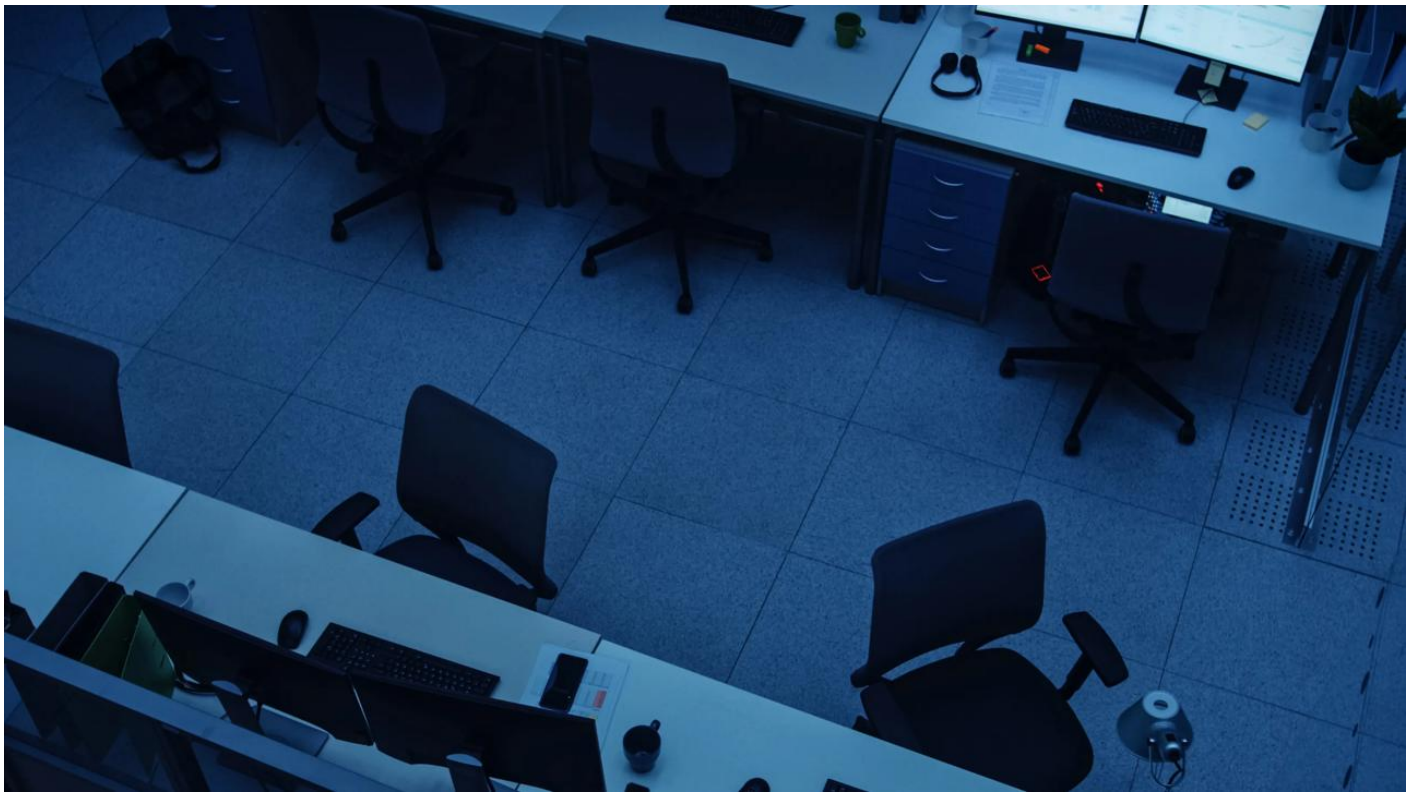
Fraudulent North Korean IT Worker Schemes: From Insider Threats to Extortion



Secureworks® Counter Threat Unit™ (CTU) researchers have observed patterns and evolutions in IT worker schemes linked to the North Korean government (officially the Democratic People's Republic of Korea (DPRK)). In these schemes, North Korean nationals use stolen or falsified identities to obtain employment with Western companies under false pretenses. This activity has been documented in the U.S., UK, and Australia.

Across numerous investigations, Secureworks incident responders identified technical and behavioral characteristics associated with these schemes. In some instances, fraudulent workers demanded ransom payments from their former employers after gaining insider access, a tactic not observed in earlier schemes. In one case, a contractor exfiltrated proprietary data almost immediately after starting employment in mid-2024 (see Figure 1). Multiple observed characteristics align with previous fraud schemes conducted by the NICKEL TAPESTRY threat group, which has historically relied on fraudulent workers to generate revenue for the North Korean regime. These funds reportedly contribute to weapons programs.

Figure 1. Progression of events. (Source: Secureworks)

A tactic documented by the U.S. Federal Bureau of Investigation (FBI) and observed by Secureworks involves fraudulent contractors requesting changes to delivery addresses for corporate laptops, often rerouting them to facilitators at laptop farms (see Figure 2). In some instances, the contractors requested permission to use a personal laptop instead of a company-issued device and displayed a strong preference for a virtual desktop infrastructure (VDI) setup. In at least one case, the corporate laptop had already been dispatched, but a request from the contractor to change the delivery address change while the device was in transit prompted the organization to cancel the shipment. This behavior aligns with NICKEL TAPESTRY tradecraft of attempting to avoid corporate laptops, potentially eliminating the need for an in-country facilitator and limiting access to forensic evidence.

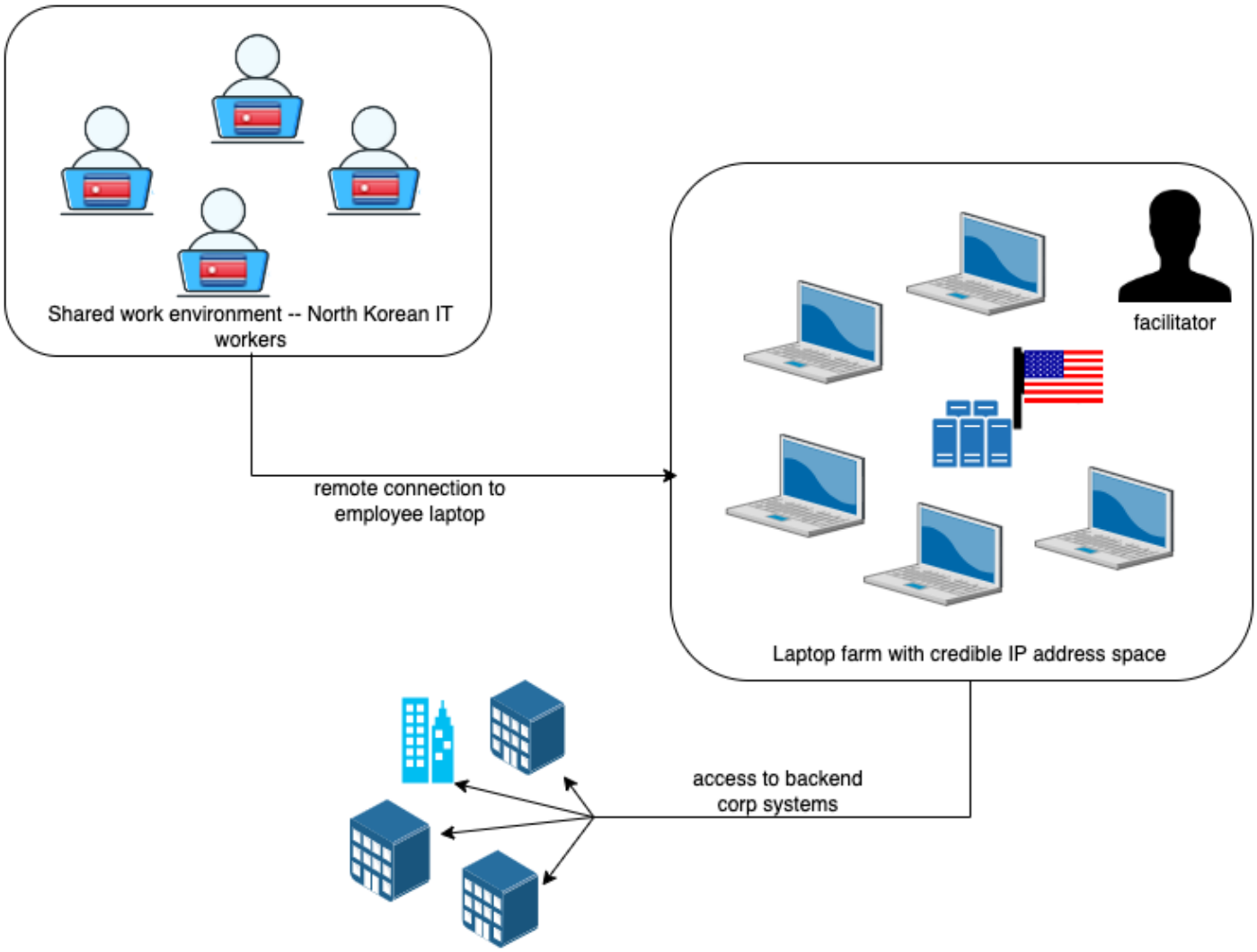


Figure 2. Laptop farm setup to hide fraudulent North Korean IT workers' location. (Source: Secureworks)

This tactic allows the contractors to use their personal laptops to remotely access the organization's network. In one case, the contractor proceeded to exfiltrate proprietary data to a personal Google Drive location via a corporate VDI solution. NICKEL TAPESTRY has accessed company data using IP addresses within Astrill VPN address space and residential proxy addresses to mask the actual source IP address used for the malicious activity. Soon after the organization terminated the contractor's employment due to poor performance, the company received a series of emails from an external Outlook email address. One of the emails included ZIP archive attachments containing proof of the stolen data, and another demanded a six-figure ransom in cryptocurrency to avoid publication of the stolen documents. Later that day, an email from a Gmail address shared a Google Drive folder containing

additional evidence of stolen data. This escalation and the behaviors listed in the FBI alert demonstrate the calculated nature of these schemes.

Secureworks incident responders have also observed the threat actors using Chrome Remote Desktop to remotely manage and access corporate systems. They also used AnyDesk for remote access, which was not typical for their assigned job duties. Analysis of AnyDesk logs in one engagement revealed connections to Astrill VPN IP addresses, indicating the application is part of NICKEL TAPESTRY's toolset.

Historically, North Korean IT workers avoided enabling video during calls when possible, even claiming to experience issues with webcams on company-issued laptops. Forensic evidence has revealed use of the free SplitCam software, which is advertised as a virtual video clone. NICKEL TAPESTRY has likely adopted SplitCam to facilitate company video calls while attempting to hide a fraudulent worker's identity and location. Based on these observations, it is highly likely that the threat group is experimenting with various methods for accommodating companies' requests to enable video on calls.

The threat actors also often demonstrate suspicious financial behavior. While employed, they will update the bank account for receiving paychecks multiple times within a brief period. CTU™ researchers have observed the use of bank accounts operated by the Payoneer Inc. digital payment service. Fraudulent North Korean IT workers commonly use these types of payment services to bypass traditional banking systems. The deceptive tactics and financial maneuvering are typical of the tradecraft in these schemes.

Many North Korean IT worker schemes also establish connections among multiple fraudulent contractors employed by the same company. Investigations have revealed links between contractors who provided references for one another, performed similar job roles, and utilized comparable resume and email formats. These individuals often adopted similar characteristics and behaviors for their personas, including rerouting deliveries and salary payments. In one engagement, several connections across multiple contractors employed by the company surfaced, with Candidate A providing a reference for a future hire (Candidate B), and another likely fraudulent contractor (Candidate C) replacing Candidate B after that contractor's termination (see Figure 3). In some instances, the same individual adopts multiple personas. In one incident, two distinct styles of writing observed in the email communications suggested that multiple individuals corresponded via the same email address. This observation indicates that North Korean IT workers are often co-located and may share jobs.

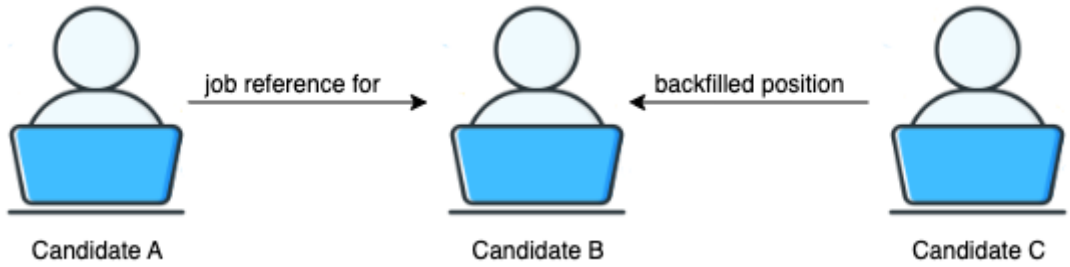


Figure 3. Example of relationships among multiple fraudulent workers employed by the same organization. (Source: Secureworks)

The emergence of ransom demands marks a notable departure from prior NICKEL TAPESTRY schemes. However, the activity observed prior to the extortion aligns with previous schemes involving North Korean workers. In addition to shared characteristics such as resume styles, address and payment changes, and

discrepancies in work history, CTU researchers observed residential proxy network infrastructure sourcing from a specific subnet used in the extortion incident and in prior fraudulent worker incidents.

In many fraudulent worker schemes, the threat actors demonstrate a financial motivation by maintaining employment and collecting a paycheck. However, the extortion incident reveals that NICKEL TAPESTRY has expanded its operations to include theft of intellectual property with the potential for additional monetary gain through extortion. This shift significantly changes the risk profile for organizations that inadvertently hire a North Korean IT worker.

Organizations should be wary of candidates for fully remote IT positions that demonstrate a majority of the following characteristics. While these characteristics are individually benign, a combination could indicate fraudulent activity and should prompt additional identity and employment eligibility checks.

- Applies for full stack developer jobs
- Claims 8-10 years of experience
- Lists 3-4 previous employers
- Often demonstrates novice to intermediate English writing and speaking skills
- Submits a resume containing elements that appear to be cloned by several applicants
- Corresponds at times of day that are unusual for their alleged location and uses varied communication styles
- Provides excuses for not enabling their camera during interviews or refuses to disable virtual backgrounds
- May sound like they are speaking from a call center environment

CTU researchers recommend that organizations thoroughly verify candidates' identities by checking documentation for consistency, including their name, nationality, contact details, and work history. Conducting in-person or video interviews and monitoring for suspicious activity (e.g., long speaking breaks) during video calls can reveal potential fraud. Organizations should be wary of candidates' requests to change their address during the onboarding process and to route paychecks to money transfer services. IT staff should restrict the use of unauthorized remote access tools and limit access to non-essential systems.

Learn more about the IT worker scheme and other North Korean threat group activity in the Secureworks 2024 State of the Threat report.

- **Tags:**
- Blog
- Research

ABOUT THE AUTHOR

The Secureworks Counter Threat Unit™ (CTU) is a dedicated threat research team that analyzes threat data across our global customer base and actively monitors the threat landscape.

MORE FROM COUNTER THREAT UNIT RESEARCH TEAM

Back to all Blogs