South Korea sanctions 15 North Koreans for IT worker scams, financial hacking schemes

By Derek B. Johnson

Published: 2024-12-26 · Archived: 2026-04-05 16:51:34 UTC

The South Korean government has sanctioned more than a dozen individuals and one organization for a wide-ranging global scheme to fund North Korea's nuclear and missile programs through impersonating IT workers abroad, stealing cryptocurrency and facilitating cyberattacks.

South Korean officials on Thursday identified 15 North Korean nationals and the Chosun Geumjeong Economic Information Technology Exchange Corporation for economic sanctions. The individuals are allegedly working for North Korea's 313th General Bureau, part of the DPRK's Ministry of Munitions Industry, which oversees Pyongyang's weapons production, research and development and ballistic missile programs.

The individuals and others "are known to be dispatched to China, Russia, Southeast Asia, Africa, and other countries as employees of regime-affiliated organizations such as the Ministry of Defense, disguising their identities and receiving work from IT companies around the world, while some are also known to be involved in information theft and cyberattacks," according to a machine-translated press release from South Korea's Peninsula Policy Bureau.

The Chosun Geumjeong Economic Information Technology Exchange Corporation is described as a company that "dispatches many North Korean IT personnel overseas and pays a large amount of military funds to the North Korean regime," according to the release.

North Koreans posing as IT workers to gain employment at Western firms — bypassing work restrictions and earning revenue for their home government — has become a frequent occurrence in recent years. The growing trend has increasingly alarmed U.S. and Western national security officials, as well as company executives who have publicly come forward with their experiences after being duped.

Beyond just earning a paycheck, placing North Korean operatives in technical roles at Western firms can also make it easier to carry out hacking operations and cryptocurrency theft. In some cases, these workers have installed malicious software on company devices, stolen hundreds of thousands of dollars from companies and attempted to gain access to sensitive software building environments. Some executives suggest the issue is likely worse than the public understands, as the stigma of hiring a fraudulent employee still pushes companies to keep quiet.

South Korea also accused its northern neighbor of playing an outsized role in global cryptocurrency theft. A 2024 report by a United Nations panel stated that it is investigating at least 58 cyberattacks by DPRK operatives against cryptocurrency companies between 2017 and 2023, with the incidents yielding an estimated $3 billion in stolen gains. The panel also investigated "reports of numerous Democratic People's Republic of Korea nationals working

overseas earning income in violation of sanctions, including in the information technology, restaurant and construction sectors.”

In addition to threatening the overall cyber ecosystem, South Korea said the actions pose “a serious threat to international peace and security in that it is being used to fund North Korea’s nuclear and missile development.”
