Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside

justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

June 7, 2021

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Monday, June 7, 2021

WASHINGTON - The Department of Justice today announced that it has seized 63.7 bitcoins currently valued at approximately $2.3 million. These funds allegedly represent the proceeds of a May 8, ransom payment to individuals in a group known as DarkSide, which had targeted Colonial Pipeline, resulting in critical infrastructure being taken out of operation. The seizure warrant was authorized earlier today by the Honorable Laurel Beeler, U.S. Magistrate Judge for the Northern District of California.

“Following the money remains one of the most basic, yet powerful tools we have,” said Deputy Attorney General Lisa O. Monaco for the U.S. Department of Justice. “Ransom payments are the fuel that propels the digital extortion engine, and today’s announcement demonstrates that the United States will use all available tools to make these attacks more costly and less profitable for criminal enterprises. We will continue to target the entire ransomware ecosystem to disrupt and deter these attacks. Today’s announcements also demonstrate the value of early notification to law enforcement; we thank Colonial Pipeline for quickly notifying the FBI when they learned that they were targeted by DarkSide.”

“There is no place beyond the reach of the FBI to conceal illicit funds that will prevent us from imposing risk and consequences upon malicious cyber actors,” said FBI Deputy Director Paul Abbate. “We will continue to use all of our available resources and leverage our domestic and international partnerships to disrupt ransomware attacks and protect our private sector partners and the American public.”

“Cyber criminals are employing ever more elaborate schemes to convert technology into tools of digital extortion,” said Acting U.S. Attorney for the Northern District of California Stephanie Hinds. “We need to continue improving the cyber resiliency of our critical infrastructure across the nation, including in the Northern District of California. We will also continue developing advanced methods to improve our ability to track and recover digital ransom payments.”

On or about May 7, Colonial Pipeline was the victim of a highly publicized ransomware attack resulting in the company taking portions of its infrastructure out of operation. Colonial Pipeline reported to the FBI that its computer network was accessed by an organization named DarkSide and that it had received and paid a ransom demand for approximately 75 bitcoins.

As alleged in the supporting affidavit, by reviewing the Bitcoin public ledger, law enforcement was able to track multiple transfers of bitcoin and identify that approximately 63.7 bitcoins, representing the proceeds of the victim’s ransom payment, had been transferred to a specific address, for which the FBI has the “private key,” or the rough equivalent of a password needed to access assets accessible from the specific Bitcoin address. This bitcoin represents proceeds traceable to a computer intrusion and property involved in money laundering and may be seized pursuant to criminal and civil forfeiture statutes.

The Special Prosecutions Section and Asset Forfeiture Unit of the U.S. Attorney’s Office for the Northern District of California is handling the seizure, with significant assistance from the Department of Justice Criminal Division’s Money Laundering and Asset Recovery Section and Computer Crime and Intellectual Property Section, and the National Security Division’s Counterintelligence and Export Control Section. The Department components who worked on this seizure coordinated their efforts through the Department’s Ransomware and Digital Extortion Task Force, which was created to combat the growing number of ransomware and digital extortion attacks.

The Task Force prioritizes the disruption, investigation, and prosecution of ransomware and digital extortion activity by tracking and dismantling the development and deployment of malware, identifying the cybercriminals responsible, and holding those individuals accountable for their crimes. The Task Force also strategically targets the ransomware criminal ecosystem as a whole and collaborates with domestic and foreign government agencies as well as private sector partners to combat this significant criminal threat.