Russian Nationals Charged With Hacking One Cryptocurrency Exchange and Illicitly Operating Another

Press Release

Friday, June 9, 2023

For Immediate Release
Office of Public Affairs

The Justice Department unsealed charges related to the 2011 hack of the cryptocurrency exchange Mt. Gox and the operation of the illicit cryptocurrency exchange BTC-e.

According to court documents, Alexey Bilyuchenko, 43, and Aleksandr Verner, 29, both Russian nationals, are charged with conspiring to launder approximately 647,000 bitcoins from their hack of Mt. Gox. Bilyuchenko is also charged with conspiring with Alexander Vinnik to operate BTC-e from 2011 to 2017.

“This announcement marks an important milestone in two major cryptocurrency investigations. As alleged in the indictments, starting in 2011, Bilyuchenko and Verner stole a massive amount of cryptocurrency from Mt. Gox, contributing to the exchange’s ultimate insolvency. Armed with the ill-gotten gains from Mt. Gox, Bilyuchenko allegedly went on to help set up the notorious BTC-e virtual currency exchange, which laundered funds for cyber criminals worldwide,” said Assistant Attorney General Kenneth A. Polite, Jr. of the Justice Department’s Criminal Division. “These indictments highlight the department’s unwavering commitment to bring to justice bad actors in the cryptocurrency ecosystem and prevent the abuse of the financial system.”

“As cyber criminals have become more sophisticated in their methods of thievery, our career prosecutors and law enforcement partners, too, have become experts in the latest technologies being abused for malicious purposes,” said U.S. Attorney Damian Williams for the Southern District of New York. “As alleged, Alexey Bilyuchenko and Aleksandr Verner thought they could outsmart the law by using sophisticated hacks

to steal and launder massive amounts of cryptocurrency, a novel technology at the time, but the charges unsealed demonstrate our ability to tenaciously pursue these alleged criminals, no matter how complex their schemes, until they are brought to justice."

"For years, Bilyuchenko and his co-conspirators allegedly operated a digital currency exchange that enabled criminals around the world – including computer hackers, ransomware actors, narcotics rings, and corrupt public officials – to launder billions of dollars," said U.S. Attorney Ismail J. Ramsey for the Northern District of California. "The Department of Justice will work tirelessly to identify cyber criminals, no matter where they are. And Bilyuchenko and his co-conspirators will learn that the Department of Justice has long arms and an even longer memory for crimes that harm our communities."

Southern District of New York indictment

According to court documents unsealed in the Southern District of New York (SDNY), in or about September 2011, Bilyuchenko, Verner, and their co-conspirators allegedly gained unauthorized access to the server holding the cryptocurrency wallets for Mt. Gox. At the time, Mt. Gox was the largest Bitcoin exchange in existence, servicing thousands of users worldwide. Mt. Gox stored the cryptocurrency wallets containing its customers' bitcoin, and the corresponding private keys used to authorize bitcoin transfers from those wallets, on a computer server in Japan.

"The FBI will continue to work with our U.S. government and international partners to relentlessly pursue and disrupt malicious cyber actors wherever they may reside," said Assistant Director Bryan Vorndran of the FBI's Cyber Division. "When cyber criminals engage in fraudulent activity, such as hacking and illicitly operating cryptocurrency exchanges, it is critical that we impose cost on the bad actors and ensure they face justice."

Bilyuchenko, Verner, and their co-conspirators allegedly used their unauthorized access to Mt. Gox's server to fraudulently cause bitcoin to be transferred from Mt. Gox's wallets to bitcoin addresses controlled by Bilyuchenko, Verner, and their co-conspirators. From September 2011 through at least May 2014, Bilyuchenko, Verner, and their co-conspirators allegedly caused the theft of at least approximately 647,000 bitcoins from Mt. Gox, representing the vast majority of the bitcoins belonging to Mt. Gox's customers. Bilyuchenko, Verner, and their co-conspirators allegedly laundered the bulk of the bitcoins stolen through Mt. Gox principally through bitcoin addresses associated with accounts Bilyuchenko, Verner, and their co-conspirators controlled at two other online bitcoin exchanges.

"Cryptocurrency offers a new way for criminals to steal and launder money, but greed and deceit are nothing new," said Chief Jim Lee of IRS Criminal Investigation (IRS-CI). "IRS-CI is specially equipped to follow the complex financial trail left by criminals, and we are dedicated to holding those accountable for crimes committed. IRS-CI is proud to stand with our law enforcement partners to announce this indictment."

In furtherance of the money laundering scheme, in or about April 2012, Bilyuchenko, Verner, and their co-conspirators allegedly negotiated and entered into a fraudulent contract (the "Advertising Contract") to provide purported advertising services to a Bitcoin brokerage service based in the Southern District of New

York (the “New York Bitcoin Broker”). Under the guise of the Advertising Contract, in order to conceal and liquidate the bitcoins stolen from Mt. Gox, Bilyuchenko and Verner allegedly made regular requests to the owner and operator of the New York Bitcoin Broker to make large wire transfers into various offshore bank accounts, including in the names of shell corporations, controlled by Bilyuchenko, Verner, and their co-conspirators. In accordance with these requests, between in or about March 2012 and in or about April 2013, the New York Bitcoin Broker allegedly transferred more than approximately $6.6 million to overseas bank accounts controlled by Bilyuchenko, Verner, and their co-conspirators. In exchange for the wire transfers, the New York Bitcoin Broker allegedly received “credit” on Exchange-1, through which Bilyuchenko, Verner, and their co-conspirators allegedly laundered more than 300,000 of the bitcoins stolen from Mt. Gox. The fraudulent Advertising Contract with the New York Bitcoin Broker allegedly enabled Bilyuchenko, Verner, and their co-conspirators to conceal and liquidate bitcoins stolen through the Mt. Gox Hack.

Mt. Gox ceased operations in 2014 after the theft was revealed.

Northern District of California indictment

According to court documents unsealed in the Northern District of California (NDCA), Bilyuchenko allegedly worked with Vinnik and others to operate the BTC-e exchange from 2011 until it was shut down by law enforcement in July 2017. During that time period, BTC-e was one of the world’s largest cryptocurrency exchanges and was one of the primary ways by which cyber criminals around the world transferred, laundered, and stored the criminal proceeds of their illegal activities.

BTC-e served over one million users worldwide, moving millions of bitcoin worth of deposits and withdrawals, and processing billions of dollars’ worth of transactions. BTC-e received criminal proceeds of numerous computer intrusions and hacking incidents, ransomware events, identity theft schemes, corrupt public officials, and narcotics distribution rings.

“The Secret Service has a long tradition of pursuing and bringing to justice those who aim to exploit our financial systems and target innocent victims,” said Special Agent in Charge William Mancino of the U.S. Secret Service’s Criminal Investigative Division. “Working together with our local, state, and federal law enforcement partners, we will continue to investigate criminal organizations that operate in the ever-evolving cyber domain.”

“Homeland Security Investigations (HSI) continues to investigate cyber criminals illicitly operating in virtual spaces, and we are proud to have worked collaboratively with our law enforcement partners to bring these two individuals to justice,” said Acting Executive Associate Director Katrina W. Berger of HSI. “Our special agents continue to investigate transnational criminal organizations operating in emerging technologies, leveraging our broad authorities to identify, and dismantle those behind sophisticated crypto-scams.”

The SDNY indictment charges Bilyuchenko and Verner with conspiracy to commit money laundering. The NDCA indictment charges Bilyuchenko with money laundering conspiracy and operating an unlicensed money services business.

The U.S. Attorney's Office for the Southern District of New York's Complex Frauds and Cybercrime Unit is handling the SDNY case. The FBI and IRS-CI are investigating the case and SDNY Assistant U.S. Attorney Olga I. Zverovich is prosecuting the case.

The Corporate and Securities Fraud Section of the U.S. Attorney's Office for the Northern District of California and the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) are handling the NDCA case. The FBI; IRS-CI Oakland Field Office and Cyber Crime Unit in Washington, D.C.; U.S. Secret Service Criminal Investigative Division; and HSI are investigating the case. CCIPS Trial Attorney C. Alden Pelker and NDCA Assistant U.S. Attorney Claudia Quiroz, both members of the National Cryptocurrency Enforcement Team, and NDCA Assistant U.S. Attorney Katherine Lloyd-Lovett are prosecuting the case. The Justice Department's Office of International Affairs provided invaluable assistance.

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

Updated June 9, 2023

Topic

Cybercrime

Press Release Number: 23-637