THE UNITED STATES DEPARTMENT of JUSTICE

FOR IMMEDIATE RELEASE
June 30, 2025
www.justice.gov

NSD
202-514-2007
TTY 866-544-5309

Justice Department Announces Coordinated, Nation-Wide Actions to Combat North Korean Remote Information Technology Workers' Illicit Revenue Generation Schemes

Law Enforcement Actions Across 16 States Result in Charges, Arrest, and Seizures of 29 Financial Accounts, 21 Fraudulent Websites, and Approximately 200 Computers

WASHINGTON – The Justice Department announced today coordinated actions against the Democratic People's Republic of North Korea (DPRK) government's schemes to fund its regime through remote information technology (IT) work for U.S. companies. These actions include two indictments, an arrest, searches of 29 known or suspected "laptop farms" across 16 states, and the seizure of 29 financial accounts used to launder illicit funds and 21 fraudulent websites.

According to court documents, the schemes involve North Korean individuals fraudulently obtaining employment with U.S. companies as remote IT workers, using stolen and fake identities. The North Korean actors were assisted by individuals in the United States, China, United Arab Emirates, and Taiwan, and successfully obtained employment with more than 100 U.S. companies.

As alleged in court documents, certain U.S.-based individuals enabled one of the schemes by creating front companies and fraudulent websites to promote the bona fides of the remote IT workers, and hosted laptop farms where the remote North Korean IT workers could remote access into U.S. victim company-provided laptop computers. Once employed, the North Korean IT workers received regular salary payments, and they gained access to, and in some cases stole, sensitive employer information such as export controlled U.S. military technology and virtual currency. In another scheme, North Korean IT workers used false or fraudulently obtained identities to gain employment with an Atlanta, Georgia-based blockchain research and development company and stole virtual currency worth approximately $740,000.

"These schemes target and steal from U.S. companies and are designed to evade sanctions and fund the North Korean regime's illicit programs, including its weapons programs," said John A. Eisenberg, Assistant Attorney General for the Department's National Security Division. "The Justice Department, along with our law enforcement, private sector, and international partners, will persistently pursue and dismantle these cyber-enabled revenue generation networks."

"North Korean IT workers defraud American companies and steal the identities of private citizens, all in support of the North Korean regime," said Assistant Director Brett Leatherman of FBI's Cyber Division. "That is why the FBI and our partners continue to work together to disrupt infrastructure, seize revenue, indict overseas IT workers, and arrest their enablers in the United

States. Let the actions announced today serve as a warning: if you host laptop farms for the benefit of North Korean actors, law enforcement will be waiting for you."

"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 Assistant Director Roman Rozhavsky of the FBI Counterintelligence Division. "North Korean IT workers posing as U.S. citizens fraudulently obtained employment with American businesses so they could funnel hundreds of millions of dollars to North Korea's authoritarian regime. The FBI will do everything in our power to defend the homeland and protect Americans from being victimized by the North Korean government, and we ask all U.S. companies that employ remote workers to remain vigilant to this sophisticated threat."

Zhenxing Wang, et al. Indictment, Seizure Warrants, and Arrest – District of Massachusetts

Today, the United States Attorney's Office for the District of Massachusetts and the National Security Division announced the arrest of U.S. national Zhenxing "Danny" Wang of New Jersey pursuant to a five-count indictment. The indictment describes a multi-year fraud scheme by Wang and his co-conspirators to obtain remote IT work with U.S. companies that generated more than $5 million in revenue. The indictment also charges Chinese nationals Jing Bin Huang (靖斌 黄), Baoyu Zhou (周宝玉), Tong Yuze (佟雨泽), Yongzhe Xu (徐勇哲 and يونجزهي أكسو), Ziyou Yuan (زيو) and Zhenbang Zhou (周震邦), and Taiwanese nationals Mengting Liu (劉 孟婷) and Enchia Liu (刘恩) for their roles in the scheme.

"The threat posed by DPRK operatives is both real and immediate. Thousands of North Korean cyber operatives have been trained and deployed by the regime to blend into the global digital workforce and systematically target U.S. companies," said U.S. Attorney Leah B. Foley for the District of Massachusetts. "We will continue to work relentlessly to protect U.S. businesses and ensure they are not inadvertently fueling the DPRK's unlawful and dangerous ambitions."

According to the indictment, from approximately 2021 until October 2024, the defendants and other co-conspirators compromised the identities of more than 80 U.S. persons to obtain remote jobs at more than 100 U.S. companies, including many Fortune 500 companies, and caused U.S. victim companies to incur legal fees, computer network remediation costs, and other damages and losses of at least $3 million. Overseas IT workers were assisted by Kejia Wang, Zhenxing Wang, and at least four other identified U.S. facilitators. Kejia Wang, for example, communicated with overseas co-conspirators and IT workers, and traveled to Shenyang and Dandong, China, including in 2023, to meet with them about the scheme. To deceive U.S. companies into believing the IT workers were located in the United States, Kejia Wang, Zhenxing Wang, and the other U.S. facilitators received and/or hosted laptops belonging to U.S. companies at their residences, and enabled overseas IT workers to access the laptops remotely by, among other things, connecting the laptops to hardware devices designed to allow for remote access (referred to as keyboard-video-mouse or "KVM" switches).

Kejia Wang and Zhenxing Wang also created shell companies with corresponding websites and financial accounts, including Hopana Tech LLC, Tony WKJ LLC, and Independent Lab LLC, to make it appear as though the overseas IT workers were affiliated with legitimate U.S. businesses.

Kejia Wang and Zhenxing Wang established these and other financial accounts to receive money from victimized U.S. companies, much of which was subsequently transferred to overseas co-conspirators. In exchange for their services, Kejia Wang, Zhenxing Wang, and the four other U.S. facilitators received a total of at least $696,000 from the IT workers.

IT workers employed under this scheme also gained access to sensitive employer data and source code, including International Traffic in Arms Regulations (ITAR) data from a California-based defense contractor that develops artificial intelligence-powered equipment and technologies. Specifically, between on or about January 19, 2024, and on or about April 2, 2024, an overseas co-conspirator remotely accessed without authorization the company's laptop and computer files containing technical data and other information. The stolen data included information marked as being controlled under the ITAR.

Simultaneously with today's announcement, the FBI and Defense Criminal Investigative Service (DCIS) seized 17 web domains used in furtherance of the charged scheme and further seized 29 financial accounts, holding tens of thousands of dollars in funds, used to launder revenue for the North Korean regime through the remote IT work scheme.

Previously, in October 2024, as part of this investigation, federal law enforcement executed searches at eight locations across three states that resulted in the recovery of more than 70 laptops and remote access devices, such as KVMs. Simultaneously with that action, the FBI seized four web domains associated with Kejia Wang's and Zhenxing Wang's shell companies used to facilitate North Korean IT work.

The FBI Las Vegas Field Office, DCIS San Diego Resident Agency, and Homeland Security Investigations San Diego Field Office are investigating the case.

Assistant U.S. Attorney Jason Casey for the District of Massachusetts and Trial Attorney Gregory J. Nicosia, Jr. of the National Security Division's National Security Cyber Section are prosecuting the case, with significant assistance from Legal Assistants Daniel Boucher and Margaret Coppes. Valuable assistance was also provided by Mark A. Murphy of the National Security Division's Counterintelligence and Export Control Section and the U.S. Attorneys' Offices for the District of New Jersey, Eastern District of New York, and Southern District of California.

Kim Kwang Jin et al. Indictment – Northern District of Georgia

Today, the Northern District of Georgia unsealed a five-count wire fraud and money laundering indictment charging four North Korean nationals, Kim Kwang Jin (김관진), Kang Tae Bok (강태복), Jong Pong Ju (정봉주) and Chang Nam Il (창남일), with a scheme to steal virtual currency from two companies, valued at over $900,000 at the time of the thefts, and to launder proceeds of those thefts. The defendants remain at large and wanted by the FBI.

"The defendants used fake and stolen personal identities to conceal their North Korean nationality, pose as remote IT workers, and exploit their victims' trust to steal hundreds of thousands of dollars," said U.S. Attorney Theodore S. Hertzberg for the Northern District of Georgia. "This indictment highlights the unique threat North Korea poses to companies that hire remote IT

workers and underscores our resolve to prosecute any actor, in the United States or abroad, who steals from Georgia businesses."

According to the indictment, the defendants traveled to the United Arab Emirates on North Korean travel documents and worked as a co-located team. In approximately December 2020 and May 2021, respectively, Kim Kwang Jin (using victim P.S.'s stolen identity) and Jong Pong Ju (using the alias "Bryan Cho") were hired by a blockchain research and development company headquartered in Atlanta, Georgia, and a virtual token company based in Serbia. Both defendants concealed their North Korean identities from their employers by providing false identification documents containing a mix of stolen and fraudulent identity information. Neither company would have hired Kim Kwang Jin and Jong Pong Ju had they known that they were North Korean citizens. Later, on a recommendation from Jong Pong Ju, the Serbian company hired "Peter Xiao," who in fact was Chang Nam Il.

After gaining their employers' trust, Kim Kwang Jin and Jong Pong Ju were assigned projects that provided them access to their employers' virtual currency assets. In February 2022, Jong Pong Ju used that access to steal virtual currency worth approximately $175,000 at the time of the theft, sending it to a virtual currency address he controlled. In March 2022, Kim Kwang Jin stole virtual currency worth approximately $740,000 at the time of theft by modifying the source code of two of his employer's smart contracts, then sending it to a virtual currency address he controlled.

To launder the funds after the thefts, Kim Kwang Jin and Jong Pong Ju "mixed" the stolen funds using the virtual currency mixer Tornado Cash and then transferred the funds to virtual currency exchange accounts controlled by defendants Kang Tae Bok and Chang Nam Il but held in the name of aliases. These accounts were opened using fraudulent Malaysian identification documents.

The FBI Atlanta Field Office is investigating the case.

Assistant U.S. Attorneys Samir Kaushal and Alex Sistla for the Northern District of Georgia and Trial Attorney Jacques Singer-Emery of the National Security Division's National Security Cyber Section are prosecuting the case.

<u>21 Searches of Known or Suspected U.S.-based Laptop Farms – Multi-District</u>

Between June 10 and June 17, 2025, the FBI executed searches of 21 premises across 14 states hosting known and suspected laptop farms. These actions, coordinated by the FBI Denver Field Office, related to investigations of North Korean remote IT worker schemes being conducted by the U.S. Attorneys' Offices of the District of Colorado, Eastern District of Missouri, and Northern District of Texas. In total, the FBI seized approximately 137 laptops.

Valuable assistance was provided by the U.S. Attorney's Offices for the District of Connecticut, the Eastern District of Michigan, the Eastern District of Wisconsin, the Middle District of Florida, the Northern District of Georgia, the Northern District of Illinois, the Northern District of Indiana, the District of Oregon, the Southern District of Florida, the Southern District of Ohio, the Western District of New York, and the Western District of Pennsylvania.

***

The Department's actions to combat these schemes are the latest in a series of law enforcement actions under a joint National Security Division and FBI Cyber and Counterintelligence Divisions effort, the DPRK RevGen: Domestic Enabler Initiative. This effort prioritizes targeting and disrupting the DPRK's illicit revenue generation schemes and its U.S.-based enablers. The Department previously announced other actions pursuant to the initiative, including in January 2025 and prior, as well as the filing of a civil forfeiture complaint in early June 2025 for over $7.74 million tied to an illegal employment scheme.

As the FBI has described in Public Service Announcements published in May 2024 and January 2025, North Korean remote IT workers posing as legitimate remote IT workers have committed data extortion and exfiltrated the proprietary and sensitive data from U.S. companies. DPRK IT worker schemes typically involve the use of stolen identities, alias emails, social media, online cross-border payment platforms, and online job site accounts, as well as false websites, proxy computers, and witting and unwitting third parties located in the U.S. and elsewhere.

Other public advisories about the threats, red flag indicators, and potential mitigation measures for these schemes include a May 2022 advisory released by the FBI, Department of the Treasury, and Department of State; a July 2023 advisory from the Office of the Director of National Intelligence; and guidance issued in October 2023 by the United States and the Republic of Korea (South Korea). As described the May 2022 advisory, North Korean IT workers have been known individually to earn up to $300,000 annually, generating hundreds of millions of dollars collectively each year, on behalf of designated entities, such as the North Korean Ministry of Defense and others directly involved in the DPRK's weapons programs.

The U.S. Department of State has offered potential rewards for up to $5 million in support of international efforts to disrupt the DPRK's illicit financial activities, including for cybercrimes, money laundering, and sanctions evasion.

The details in the above-described court documents are merely allegations. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Links to Court Documents:

DMA Indictment
NDGA Indictment