Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators

Press Release

Tuesday, July 19, 2022

For Immediate Release
Office of Public Affairs

Two Ransom Payments Made by U.S. Health Care Providers Recovered by Law Enforcement Will Be Returned to Victims

The Justice Department today announced a complaint filed in the District of Kansas to forfeit cryptocurrency paid as ransom to North Korean hackers or otherwise used to launder such ransom payments. In May 2022, the FBI filed a sealed seizure warrant for the funds worth approximately half a million dollars. The seized funds include ransoms paid by health care providers in Kansas and Colorado.

“Thanks to rapid reporting and cooperation from a victim, the FBI and Justice Department prosecutors have disrupted the activities of a North Korean state-sponsored group deploying ransomware known as ‘Maui,’” said Deputy Attorney General Lisa O. Monaco today at the International Conference on Cyber Security. “Not only did this allow us to recover their ransom payment as well as a ransom paid by previously unknown victims, but we were also able to identify a previously unidentified ransomware strain. The approach used in this case exemplifies how the Department of Justice is attacking malicious cyber activity from all angles to disrupt bad actors and prevent the next victim.”

According to court documents, in May 2021, North Korean hackers used a ransomware strain called Maui to encrypt the files and servers of a medical center in the District of Kansas. After more than a week of being unable to access encrypted servers, the Kansas hospital paid approximately $100,000 in Bitcoin to regain

the use of their computers and equipment. Because the Kansas medical center notified the FBI and cooperated with law enforcement, the FBI was able to identify the never-before-seen North Korean ransomware and trace the cryptocurrency to China-based money launderers.

Then, as a result, in April 2022, the FBI observed an approximately $120,000 Bitcoin payment into one of the seized cryptocurrency accounts identified thanks to the cooperation of the Kansas hospital. The FBI's investigation confirmed that a medical provider in Colorado had just paid a ransom after being hacked by actors using the same Maui ransomware strain. In May 2022, the FBI seized the contents of two cryptocurrency accounts that had received funds from the Kansas and Colorado health care providers. The District of Kansas then began proceedings to forfeit the hackers' funds and return the stolen money to the victims.

"Reporting cyber incidents to law enforcement and cooperating with investigations not only protects the United States, it is also good business," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "The reimbursement to these victims of the ransom shows why it pays to work with law enforcement."

"These sophisticated criminals are constantly pushing boundaries to search for ways to extort money from victims by forcing them to pay ramsons in order to regain control of their computer and record systems," said U.S. Attorney Duston J. Slinkard for the District of Kansas. "What these hackers don't count on is the tenacity of the U.S. Justice Department in recovering and returning these funds to the rightful owners."

"The FBI is dedicated to working with our federal and private sector partners to disrupt nation state actors who pose a critical cyber threat to the American people," said FBI Cyber Division Assistant Director Bryan Vorndran. "Today's success demonstrates the result of reporting to the FBI and our partners as early as possible when you are a victim of a cyber attack; this provides law enforcement with the ability to best assist the victim. We will continue to pursue these malicious cyber actors, such as these North Korean hackers, who threaten the American public regardless of where they may be and work to successfully retrieve ransom payments where possible."

"Today's announcement reiterates the FBI and Justice department's continued commitment to working with our critical infrastructure and private sector partners to identify and dismantle cyber threats, including new and emerging ransomware variants," said Special Agent in Charge Charles Dayoub of the FBI Kansas City Field Division. "Because of swift reporting by the victim medical center, action was taken to lessen the loss to the victim company, as well as identify the malware deployed, preventing additional cyber-attacks. The relationship between the FBI and our private sector partners are critical to discover, disrupt and dismantle cyber threats to our nation's infrastructure."

On July 6, 2022, based on information obtained during the Department's investigation, the FBI, the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of the Treasury issued a joint cybersecurity advisory regarding the North Korean threat to U.S. health care and public health sector organizations, which included indicators of compromise and mitigation advice.

Deputy Attorney General Lisa O. Monaco; Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division; U.S. Attorney Duston J. Slinkard for the District of Kansas; Special Agent in Charge Charles Dayoub of the FBI's Kansas City Field Office; and Assistant Director Bryan Vorndran of the FBI's Cyber Division made the announcement.

The FBI is investigating the case.

Updated July 19, 2022

Topic

Cybercrime

Press Release Number: 22-767