United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors

Press Release

Thursday, August 27, 2020

For Immediate Release
Office of Public Affairs

The Justice Department today filed a civil forfeiture complaint detailing two hacks of virtual currency exchanges by North Korean actors. These actors stole millions of dollars' worth of cryptocurrency and ultimately laundered the funds through Chinese over-the-counter (OTC) cryptocurrency traders. The complaint follows related criminal and civil actions announced in March 2020 pertaining to the theft of $250 million in cryptocurrency through other exchange hacks by North Korean actors.

"Today's action publicly exposes the ongoing connections between North Korea's cyber-hacking program and a Chinese cryptocurrency money laundering network," said Acting Assistant Attorney General Brian C. Rabbitt of the Justice Department's Criminal Division. "This case underscores the department's ongoing commitment to counter the threat presented by North Korean cyber hackers by exposing their criminal networks and tracing and seizing their ill-gotten gains."

"Today, prosecutors and investigators have once again exemplified our commitment to attribute national security cyber threats, to impose costs on these actors, and bring some measure of relief to victims of malicious cyber activities," said Assistant Attorney General John C. Demers of the Justice Department's National Security Division. "Although North Korea is unlikely to stop trying to pillage the international financial sector to fund a failed economic and political regime, actions like those today send a powerful message to the private sector and foreign governments regarding the benefits of working with us to counter this threat."

“As part of our commitment to safeguarding national security, this office has been at the forefront of targeting North Korea’s criminal attacks on the financial system,” said Acting U.S. Attorney Michael R. Sherwin of the District of Columbia. “This complaint reveals the incredible skill of our Cryptocurrency Strike Force in tracing and seizing virtual currency, which criminals previously thought to be impossible.”

“Despite the highly sophisticated laundering techniques used, IRS-CI’s Cybercrimes Unit was able to successfully trace stolen funds directly back to North Korean actors,” said Don Fort, Chief of IRS Criminal Investigation (IRS-CI). “IRS-CI will continue to collaborate with its law enforcement partners to combat foreign and domestic operations that threaten the United States financial system and national security.”

“FBI efforts to stop the flow of threat finance around the world are central to our strategy to address transnational crime,” said Assistant Director Calvin A. Shivers of the FBI’s Criminal Investigative Division. “This strategy is strengthened by the skills and expertise we continue to develop in virtual asset investigations such as this, which enable the FBI and our partners to identify and seize illicit assets.”

“As North Korea becomes bolder and more desperate in their efforts to steal money using sophisticated money laundering techniques, HSI will continue to apply pressure by exposing their fraudulent transactions,” said Special Agent in Charge Steven Cagen of U.S. Immigration and Customs Enforcement’s Homeland Security Investigations (HSI) Denver. “We are committed to safeguarding the interest of the United States against the criminal elements in North Korea to protect the integrity of the cyber financial system.”

“At U.S. Cyber Command, we leverage a persistent engagement approach to challenge our adversaries’ actions in cyberspace,” said Brigadier General Joe Hartman, Commander of the Cyber National Mission Force. “This includes disrupting North Korean efforts to illicitly generate revenue. Department of Defense cyber operations do not occur in isolation. Persistent engagement includes acting through cyber-enabled operations as much as it does sharing information with our interagency partners to do the same.”

“Today’s complaint demonstrates that North Korean actors cannot hide their crimes within the anonymity of the internet. International cryptocurrency laundering schemes undermine the integrity of our financial systems at a global level, and we will use every tool in our arsenal to investigate and disrupt these crimes,” said Special Agent in Charge Emmerson Buie Jr. of the FBI’s Chicago Field Office. “The FBI will continue to impose risks and consequences on criminals who seek to undermine our national security interests.”

The forfeiture complaint filed today details two related hacks of virtual currency exchanges.

As alleged in the complaint, in July 2019, a virtual currency exchange was hacked by an actor tied to North Korea. The hacker allegedly stole over $272,000 worth of alternative cryptocurrencies and tokens, including Proton Tokens, PlayGame tokens, and IHT Real Estate Protocol tokens. Over the subsequent months, the funds were laundered through several intermediary addresses and other virtual currency exchanges. In many instances, the actor converted the cryptocurrency into BTC, Tether, or other forms of cryptocurrency – a process known as “chain hopping” – in order to obfuscate the transaction path. As detailed in the pleadings, law enforcement was nonetheless able to trace the funds, despite the sophisticated laundering techniques used.

As also alleged in the pleadings, in September 2019, a U.S.-based company was hacked in a related incident. The North Korea-associated hacker gained access to the company's virtual currency wallets, funds held by the company on other platforms, and funds held by the company's partners. The hacker stole nearly $2.5 million and laundered it through over 100 accounts at another virtual currency exchange.

The funds from both of the above hacks, as well as hacks previously detailed in a March 2020 forfeiture action (1:20-cv-00606-TJK), were all allegedly laundered by the same group of Chinese OTC actors. The infrastructure and communication accounts used to further the intrusions and fund transfers were also tied to North Korea.

The claims made in this complaint are only allegations and do not constitute a determination of liability. The burden to prove forfeitability in a civil forfeiture proceeding is upon the government.

The investigation was conducted by IRS-CI's Washington, D.C. Cyber Crimes Unit, the FBI's Chicago and Atlanta Field Offices, and HSI's Colorado Springs Office with additional support from the FBI's San Francisco Field Office. Trial Attorney C. Alden Pelker of the Criminal Division's Computer Crime and Intellectual Property Section, Trial Attorney David Recker of the National Security Division's Counterintelligence and Export Control Section and Assistant U.S. Attorneys Zia M. Faruqui, Jessi Camille Brooks, and Christopher Brown are prosecuting the case, with assistance from Supervisory Paralegal Specialist Elizabeth Swienc and Legal Assistant Jessica McCormick.

Support to this effort was provided by FBI's San Francisco Field Office and the U.S. Attorney's Office of the Northern District of Georgia.

Support to this effort was also provided by United States Cyber Command. More information about the command's efforts to combat North Korean and other malware activity can be found on Twitter and VirusTotal.

The year 2020 marks the 150th anniversary of the Department of Justice. Learn more about the history of our agency at www.Justice.gov/Celebrating150Years.

Updated July 13, 2022

Topics

Countering Nation-State Threats

Counterintelligence

Asset Forfeiture

Cybercrime

Press Release Number: 20-836