US offers $5 million for info on North Korean IT worker farms

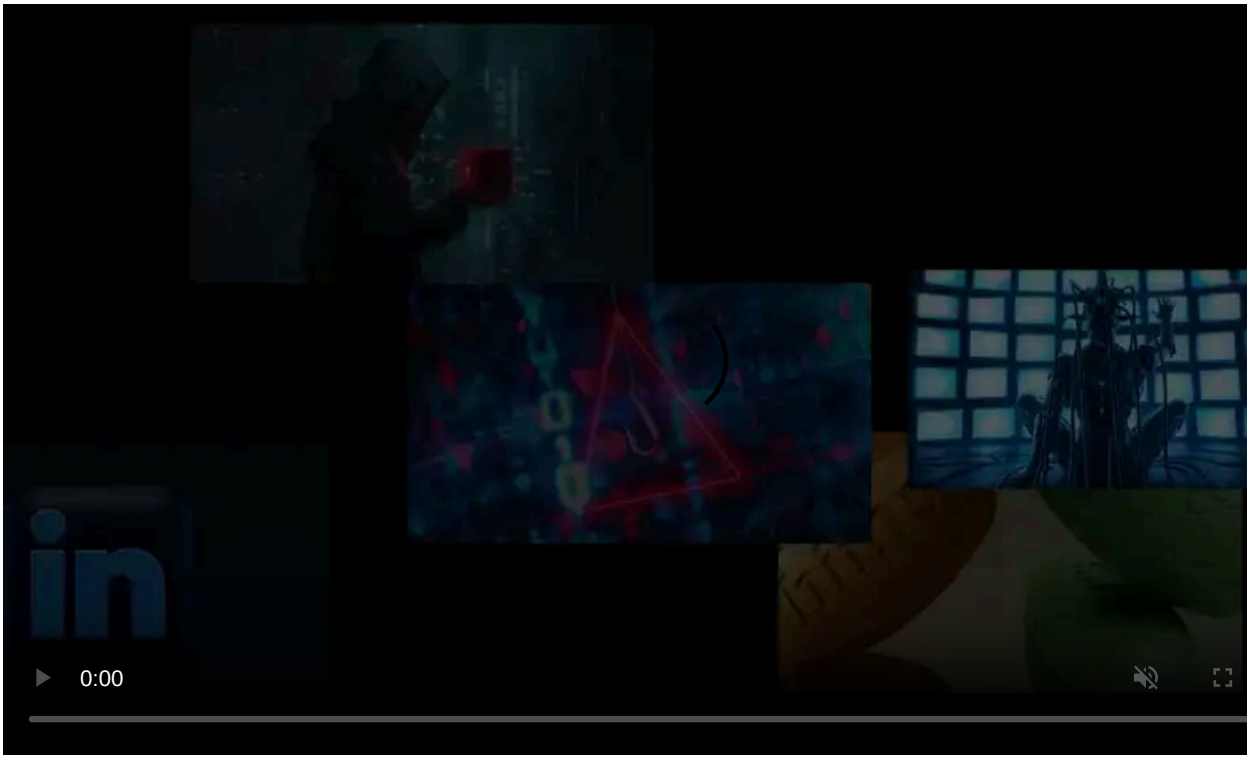
By Sergiu Gatlan

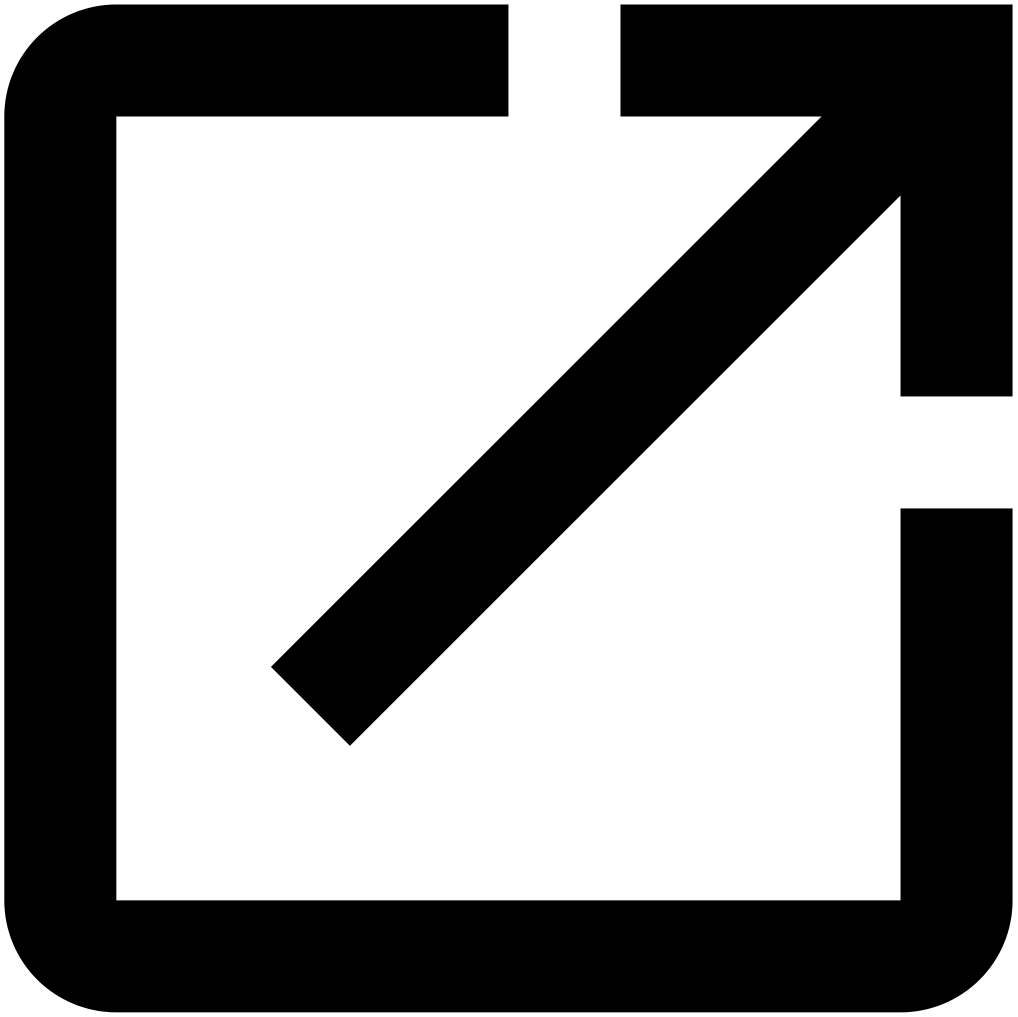
Published: 2024-12-12 · Archived: 2026-04-05 17:05:57 UTC

The U.S. State Department is offering a reward of up to $5 million for information that could help disrupt the activities of North Korean front companies and employees who generated over $88 million via illegal remote IT work schemes in six years.

The two companies, Chinese-based Yanbian Silverstar and Volasys Silverstar from Russia, tricked businesses worldwide into employing North Korean staff as freelance IT workers.

These illegally obtained funds are then laundered in violation of international sanctions and sent back to the Pyongyang regime to support the country's UN-prohibited nuclear missile programs. As the FBI, the State Department, and the Justice Department said in a May 2022 tri-seal advisory, each of North Korea's IT workers can earn up to $300,000 annually, generating hundreds of millions of dollars collectively every year.


0:00



"Yanbian Silverstar and Volasys Silverstar together employ more than 130 DPRK IT workers, who refer to themselves as 'IT warriors,'" the State Department said on Thursday.

"These IT workers use the fraudulently acquired identities of hundreds of U.S. persons to gain remote employment and generate tens of millions of dollars which are laundered and sent back to the North Korean regime."

14 Yanbian and Volasys Silverstar employees indicted

Today, the DOJ also indicted 14 North Korean "IT warriors" linked to Yanbian Silverstar and Volasys Silverstar for their involvement in conspiracies to violate U.S. sanctions and to commit identity theft, wire fraud, and money laundering.

Led by Jong Song Hwa, Yanbian Silverstar's and Volasys Silverstar's CEO, they generated at least $88 million over approximately six years.

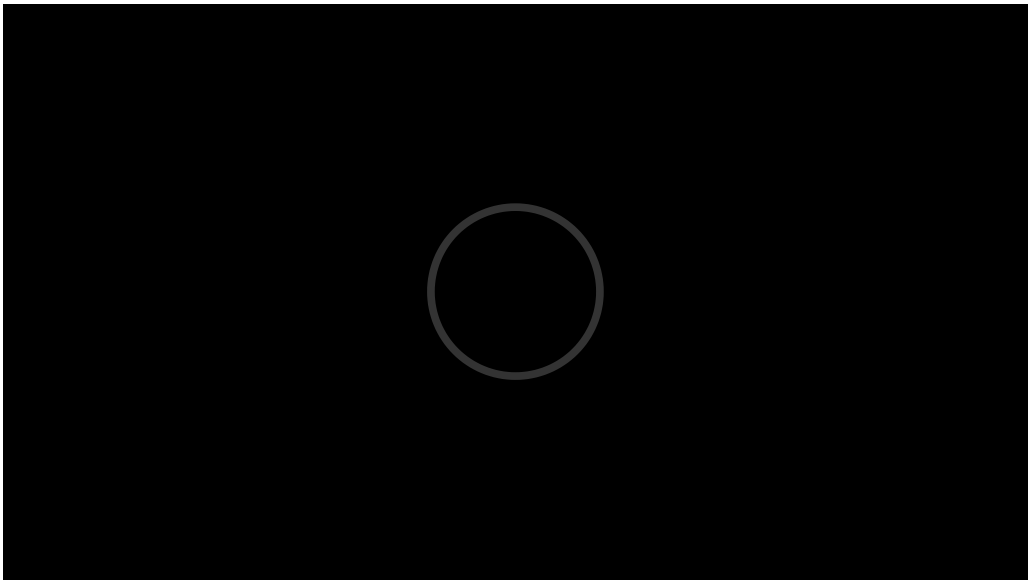
Prior DOJ actions targeting this group include the seizure of roughly $320,000 in January, another approximately $444,800 in July, court-authorized seizures of around $1.5 million in October 2022 and January 2023, and the seizure of 29 internet domains in October 2023 and May 2024.

When communicating with prospective employers, the threat actors used dozens of such domains to make their stolen identities more legitimate.

Throughout the conspiracy, Volasys Silverstar and Yanbian Silverstar workers stole, borrowed, and purchased the identities of U.S. citizens, which were used to hide their true identities and obtain remote employment with U.S. businesses and organizations.

They also used them to register domain names to host websites that helped dupe U.S. employers into thinking they were previously hider by other reputable U.S. companies and to create accounts to collect the funds earned from employers, which were later transferred to North Korean-controlled accounts at Chinese banks.

After being discovered and fired, some of the North Korean IT workers used insider knowledge and coding skills to extort their former employers, threatening to leak stolen sensitive information online.



In August, U.S. law enforcement dismantled a laptop farm used by undercover North Korean "IT warriors" to work from locations in China while appearing to connect to the victim companies' systems from Nashville.

In May, Arizona woman Christina Marie Chapman was also arrested and charged with running another North Korean laptop farm in her own home.

Today's charges emphasize the ongoing danger presented by North Korean IT workers who impersonate U.S.-based IT staff, something that the FBI has warned for years. As it has repeatedly cautioned, North Korea maintains a large army of IT workers trained to conceal their true identities to secure employment at hundreds of American companies.

Most recently, cybersecurity company KnowBe4 hired a North Korean malicious actor as a Principal Software Engineer. However, the "IT warrior" immediately attempted to install information-stealing malware on company-provided devices.

Even though KnowBe4 had conducted background checks, verified references, and held four video interviews before hiring the North Korean, they later discovered that the person had used a stolen identity and AI tools to deceive the company during video calls.

Source: https://www.bleepingcomputer.com/news/security/us-offers-5-million-for-info-on-north-korean-it-worker-farms/