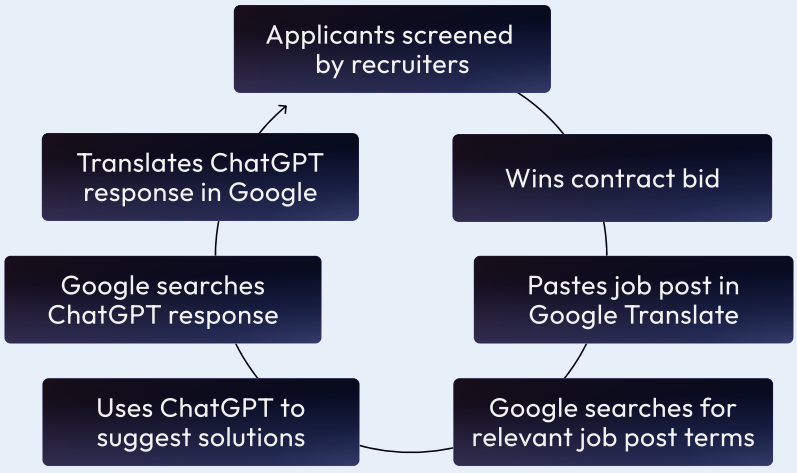
NKITWs are generally at least moderately proficient in English, and most of their internal communications occur in English rather than Korean. Interestingly, a large portion of their Google Translate activity is from English to Korean. This suggests that workers often draft messages in English first and then translate them back into Korean to check for accuracy and ensure the intended meaning holds. Because Google Translate updates the URL bar with each character typed, browser histories showing long sequences of incremental Google Translate URLs typically indicate the worker was composing the message directly. In contrast, when only a single URL appears for a given translation, it usually means the full text was pasted in at once—often a sign that the message came from an external party and was being translated by the worker.

```
https://translate.google.com/?sl=en&tl=ko&text=Yesters&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yestersd&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yestersdy&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yestee&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20fina&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20finai&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20finaih&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20t&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20th&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20l&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20la&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20las&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last%20&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last%20r&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last%20re&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last%20rem&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last%20rema&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last%20remai&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last%20remain&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last%20remaine&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last%20remained&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last%20remained%20&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last%20remained%20i&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last%20remained%20is&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last%20remained%20iss&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last%20remained%20issu&op=translate
https://translate.google.com/?sl=en&tl=ko&text=Yesterday%20I%20have%20completed%20the%20last%20remained%20issue&op=translate
```

Example of the sequence of URLs visited as a North Korean IT worker types their daily scrum update letter-by-letter into Google Translate in English, and translating to Korean to validate that it makes sense

**Maintaining a Job & Communication**

The worker will post the description of the work request into Google Translate, then conduct Google searches for some of the terms in the description. ChatGPT is used heavily to suggest solutions, followed by translating the response, then by more Googling. This cycle of applying for freelance jobs, winning a contract, Googling, translating, and using ChatGPT continues indefinitely, often until the account is suspended from the platform for suspicious activity, at which point a brand new identity is created on a new profile, and this entire process begins again.

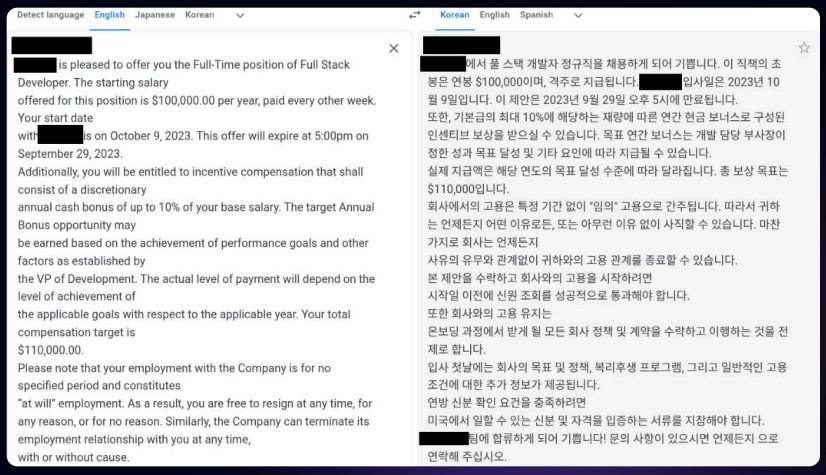


It is usually evident when a worker is lucky enough to land a full-time job by their use of Google Translate. We observed several instances where the worker pasted an acceptance letter into Google Translate, followed by a string of onboarding messages regarding various platforms belonging to the employer, such as corporate email, Slack, Zoom, Teams, Jira, and BambooHR.

Web agencies that do contract work for multiple clients are a popular choice for NKITW to apply to. The worker will often get onboarded to the agency's platforms and accounts, and then get onboarded to agency client accounts. They sometimes get a corporate email in the client's workspace, and have access to their internal Slack, Shopify, CRM, and other corporate platforms. In these analyzed scenarios, the NKITW has access to the agency they work for full-time, and to the clients that the agency serves.


Evidence of a NKITW posing as a French citizen, working for a web agency and being onboarded to the agency's corporate email and Slack workspace

The worker gets onboarded to one of the agency's clients, including an email in the client's workspace, as well as Jira and Sharepoint access




This worker landed a full-time job and used Google Translate to read the offer letter

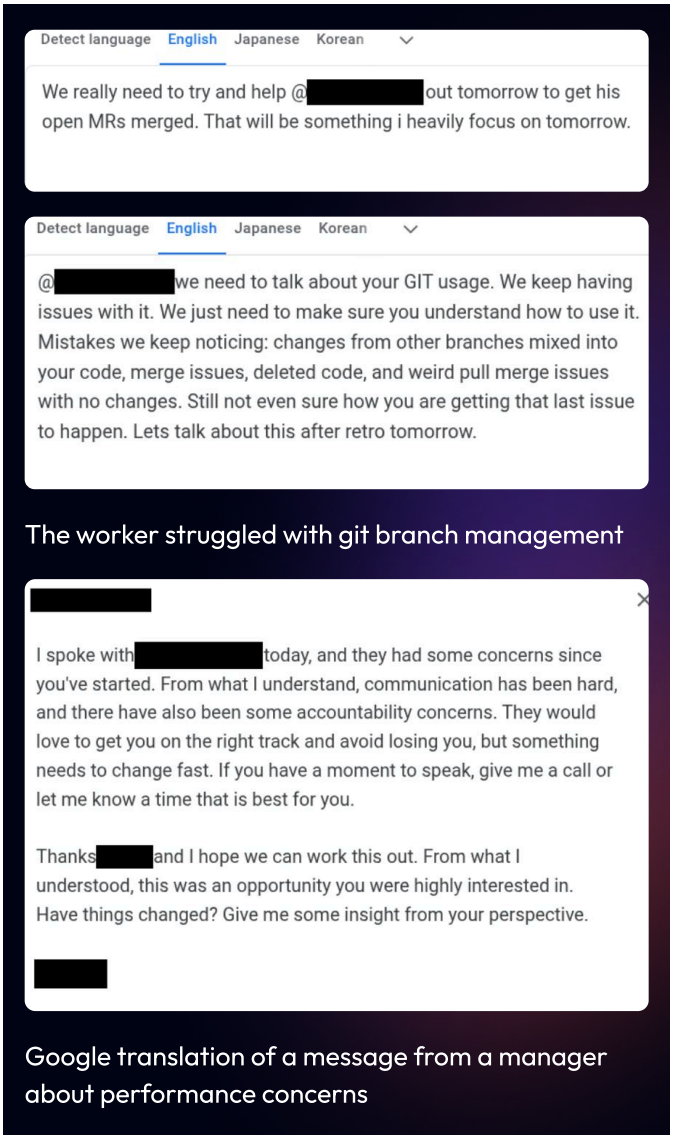

The worker is happy to be part of the team. This message was found in the Google Translate history, such that it was constructed letter by letter, with a separate URL for each letter entered, which indicates that the worker was crafting this message slowly in English, and translating back to Korean to validate that it makes sense.

From available analysis, at this point, there are multiple weeks or months of work being done for the employer. There is a cycle of browsing Jira tickets, translating the contents of the ticket, asking ChatGPT how to solve it, translating the ChatGPT response, Googling some things, translating Slack messages, and submitting pull requests in GitHub. Analyzed data points to evidence of daily scrum/stand-up updates in Google Translate, describing the tasks being worked on and the questions they have for the team, followed by more translations of Slack replies.

## Termination

At some point, there are often questions from teammates and management about the quality of the work being done. The worker may have trouble communicating with the team, or may not be as familiar with the technologies listed on their resume. Google Translate entries show messages from management about

needing to help the worker on issues with their git branch, or having to walk them through some solution. There are sometimes messages from HR regarding performance improvement plans, or relaying concerns from management.



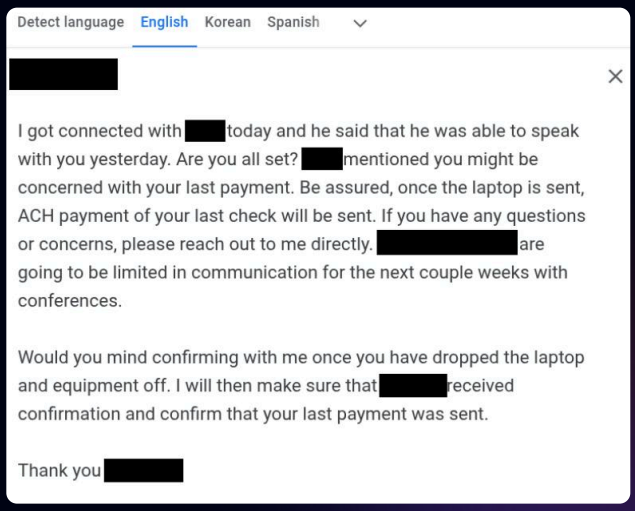

The worker struggled with git branch management



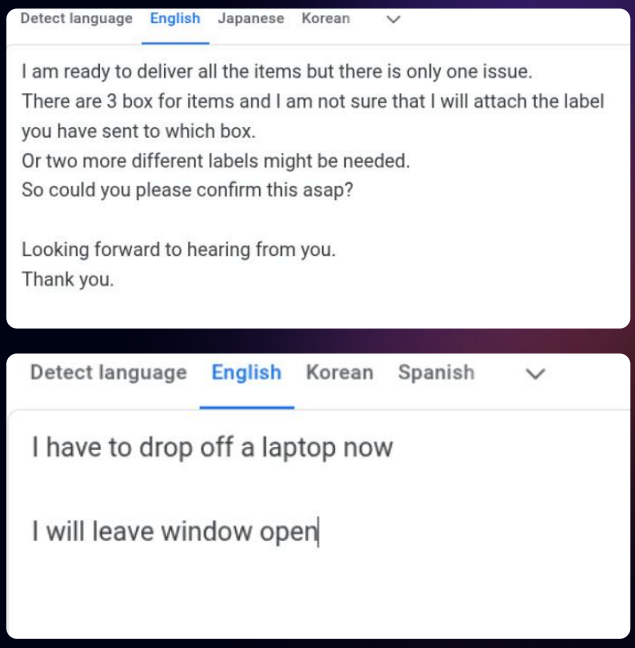

Google translation of a message from a manager about performance concerns

Eventually, the worker may get fired, and the process of returning the laptop mailed to the western collaborator begins. There is often chatter between the DPRK worker and the western collaborator about how to mail packages back to the employer, and how to collect the last paycheck. The cycle is constant and unending.

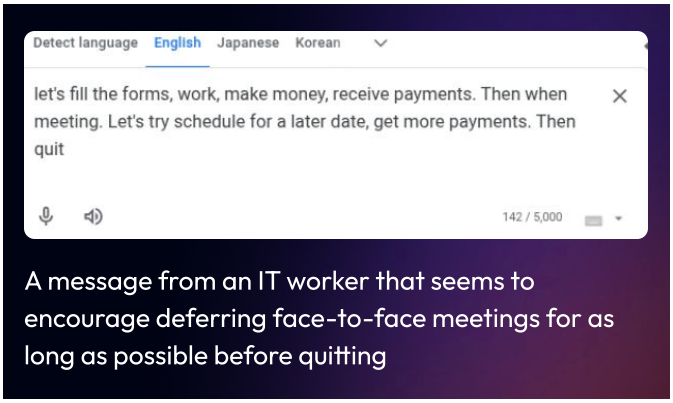
North Korean IT workers understand that, sooner or later, they will either quit or be dismissed from any given role. As a result, they are continually shifting between jobs, identities, and accounts—never remaining in one position or using a single persona for very long.




A message from an employer informing the NKITW who was just fired that the last paycheck will be sent when the laptop arrives




A western collaborator leaves to drop off a laptop and leaves the AnyDesk window open for the DPRK worker




A message from an IT worker that seems to encourage deferring face-to-face meetings for as long as possible before quitting

## Software Tools Associated with North Korean IT Workers

Analysts have identified a handful of tools and workflows specific to NKITW operations. The following sections describe these tools and how North Korean operatives use them in the course of their work. Organizations should look for the presence or use of these tools, especially in combination. Employee device logs that show some combination of these tools in the list of installed software, or browser history containing entries for DPRK-specific web portals, are grounds for further investigation.

### NetKey and OConnect

Data analyzed revealed that most identified computers likely belonging to NKITW contained installed software called OConnect and/or NetKey, a known DPRK-owned VPN. It is highly likely that OConnect and NetKey are used to authenticate users to North Korean internal networks. The following software versions were observed to be installed on machines likely belonging to North Korean IT workers:

- NetKey 4.1
- NetKey 5.0
- NetKey 5.1
- OConnect 5.3
- OConnect 5.5
- OConnect 5.7
- OConnect 5.9.3
- OConnect 6.0.0

The following processes were observed running on machines likely belonging to NKITW:

```
NetKey.exe
OConnect.exe
C:\Program Files (x86)\STN Corp\OConnect 5.7\OConnect.exe
C:\Program Files (x86)\STN Corp\OConnect 6.0.0\OConnect.exe
C:\Program Files (x86)\rb corp\oconnect 5\NetKey.exe
```

In one file path, the NetKey.exe executable is in the directory oconnect 5. Considering this file path, plus the fact that there seems to be a continuity in versioning from NetKey 5.1 to OConnect 5.3, we assess that at some point before or after version 5.2, NetKey was possibly rebranded to OConnect. In addition, some executable file paths were found in directories named rb corp and STN Corp. We also observed the publisher of OConnect show up as star on some machines.

### IP Messenger

IP Messenger, or IPMsg, an open-source, serverless messaging application, has been observed as a communication tool among NKITW workers on local networks. Its decentralized architecture, which does not require a central server, makes it particularly attractive because it allows communication without relying on centralized platforms operated by US companies such as Discord or Google.

One observed entry in the search history contained a message referencing the aforementioned Google Slides presentation including statistics on high-performing resumes, advice for resume writing, and tips on using Google Dorking techniques to search for tech jobs. The message header read:

```
None
==================================== From: Jockey
(PH-2609/DESKTOP-5K4B423/192.168.118.98/Jockey-<2b1a7b2c17d18477>) Cc:
!P@nther! (PH-2609/DESKTOP-DM8PVJ9/192.168.118.100/Rising-<93aa6125ae12b58e>)
Cc: *Genie* (PH-2609/DESKTOP-7C9C52F/192.168.118.55/rtyu-<ebb7795d2f119bca>)
Cc: *Hera* (PH-2609/DESKTOP-2OG3VH3/192.168.118.93/Helios-<3c75203d51c95280>)
Cc: @Viper@ (PH-2609/DESKTOP-55AHA0O/192.168.118.112/Viper-<ecbbc3f4006da4fe>)
Cc: @smile (PH-2609/DESKTOP-N6SA7AH/192.168.118.110/AKIRA-<dba812f4ca1e6705>)
Cc: BoB (PH-2609/DESKTOP-OL5F85I/192.168.118.99/Hyomo-<1d0de175109863cc>) Cc:
CCI (PH-2609/DESKTOP-SGVO3K2/192.168.118.92/Hiroshi-<5bdedaf36020f4e9>) Cc: Fly
Snake (PH-2609/DESKTOP-5S7ORM9/192.168.118.104/Dream
Catcher-<6428b18478aa9d85>) Cc: James Bond
(PH-2609/DESKTOP-0VMTBN6/192.168.118.105/James-<30933829c6e2c559>) Cc:
KasperSky
(PH-2609/DESKTOP-9FR0A4K/192.168.118.109/KasperSky-<2839fd76f5c982ad>) Cc:
Sharplancer
(PH-2609/DESKTOP-642O6TT/192.168.118.114/sharplancer-<ef71f746b1fc90db>) Cc:
Superman (PH-2609/DESKTOP-FMO1KQQ/192.168.118.103/Superman-<5f07eb5f610ab952>)
Cc: Yamato (PH-2609/DESKTOP-VMP50UI/192.168.118.107/Dracula-<a4d3d90925f8dbb9>)
at Tue Jul 11 20:20:00 2023 ------------------------------------
```

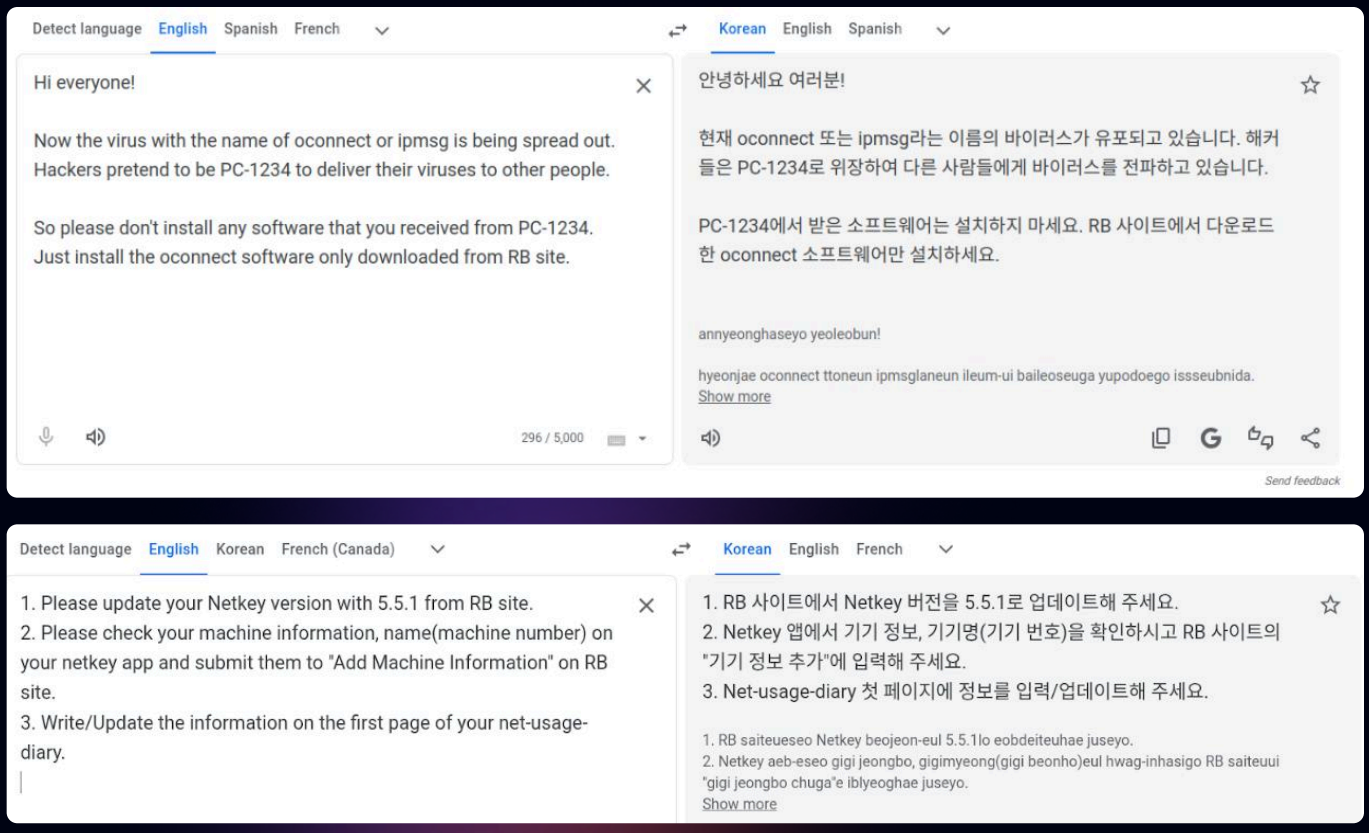
Given the string Jockey (PH-2609/DESKTOP-5K4B423/192.168.118.98/Jockey-<2b1a7b2c17d18477>) as an example, the formatting on IP Messenger messages is as follows:

Jockey is the IP Messenger username,
PH-2609 is the group chat name,
DESKTOP-5K4B423 is the hostname of the user's computer,
192.168.118.98 is the user's internal IP,
Jockey-<2b1a7b2c17d18477> is the Windows username, plus a unique conversation identifier.

Based on the analysis of available IP Messenger logs, we assess that IP Messenger is used for internal communication between IT workers and teams, seemingly across multiple departments of the DPRK party-state. IP Messenger itself is not specific to North Korean IT workers, nor is it a reliable indicator of NKITW operations, but it has been consistently seen in the list of installed software on devices belonging to DPRK operatives.

## RB Site

From an observed Google Translate entry, a message was found translated from English to Korean, warning users to download IPMsg and OConnect from legitimate sources due to an ongoing malware campaign. The message advises users to install OConnect from the RB site, in which we observed RB in the file path of an OConnect/NetKey binary: C:\Program Files (x86)\rb corp\oconnect 5\NetKey.exe, and to update their machine information.




Translated messages regarding downloading software from the RB site, and adding machine information.

We observed users accessing a web page titled Add Machine Info, with the following URL:

http://192[.]168.109.2/machine_info_new

This internal IP shows up consistently in almost all available data analysed. We assess that this is the “RB Site” referenced, and is a back-office management UI to track IT work, update infrastructure, and download software updates. The following URLs and page titles have been seen at that internal IP address:

| URL | Title |
|---|---|
| http://192[.]168.109.2/ | HOME |
| http://192[.]168.109.2/login | Login |
| http://192[.]168.109.2/machine_info_new | Add Machine Info |
| http://192[.]168.109.2/machine_info | Machine Info |
| http://192[.]168.109.2/network_reports | Network Report |
| http://192[.]168.109.2/payment | PAYMENT ADDRESS |
| http://192[.]168.109.2/blocked_urls | URLS |
| http://192[.]168.109.2/user | (No Title Provided) |

## NetkeyRegister Site

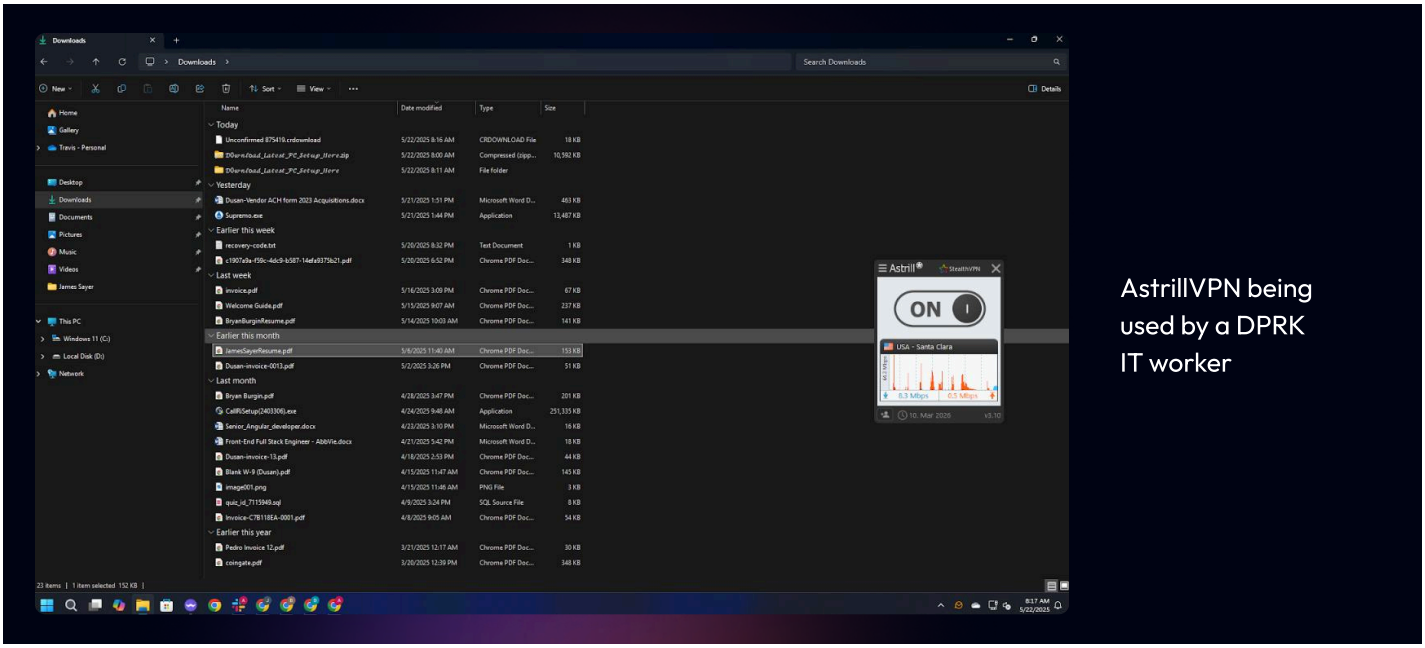
Another entry repeatedly observed on some systems is a website with an internal IP 172[.]20.100.7, the title “NetkeyRegister,” as well as numerous autofill entries for netkey_id. It is possible that NetKey/OConnect are required to connect to the internal network within which these sites are hosted. The following URLs were observed:

http://172[.]20.100.7:8000/login
http://172[.]20.100.7:8000/change-password
http://172[.]20.100.7:8000/upload
http://172[.]20.100.7:8000/register
http://172[.]20.100.7:8000/register-port
http://172[.]20.100.7:8000/register-service
http://172[.]20.100.7:8000/register-form?netkey_id=*******

## VPN Software & Piracy

Aside from NetKey/OConnect, which seemingly allow IT workers to connect to internal DPRK-run networks, the IT workers also need a way to get a North American or European IP address. Since they are usually based in North Korea, China, or Russia, it is often necessary to use a commercial VPN to bypass domestic internet restrictions, or to appear as a westerner with a western IP.

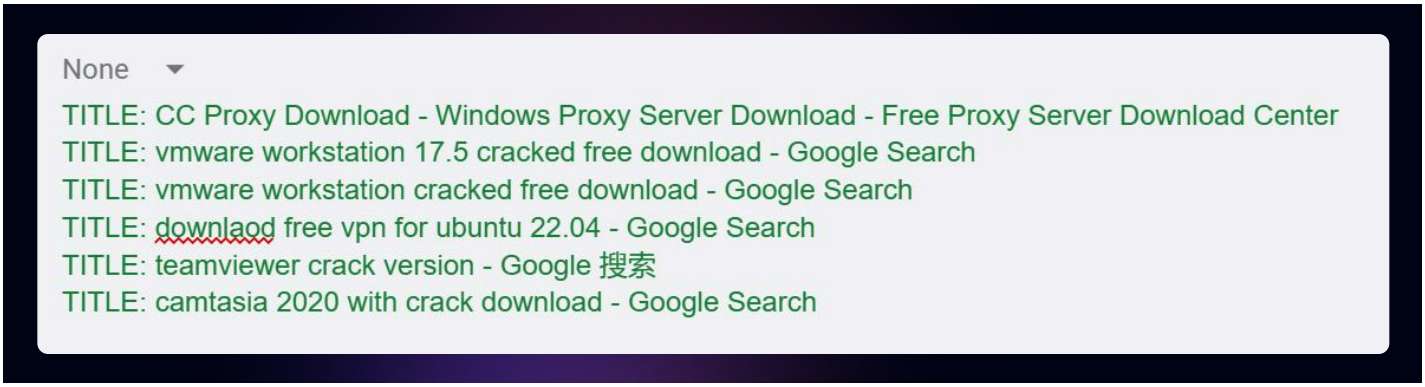
Research indicates that North Korean IT workers frequently use commercial VPN services, most notably Astrill VPN, as seen in the following image. These services allow them to align with the purported country of origin associated with their online personas, thereby supporting their cover identities in freelancing or remote work platforms.




AstrillVPN being used by a DPRK IT worker

However, analyzed data from other likely DPRK-controlled systems reveals a trend of searching for pirated software, including queries such as “free proxy” and “free VPN,” which are often downloaded from less than reputable sites.

Queries observed:




## North Korea Affiliated Websites

Analyzed data indicates direct visits to North Korean .kp domains, and in some instances included reading local North Korean news sites. Additionally, some .kp domains visited did not resolve to publicly accessible IP addresses, potentially suggesting access to internal North Korean networks.

We observed the following North Korean websites within available data:

- mfa.gov[.]kp
- vok.rep[.]kp
- gnu.rep[.]kp
- pt.net[.]kp
- pic.co[.]kp
- rodong.rep[.]kp
- kcna[.]kp
- airkoryo[.]kp
- naenara.com[.]kp
- star[.]kp

## Mitigation Strategies

Unlike traditional threat actors, defending an organization from North Korean IT worker infiltration is not solely the domain of security teams, but rather a joint effort between human resources, security operations, hiring managers, and interviewers. All parties involved in the hiring and onboarding process can threat-hunt for DPRK-affiliated operators. The appendices following this report contain indicators of compromise such as email addresses, visited URLs, and installed software known to be associated with NKITW, which can be used to identify job applicants or employees potentially aligned with the DPRK.

During the interview and onboarding process, extensive identity verification and background checks are important in general, but especially when dealing with DPRK-affiliated operators engaged in identity fraud. Exercise vigilance in video calls. Look for signs of fake backgrounds, AI face changers, or AI voice changers. When a western collaborator is involved, it is easier for the worker to bypass traditional vetting procedures. Doing an interview, laptop pickup, or onboarding on-site and in-person would greatly mitigate the risk of infiltration by DPRK operatives fronted by western collaborators, provided the advertised role is specific to a geographic location. Western collaborators may not in fact reside in the place they claim to reside, and might not be able or willing to meet in-person. Treat seriously any discrepancies between the resume and what the candidate says in interviews, for example what languages they claim to be able to speak, what skills they purport to possess, and where they claim to reside.

After hiring and onboarding, look for noticeable differences between their spoken and written communication, or between their communication style during the interview process and during employment. Watch for suspicious VPN, proxy, or remote access software installed on workstations. Check for the presence of DPRK-specific tools such as NetKey or OConnect, or access to the aforementioned RB Site and NetkeyRegister web pages. Engage with remote employees frequently, get on calls with them and get to know them. DPRK IT workers may quit if they have to meet face-to-face in video calls too often.

## Conclusion

North Korea's IT worker operations are widespread and deeply integrated within the DPRK party-state. It is an integral component in the DPRK's revenue-generation and sanctions-evasion machinery. With an intimate knowledge of their operations, tools, motivations, and goals, organizations can know what to look for and prevent infiltration from operators.

When interviewers, managers, and human resources have a close relationship with candidates and employees, it is more difficult for North Korean IT workers to gain a foothold in an organization. NKITW thrive in environments of disengagement and neglect, and will shy away from roles where it is clear they will have close relationships with others in the organization. With the help of western collaborators, North Korean operatives have more capability to bypass traditional vetting processes such as identity verification and background checks, but by building a personal relationship with candidates from day one, the warning signs can be detected early, and the level of personal engagement can make an infiltration attempt infeasible for the operative and the collaborator.

Because the deployment of IT workers has been so lucrative for the DPRK, the tactics of IT worker teams continue to evolve to ensure their continued success. This report has given a snapshot of their techniques to date, but with the dearth of new reports released about their operations, they will continue to adapt their methodologies to avoid detection.

# Appendix A: Email Indicators

The following is a list of email addresses known to be controlled by DPRK-affiliated IT workers, facilitators, or collaborators. Human resources, hiring managers, and interviewers can reference this list of emails when communicating with candidates, and security teams can look in employee device logs to check for access to these accounts' inboxes. This is not an exhaustive list.

hotaruemori@gmail.com
veerapandianvijai@gmail.com
akijohansson116@gmail.com
paulmillet0803@gmail.com
henryan373@gmail.com
wulong.sky@gmail.com
saburo.snow@gmail.com
stanleyc.sky@gmail.com
longx695@gmail.com
dragonfighter0120@gmail.com
garciav.dev@gmail.com
m.in.space45@gmail.com
derek.otieno.2020@gmail.com
usmanjaggi1@gmail.com
mr.martin.adrian@gmail.com
kalezhang000@gmail.com
what.a.fabulous1@gmail.com
tinydever@gmail.com
dashhello4@gmail.com
simonbergman516@gmail.com
robertgreen1217@gmail.com
ashleyspalliero408@gmail.com
jackkarlsson1025@gmail.com
adambinharun1010@gmail.com
minamotohitoshi912@gmail.com
muhammadhamid4760@gmail.com
scott.brown0629@gmail.com
scott.brown00629@gmail.com
guzmandelfino1992@gmail.com
codelover111@gmail.com
alexnikolaos007@gmail.com
botofprince@gmail.com
jaggiusman@gmail.com
boava94722@gmail.com
rabbitking0130@gmail.com
bengrantsoft@gmail.com
sotaro.yoshimoto@gmail.com
proguardseo@gmail.com
justin424w@gmail.com
satoshi.fukuzumi309@gmail.com
martinjosipovic17@gmail.com
venturewell@gmail.com
satoshi.fukuzumi47@gmail.com
blocklimax@gmail.com
dcnc336@gmail.com
myronenkoyaroslav4@gmail.com
avoroy@biztechadvisors.com
katelevsk@gmail.com
savonik.alina00@gmail.com
purplestrawberrymilk@gmail.com
yellowstrawberrymilk@gmail.com
bluestrawberrymilk1025@gmail.com
pinkstrawberrymilk1025@gmail.com
luis.gamez1004@gmail.com
cliff.luo226@gmail.com
semochkomaksym@gmail.com
sun.james1025@gmail.com
coolguy.arber09@gmail.com
arber.berisha995@gmail.com
arber.berisha009@gmail.com
millionsapphire@outlook.com
derekdev2023@outlook.com
garciav.dev@gmail.com
dragonfighter0115@outlook.com
fullstackdev1006@gmail.com
blockchaindev0227@gmail.com
sotaro.yoshimoto@gmail.com
super.dev1124@outlook.com
justin309w@outlook.com
proguardseo@gmail.com
azduoedon@outlook.com
supernova1111a@outlook.com
myronenkoyaroslav4@gmail.com
savonik.alina00@gmail.com
blacktigerbusinesswork@outlook.com
nick2022lane@gmail.com
yellowstrawberrymilk@gmail.com
autumnhappyfamily@gmail.com
blue621dream@gmail.com
james.jenaty031@gmail.com
quangtu676957e1525ncz@hotmail.com
danhphoze_2364@hotmail.com
hangquan5594sxbf72@hotmail.com
mahamaslam805@gmail.com
adamvenord8@gmail.com

# Appendix B: Software Indicators

The following software versions have been observed in the list of installed software on user systems, which are reliable indicators of DPRK-affiliated activity. Security teams can search for these strings on employee devices.

| | | | |
|---|---|---|---|
| NetKey 4.1 | NetKey 5.1 | OConnect 5.5 | OConnect 5.9.3 |
| NetKey 5.0 | OConnect 5.3 | OConnect 5.7 | OConnect 6.0.0 |

Use of AstrillVPN and IP Messenger are not reliable indicators of North Korean IT worker activity in and of themselves, but combined with other behaviour patterns, their presence can be motivation to investigate further.

```
NetKey.exe
OConnect.exe
C:\Program Files (x86)\STN Corp\OConnect 5.7\OConnect.exe
C:\Program Files (x86)\STN Corp\OConnect 6.0.0\OConnect.exe
C:\Program Files (x86)\rb corp\oconnect 5\NetKey.exe
```

Use of AstrillVPN and IP Messenger are not reliable indicators of North Korean IT worker activity in and of themselves, but combined with other behaviour patterns, their presence can be motivation to investigate further.

The following running processes were detected on devices used by North Korean IT workers, which are reliable indicators of North Korean IT worker activity:

```
OConnect.exe
C:\Program Files (x86)\STN Corp\OConnect 5.7\OConnect.exe
C:\Program Files (x86)\STN Corp\OConnect 6.0.0\OConnect.exe
C:\Program Files (x86)\rb corp\oconnect 5\NetKey.exe
```

# Appendix C: URL Indicators

The following URLs are associated with internal back-office web platforms specific to North Korean IT worker operations. The IP addresses in the URLs are internal, and are not by themselves reliable indicators of DPRK activity, but combined with one of the URL paths and/or page titles below, their presence in employee device logs should prompt immediate investigation.

| URL | Flare Use Case |
|---|---|
| http://192[.]168.109.2/ | HOME |
| http://192[.]168.109.2/login | Login |
| http://192[.]168.109.2/machine_info_new | Add Machine Info |
| http://192[.]168.109.2/machine_info | Machine Info |
| http://192[.]168.109.2/network_reports | Network Report |
| http://192[.]168.109.2/payment | PAYMENT ADDRESS |
| http://192[.]168.109.2/blocked_urls | URLS |
| http://192[.]168.109.2/user | (No Title Provided) |
| http://172[.]20.100.7:8000/login | (No Title Provided) |
| http://172[.]20.100.7:8000/change-password | (No Title Provided) |
| http://172[.]20.100.7:8000/upload | (No Title Provided) |
| http://172[.]20.100.7:8000/register | (No Title Provided) |
| http://172[.]20.100.7:8000/register-port | (No Title Provided) |
| http://172[.]20.100.7:8000/register-service | (No Title Provided) |