# DOJ raids 29 ‘laptop farms’ in operation against North Korean IT worker scheme

By Jonathan Greig

Published: 2025-06-30 · Archived: 2026-04-05 13:14:15 UTC

Nearly 30 “laptop farms” across 16 states have been raided by U.S. law enforcement in recent months for their suspected role in a long-running North Korean IT worker scheme.

The Justice Department on Monday announced a coordinated action that involved three indictments, one arrest, the seizure of 29 financial accounts and the shutdown of 21 websites alongside the laptop farm raids.

FBI officials said the laptop farms allowed an undisclosed number of North Koreans to illegally work at more than 100 U.S. companies. The farms host work devices sent by legitimate companies who unwittingly hired North Koreans, allowing the employees to appear as if they are working from the U.S.

Investigators have spent years working to stop the scheme, which has seen the North Korean regime earn millions through thousands of people who use fake identities to get hired as IT workers at companies based in the West.

The FBI said it conducted searches at eight locations in October 2024 across three states that led to the discovery of more than 70 laptops and remote access devices.

The FBI conducted 21 more searches in June across 14 states. The locations were not disclosed but FBI offices in Colorado, Missouri and Texas were involved. About 137 laptops were seized as part of the searches.

Court documents say the North Koreans were helped by multiple people in the U.S., China, United Arab Emirates and Taiwan. On a call with reporters, the Justice Department did not explain why there were not more arrests associated with the raids.

A DOJ spokesperson told Recorded Future News that it is an “ongoing investigation and there could be more arrests or enforcement actions down the line.”

In at least one case, North Korean IT workers gained access to “sensitive employer data and source code, including International Traffic in Arms Regulations (ITAR) data,” after they were hired by a California-based defense contractor that develops artificial intelligence-powered equipment and technologies.

U.S. residents created front companies and fake websites to bolster the credentials of North Korean IT workers while also housing laptops that allowed the workers to remotely access devices provided by the victim companies.

The Justice Department outlined one situation where workers used fake identities to get hired at an Atlanta-based blockchain research company before stealing about $740,000 worth of cryptocurrency.

John Eisenberg, assistant attorney general for the DOJ's National Security Division, said the scheme is designed to steal from American companies, evade sanctions and "fund the North Korean regime's illicit programs, including its weapons programs."

FBI Assistant Director Brett Leatherman added that in many cases the North Koreans steal the real identities of American citizens and warned residents to be wary of hosting laptop farms on their property.

## A 'massive campaign'

The Justice Department said it arrested Zhenxing "Danny" Wang, a U.S. national and New Jersey resident now facing a five-count indictment.

Zhenxing Wang allegedly worked with others to help North Koreans get hired and helped generate $5 million in revenue for Pyongyang. The indictment also names six Chinese nationals — Jing Bin Huang, Baoyu Zhou, Tong Yuze, Yongzhe Xu, Ziyou Yuan and Zhenbang Zhou — and two people from Taiwan, Mengting Liu and Enchia Liu.

From 2021 to October 2024, the group allegedly stole the identities of about 80 U.S. citizens and provided them to North Koreans — allowing them to gain employment at several Fortune 500 companies. The court documents claim the American companies dealt with about $3 million in losses due to legal fees, network remediation costs and more.

In court documents, prosecutors said Zhenxing Wang worked with Kejia Wang, another New Jersey-based U.S. citizen, and four others to run the scheme. Kejia Wang traveled in 2023 to Shenyang and Dandong, both of which are near the border of North Korea and China, to organize the scheme.

Zhenxing Wang was allegedly one of several U.S. residents to receive laptops and host them at their homes, connecting the laptops to devices investigators called "keyboard-video-mouse or 'KVM' switches" that allowed people overseas to control them remotely.

Zhenxing Wang and Kejia Wang are also accused of setting up shell companies, websites and financial accounts. Kejia Wang transferred millions of dollars to overseas bank accounts and paid people running laptop farms in California and elsewhere, the indictments say.

Kejia Wang, Zhenxing Wang, and the four other U.S. facilitators were allegedly paid at least $696,000. The FBI said it seized 17 web domains used to facilitate the scheme and 29 financial accounts that held thousands of dollars.

The Justice Department did not say whether Kejia Wang has been detained.

A separate indictment charged four North Korean nationals with wire fraud and money laundering. Kim Kwang Jin, Kang Tae Bok, Jong Pong Ju and Chang Nam Il are accused of stealing and then laundering over $900,000 in cryptocurrency.

All four are at large, according to the FBI. The indictment said the four traveled to the UAE and used stolen identities to get hired by an Atlanta-based cryptocurrency company as well as a virtual token company in Serbia.

In 2022, about $175,000 was stolen from the Serbian company in addition to the $740,000 taken from the Atlanta-based company. The men allegedly used Tornado Cash to launder the funds and fake Malaysian IDs to cash out the funds.

In February, an Arizona woman pleaded guilty to running a laptop farm to assist North Korean IT workers. She faces nine years in prison.

“North Korea remains intent on funding its weapons programs by defrauding U.S. companies and exploiting American victims of identity theft, but the FBI is equally intent on disrupting this massive campaign and bringing its perpetrators to justice,” said FBI Counterintelligence Division Assistant Director Roman Rozhavsky of the FBI Counterintelligence Division.



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.

---