TLP:CLEAR

North Korea IT Worker Threat Report:

Threat Overview and Mitigation

10 July 2025

This report is a collaboration that incorporates analysis from several leading Information Sharing and Analysis Centers (ISACs), including Crypto ISAC, Oil and Natural Energy ISAC (ONE-ISAC), Real Estate ISAC, Tribal ISAC, WaterISAC, the Faith-Based Information Sharing and Analysis Organization (ISAO), and Gate 15.

INTRODUCTION

Over the last few months, there has been much reporting on threats relating to remote North Korean IT workers. Some critical infrastructure sectors, as well as other communities, experienced this threat directly, with a variety of impacts. Different communities have not yet directly observed this threat, but they are still strongly encouraged to understand it and consider the recommendations in this report. In addition, through conversations the authors and contributors of this report have had with security partners, private sector entities, and U.S. government partners, we believe that most organizations do not fully appreciate the extent of this threat. We are sharing this report to encourage leaders to pause, take the time to understand the threat, consider the mitigation guidance, and have the appropriate conversations with members across their organizations to educate them and collaborate with them to reduce the risk from this relatively new but likely enduring threat.

OVERVIEW

At the end of June, the Justice Department announced a coordinated action against the Democratic People's Republic of North Korea (DPRK) government's schemes to fund its regime through remote information technology (IT) work for U.S. companies. This action included two indictments, an arrest, searches of 29 known or suspected "laptop farms" across 16 states, the seizure of 29 financial accounts used to launder illicit funds, and the shutdown of 21 fraudulent websites. On 08 July, the Justice Department imposed added sanctions. Individuals from the United States, China, the United Arab Emirates, and Taiwan contributed to these efforts, resulting in employment with over 100 U.S. companies.

This threat represents a significant disruption, but hardly the end, to a multi-year threat to companies worldwide. In June 2022, the United States Government (USG) issued an advisory calling attention to an emerging risk and to understand better and guard against inadvertent recruitment, hiring, and facilitation of Democratic People's Republic of Korea, hereinafter referred to as North Korea, information technology (IT) workers. Through this work, threat actors connected directly and indirectly to North Korea waged a campaign to generate wealth and steal intellectual property and data at the expense of companies around the world, and across all industries.

These activities were designed to infiltrate companies through legitimate job postings, enabling the regime to benefit from several billion dollars in revenue and to circumvent sanctions and international laws. In 2022, it was estimated that thousands of workers had been dispatched and had already penetrated many organizations.

Over the past several years, public and private sector organizations have been identifying and mitigating risks associated with this campaign. However, the tactics continue to evolve as more visibility and insight into this campaign are uncovered and shared publicly.

This report incorporates analysis from Gate 15, several leading Information Sharing and Analysis Centers (ISACs), and the Faith-Based Information Sharing and Analysis Organization (ISAO). Specifically, this report will:

- Outline the common indicators
- Evaluate tactics that may be employed
- Identify potential targets and how the risk can manifest within those areas
- Provide mitigation activities that organizations can consider to reduce the risk to their organization

The scam campaign is designed to gain employment at an organization for two distinct purposes:

1. To get paid as a freelance / contract worker, which will generate revenue for North Korean programs. This tactic involves using pseudonymous email, social media, payment platform, and online job site accounts, as well as false websites, proxy computers, and witting and unwitting third parties located in the United States and elsewhere.
2. While some workers may complete activities to earn a paycheck, they may also use their access to the organization's network to collect sensitive or proprietary information, which they can later use to extort the company.

At times, the two actions above work together. Earlier this year, the FBI published a Public Service Announcement Alert Number: I-012325-PSA: North Korean IT Workers Conducting Data Extortion, which noted that "After being discovered on company networks, North Korean IT workers have extorted victims by holding stolen proprietary data and code hostage until the companies meet ransom demands." They have even publicly released the proprietary code of victim companies. To do this, they often copy company code repositories, such as GitHub, to their own user profiles and personal cloud accounts. They may also attempt to harvest sensitive company credentials and session cookies to initiate work sessions from non-company devices, thereby creating further compromise opportunities. For more details about North Korea's use of this scheme beyond the above purposes, the security company DTEX conducted a deep dive into the motivations behind the campaign. Similarly, Microsoft published a report late last month on its constantly evolving tactics.

These schemes involve a significant number of logistical support activities, which, in turn, can be indicators for identifying the scheme and will be detailed in a section below. A 2024 indictment reveals that a U.S. citizen in Tennessee was arrested for participating in a scheme to obtain remote employment with American and British companies for these IT workers, highlighting the extent of these infiltrations.

- **The use of fraudulent identities.** These identities could be stolen or purposed from various dark web sites or access brokers.
- **Laptop farms.** These are locations where the hiring company would ship laptops and other equipment for the new hire to do work-related activities. However, as described in the indictment above, the threat groups would log on to the shipped laptop, download and install unauthorized remote desktop applications, and access the victim companies' networks, causing damage to the computers. The remote desktop applications enabled the North Korean IT workers to work from locations in China, while appearing to the victim companies that they were working from other residences.
- **Use of third parties.** As more organizations and government agencies assess the risk to their operations and closely scrutinize applicants, these schemes are attempting to gain access to the target organization through contract positions, where the third party may not undergo the same level of scrutiny. Therefore, the organization's process must ensure that any third party has stringent hiring practices in place.

KEY INDICATORS

Several indicators can alert an organization to risks posed by these workers within their environment.

Employee Profile or Background Information

- Inconsistent or changing name spelling, nationality, location, contact information, education, work history, and online presence.
- Refusal to appear on camera, conduct video interviews or meetings (favoring text-based chat).
- Initially, offer free services to establish trust and secure long-term contracts.
- False claims of previous employment to solicit employment.

- The biographical information provided does not match the applicant's details.
- Indications of cheating on coding tests or when conducting interviews.
- The online presence does not align with the hired worker's resume—multiple online profiles with different pictures, or online profiles with no pictures at all.
- Request individuals with a native or high level of English to conduct video and phone interviews with prospective employers and/or clients on their behalf.
- Request hardware to be sent to an address not listed on the IT worker's ID documentation.
- Claim inability to receive items at the address on ID documentation.

Work Performance

- Failure to complete project tasks.
- Refusal to appear on camera, conduct video interviews or meetings (favoring text-based chat).
- Request prepayment, but do not meet project benchmarks or attend check-in meetings.
- Inconsistencies when they appear on camera (time, location, or appearance).
- Prefers remote working arrangements.
- Multiple logins into one account from various IP addresses in a short time.
- Logins into multiple accounts on the same platform from a single IP address.
- Logged into account continuously for 1+ days (mouse jiggler or coffee cupping).
- Ask co-workers to borrow personal information to obtain other contracts.
- Propose collaboration on development projects with non-DPRK freelancers.
- Ask to be contacted directly via social media or messaging applications.
- Operate outside declared business hours.
- Not reachable on time.
- May recommend other individuals for open positions, especially within 3–6 months of employment.

Payments

- Request to be paid into an account using someone else's name.
- The IT worker's bank account is either blocked or not accepting payments.
- The IT worker needs to switch bank accounts.
- Payments are made to bank accounts based in China.
- Request to be paid in cryptocurrency.
- Seek out web3, blockchain, smart contracts, and cryptocurrency projects

SECTOR/INDUSTRY IMPACT

The following section describes how this threat may impact specific sectors or industries and how it may manifest within those communities.

Commercial Facilities. While there is no public evidence that North Korean IT workers have directly infiltrated the Commercial Facilities (CF) Sector, building owners and operators still face credible risk. In today's smart, multi-tenant environments, their exposure extends beyond their systems. The growing reliance on shared infrastructure—paired with tenants in high-risk industries such as healthcare, finance, defense, or technology—means that a compromise elsewhere in the building can have direct consequences for the operator.

Shared platforms such as building management systems (BMS), HVAC, badge access, and elevators are often network-connected and may rely on overlapping IT infrastructure or cloud services. If a tenant's breach leads to lateral movement — whether through shared VPNs, unsecured APIs, or remote desktop tools — attackers could potentially pivot into operational technology (OT) environments. While there is no public confirmation, this type of adjacent risk is increasingly relevant in buildings with smart IoT deployments, co-located IT closets, or hybrid digital-physical services.

Building owners and operators can recognize that their systems, such as BMS, access control, HVAC, and surveillance, are increasingly exposed to remote access threats. These platforms often rely on cloud connectivity, third-party integrations, and remote maintenance, creating potential entry points for deceptive actors. If compromised, the operational, financial, and reputational impacts can be severe, ranging from service outages to regulatory consequences resulting from the misuse of data or systems.

Given these risks, the DPRK IT worker threat underscores the need for rigorous cyber hygiene within building operations. Owners should implement strict network segmentation across BMS and administrative systems, require robust identity verification for remote access vendors, and maintain active monitoring of all third-party integrations. When conducting threat assessments, operators must also consider external factors, such as the nature of service providers, contractors, or occupants, that may increase the facility's risk profile. These assessments should address both cyber and physical vulnerabilities and be grounded in precise controls, incident response plans, and continuous oversight.

Crypto Assets & Blockchain. In many cases, DPRK operatives obtain roles with access to DevOps tools, backend services, or blockchain infrastructure by using fake or stolen identities. This access enables them to insert malicious code, siphon credentials, or quietly redirect assets, often without raising immediate red flags.

North Korean operatives employ tactics that are effective across various industries, but they find success in the crypto sector due to its remote and distributed nature. They turn off webcams during interviews, route traffic through VPNs or virtual desktops, and mimic legitimate development activity to blend in. Many users stole or purchased freelance accounts—sometimes with verified work histories—to bypass onboarding scrutiny. In some cases, they have employed multi-factor authentication (MFA) fatigue attacks to break into accounts without triggering alarms. Exchanges like Kraken have flagged DPRK-affiliated contractors using behavioral analytics, demonstrating that well-instrumented teams can surface anomalies in session behavior, repo activity, or code deployment patterns.

What makes these actors especially difficult to detect is that they are not exploiting zero-days or brute-forcing firewalls—they are exploiting trust. Once hired, they typically fulfill tasks like any other contributor, using their access to learn internal workflows and map out escalation paths. In decentralized projects, they may rotate between roles or identities, often subcontracting work to others or switching accounts mid-engagement. Because many firms lack full-session monitoring or enforce minimal access control for non-employees, the door stays open longer than it should, giving these operatives time to embed, observe, and eventually extract sensitive keys, credentials, or backend access.

Beyond direct theft, DPRK-linked operatives use their access to manipulate internal processes, siphon sensitive data, and deploy ransomware or extortion schemes leveraging stolen information. These activities disrupt operations and undermine trust in crypto platforms, which are highly dependent on reputation and transparency. Reports indicate coordination with ransomware gangs, expanding the threat beyond asset theft to encompass broader cybercrime collaboration that exploits cryptocurrency as both a target and a tool.

As a result, Crypto organizations can prioritize stringent identity verification, continuous monitoring of remote access behaviors, and comprehensive third-party risk management to mitigate this evolving threat. Incident response plans should anticipate scenarios involving insider threats originating from remote hires. The DPRK remote IT job scam exemplifies a strategic approach to cybercrime that targets the unique operational models of the cryptocurrency industry, underscoring the critical need for sector-specific defenses that are grounded in both technical controls and workforce vigilance.

Energy (Oil, Gas, Electricity). Unauthorized access to SCADA/ICS software, malware insertion via remote IT roles, industrial espionage, and DDoS to disrupt supply. Workers with suspected links to the Democratic People's Republic of Korea have applied for remote jobs within the electric utilities sector. These roles included Data Scientist, Software Engineer, Business Intelligence Engineer, Stack Engineer, and Data Engineer, and typically require high-level access, including administrative access. Due to these observed potential threats, the energy sector has an increased risk of being targeted again in the future.

Faith-Based Organizations. Faith-Based Organizations (FBOs) currently face limited direct exposure to the DPRK remote IT job scam, primarily due to their typical hiring practices. Most FBOs do not regularly employ remote IT contractors or outsource technical roles through online marketplaces – factors that significantly reduce the likelihood of unknowingly hiring a North Korean operative under a false identity. As a result, the assessment indicates that the immediate threat of DPRK-affiliated remote workers gaining access to sensitive systems within FBOs is low.

However, the tactics employed in the broader DPRK remote work campaigns, such as the use of false identities, resume fraud, and evasion of in-person verification, highlight a general risk relevant to all sectors, including FBOs: the potential for insider threats. Even if state-backed actors are unlikely to target FBOs directly, similar techniques could be adopted by opportunistic individuals seeking to gain physical access or employment to steal equipment, misappropriate funds, or access sensitive information. In smaller or resource-constrained organizations, particularly those with limited personnel screening or IT oversight, such risks may often go undetected.

For FBOs, the key takeaway is awareness rather than alarm. Organizations can stay informed about impersonation and social engineering tactics being used in other sectors and consider implementing basic safeguards, such as conducting background checks, maintaining clear IT asset inventories, and implementing stricter controls around staff access, particularly for facilities that manage donation systems, livestreaming equipment, or member data. While they are not primary targets of DPRK campaigns, FBOs can view these threats as case studies in how insider tactics can evolve and migrate across sectors.

Tribal Organizations. At first blush, it may seem far-fetched for tribal entities to be concerned about the threat of Democratic People's Republic of Korea (DPRK) IT workers infiltrating their organizations. However, given the penchant for financial gain, DPRK has demonstrated an interest in exploiting gaming over the years, including a recent attack against a Canadian online gaming provider. While it is likely fair to say that tribes are ultimately less likely to hire someone in a geographically disparate location (especially overseas), DPRK IT workers have demonstrated themselves to be adaptable, tailoring their approach to suit the needs of the regime. This flexible behavior has eluded other organizations, thus giving these actors initial access to targeted companies. Additionally, tribes may be potentially impacted by the abuse of grant / data systems, member records, and financial payments. Most tribal organizations maintain a cross-sector presence, and some of those areas are addressed elsewhere in this report.

Water. Insider threats continue to pose a persistent threat to the water and wastewater sector. Furthermore, this campaign underscores the growing security threat that hostile nation states – Russia, China, Iran, and North Korea – pose to critical infrastructure organizations.

WaterISAC has reported in past assessments that rising geopolitical tensions between the U.S. and these adversarial states, coupled with their growing cooperation across multiple domains, have increased the risk to critical infrastructure organizations of being targeted by these hostile states. Moreover, due to these dynamics, the potential for adversarial nation-states to recruit, coerce, manipulate, or, in this case, plant insiders at critical infrastructure organizations to facilitate malicious activity is an increasing concern.

Regarding the North Korean IT worker threat, WaterISAC has not tracked any instances of them attempting to gain employment in the water and wastewater sector. Still, the current geopolitical landscape necessitates contingent preparedness by the water sector. WaterISAC has tracked cases of remote IT workers suspected of operating on behalf of North Korea who have applied for jobs at electric utilities in North America.

Based on past cases, the IT Workers applied for jobs designated as "remote" and are technology-focused, including, but not limited to, Data Scientist, Software Engineer, Business Intelligence Engineer, Stack Engineer, and Data Engineer. The job roles and responsibilities typically require high-level access, including administrative access to execute the job requirements. Given that these threat actors have attempted to gain employment at electric utilities, it is likely they would also seek to gain fraudulent employment at water and wastewater utilities.

Lastly, it is essential to understand the evolving tactics of these threat actors and their potential impact on an organization. These IT workers continue to adopt new tactics to gain access to organizations across the 16 critical infrastructure sectors. Potential impacts to an organization could include a data breach of sensitive information, the installation of malicious and rogue software, persistent unauthorized remote access, or potentially operational disruptions.

MITIGATION STRATEGIES

The North Korean IT Worker scheme implementation is unique, but the application is simply an exploitation of weaknesses within an organization's hiring practices. Similar to phishing scams, this tactic employs a "shotgun approach," allowing fictitious IT workers to apply for numerous jobs across various industries and worldwide. It is a low-risk, high-reward proposition for them, and the reward over the years has been remarkably high. One security expert noted that they had seen personas associated with this scheme in up to 90% of some companies' open job postings.

Bottom Line. Organizations are encouraged to conduct an end-to-end review of their employee population and their applicants (pending or previously applied) to assess the risk within the organization. Using the indicators above and the strategies below, organizations can quickly understand the impact, if any, and ultimately strengthen their processes against this threat or others.

Build or enhance your insider risk-management program. Build or enhance your insider risk-management program. Organizations that do not have a dedicated group to identify, monitor, prevent, and respond to insider threat risk should strongly consider a risk management program. Having a program with a comprehensive strategy, transparent governance and policies, standardizing incident response actions, and providing employee training to foster a security-conscious culture can create the conditions to mitigate this type of risk, as well as others.

- If your organization already has an insider risk program, it can utilize the indicators above to analyze similar types of information and establish processes and procedures that strengthen detection and monitoring platforms for key indicators. This analysis will enable the assessment of current risk levels and inform the enhancement of existing processes and procedures.
- In addition, insider threat/risk programs can collaborate with detection and monitoring groups to incorporate these tactics and indicators into monitoring rules or requirements, thereby identifying data exfiltration events or incidents, as well as unusual access activity.

Strengthen hiring practices. This scheme attempts to exploit poor hiring and background screening processes.

- Deploy stringent background checks, in-person or on-camera interviews, and vigilant job-history / resume vetting can all help mitigate this risk. Some best practices include:

  - Implement identity-verification processes during the interviewing, onboarding, and employment of any remote worker.
  - Require notarized proof of identity before employment.
  - Whenever possible, fingerprinting/biometrics should be used.
- Cross-check HR systems for other applicants with the duplicate resume content and/or contact information. The FBI has observed that these workers are using artificial intelligence and face-swapping technology during video job interviews to obfuscate their true identities.
- Educate HR staff, hiring managers, and development teams regarding the North Korean IT worker threat, explicitly focusing on changes in address or payment platforms during the onboarding process.
- Review each applicant's communication accounts, as North Korean IT workers have reused phone numbers (particularly voice-over-IP numbers) and email addresses on multiple resumes purportedly belonging to different applicants.
- Use "soft" interview questions to ask applicants for specific details about their location or educational background. North Korean IT workers often claim to have attended non-US educational institutions.
- Check applicant resumes for typos and unusual nomenclature.
- Avoid payments in cryptocurrency and require verification of banking information corresponding to other identifying documents.
- Be suspicious if an applicant cannot receive items at the address on their identification documentation.

Post-hiring practices

- Enable the geolocation feature and verify that the corporate laptop is at the location shipped to.
  - Compare the identity and location of remote workers, including being cautious if the worker suddenly suggests a different shipping address, and requiring in-person device pickup whenever possible.
  - There have been observed instances where a deployed corporate laptop was never geolocated in the location that the individual reported as their residence.
  - Such examples could be evidence of a laptop farm.
- After the equipment has been shipped and received, request verification of the serial number. This information should be readily available for anyone with physical possession of a corporate device.
- Use hardware-based multi-factor authentication to enforce physical access to corporate devices.
- Watch for low engagement across emails, messaging, and meetings.

Access and Monitoring Practices

- Practice the Principle of Least Privilege on networks, to include deactivating local administrator accounts and limiting privileges for installing remote desktop applications.
- Monitor and investigate unusual network traffic, including remote connections to devices, as well as the installation and presence of prohibited remote desktop protocols or software. North Korean IT workers often have multiple logins into a single account within a short period, from various IP addresses frequently associated with different countries.
- Monitor network logs and browser session activity to identify data exfiltration through easily accessible means such as shared drives, cloud accounts, and private code repositories.
- Monitor endpoints for the use of software that enables multiple audio and video calls to occur concurrently.
  - Monitor for the use of "mouse jiggling" software, which we have observed North Korean IT workers using to remain active across several laptops and profiles.
  - Monitor and restrict the use of IP-based KVM devices, which North Korean IT workers have frequently utilized to maintain persistent remote access to corporate devices.
- Monitor and restrict the use of remote administration tools:
  - Prevent any remote connections to company-issued computers that can access the corporate network.
  - Monitor for uncommon remote administration tools and multiple remote administration tools installed on a single device.
  - Monitor the use of VPN services to connect to corporate infrastructure, including the IP addresses associated with these services.
- Consider enhanced monitoring for all new hires and remote workers. Such monitoring can include behavioral analytics and user activity monitoring tools. This approach can help identify anomalies, particularly around privilege elevation, and promote a layered and proactive security posture.

ADDITIONAL REFERENCES

1. DTEX: Exposing DPRK: Nation-State Threat Actors
2. Google: DPRK IT Workers Expanding in Scope and Scale, April 1, 2025
3. U.S. Treasury: Publication of North Korea Information Technology Workers Advisory
4. Unit 42: Global Companies Are Unknowingly Paying North Koreans: Here's How to Catch Them, November 13, 2024
5. Recorded Future: Inside the Scam: North Korea's IT Worker Threat, February 13, 2025
6. IC3 PSA: North Korea Aggressively Targeting Crypto Industry with Well-Disguised Social Engineering Attacks, September 3, 2024
7. Sentinel One: A Network of Active Front Companies and Their Links to China, November 24, 2024
8. Reliaquest: Red Flags for Red Star Hackers: Hunting for North Korean Insiders, May 8, 2025
9. Axios: OpenAI blocks ChatGPT accounts linked to North Korean IT worker fraud, June 5, 2025
10. DOJ: Department Files Civil Forfeiture Complaint Against More Than $7.74 Million Laundered on Behalf of the North Korean Government, June 5, 2025
11. TRM: DOJ Seeks Forfeiture of $7.7 Million in Cryptocurrency Tied to North Korean IT Worker Laundering Network, June 5, 2025
12. Infosecurity Magazine: New Fortinet and Ivanti Zero Days Exploited in the Wild, May 14, 2025
13. Dark Reading: Fortinet Zero-Day Bug May Lead to Arbitrary Code Execution, April 14, 2025
14. The Record: North Korean hackers seen collaborating with Play ransomware group, researchers say, October 30, 2024
15. The Record: North Korean IT worker scam is now a threat to all companies, cybersecurity experts say, May 1, 2025