2-The New York Times-U.S. Seizes Share of Ransom

U.S. Seizes Share of Ransom From Hackers in Colonial Pipeline Attack

Investigators traced 75 Bitcoins worth more than $4 million through nearly two dozen cryptocurrency accounts.

The cyberattack on Colonial Pipeline last month shut down its computer systems, leading to soaring gas prices and panic buying.Credit…Shawn Thew/EPA, via Shutterstock

By Katie Benner and Nicole Perlroth

June 7, 2021

WASHINGTON — The Justice Department said on Monday that it had seized much of the ransom that a major U.S. pipeline operator had paid last month to a Russian hacking collective, turning the tables on the hackers by reaching into a digital wallet to snatch back millions of dollars in cryptocurrency. *[Compliance, Reinforce]*

Investigators in recent weeks traced 75 Bitcoins worth more than $4 million that Colonial Pipeline had paid to the hackers as the attack shut down its computer systems, prompting fuel shortages, a spike in gasoline prices and chaos at airlines. *[Worry]*

Federal investigators tracked the ransom as it moved through a maze of at least 23 different electronic accounts belonging to DarkSide, the hacking group, before landing in one that a federal judge allowed them to break into, according to law enforcement officials and court documents .

The Justice Department said it seized 63.7 Bitcoins, valued at about $2.3 million. (The value of a Bitcoin has dropped over the past month.)

“The sophisticated use of technology to hold businesses and even whole cities hostage for profit is decidedly a 21st-century challenge, but the old adage ‘follow the money’ still applies,” Lisa O. Monaco, the deputy attorney general, said at the news conference at the Justice Department.

Law enforcement officials highlighted the seizure in an effort to warn cybercriminals that the United States planned to take aim at their profits, which are often gained through cryptocurrencies like Bitcoin. It was also intended to encourage victims of ransomware attacks — which occur every eight minutes , on average — to notify the authorities to help recover ransoms. *[Hope]*

For years, victims have opted to quietly pay cybercriminals, calculating that the payment would be cheaper than rebuilding data and services. Though the F.B.I. discourages ransom payments, they are legal and even tax deductible. But the payments — which collectively total billions of dollars — have funded and emboldened ransomware groups.

Justice Department officials said that Colonial’s willingness to quickly loop in the F.B.I. helped recoup the ransom portion, and they credited the company for its role in a first-of-its-kind effort by a new ransomware task force in the department to hijack a cybercrime group’s profits. *[Reinforce]*

“We must continue to take cyberthreats seriously and invest accordingly to harden our defenses,” Joseph Blount, the chief executive of Colonial, said

in a statement. Mr. Blount said that after his company contacted the F.B.I. and the Justice Department to notify them of the attack, investigators helped Colonial understand the hackers and their tactics. *[Reinforce]*

The Justice Department's announcement also came before President Biden's scheduled meeting with President Vladimir V. Putin of Russia next week in Geneva, where Mr. Biden is expected to address what American officials see as the Kremlin's willingness to provide protection for hackers. *[Worry]* Russia typically does not arrest or extradite suspects in ransomware attacks.

The New York Times reported last month that Colonial Pipeline's ransom payout had moved out of DarkSide's Bitcoin wallet, though it was not clear who had orchestrated the move.

Image

Lisa O. Monaco, the deputy attorney general, announced the recovery of millions of dollars' worth of cryptocurrency that Colonial Pipeline had paid to the hackers.Credit…Pool photo by Jonathan Ernst

On Monday, the government filled in some of the blanks. DarkSide operates by providing ransomware to affiliates. In exchange, DarkSide reaps a cut of their profits.

Officials said they had identified a virtual currency account, often referred to as a wallet, that DarkSide used to collect payment from a ransomware victim — identified in court papers only as Victim X, but whose hacking details match Colonial's. The officials said that a magistrate judge in the Northern District of California had approved a warrant on Monday to seize funds from the wallet.

The F.B.I. began investigating DarkSide last year and identified more than 90 victims across multiple sectors of the economy, including manufacturing, law, insurance, health care and energy, Paul M. Abbate, the deputy director of the F.B.I., said at the news conference.

DarkSide first surfaced in August and is believed to have started as an affiliate of another Russian hacking group, called REvil, before opening its own operation last year.

Weeks after DarkSide attacked Colonial , REvil used ransomware to try to extort money from JBS , one of the world's largest meat processors. The attack forced the company to shutter nine beef plants in the United States, disrupted poultry and pork plants, and had significant effects on grocery stores and restaurants, which have had to charge more or remove meat products from their menus.

In recent weeks, ransomware has also crippled the hospital that serves the Villages in Florida, the largest retirement community in the United States; television networks; N.B.A. and minor league baseball teams; and even ferries to Nantucket and Martha's Vineyard in Massachusetts.

The episodes have elevated digital vulnerabilities into the national consciousness. *[Worry]* White House officials said last week that they were working to address issues with cryptocurrency, which has enabled ransomware attacks for years.

Last week, Christopher A. Wray, the F.B.I. director, likened the threat of ransomware attacks to the challenge of global terrorism in the days after the Sept. 11, 2001, attacks.

"There are a lot of parallels, there's a lot of importance, and a lot of focus by us on disruption and prevention," he said. "There's a shared responsibility, not just across government agencies, but across the private sector and even the average American."

A Guide to Cryptocurrency

Card 1 of 7

A glossary. Cryptocurrencies have gone from a curiosity to a viable investment, making them almost impossible to ignore. If you are struggling with the terminology, let us help:

Bitcoin. A Bitcoin is a digital token that can be sent electronically from one user to another, anywhere in the world. Bitcoin is also the name of the payment network on which this form of digital currency is stored and moved.

Blockchain. A blockchain is a database maintained communally, that reliably stores digital information . The original blockchain was the database on which all Bitcoin transactions were stored, but non-currency-based companies and governments are also trying to use blockchain technology to store their data.

Cryptocurrencies. Since Bitcoin was first conceived in 2008 , thousands of other virtual currencies, known as cryptocurrencies , have been developed. Among them are Ether , Dogecoin and Tether .

Coinbase. The first major cryptocurrency company to list its shares on a U.S. stock exchange, Coinbase is a platform that allows people and companies to buy and sell various digital currencies , including Bitcoin, for a transaction fee.

Crypto finance. The development of cryptocurrencies spawned a parallel universe of alternative financial services, known as Decentralized Finance, or DeFi , allowing crypto businesses to move into traditional banking territory, including lending and borrowing.

NFTs. A “nonfungible token,” or NFT, is an asset verified using blockchain technology , in which a network of computers records transactions and gives buyers proof of authenticity and ownership. NFTs make digital artworks unique, and therefore sellable.

Mr. Wray added that the F.B.I. was investigating 100 software variants used in ransomware attacks, demonstrating the scale of the problem.

Though U.S. officials have been careful not to directly tie the ransomware attacks to Russia, Mr. Biden, Mr. Wray and others have said that the country protects cybercriminals.

In many cases, Russia treats them as national assets. In a 2014 breach of Yahoo , for example, Russian intelligence officers worked side by side with cybercriminals, allowing them to profit off stolen data, while instructing them to pass email accounts to the F.S.B., the successor agency to the Soviet-era K.G.B.

Mr. Putin has likened hackers to “artists who wake up in the morning in a good mood and start painting.” The reality, U.S. officials say, is that they give Mr. Putin and Russian intelligence services a layer of plausible deniability.

Not only is Mr. Biden expected to address the issue with Mr. Putin, but the State Department is also in talks with some two dozen other countries on ways to mutually pressure Russia to address cybercrime.

“If the Russian government wants to show that it’s serious about this issue, there’s a lot of room for them to demonstrate some real progress that we’re not seeing,” Mr. Wray said last week.

Anne Neuberger, the deputy national security adviser for cyber and emerging technologies, warned American businesses last week that ransomware had taken a dark turn, noting a recent shift “from stealing data to disrupting operations.” *[Worry]*

The hackers took direct aim at Colonial’s billing systems. With those frozen, executives found they had no way to charge customers and pre-emptively shut down operations. A confidential government assessment determined that if the pipeline had been shuttered for even two more days, the attack could have brought mass transit and chemical refineries, which rely on Colonial to transport diesel, to their knees. *[Worry]*

The White House held emergency meetings to address the attack. The Biden administration announced that it would require pipeline companies to report significant cyberattacks and that the government would create 24-hour emergency centers to handle serious hackings.

Cybersecurity experts welcomed the Justice Department’s move.

“It has become clear that we need to use several tools to stem the tide” of ransomware, said John Hultquist, a vice president at the cybersecurity firm FireEye. “A stronger focus on disruption may disincentivize this behavior, which is growing in a vicious cycle.”

David E. Sanger contributed reporting.