News

All News
Blogs
Photo Galleries
Podcasts
Press Releases
Speeches
Videos

Archived News

Para Noticias en Español

PRESS RELEASE

Justice Department Disrupts North Korean Remote IT Worker Fraud Schemes Through Charges and Arrest of Nashville Facilitator

Thursday, August 8, 2024

Share

For Immediate Release
Office of Public Affairs

Defendant Used a "Laptop Farm" to Deceive Companies Into Thinking They Had Hired a U.S.-Located Worker

Matthew Isaac Knoot, 38, of Nashville, Tennessee, was arrested today for his efforts to generate revenue for the Democratic People's Republic of Korea's (DPRK or North Korea) illicit weapons program, which includes weapons of mass destruction (WMD).

The FBI, along with the Departments of State and Treasury, issued a May 2022 advisory to alert the international community, private sector, and public about the North Korea IT worker threat. Updated guidance was issued in October 2023 by the United States and the Republic of Korea (South Korea) and in May 2024 by the FBI, which include indicators to watch for that are consistent with the North Korea IT worker fraud and the use of U.S.-based laptop farms.

According to court documents, Knoot participated in a scheme to obtain remote employment with American and British companies for foreign information technology (IT) workers, who were actually North Korean actors. Knoot allegedly assisted them in using a stolen identity to pose as a U.S. citizen; hosted company laptops at his residences; downloaded and installed software without authorization on such laptops to facilitate access and perpetuate the deception; and conspired to launder payments for the remote IT work, including to accounts tied to North Korean and Chinese actors.

"As alleged, this defendant facilitated a scheme to deceive U.S. companies into hiring foreign remote IT workers who were paid hundreds of thousands of dollars in income funneled to the DPRK for its weapons program," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "This indictment should serve as a stark warning to U.S. businesses that employ remote IT workers of the growing threat from the DPRK and the need to be vigilant in their hiring processes."

"North Korea has dispatched thousands of highly skilled information technology workers around the world to dupe unwitting businesses and evade international sanctions so that it can continue to fund its dangerous weapons program," said U.S. Attorney Henry C. Leventis for the Middle District of Tennessee. "Today's indictment, charging the defendant with facilitating a complex, multi-year scheme that funneled hundreds of thousands of dollars to foreign actors, is the most recent example of our office's commitment to protecting the United States' national security interests."

"As today's charges demonstrate, the FBI will relentlessly pursue those who aid the North Korean government's illegal efforts to generate revenue," said Assistant Director Bryan Vorndran of the FBI's Cyber Division. "Where illicit proceeds may be used to fund the regime's kinetic capacity, we will prioritize our work to disrupt that flow of money. This indictment should demonstrate the risk faced by those who support the DPRK's malicious cyber activity."

The DPRK has dispatched thousands of skilled IT workers to live abroad, primarily in China and Russia, with the aim of deceiving U.S. and other businesses worldwide into hiring them as freelance IT workers to generate revenue for its WMD programs. DPRK IT worker schemes involve the use of pseudonymous email, social media, payment platform and online job site accounts, as well as false websites, proxy computers, and witting and unwitting third parties located in the United States and elsewhere. As described in a May 2022 tri-seal public service advisory released by the FBI, the Department of the Treasury, and the Department of State, such IT workers have been known to individually 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 UN-prohibited WMD programs.

The indictment unsealed today in the Middle District of Tennessee alleges that Knoot participated in a scheme to assist overseas IT workers to obtain remote IT work at U.S. companies which believed that they were hiring U.S.-based personnel. The IT workers, who were North Korean nationals, used the stolen identity of a U.S. citizen, "Andrew M.," to obtain this remote IT work. The scheme defrauded U.S. media, technology, and financial companies, ultimately causing them hundreds of thousands of dollars in damages.

According to court documents, Knoot ran a "laptop farm" at his Nashville residences between approximately July 2022 and August 2023. The victim companies shipped laptops addressed to "Andrew M." to Knoot's residences. Following receipt of the laptops, and without authorization, Knoot logged on to the laptops, downloaded and installed unauthorized remote desktop applications, and accessed the victim companies' networks, causing damage to the computers. The remote desktop applications enabled the North Korean IT workers to work from locations in China, while appearing to the victim companies that "Andrew M." was working from Knoot's residences in Nashville. For his participation in the scheme, Knoot was paid a monthly fee for his services by a foreign-based facilitator who went by the name Yang Di. A court-authorized search of Knoot's laptop farm was executed in early August 2023.

The overseas IT workers associated with Knoot's cell were each paid over $250,000 for their work between approximately July 2022 and August 2023, much of which was falsely reported to the Internal Revenue Service and the Social Security Administration in the name of the actual U.S. person, Andrew M., whose identity was stolen. Knoot and his conspirators' actions also caused the victim companies more than $500,000 in costs associated with auditing and remediating their devices, systems, and networks. Knoot, Di, and others conspired to commit money laundering by conducting financial transactions to receive payments from the victim companies, transfer those funds to Knoot and to accounts outside of the United States, in an attempt both to promote their unlawful activity and to hide that transferred funds were the proceeds of it. The non-U.S. accounts include accounts associated with North Korean and Chinese actors.

Knoot is charged with conspiracy to cause damage to protected computers, conspiracy to launder monetary instruments, conspiracy to commit wire fraud, intentional damage to protected computers, aggravated identity theft and conspiracy to cause the unlawful employment of aliens. If convicted, Knoot faces a maximum penalty of 20 years in prison, including a mandatory minimum of two years in prison on the aggravated identity theft count.

Under the Department-wide "DPRK RevGen: Domestic Enabler Initiative," launched in March 2024 by the National Security Division and the FBI's Cyber and Counterintelligence Divisions, Department prosecutors and agents are prioritizing the identification and shuttering of U.S.-based "laptop farms" — locations hosting laptops provided by victim U.S. companies to individuals they believed were legitimate U.S.-based freelance IT workers — and the investigation and prosecution of individuals hosting them. Today's announcement follows successful action taken by the Department in October 2023 and May 2024 , which targeted identical and related conduct.

The FBI is investigating the case.

Assistant U.S. Attorney Josh Kurtzman for the Middle District of Tennessee and Trial Attorney Greg Nicosia of the National Security Division's Cyber Section are prosecuting the case.

An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Updated August 8, 2024

Topic

NATIONAL SECURITY

Components

Federal Bureau of Investigation (FBI) | National Security Division (NSD) | USAO - Tennessee, Middle

Press Release Number: 24-987

Related Content

PRESS RELEASE

U.S. Army Soldier Sentenced to 14 Years in Prison For Attempting to Assist ISIS to Conduct Deadly Ambush on U.S. Troops

Cole Bridges, also known as Cole Gonzales, 24, of Stow, Ohio, was sentenced to 168 months in prison followed by 10 years of supervised release for attempting to provide material...

October 11, 2024

PRESS RELEASE

Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers

The Justice Department today announced a court-authorized law enforcement operation that disrupted a botnet consisting of more than 200,000 consumer devices in the United States and worldwide. As described in...

September 18, 2024

PRESS RELEASE

Suspect at Trump International Golf Course Charged with Firearms Offenses

Ryan Wesley Routh, 58, of Hawaii, has been charged by a criminal complaint in the Southern District of Florida with firearms charges related to an incident at Trump International Golf...

September 16, 2024

Office of Public Affairs
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington DC 20530

Office of Public Affairs Direct Line
202-514-2007

Department of Justice Main Switchboard
202-514-2000

Signup for Email Updates
Social Media