The North Korea worker problem is bigger than you think

By Matt Kapko

Published: 2025-03-31 · Archived: 2026-04-06 00:16:49 UTC

North Korean nationals have infiltrated businesses across the globe with a more expansive level of organization and deep-rooted access than previously thought, insider risk management firm DTEX told CyberScoop.

This swarm of technical North Korean experts isn't just intruding businesses as ad hoc freelance IT workers; they've gained full-time employment as engineers and specialists of various skill sets with the highest degree of access in enterprise systems.

"We work with a fair cross-section of the Fortune Global 2000 organizations, and right now we have active investigations going on with 7% of our customer base," Mohan Koo, co-founder and president of DTEX, said in an interview. DTEX has a couple hundred customers and estimates thousands of critical infrastructure organizations have been infiltrated by North Korean operatives.

"Some of the roles that we're investigating, the infiltrators that we're investigating right now, have actually got the keys to the kingdom," Koo said. "They have privileged-access rights. They have the ability to turn on access and turn off access for other workers. They have the ability to install and uninstall software. They have the ability to write code."

DTEX's ongoing research indicates the North Korean regime's yearslong scheme goes much deeper than contract work and extends to roles beyond traditional IT. The Justice and Treasury Departments have issued indictments and sanctioned people and entities allegedly involved in North Korea's effort to send thousands of specialized technical professionals outside of the country to secure freelance jobs under false pretenses and funnel their wages back to Pyongyang.

Multiple threat hunters have observed a surge of insider threat activity linked to North Korea. Adam Meyers, head of CrowdStrike's counter adversary operations, last month said a "tremendous amount of companies" have unknowingly hired North Koreans for technical development roles.

Nearly 40% of the incident response cases CrowdStrike worked on last year involving the North Korea state-backed group it tracks as Famous Chollima were insider-threat operations. Insider threats accounted for 5% of Palo Alto Networks' Unit 42 incident response cases last year, and the number of those tied to North Korea tripled in 2024.

Oftentimes, organizations unknowingly hire multiple North Korean nationals. "It's typically not just one," said Rob Schuett, director of insider intelligence investigations at DTEX.

"A single compromise is just the beginning," he said. "It's kind of like an insect infestation in your home. You see that one insect and you may be able to spray that one with chemicals and get rid of it, or move it outside. However, you know that in the walls and the cracks and the crevices there's a bigger problem underfoot."

Quick pivots, hops to other networks

Once a North Korean national is hired and starts the employment onboarding process, they move quickly to further infiltrate the organization.

They move into virtual desktop infrastructure environments, using access granted from one entity to pivot to a third party, often a trusted partner.

“That opens up the whole threat of the supply chain being infiltrated, and that’s a very, very complex problem,” Koo said.

DTEX’s investigation into insider threats backed by North Korea reached an “alarming conclusion,” Koo said, a shocking reality that the extent of known compromise is widespread and likely more prevalent than confirmed thus far.

“We’re only really catching the dumb ones, the ones that are making OpSec mistakes, and they’re pivoting around in places that we didn’t know were infiltrated,” Schuett said. This means, North Korean technical workers are probably operating in dozens of infiltrated organizations, including those they aren’t employed by, simultaneously.

North Korean nationals are also installing various remote access tools, which are approved for use and often blend in to typical onboarding activities, when most employees set up and gain initial access to work systems.

“They’re using a specific identity and a specific individual to gain employment, and that individual’s skill set is specifically targeted to gain employment at the organization,” Koo said. “But once they’ve gained employment, it’s just an access right, and then they use these remote tools to enable the others to do the work.”

North Koreans are doing the job — better than most

The threat posed by North Korean technical workers stands out, compared to other nation-state backed activity, because they’re doing the work companies are paying them to do. “In some cases, they’re doing a better job than most,” Koo said.

With multiple people performing tasks assigned to one person, pulling in assistance from thousands of experts in any given field, these employees may become a rock star in the eyes of their employer. To the organization, it looks like their best employee is doing an inordinate amount of work.

Yet, DTEX discovered multiple red flags as it began tracking suspected North Korean workers’ activities on their work machines.

“What we see with the DPRK worker is completely anomalous compared to everybody else, meaning you’ll see a login time that runs an extremely long amount of time and then there is no logout activity,” Schuett said.

“They’ll run impossible amounts of times for a human being to endure to work, so they’ll go like four to five days at a time before you’ll see another logout, if you even see one,” he said.

This heightened and unimaginable level of productivity occurs because North Korean workers open remote sessions and share their desktop with other alleged co-conspirators with similar specialized skills. Spikes in activity are attributed to the handover period, from one shift worker to the next, or when multiple people are working side by side, shadowing each other.

While the average time lapsed between North Korean worker logins and logoffs or the unlocking and locking of machines is six to seven days, DTEX observed one instance of unrelenting activity that went on for three weeks.

Financially motivated by salaries now, but what's next?

For now, North Korean technical workers are focused on attaining employment, doing those jobs, and sending the money they earn back to Pyongyang.

North Korean technical workers generate hundreds of millions of dollars for the North Korean regime, according to Unit 42.

The potential for follow-on activity, including espionage, extortion and disruptive attacks on critical infrastructure is abundant.

"For any of us to be naive enough to think that that's all they're ever going to do is ridiculous," Koo said. "We have to be vigilant because, at the point that they decide to weaponize in a different way, they have the access to do it."

While it remains hypothetical, Koo said it's "inconceivable" to think North Korean technical professionals working for an unknown number of businesses around the globe won't plant a backdoor, switch off critical infrastructure or otherwise commit sabotage at some point.

"It just requires the right point in time where they have that motivation to do so," he said.

Security professionals acknowledge it's difficult for organizations to identify a potential insider threat from job applicants, but not impossible.

Requiring remote job candidates to be on camera and show government-issued identification is a good practice, but not fool-proof. Paying attention to what people do on camera — looking away, possibly taking prompts from someone else helping them through the interview — can provide meaningful insights, Schuett said.

"We can see other people in the room with them taking an interview," Schuett said. "I don't know about you, but when I'm applying for a job, I'm probably not doing it in a Starbucks or some other public location."

Other potential tells include long pauses and inconsistencies on candidates' resumes, such as claimed expertise in technologies before they were developed and widely available.

Human resources professionals and recruiters are the first line of defense against North Korean insider threats. But if they pass that stage and make it to employment, companies can still look for idiosyncrasies, such as lack of communication in meetings, emails or collaboration platforms, to spot potential problems.

North Korean technical workers “don’t ask how your kid did in soccer last night,” Schuett said. “They don’t talk about the new, cool restaurant they found, because they can’t.”
