North Korean IT worker scam is now a threat to all companies, cybersecurity experts say

By Jonathan Greig

Published: 2025-05-01 · Archived: 2026-04-05 19:50:00 UTC

SAN FRANCISCO — North Korea's ability to surreptitiously slip thousands of its workers into Fortune 500 companies was a main focus for cybersecurity professionals at this year's RSA Conference.

Recorded Future News spoke to and heard from dozens people on every side of the issue — from incident responders helping companies that hired them to researchers embedded in the chat rooms where DPRK workers provide updates to senior officials.

While many initially thought the issue was confined to the crypto industry or even tech firms, multiple experts said it has grown far beyond that.

To illustrate this, cybersecurity expert Michael Barnhart said he recently found evidence that a U.S. political campaign in Oregon hired a North Korean IT worker.

Barnhart, who works for DTEX, a company that focuses on preventing insider threats, said the worker was hired to create a campaign website and evidence shows the operator accessed WordPress administrative portals under a false identity.

The email address used suggests they were hired from a front company or an unwitting intermediary.

While the worker's access was not weaponized, Barnhart told Recorded Future News that the kind of access the person had was an open door to more serious outcomes that may have included propaganda or passing off their access to a nation-state hacker that may have used the campaign site to deliver malware to visitors.

90% of the postings

Multiple security experts said that despite months of reporting and law enforcement action, the public was still not aware of the scale of the campaign. Palo Alto Networks' Sam Rubin said they had one client that, within 12 hours of posting a job, had at least one North Korean surreptitiously apply.

After investigating their situation, Rubin said they found 90% of the unnamed company's postings had at least one North Korean in the applicant pool. Some of Palo Alto Networks' clients in the crypto space see North Koreans applying every day to join their companies.

"If you're hiring contract workers, you either are interviewing or have already hired a North Korean," Rubin said. "So this is a real problem."

Charles Carmakal, CTO of Google security company Mandiant, said he has spoken to chief security officers at many Fortune 500 companies and nearly every one admitted they have hired at least one North Korean IT worker.

At an RSA panel on Monday featuring FBI assistant director Bryan Vorndran and several other law enforcement officials, Crowdstrike's Adam Myers said they have seen situations where North Korean IT workers have spent up to 14 months inside an organization — often doing the work somewhat adequately.

"In the last couple years, I've received calls from many companies, as well as many very sophisticated people in emerging tech that are associated with VC firms at their own portfolio companies. This is a problem for all of them as well," Vorndran said.

In most situations, the workers were able to slip past detection using a combination of AI and guile — answering questions quickly and getting translations through ChatGPT. Once hired, they say a family emergency has made it so they need their work laptop sent to a different address than the one listed on the application.

The laptops are sent to U.S.-based laptop farms, where witting or unwitting Americans get paid menial fees to host the laptops, install remote access software and keep the lights on.

FBI special agent Elizabeth Pelker said the people running the U.S. laptop farms often don't know they are doing this on behalf of North Koreans, typically assuming they are running the laptops for businesses in China.

According to Pelker, it often starts with one laptop and then grows to dozens. Another expert on the panel noted the cruel irony of some laptop farms being run in Ukraine by people who do not know their work is going to support a regime currently sending soldiers to assist Russia's invasion of the country.

On the North Korean side

FBI officials and security experts explained that North Korea has distinct teams working on every aspect of the scheme.

There are North Korean squads whose sole job is to get IT workers through every step of the hiring process, using AI to create the perfect resumes and providing answers during technical interviews.

Since disruptions began last year and law enforcement has publicly warned companies of the practice, DTEX's Barnhart and others said they have seen some workers try to extort companies or hand off their access to more sophisticated North Korean hacking groups who deploy malware on company systems, steal data or siphon millions in cryptocurrency.

Barnhart viewed the scam holistically, tying it directly to North Korean APT groups, cryptocurrency hackers and the country's missile program.

IT workers are typically held in call center-style facilities in Southeast Asia or China where they are tasked with generating a certain income. Barnhart said when he first began investigating the scheme and monitoring IT worker chats, most workers had to earn about $5,000 a month or they were beaten, with most only being allowed to keep about $200.

These figures have now doubled and tripled, with workers being tasked with generating up to $20,000 under the threat of being sent back to North Korea. Many of the workers have to make this money by any means necessary – whether it's IT work or crypto hacks, according to Barnhart.

“I see communications between IT workers where they're saying, ‘How much money did you make this month? Because you made $4,000 and I’ve only made $2,000. Can you show me what you're doing?’ So it's just any of these schemes,” he said.

The workers are typically housed in apartments where 10 people are working multiple jobs, meaning one group could generate more than 70 paychecks per month.

Law enforcement leads to extortion

Last October, as law enforcement disrupted laptop farms and warned companies of workers in their employee pool — many IT workers handed off their access to more senior officials who either conduct malware focused cyberattacks or attempt to extort companies for a final payout.

Barnhart dealt with multiple extortion incidents where the fired IT workers demanded ransoms. Some were relatively small ransoms that are typically paid by companies, but the ransoms grew as the IT workers became more desperate to cover the loss of future earnings.

One notable aspect of the ransoms is the escalation, he explained. When the North Korean IT workers are initially fired, they demand access back before escalating to threatening the sale of sensitive data to competitors. If that does not secure a ransom, the person claims to still have access to some systems that will be handed off to North Korean APT groups.

Mandiant’s Carmakal echoed much of Barnhart’s assessments during a Google press briefing, noting that in their incident response situations, they dealt with hackers who reached out to companies in extortion attempts using data that a suspected North Korean IT worker had obtained.

“The thing that really worries us is that there are hundreds of Fortune 500 organizations that have hired these North Korean IT workers,” Carmakal said. “And the concern we have is that there's always the potential that at some point in time, these actors that have taken data as part of their employment may publish it on the internet. We haven't seen it happen yet, but that's the fear that most of these organizations have today.”

Google officials noted that they have seen North Korean IT workers attempt to get hired at the company.

Multiple experts also warned that the scheme was expanding beyond North Korea, with people in several different countries including Pakistan now attempting to replicate the hermit nation’s success. Barnhart noted that some criminal operations in Pakistan and Iran are getting involved in the scheme.

One of the biggest problems in addressing the issue is that the IT workers are generally considered competent. Mandiant’s Carmakal said most performance reviews for the IT workers are “pretty good” and that “99%” were not found to be implanting backdoors or causing issues.

“I think more often than not, I always get the comment ‘but Johnny is our best performer. Do we actually need to fire him?’” the FBI’s Pelker said.

No previous article

No new articles

[Jonathan Greig]

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
