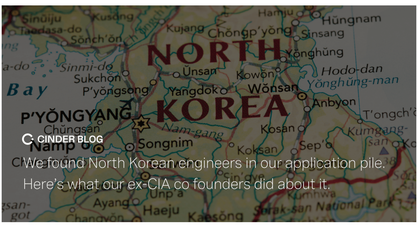

We found North Korean engineers in our application pile. Here's what our ex-CIA co founders did about it.

ENGINEERING

Declan Cummings,
Head of Engineering

Cinder is part of a growing list of US-based tech companies that encounter engineering applicants who are actually suspected North Korean nationals. These North Koreans almost certainly work on behalf of the North Korean government to funnel money back to their government while working remotely via third countries like China. Since at least early 2023, many have applied to US-based remote-first tech companies like Cinder. If you've been running into this issue, here are some tips for how you can handle this at your own company.

It's important to note that funding the North Korean government could constitute a crime given the sanctions the regime is under. And nobody wants that kind of paperwork headache!

Cinder is unique in our ability to interface with this issue given our co-founders' backgrounds as ex-CIA operatives, as well as an expert on North Korea. Our prior experience spurred our interest in building internet safety software to begin with, and inspires a particular vigilance to maintain it to the best of our abilities.

I first learned of North Korea's practice of sending workers abroad in 2014. I joined the board of a leadership development program for North Korean escapees and learned of North Korea's government and its use of technology from those who experienced it firsthand. Later, I volunteered for a nonprofit developing information access technology for clandestine use inside closed countries like North Korea. I have spoken with North Korean escapees who have recent knowledge of the latest North Korean tech worker trends. But I never expected I would one day experience them as applicants attempting to join my company.

North Koreans are applying to US tech companies?

The North Korean government has a long history of sending workers abroad to earn money for the regime. The workers are sent to countries like China where they must earn a salary quota, most of which will be taken by the government for its own needs. These workers are under close supervision by North Korean officials while abroad. They are often required to leave family members behind as collateral to prevent them from defecting while outside their home country.

North Koreans have been working undercover as software freelancers for part time contract jobs for years. And recently, they have started to apply to American tech companies that offer remote, full time work. This may be exacerbated by the rise of remote work after the COVID pandemic and the fact that working at US tech companies can be so lucrative. Hyun-Seung Lee, a former North Korean businessman and former chair of the Kim Il Sung Socialist Youth League branch in Dalian, China, told us that the earnings quota for a North Korean IT worker based in China is typically $6,000 per month. This quota is more than covered by many US tech salaries.

The application process

In our experience, North Koreans applying to US tech companies under false pretenses will often use a standard process: they will create profiles on multiple professional networking and job posting sites using a name that is not Korean and sometimes with an AI-edited profile image.

Once they go through the interview process and have received a job offer, they may ask their new company-provided laptop be sent to a US-based partner. According to a Department of Justice indictment, the US-based partner may install remote desktop software so that the North Korean engineer can appear to be working from a US location, with a laptop physically located in the US, while remotely controlling the laptop from abroad.

By demonstrating sufficient technical capability and minimal English language skills, North Korean applicants can meet minimum thresholds for junior software engineer roles. Fast-growing start-ups eager to ship more products might overlook gaps in resume, unreliable or missing education records, or poor command of written or spoken English for an engineer with sufficient skill who is ready to start working soon.

We suspect if the worker is employed even for just a few months before being terminated, this can still be quite profitable for the regime.

Cinder's approach

We have a unique perspective on this problem for a few reasons: our company is in the internet safety industry, two of our co-founders came from the CIA, and I have twelve years of experience working on cybersecurity and human rights issues related to North Korea. So when North Korean IT workers applied to Cinder, they had a different experience than they might have expected.

> *Pyongyang has a long history of exploiting its people to further the regime's ambitions and this activity is no exception. Two of Cinder's founders bring years of CIA experience, so we're no strangers to creating and running virtual operations, nor detecting and countering those of hostile nation states.*
>
> *– Phil Brennan, Cinder co-founder and 10-year CIA veteran*

What tipped us off

Fifteen months prior to any FBI indictments, our COO first noticed a few unusual trends in our applicant pool. Upon further inspection he discovered these candidates either didn't seem to exist on the internet, or were mapped to people who weren't them, who did have an internet presence. Over time, we realized many applicants that had the following characteristics:

1. No online presence outside of professional networking websites; and professional networking profiles were recently created, typically with profile pictures that obscured the individual's image (in ski goggles, sunglasses), were too zoomed out to be helpful, were AI-generated, or were simply blank.
2. Completely fabricated job history including office locations that don't actually exist.
3. Unable to find these applicants online outside of the standard professional networking sites (e.g. no presence on GitHub, social media etc).
4. Inability to answer basic questions about the cities in which they allegedly worked ("What was your Metro stop in Paris?") or technology on which they worked ("What org were you in at Uber?").
5. Background noise during their interview that indicated other people speaking in an interview-like setting, implying a crowded room of people on separate professional video calls.
6. Highly scripted answers with explicit preference for remote work, and little ability to deviate from the script.
7. A mismatch between the name displayed on the resume or networking site, and the candidate's command of English (e.g. Chris Smith with a B.A. from a large US research university who can barely speak interview-level English is surprising).

We also noticed vague cover letter language:

> *Hi, team!*
> *I hope you're fine and safe.*
> *I am really excited about this potential opportunity with the ambitious project.*
> *As a Senior Frontend Developer with 8+ years of experience, I have great experience in working with React.js/Redux, RTK, React Query, Vue, Next.js, Vercel, TypeScript, GraphQL, etc.*
> *Please have a look at my previous works.*

Another example:

> *Hi,*
> *I love what you are doing in your company. With my eight-plus years of development, I'd love to be one of you. As an FE-heavy developer, I have a track record of building successful products. And I am familiar with startup environment. I'd love to use my strong debugging and problem-solving abilities to be a powerful force in the workplace. I can wear multiple hats and adapt to a fast-paced team. I look forward to meeting you to learn more about this role and share my relevant skills. Best,*

Taken together, to me these details suggested fake identities. And while I knew North Korea had a history of sending workers abroad to freelance, I didn't expect that they would apply to full time roles at US-based companies.

What we did

First, because we come from the Trust and Safety industry, I was able to reach out to our partners at various security companies and confirm these patterns were consistent with North Koreans attempting to pass themselves off as Americans. I also learned a lot from published investigations like the one Nisos published last year.

With more knowledge, we were able to go digging. And we had a lot of material: For applicants from some job sites, roughly 80% of inbound applicants with experience matching our stack were suspected North Koreans.

We started filtering out suspected North Korean applicants by doing quick internet searches and closer examinations of job history, profile imagery, and a social media screening. However, our process wasn't perfect, and we still ended up on occasional Zoom calls screening applicants who we would quickly discover, mid-call, had fabricated their career history and only recently created their online presence.

When we first started receiving North Korean applications, some of our interviewers noted applicants' strong resistance to travel in their post-interview write ups:

> *One clarifying question that I neglected to ask about is that on his LinkedIn profile he says he is looking for "100% Remote job only without travel". I did not notice the "without travel" part until after the interview. We should make sure he would be willing to travel sometimes for team offsites as this is an important part of Cinder's culture.*

I started informing candidates that Cinder's customer base includes companies investigating nation-state espionage and insider threat issues. I added that this is a natural fit for us, because our co-founders came from the US intelligence community including the CIA.

Upon hearing this, one suspected North Korean applicant immediately dropped from the Zoom call and never contacted us again.

What Cinder is doing now

We continue to receive dozens of suspected North Korean applicants to Cinder. We take steps to share relevant information with security teams at networking and job listing sites that we work with. If your company is also affected by this growing threat, I encourage you to get in touch with me at declan@cndr.io and I'd be happy to share more tips and prevention strategies.

BOOK A MEETING

Read More