

New DOJ Enforcement Team Suggests DOJ May Take Additional Efforts to Recover Cyberattack Ransoms

October 14, 2021

On October 6, the U.S. Department of Justice (DOJ) announced the launch of a National Cryptocurrency Enforcement Team (NCET) to add structure to and coordinate the DOJ's investigative capabilities concerning unlawful uses of cryptocurrency, to increase prosecutions of criminal misuses of cryptocurrency, and to recover illicit proceeds. That last piece is especially striking, as it may provide a positive incentive for victims of cyberattacks to contact law enforcement, and to do so quickly.

The DOJ stated that one focus of NCET will be to “assist in tracing and recovery of assets lost to fraud and extortion, including cryptocurrency payments to ransomware groups.”

Cyberattacks using ransomware have been a serious and increasing problem in recent years, with victims including educational institutions, utilities, hospitals, and other critical infrastructure providers. For example:

- In September, it took Howard University almost three weeks to recover from a ransomware incident that led to several days of canceled classes.
- In June, an attack on the multinational meat manufacturer JBS S.A. closed a quarter of American beef operations for two days, as the company shut down its computer systems to limit the breach.
- In May, a cyberattack on Colonial Pipeline Co. forced the company to shut down the gasoline supply to much of the Eastern Seaboard, resulting in shortages throughout the South.

- Also in May, an attack shut down the databases of a hospital system in San Diego for two weeks, which significantly disrupted patient care and forced medical personnel to use paper records.
- In February, hackers accessed a water treatment plant in Oldsmar, Florida, briefly raising the lye in drinking water to dangerous levels.

Some commenters estimate that there were more than 65,000 successful ransomware attacks in 2020. Around the time of the Colonial Pipeline attack, Homeland Security Secretary Alejandro Mayorkas estimated that ransomware groups received \$350 million in ransom payments last year.

Cryptocurrency plays a significant role in ransomware schemes because attackers prefer this method of payment. It allows for the quick transfer of funds internationally and outside of traditional banking systems. Digital asset exchanges are thus an unsurprising area of scrutiny for regulators and prosecutors. For example, in September, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Suex OTC, S.R.O., a Russian virtual currency exchange, for its alleged role in facilitating and laundering financial transactions for ransomware groups.

Remarkably, on June 7, the DOJ seized 63.7 bitcoins, valued at about \$2.3 million, in cryptocurrency ransom paid by Colonial Pipeline. Although cryptocurrency seizures are rare, authorities have gained some experience in tracking the flow of digital money.

- In January, the DOJ announced the seizure of more than \$454,000 in cryptocurrency from the ransomware group NetWalker.
- Last November, the DOJ announced the seizure of roughly \$1 billion in cryptocurrency associated with the online black market Silk Road.
- Last August, the DOJ announced the seizure of more than 300 cryptocurrency accounts tied to al-Qaida and the Izz ad-Din al-Qassam Brigades, the armed wing of Palestinian militant group Hamas.

Although the FBI shared scant details on how it seized a portion of Colonial Pipeline's ransom payment, the broad method by which investigators can at least trace cryptocurrency ransoms is relatively straightforward. Cryptocurrencies are held in digital accounts called wallets, which store addresses for the virtual locations of crypto funds and the private keys, or passwords, to access them. The movement of funds between addresses is recorded in a public ledger called a blockchain.

Crypto wallets provide owners a measure of personal privacy, but blockchains are visible to the public. Blockchains enable law enforcement investigators to observe the movement of funds between addresses and through exchanges. Should law enforcement gain access to the private key for an address containing a ransom payment, it can seize, with a properly issued warrant, the portion of funds that makes up the ransom. In essence, they can make a prejudgment seizure, which is a

legal power that private parties generally lack (with a very limited set of exceptions). After seizing the funds, the DOJ can initiate a forfeiture action. Forfeiture removes ownership of the funds from the bad actor and, if the government elects to pursue a process called “restoration,” returns property obtained under fraudulent pretenses to the victim.

The DOJ intends to have NCET involved in cryptocurrency and blockchain technologies across all aspects of the department’s work. The initiative seeks to employ and build upon the work of the DOJ’s Money Laundering and Asset Recovery Section (MLARS) and Computer Crime and Intellectual Property Section (CCIPS), as well as assistant U.S. attorneys detailed from U.S. attorney’s offices across the country.

If NCET commits to recovering ransom payments for victims, then it could create a positive incentive for victims of cyberattacks to contact law enforcement with alacrity. And if NCET has any degree of success in its recovery efforts, it could have a significant impact on a significant national problem.

Authored By



Michael L. Yaeger



Erin J. Hoyle

Related Practices

[Cybersecurity and Privacy](#)

[White Collar Crime & Government Investigations](#)

[Blockchain and Digital Currency](#)

[Digital and E-Commerce Engagement and Innovation](#)

may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.