IMAGE: UNSPLASH

Jonathan Greig
September 23rd, 2024

Cybercrime News Nation-state

Dozens of Fortune 100 companies have unwittingly hired North Korean IT workers, according to report

It's difficult to imagine a bigger hiring blunder.

Google said it has been contacted by several major U.S. companies recently who discovered that they unknowingly hired North Koreans using fake identities for remote IT roles.

In a report published Monday by the company's Mandiant unit, researchers describe a common scheme orchestrated by the group it tracks as UNC5267, which has been active since 2018. In most cases, the IT workers "consist of individuals sent by the North Korean government to live primarily in China and Russia, with smaller numbers in Africa and Southeast Asia."

The goal is for workers to earn salaries at multiple companies — generating revenue for the North Korean government — and to gain pivotal access to U.S. tech firms that can be used for further cyberattacks or intrusions.

The remote workers "often gain elevated access to modify code and administer network systems," Mandiant found, warning of the downstream effects of allowing malicious actors into a company's inner sanctum.

Charles Carmakal, CTO of Mandiant, said in a statement that he has spoken to "dozens of Fortune 100 organizations that have accidentally hired North Korean IT workers."

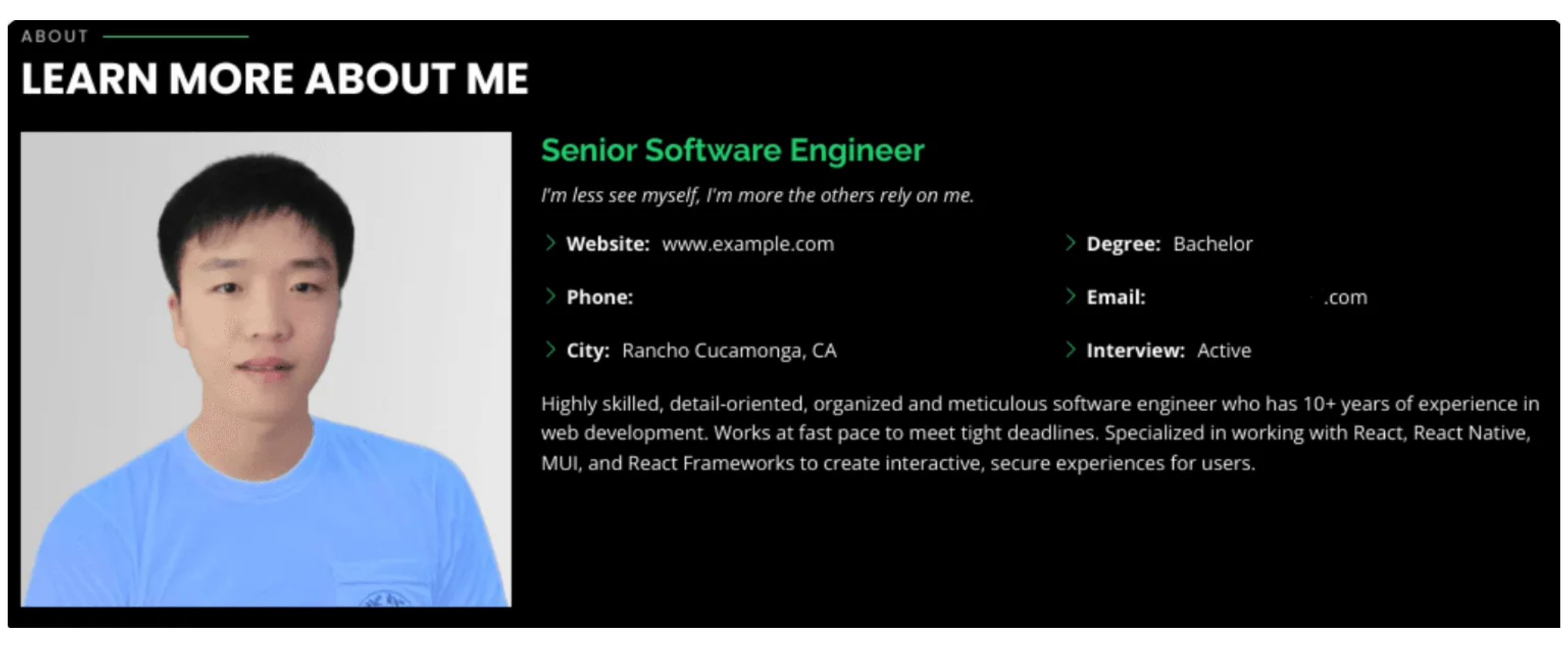
"North Korean IT workers often have multiple jobs with different organizations concurrently, and they often have elevated access to production systems, or the ability to make changes to application source code," Carmakal said.

"There is a concern that they may use this access to insert backdoors in systems or software in the future. Every Fortune 100 organization should be thinking about this problem."

Caffeine and serial numbers

Using stolen identities or fictitious ones, the actors are generally hired as remote contractors. Mandiant has seen the workers hired in a variety of complex roles across several sectors. Some workers are employed at multiple companies, bringing in several salaries each month.

The tactic is facilitated by someone based in the U.S. who runs a laptop farm where workers' laptops are sent. Remote technology is installed on the laptops, allowing the North Koreans to log in and conduct their work from China or Russia.



ABOUT

LEARN MORE ABOUT ME

Senior Software Engineer

I'm less see myself, I'm more the others rely on me.

- Website: www.example.com
- Degree: Bachelor
- Phone:
- Email: .com
- City: Rancho Cucamonga, CA
- Interview: Active

Highly skilled, detail-oriented, organized and meticulous software engineer who has 10+ years of experience in web development. Works at fast pace to meet tight deadlines. Specialized in working with React, React Native, MUI, and React Frameworks to create interactive, secure experiences for users.

Image: Mandiant

The Justice Department in recent months has arrested and charged several U.S. citizens for running these laptop farms and in one instance, found an American that used 60 stolen identities to facilitate North Korean employment at more than 300 U.S. companies. The workers earned at least $6.8 million from October 2020 to October 2023.

Workers typically asked for their work laptops to be sent to different addresses than those listed on their resumes, raising the suspicions of companies.

Mandiant said it found evidence that the laptops at these farms are connected to a "keyboard video mouse" device or multiple remote management tools including LogMeIn, GoToMeeting, Chrome Remote Desktop, AnyDesk, TeamViewer and others.

"Feedback from team members and managers who spoke with Mandiant during investigations consistently highlighted behavior patterns, such as reluctance to engage in video communication and below-average work quality exhibited by the DPRK IT worker remotely operating the laptops," Mandiant reported.

In several incident response engagements, Mandiant found the workers used the same resumes that had links to fabricated software engineer profiles hosted on Netlify, a platform often used for quickly creating and deploying websites.

Many of the resumes and profiles included poor English and other clues indicating the actor was not based in the U.S.

One characteristic repeatedly seen was the use of U.S-based addresses accompanied by education credentials from universities outside of North America, frequently in countries such as Singapore, Japan or Hong Kong. Companies, according to Mandiant, typically don't verify credentials from universities overseas.

Mandiant urged companies to conduct more stringent background checks, require on-camera interviews, require notarized proof of identity and verify that the laptop location matches the worker's address.

Companies also should consider monitoring and banning the use of remote administration tools, VPN tools and "mouse jiggling" software like Caffeine. One trick Mandiant suggested is asking workers to say the laptop serial number out loud during IT onboarding as a test.

Mandiant principal analyst Michael Barnhart said his biggest concern is what happens when workers have been hired long enough that they could launch wide-scale attacks on an organization.

"These IT workers could easily receive instructions tomorrow to deploy ransomware and simultaneously disable major organizations all over the U.S. and Europe very quickly if they wanted to," he said.

Previous advisories from U.S. law enforcement agencies have said some of the workers earn up to $300,000 annually, collectively generating hundreds of millions for the North Korean regime and its weapons programs.

Several federal law enforcement agencies launched an initiative in March 2024 designed to shutter the U.S. laptop farms.

U.S. officials previously shut down 17 website domains and seized $1.5 million last year in an operation targeting the infrastructure used by the North Korean government to facilitate the IT worker scheme.

Last year, the U.S. Treasury Department announced sanctions on four entities that employ thousands of North Korean IT workers who help illicitly finance the regime's missile and weapons-of-mass-destruction programs.

At least one U.S. company — cybersecurity giant KnowBe4 — has come forward to acknowledge hiring a worker last year that it later discovered was part of the same North Korean scheme.

Tags North Korea Google Mandiant hiring fraud

Previous article
← Legislation to mandate universal data privacy opt-outs vetoed in...

Next article
US intelligence agencies confirm Russia is pushing fake videos of... →

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.

BRIEFS

Police records show ShotSpotter is wildly inaccurate in New York City | December 4th, 2024

Germany arrests suspected admin of country's largest criminal marketplace | December 4th, 2024

British telecoms giant BT confirms attempted cyberattack after ransomware gang claims hack | December 4th, 2024

Senators urge DOD watchdog to probe 'failure to secure' communications amid Salt Typhoon hacks | December 4th, 2024

FTC settles with facial recognition technology company for deceptive marketing | December 3rd, 2024

Finland says latest fiber-optic cable break was an accident, not sabotage | December 3rd, 2024

Energy industry contractor says ransomware attack has limited access to IT systems | December 2nd, 2024

Former Polish spy chief arrested to testify before parliament in spyware probe | December 2nd, 2024

Italian football club Bologna FC says company data stolen during ransomware attack | November 29th, 2024

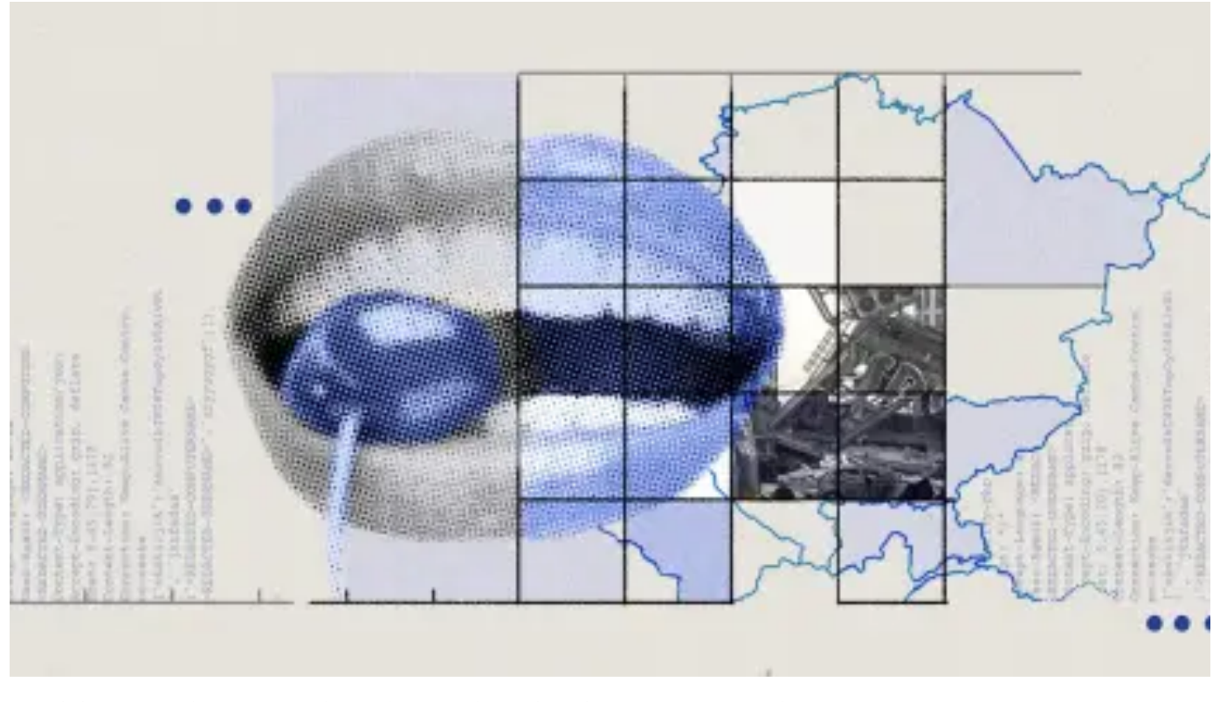
SCAM WEBSITES TAKE ADVANTAGE OF SEASONAL OPENINGS AND ESTABLISHED METHODS TO MAXIMIZE IMPACT

SCAM WEBSITES TAKE ADVANTAGE OF SEASONAL OPENINGS AND ESTABLISHED METHODS TO MAXIMIZE IMPACT

"OPERATION UNDERCUT" SHOWS MULTIFACETED NATURE OF SDA'S INFLUENCE OPERATIONS

"OPERATION UNDERCUT" SHOWS MULTIFACETED NATURE OF SDA'S INFLUENCE OPERATIONS

RUSSIA-ALIGNED TAG-110 TARGETS ASIA AND EUROPE WITH HATVIBE AND CHERRYSPY



RUSSIA-ALIGNED TAG-110 TARGETS ASIA AND EUROPE WITH HATVIBE AND CHERRYSPY

RUSSIAN SABOTAGE ACTIVITIES ESCALATE AMID FRAUGHT TENSIONS

RUSSIAN SABOTAGE ACTIVITIES ESCALATE AMID FRAUGHT TENSIONS

CHINA-NEXUS TAG-112 COMPROMISES TIBETAN WEBSITES TO DISTRIBUTE COBALT STRIKE

CHINA-NEXUS TAG-112 COMPROMISES TIBETAN WEBSITES TO DISTRIBUTE COBALT STRIKE