US woman allegedly aided North Korean IT workers infiltrate 300 firms

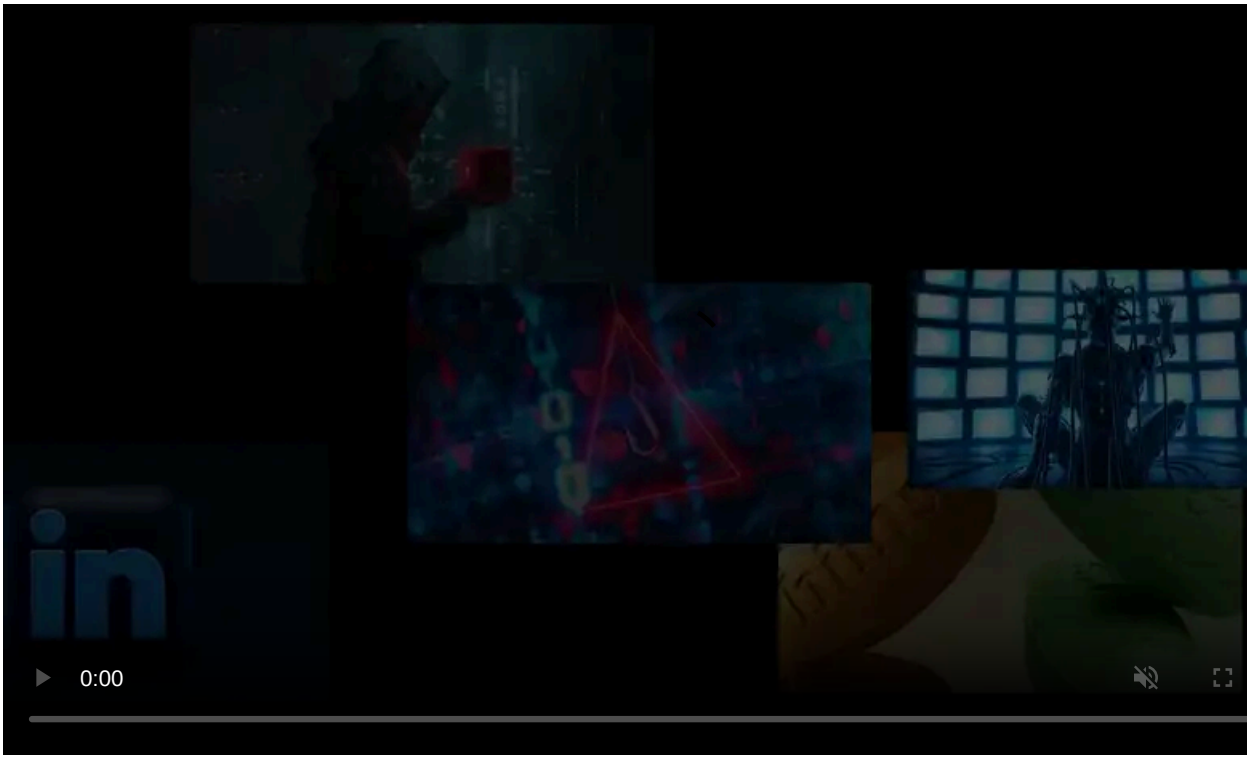
By Sergiu Gatlan

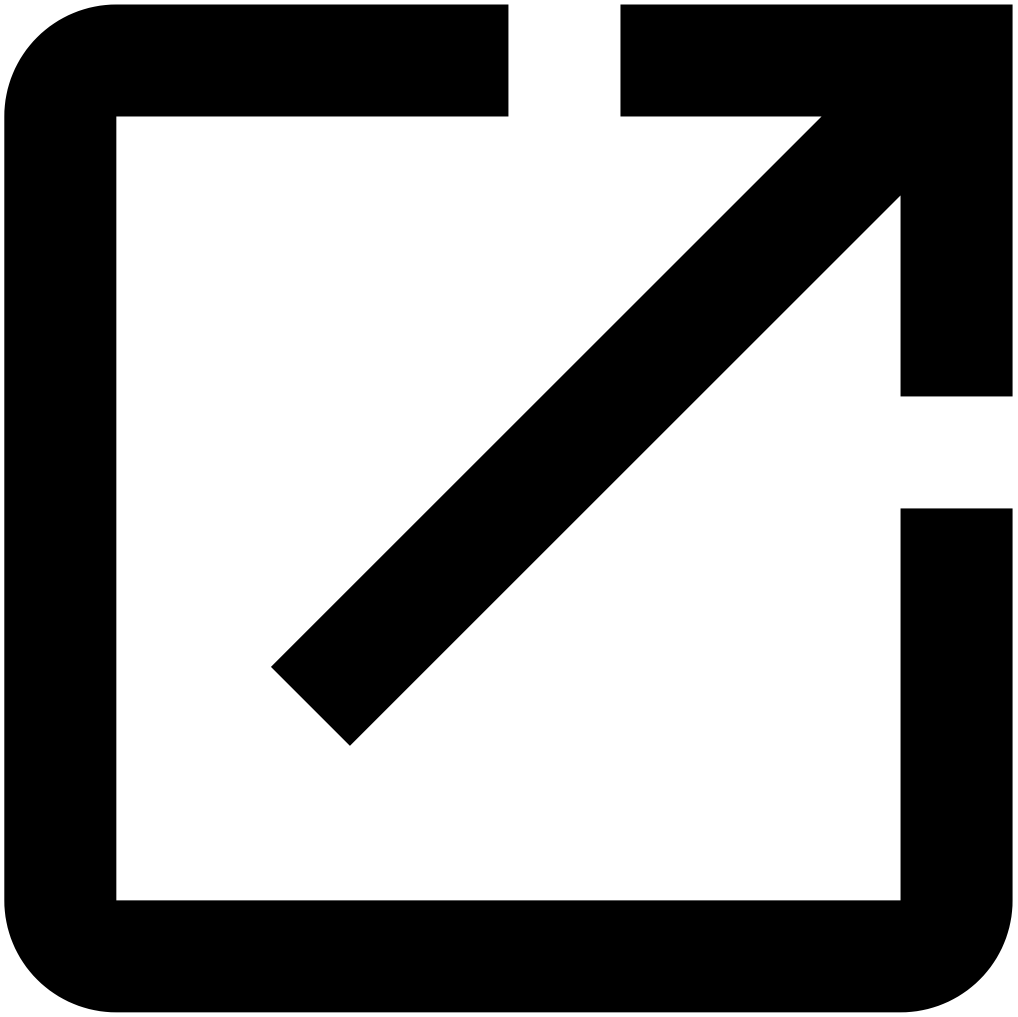
Published: 2024-05-16 · Archived: 2026-04-05 15:55:57 UTC

The U.S. Justice Department charged five individuals today, a U.S. Citizen woman, a Ukrainian man, and three foreign nationals, for their involvement in cyber schemes that generated revenue for North Korea's nuclear weapons program.

They were allegedly involved between October 2020 and October 2023 in a campaign coordinated by the North Korean government "to infiltrate U.S. job markets through fraud in an effort to raise revenue for the North Korean government and its illicit nuclear program."

Two of them, Christina Marie Chapman and Oleksandr Didenko, were arrested on May 15 in Litchfield Park, Arizona, and in Poland on May 7, 2024, with the DOJ now seeking Didenko's extradition to the United States.


0:00



They were both charged with conspiracy to defraud the United States, aggravated identity theft, and conspiracy to commit money laundering, wire fraud, identity fraud, and bank fraud.

Three other foreign nationals, known only by their aliases (Jiho Han, Haoran Xu, and Chunji Jin), were also charged with conspiracy to commit money laundering.

If convicted, Chapman faces a maximum of 97.5 years in prison, while Didenko's maximum penalty can reach 67.5 years. Each of the John Does also faces a maximum penalty of 20 years.

"Chapman and her co-conspirators committed fraud and stole the identities of American citizens to enable individuals based overseas to pose as domestic, remote IT workers," said Nicole M. Argentieri, the head of the Justice Department's Criminal Division.

Today, the U.S. State Department announced a reward of up to $5 million for any information related to Chapman's co-conspirators, the North Korean IT workers charged today, and their manager, only known as Zhonghua.

Reward for information on North Korean IT workers (State Department)

North Koreans worked remotely via U.S. laptop farms

According to the indictment, Chapman housed the North Korean IT workers' computers in her own home, creating a "laptop farm" to make it appear as though her co-conspirators' devices were in the United States.

They were hired as remote software and application developers with multiple Fortune 500 companies, including an aerospace and defense company, a major television network, a Silicon Valley technology company, and a high-profile company.

They were paid millions for their work, and Chapman processed their paychecks from U.S. companies through her financial accounts.

Didenko also ran an online platform known as UpWorkSell (whose domain was seized by the DOJ), knowingly providing services to allow North Koreans to use false identities while hunting for remote IT work positions.

UpWorkSell seizure banner (BleepingComputer)

"Didenko is alleged to have managed as many as approximately 871 proxy identities, provided proxy accounts for three freelance IT hiring platforms, and provided proxy accounts for three different money service transmitters," the DOJ said.

"In coordination with co-conspirators, Didenko facilitated the operation of at least three U.S.-based 'laptop farms,' hosting approximately 79 computers. Didenko sent or received $920,000 in U.S.D. payments since July 2018."

Their scheme compromised over 60 U.S. identities and affected more than 300 U.S. companies. It also resulted in false tax liabilities for more than 35 U.S. citizens and generated at least $6.8 million in revenue for overseas IT workers.

Today, the FBI also issued an advisory with more information on how North Korea's IT workers undermine the security of companies that hire them and guidance on how to spot North Korean IT worker schemes.

Previously, the United States also published joint advisories with foreign partners warning of North Korean IT worker schemes and sanctioned multiple organizations involved in North Korea's IT worker revenue generation schemes.

Source: https://www.bleepingcomputer.com/news/security/five-arizona-ukraine-charged-for-cyber-schemes-infiltrating-over-300-companies-to-benefit-north-koreas-weapons-program/