CYBERSECURITY

June 07, 2021 - 03:04 PM EDT

US recovers millions in cryptocurrency paid to Colonial Pipeline hackers

BY MYCHAEL SCHNELL AND MAGGIE MILLER

U.S. investigators have recovered millions of dollars in cryptocurrency that Colonial Pipeline paid hackers last month to end a ransomware attack on its systems.

Deputy Attorney General Lisa Monaco announced Monday afternoon that the Department of Justice "found and recaptured the majority of the ransom" paid to the DarkSide network, the group responsible for the attack.

Paul Abbate, the deputy director of the FBI, said the bureau successfully seized the ransom funds from a bitcoin wallet that DarkSide used to collect Colonial Pipeline's payment.

Monaco, however, would not reveal how much money was taken from the account.

Colonial Pipeline, a network that provides around 45 percent of the East Coast's fuel, was the target of a crippling cyberattack last month that forced it to shut down operations for several days.

Joseph Blount, the company's CEO, later revealed in an interview with The Wall Street Journal that he authorized the company to pay the cyber criminals behind the attack the equivalent of $4.4 million in bitcoin on the day of the breach in exchange for the keys to decrypt the network.

The FBI recommends against paying the ransom, as it may encourage the hackers to go after another group, and the payment may be used for criminal operations. The Biden administration has reiterated this stance in recent weeks.

Blount on Monday applauded the FBI for their "swift work and professionalism in responding to this event," and stressed in a statement that "the private sector also has an equally important role to play" in defending against cyber threats.

"When Colonial was attacked on May 7, we quietly and quickly contacted the local FBI field offices in Atlanta and San Francisco, and prosecutors in Northern California and Washington D.C. to share with them what we knew at that time," Blount said in a statement. "The Department of Justice and FBI were instrumental in helping us to understand the threat actor and their tactics. Their efforts to hold these criminals accountable and bring them to justice are commendable."

"As our investigation into this event continues, Colonial will continue its transparency in sharing intelligence and learnings with the FBI and other federal agencies," he added. "Our goal is to help our peers in the critical infrastructure space strengthen their cyber defenses and to collaborate across industry so that we can thwart these types of attacks before they happen. Together, through intelligence sharing and lessons learned, we can work to better protect our nation, its people, and our most critical assets."

Blount is set to testify before both the Senate Homeland Security and Governmental Affairs Committee and the House Homeland Security Committee later this week.

President Biden said his administration had "strong reason to believe" that the "criminals" behind the attacks were living in Russia, but he said officials do not believe the Russian government was involved.

CNN, which first reported the news, said that the FBI led the operation to recover the ransom, with cooperation from the Colonial Pipeline operator, according to people briefed on the matter.

The news from the Justice Department comes after another cyberattack targeted JBS USA, one of the country's largest meat suppliers.

The company revealed in a statement last week that it was the "target of an organized cybersecurity attack" that affected servers in North America and Australia.

The FBI has since determined that a Russia-linked group, REvil, which is also known as Sodinokibi, was behind the cyberattack.

Ransomware attacks have spiked more generally over the last year and have become a major threat for critical organizations such as hospitals and health care groups, among many others.

Biden will discuss ransomware and cybersecurity concerns during his upcoming trip to Europe this week, and the Russian-based cyberattacks will be on the agenda for a planned summit with Russian President Vladimir Putin later this month.

The Justice Department has also put a laser focus on cyberattacks in recent weeks.

Monaco's first action when confirmed by the Senate in her role as deputy director was to launch a 120-day review of how the agency handles cybersecurity issues such as digital currencies and supply chain attacks and how countries such as Russia and China leverage cyber operations against other nations.

The Justice Department also established a Ransomware and Digital Extortion Task Force in April, which carried out the seizure of the cryptocurrency involved in the Colonial Pipeline attack.

Monaco on Monday said the task force was established to combat "the epidemic of ransomware attacks by criminal groups."

"Today, we turned the tables on DarkSide by going after the entire ecosystem that fuels ransomware and digital extortion attacks, including criminal proceeds in the form of digital currency," Monaco said.

Cybersecurity group FireEye was engaged by Colonial Pipeline to investigate the attack last month. John Hultquist, the vice president of Analysis at FireEye's Mandiant Threat Intelligence, said in a statement provided to The Hill on Monday that the Justice Department's move was "a welcome development."

"It has become clear that we need to use several tools to stem the tide of this serious problem, and even law enforcement agencies need to broaden their approach beyond building cases against criminals who may be beyond the grasp of the law," Hultquist said.

"In addition to the immediate benefits of this approach, a stronger focus on disruption may disincentivize this behavior, which is growing in a vicious cycle," he added.

Updated at 5:07 p.m.

More in Cybersecurity

JBS paid $11 million to hackers to resolve ransomware attack

Hillicon Valley: Biden gives TikTok and WeChat a reprieve | Colonial Pipeline CEO addresses Congress again | Thomson Reuters shareholders want review of ICE ties

Colonial Pipeline may use recovered ransomware attack funds to boost cybersecurity

Hillicon Valley: Colonial Pipeline CEO grilled over ransomware attack | Senate debates sweeping Chinese competitiveness bill | Ohio files lawsuit to declare Google a public utility

Colonial Pipeline CEO grilled over ransomware attack