Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe

Press Release

Wednesday, February 17, 2021

For Immediate Release
Office of Public Affairs

Indictment Expands 2018 Case that Detailed Attack on Sony Pictures and Creation of WannaCry Ransomware by Adding Two New Defendants and Recent Global Schemes to Steal Money and Cryptocurrency from Banks and Businesses while Operating in North Korea, China

---

Note: Audio and Transcript of the February 17, 2021 press call is available on our videos page.

A federal indictment unsealed today charges three North Korean computer programmers with participating in a wide-ranging criminal conspiracy to conduct a series of destructive cyberattacks, to steal and extort more than $1.3 billion of money and cryptocurrency from financial institutions and companies, to create and deploy multiple malicious cryptocurrency applications, and to develop and fraudulently market a blockchain platform.

A second case unsealed today revealed that a Canadian-American citizen has agreed to plead guilty in a money laundering scheme and admitted to being a high-level money launderer for multiple criminal schemes, including ATM “cash-out” operations and a cyber-enabled bank heist orchestrated by North Korean hackers.

“As laid out in today’s indictment, North Korea’s operatives, using keyboards rather than guns, stealing digital wallets of cryptocurrency instead of sacks of cash, are the world’s leading bank robbers,” said Assistant Attorney General John C. Demers of the Justice Department’s National Security Division. “The Department will continue to confront malicious nation state cyber activity with our unique tools and work with our fellow agencies and the family of norms abiding nations to do the same.”

“Today's unsealed indictment expands upon the FBI’s 2018 charges for the unprecedented cyberattacks conducted by the North Korean regime,” said the FBI Deputy Director Paul Abbate. “The ongoing targeting, compromise, and cyber-enabled theft by North Korea from global victims was met with the outstanding, persistent investigative efforts of the FBI in close collaboration with U.S. and international partners. By arresting facilitators, seizing funds, and charging those responsible for the hacking conspiracy, the FBI continues to impose consequences and hold North Korea accountable for its criminal cyber activity."

“The scope of the criminal conduct by the North Korean hackers was extensive and long-running, and the range of crimes they have committed is staggering,” said Acting U.S. Attorney Tracy L. Wilkison for the Central District of California. “The conduct detailed in the indictment are the acts of a criminal nation-state that has stopped at nothing to extract revenge and obtain money to prop up its regime.”

“This case is a particularly striking example of the growing alliance between officials within some national governments and highly sophisticated cyber-criminals,” said U.S. Secret Service Assistant Director Michael R. D’Ambrosio. “The individuals indicted today committed a truly unprecedented range of financial and cyber-crimes: from ransomware attacks and phishing campaigns, to digital bank heists and sophisticated money laundering operations. With victims strewn across the globe, this case shows yet again that the challenge of cybercrime is, and will continue to be, a struggle that can only be won through partnerships, perseverance, and a relentless focus on holding criminals accountable.”

The hacking indictment filed in the U.S. District Court in Los Angeles alleges that Jon Chang Hyok (전창혁), 31; Kim Il (김일), 27; and Park Jin Hyok (박진혁), 36, were members of units of the Reconnaissance General Bureau (RGB), a military intelligence agency of the Democratic People’s Republic of Korea (DPRK), which engaged in criminal hacking. These North Korean military hacking units are known by multiple names in the cybersecurity community, including Lazarus Group and Advanced Persistent Threat 38 (APT38). Park was previously charged in a criminal complaint unsealed in September 2018.

The indictment alleges a broad array of criminal cyber activities undertaken by the conspiracy, in the United States and abroad, for revenge or financial gain. The schemes alleged include:

- ***Cyberattacks on the Entertainment Industry***: The destructive cyberattack on Sony Pictures Entertainment in November 2014 in retaliation for “The Interview,” a movie that depicted a fictional assassination of the DPRK’s leader; the December 2014 targeting of AMC Theatres, which was scheduled to show the film; and a 2015 intrusion into Mammoth Screen, which was producing a fictional series involving a British nuclear scientist taken prisoner in DPRK.

- ***Cyber-Enabled Heists from Banks***: Attempts from 2015 through 2019 to steal more than $1.2 billion from banks in Vietnam, Bangladesh, Taiwan, Mexico, Malta, and Africa by hacking the banks' computer networks and sending fraudulent Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages.
- ***Cyber-Enabled ATM Cash-Out Thefts***: Thefts through ATM cash-out schemes – referred to by the U.S. government as "FASTCash" – including the October 2018 theft of $6.1 million from BankIslami Pakistan Limited (BankIslami).
- ***Ransomware and Cyber-Enabled Extortion***: Creation of the destructive WannaCry 2.0 ransomware in May 2017, and the extortion and attempted extortion of victim companies from 2017 through 2020 involving the theft of sensitive data and deployment of other ransomware.
- ***Creation and Deployment of Malicious Cryptocurrency Applications***: Development of multiple malicious cryptocurrency applications from March 2018 through at least September 2020 – including Celas Trade Pro, WorldBit-Bot, iCryptoFx, Union Crypto Trader, Kupay Wallet, CoinGo Trade, Dorusio, CryptoNeuro Trader, and Ants2Whale – which would provide the North Korean hackers a backdoor into the victims' computers.
- ***Targeting of Cryptocurrency Companies and Theft of Cryptocurrency***: Targeting of hundreds of cryptocurrency companies and the theft of tens of millions of dollars' worth of cryptocurrency, including $75 million from a Slovenian cryptocurrency company in December 2017; $24.9 million from an Indonesian cryptocurrency company in September 2018; and $11.8 million from a financial services company in New York in August 2020 in which the hackers used the malicious CryptoNeuro Trader application as a backdoor.
- ***Spear-Phishing Campaigns***: Multiple spear-phishing campaigns from March 2016 through February 2020 that targeted employees of United States cleared defense contractors, energy companies, aerospace companies, technology companies, the U.S.Department of State, and the U.S. Department of Defense.
- ***Marine Chain Token and Initial Coin Offering***: Development and marketing in 2017 and 2018 of the Marine Chain Token to enable investors to purchase fractional ownership interests in marine shipping vessels, supported by a blockchain, which would allow the DPRK to secretly obtain funds from investors, control interests in marine shipping vessels, and evade U.S. sanctions.

According to the allegations contained in the hacking indictment, which was filed on Dec. 8, 2020, in the U.S. District Court in Los Angeles and unsealed today, the three defendants were members of units of the RGB who were at times stationed by the North Korean government in other countries, including China and Russia. While these defendants were part of RGB units that have been referred to by cybersecurity researchers as Lazarus Group and APT38, the indictment alleges that these groups engaged in a single conspiracy to cause damage, steal data and money, and otherwise further the strategic and financial interests of the DPRK government and its leader, Kim Jong Un.

Money Launderer Charged in California and Georgia

Federal prosecutors today also unsealed a charge against Ghaleb Alaumary, 37, of Mississauga, Ontario, Canada, for his role as a money launderer for the North Korean conspiracy, among other criminal schemes. Alaumary agreed to plead guilty to the charge, which was filed in the U.S. District Court in Los Angeles on Nov. 17, 2020. Alaumary was a prolific money launderer for hackers engaged in ATM cash-out schemes, cyber-enabled bank heists, business email compromise (BEC) schemes, and other online fraud schemes. Alaumary is also being prosecuted for his involvement in a separate BEC scheme by the U.S. Attorney's Office for the Southern District of Georgia.

With respect to the North Korean co-conspirators' activities, Alaumary organized teams of co-conspirators in the United States and Canada to launder millions of dollars obtained through ATM cash-out operations, including from BankIslami and a bank in India in 2018. Alaumary also conspired with Ramon Olorunwa Abbas, aka "Ray Hushpuppi," and others to launder funds from a North Korean-perpetrated cyber-enabled heist from a Maltese bank in February 2019. Last summer, the U.S. Attorney's Office in Los Angeles charged Abbas in a separate case alleging that he conspired to launder hundreds of millions of dollars from BEC frauds and other scams.

Accompanying Mitigation Efforts

Throughout the investigation, the FBI and the Justice Department provided specific information to victims about how they had been targeted or compromised, as well as information about the tactics, techniques, and procedures (TTPs) used by the hackers with the goals of remediating any intrusion and preventing future intrusions. That direct sharing of information took place in the United States and in foreign countries, often with the assistance of foreign law enforcement partners. The FBI also collaborated with certain private cybersecurity companies by sharing and analyzing information about the intrusion TTPs used by the members of the conspiracy.

In addition to the criminal charges, the FBI and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, in collaboration with the U.S. Department of Treasury, today released a joint cybersecurity advisory and malware analysis reports (MARs) regarding North Korean cryptocurrency malware. The joint cybersecurity analysis and MARs highlight the cyber threat North Korea – which is referred to by the U.S. government as HIDDEN COBRA – poses to cryptocurrency and identify malware and indicators of compromise related to the "AppleJeus" family of malware (the name given by the cybersecurity community to a family of North Korean malicious cryptocurrency applications that includes Celas Trade Pro, WorldBit-Bot, Union Crypto Trader, Kupay Wallet, CoinGo Trade, Dorusio, CryptoNeuro Trader, and Ants2Whale). The joint cybersecurity advisory and MARs collectively provide the cybersecurity community and public with information about identifying North Korean malicious cryptocurrency applications, avoiding intrusions, and remedying infections.

The U.S. Attorney's Office and FBI also obtained seizure warrants authorizing the FBI to seize cryptocurrency stolen by the North Korean hackers from a victim in the indictment – a financial services company in New York – held at two cryptocurrency exchanges. The seizures include sums of multiple cryptocurrencies totaling approximately $1.9 million, which will ultimately be returned to the victim.

Jon, Kim, and Park are charged with one count of conspiracy to commit computer fraud and abuse, which carries a maximum sentence of five years in prison, and one count of conspiracy to commit wire fraud and bank fraud, which carries a maximum sentence of 30 years in prison.

In relation to the case filed in Los Angeles, Alaumary has agreed to plead guilty to one count of conspiracy to commit money laundering, which carries a maximum sentence of 20 years in prison.

The charges contained in the indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt.

The investigation of Jon, Kim, and Park was led by the FBI's Los Angeles Field Office, which worked closely with the FBI's Charlotte Field Office. The U.S. Secret Service's Los Angeles Field Office and Global Investigative Operations Center provided substantial assistance. The FBI's Cyber Division also provided substantial assistance.

The investigations of Alaumary were conducted by the U.S. Secret Service's Savannah Field Office, FBI's Los Angeles Field Office, and the U.S. Secret Service's Los Angeles Field Office and Global Investigative Operations Center. The FBI's Criminal Investigative Division also provided substantial assistance.

The case against Jon, Kim, and Park is being prosecuted by Assistant U.S. Attorneys Anil J. Antony and Khaldoun Shobaki of the Cyber and Intellectual Property Crimes Section, with substantial assistance from Trial Attorney Scott Claffee of the Department of Justice National Security Division's Counterintelligence and Export Control Section.

Assistant U.S. Attorneys Antony and Shobaki are also prosecuting the case against Alaumary, in which the U.S. Attorney's Office for the Southern District of Georgia and the Criminal Division's Computer Crimes and Intellectual Property Section (CCIPS) provided substantial assistance. Assistant U.S. Attorneys Antony and Shobaki, along with Assistant U.S. Attorney Jonathan Galatzan of the Asset Forfeiture Section, also obtained the seizure warrants for cryptocurrency stolen from the financial services company in New York.

The Criminal Division's Office of International Affairs provided assistance throughout these investigations, as did many of the FBI's Legal Attachés, as well as foreign authorities around the world. Numerous victims cooperated and provided valuable assistance.

Updated July 13, 2022

Topics

Countering Nation-State Threats

National Security

Cybercrime

Press Release Number: 21-154