COURAGE GARIKAI



THROUGH THE FRONT DOOR

North Korean IT Workers, the $6 Billion Binance Heist, and the New Shape of Cyber Threat

COLDCODE SI LABS · HARARE

For every hiring manager who has ever wondered who is really on the other side of that screen.

And for every IT security person who has told you, for years, that the insider threat isn't always an insider.

Through the Front Door

North Korean IT Workers, the $6 Billion Binance Heist, and the New Shape of Cyber Threat

Courage Garikai

ColdCode Si Labs Working Paper · Harare · November 2026 © 2026 Courage Garikai. All rights reserved.

About this essay

In September 2026, FBI agents raided more than 40 homes across the United States and found something that should concern every business that hires remote workers: rows of laptops on shelves, humming, each one logged in to a different American company, operated remotely by workers in North Korea.

This is not a story about spear-phishing or zero-day exploits. It is a story about a simpler, more brazen approach to cyber espionage: getting hired. North Korean IT workers apply for jobs at American companies using stolen identities, AI-altered photographs, and fake references. They pass interviews, background checks, and coding tests. The companies ship them laptops. The laptops are delivered to drop houses in American suburbs, plugged in, and left running. The worker, sitting in North Korea or China or Russia, logs in remotely, does the job, attends meetings, writes code, gets positive performance reviews, collects a paycheck, and sends 85–90% of the salary back to the North Korean regime.

In a separate, mirror-image operation, North Korean hackers offer fake jobs to engineers at target companies, and deliver malware through the coding assignment — a file the candidate downloads and opens because it is what any job applicant would do. That is how they stole approximately $6.3 billion from Binance in October 2026. The heist nearly matched the total of ten years of North Korean crypto theft in a single day.

This essay examines both operations. It explains how they work, why they are so hard to detect, and what every company that hires remote workers or accepts job applications must now do to defend against them.

The events described here are based on public records: FBI press releases, Department of Justice filings (including the Christina Chapman indictment and sentencing), US Treasury sanctions announcements, Binance's public post-mortem of the October 2026 breach, reporting from cybersecurity firms (Nobera 4 [NOB4], HYPR, Mandiant, Chainalysis), and on-the-record coverage from major outlets. No classified information is used.

Harare, November 2026

I · The Texas raids

In September 2026, FBI agents walked into an ordinary house in Texas.

It looked like any other suburban home. Family photos on the walls. A car in the driveway. A lawn that needed cutting. Then they opened the door to one room. Inside were shelves. On those shelves were laptops, rows of them, open, plugged in, humming. Each laptop belonged to a different American company. The people using those laptops were not in Texas. They were not in America. They were working for North Korea.

That week, agents raided more than 40 homes like that one. The FBI said something afterward that should make every business owner stop and think: each laptop potentially represented one company that had hired a North Korean worker. Each laptop, one company.

Which means that, right now, somewhere in America, a company is running payroll on a Friday — direct deposit, health insurance, a holiday party invitation in the inbox — and sending part of that paycheck to someone who sends 85 to 90% of it to Kim Jong-un's regime. And that company has no idea.

This is not a story about sophisticated zero-day exploits. It is not a story about SQL injection or cross-site scripting or unpatched servers. It is a story about attackers who walk through the front door. They apply for jobs. They get hired. They show up to meetings. They write code. They get paid.

II · The company that caught one

NOB4 is an American cybersecurity company. Its whole business is teaching other companies how to spot hackers. It is the kind of firm that other companies hire specifically because they know how this game works.

A few years ago, NOB4 hired a new software engineer for its AI team. The candidate went through several rounds of video interviews. He passed a background check. His photo looked normal. His references checked out. The company mailed him a brand-new laptop.

Twenty-five minutes after he turned it on, it started loading malware.

The security team called him to ask what was going on. He said he was not available. Then he stopped responding completely.

His identity was stolen from a real American. His photograph was a stock image edited with artificial intelligence. The laptop had been shipped to what the company later called a "laptop farm."

Now imagine that is your company. Imagine he is on your team. He is in your meetings. He is on your Slack. Would you notice?

NOB4 noticed in 25 minutes because he got greedy on day one. The smart ones don't. They do the job. They show up to meetings. They write the code. They get good reviews. They collect a paycheck every two weeks. They stay for months. They stay for years.

Sample provided free for review. The complete book is available at https://library.coldcode-si-labs.workers.dev/