Justice Department Announces Court-Authorized Action to Disrupt Illicit Revenue Generation Efforts of Democratic People's Republic of Korea Information Technology Workers

Press Release

Wednesday, October 18, 2023

For Immediate Release
Office of Public Affairs

Seizures of Money and Infrastructure from Democratic People's Republic of Korea (DPRK) IT Workers Follows Successful Efforts to Empower Independent Private Sector Disruptive Actions

On Oct. 17, pursuant to a court order issued in the Eastern District of Missouri, the United States seized 17 website domains used by Democratic People's Republic of Korea(DPRK) information technology (IT) workers in a scheme to defraud U.S. and foreign businesses, evade sanctions and fund the development of the DPRK government's weapons program. These seizures follow the previously sealed October 2022 and January 2023 court-authorized seizures of approximately $1.5 million of the revenue that the same group of IT workers collected from unwitting victims as a result of their scheme, as well as the development of public-private information-sharing partnerships that denied the IT workers access to their preferred online freelance work and payment service providers.

"The seizures announced today protect U.S. companies from being infiltrated with North Korean computer code and help ensure that American businesses are not used to finance that regime's weapons program," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "The Department of Justice is committed to working with private sector partners to protect U.S. business from this kind of fraud, to enhance our collective cybersecurity and to disrupt the funds fueling North Korean missiles."

“Today's seizures exemplify our commitment to working with our federal and international partners to recognize and disrupt the threat from illicit actors working on behalf of the Democratic People’s Republic of Korea,” said Assistant Director Bryan Vorndran of the FBI's Cyber Division. “These takedowns also serve as reminders to ensure that our private sector partners are equipped and prepared with due diligence measures to prevent the inadvertent hiring of these bad actors across American businesses. The FBI encourages U.S. companies to report suspicious activities, including any suspected DPRK IT worker activities, to your local FBI field office.”

“Employers need to be cautious about who they are hiring and who they are allowing to access their IT systems,” said U.S. Attorney Sayler A. Fleming for the Eastern District of Missouri. “You may be helping to fund North Korea’s weapons program or allowing hackers to steal your data or extort you down the line.”

“The Democratic People’s Republic of Korea has flooded the global marketplace with ill-intentioned information technology workers to indirectly fund its ballistic missile program. The seizing of these fraudulent domains helps protect companies from unknowingly hiring these bad actors and potentially damaging their business,” said Special Agent in Charge Jay Greenberg of the FBI St. Louis Division. “This scheme is so prevalent that companies must be vigilant to verify whom they're hiring. At a minimum, the FBI recommends that employers take additional proactive steps with remote IT workers to make it harder for bad actors to hide their identities. Without due diligence, companies risk losing money or being compromised by insider threats they unknowingly invited inside their systems.”

As alleged in court documents, the Government of the Democratic People’s Republic of Korea (DPRK) 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, in order to generate revenue for its weapons of mass destruction (WMD) programs. Through this scheme, which involves the use of pseudonymous email, social media, payment platform and online job site accounts, as well as false websites, proxy computers located in the United States and elsewhere, and witting and unwitting third parties, the IT workers generated millions of dollars a 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.

In some instances, the IT workers also infiltrated the computer networks of unwitting employers to steal information and maintain access for future hacking and extortion schemes. The U.S. government described this scheme in a May 2022 advisory. An update to that advisory, issued today, is available here.

Certain DPRK IT workers designed the 17 website domains seized yesterday to appear as domains of legitimate, U.S.-based IT services companies, thereby helping the IT workers to hide their true identities and location when applying online to do remote work for U.S. and other businesses worldwide. In reality, this specific group of DPRK IT workers, who work for the PRC-based Yanbian Silverstar Network Technology Co. Ltd. and the Russia-based Volasys Silver Star, had previously been sanctioned in 2018 by the Department of the Treasury. These IT workers funneled income from their fraudulent IT work back to the DPRK through the use of online payment services and Chinese bank accounts.

The efforts to disrupt the DPRK IT worker threat are not limited to those of the U.S. government. Since 2022, the United States has partnered with the Republic of Korea (ROK) to provide threat information about fraudulent DPRK IT worker activity, primarily consisting of thousands of indicators (e.g., email addresses), to multiple U.S.-based online freelance work and payment service platforms used by the IT workers. These information-sharing efforts include a May 2023 symposium , jointly hosted by the U.S. Department of State and the ROK, where representatives from the United States and ROK, and the providers, jointly discussed efforts to enhance public-private partnerships to counter the DPRK IT worker threat. These private companies later informed the U.S. government that, armed with that threat information, they conducted independent investigations, improved their fraud detection mechanisms and, according to at least some of the providers, shut down thousands of additional, previously unidentified fraudulent accounts used by the same DPRK IT workers.

The National Security Division's National Security Cyber Section and the U.S. Attorney's Office for the Eastern District of Missouri are investigating this case. The FBI's St. Louis Field Office conducted the investigation, with the assistance of the FBI Cyber Division.

Affidavit and Application for Seizure - $397k ;
Affidavit and Application for Seizure - 12 Domain Names
Affidavit and Application for Seizure - $1.1 million ;
Affidavit and Application for Seizure - 5 Domain Names ;
Updated October 18, 2023

Topics

Cybercrime

National Security

Press Release Number: 23-1,156