Colonial Pipeline did pay ransom to hackers, sources now say

By Natasha Bertrand, Evan Perez, Zachary Cohen, Geneva Sands and Josh Campbell, CNN

Updated 2300 GMT (0700 HKT) May 13, 2021

Biden issues warning to gas station owners on price gouging 02:11

Washington (CNN) — Colonial Pipeline paid the ransomware group that carried out a crippling cyberattack, two sources familiar with the matter told CNN on Thursday.

The group, previously identified as DarkSide, demanded nearly $5 million, two other sources familiar with the incident said. The sources CNN spoke to Thursday did not say how much the company paid. Bloomberg first reported the ransom payment.

CNN was previously told by multiple sources that Colonial Pipeline had not yet paid the ransom, but two sources said on Thursday that the company did pay as it sought to retrieve the stolen information. It is not clear when the payment was made.

The fact that the critical infrastructure company paid the ransom appears not to have been widely shared, despite federal entities working with the pipeline company to build back its networks following the ransomware attack.

Brandon Wales, the acting director of the Cybersecurity and Infrastructure Security Administration (CISA), said on Thursday that he has "no knowledge of whether a ransom was paid, how much was paid, if it was paid, when it was paid."

President Joe Biden declined to comment when asked on Thursday whether Colonial Pipeline had paid the ransom.

And government officials said they did not know if a ransom had been paid during briefings with lawmakers on Capitol Hill, according to multiple sources familiar with the matter.

Colonial Pipeline has also repeatedly declined to comment on the ransom payment.

retaliatory cyberattack on group responsible for pipeline hack and says Russia isn't to blame

experts and US government officials, managed to retrieve the most important data that was stolen, according to a person familiar with the response. The person said at least some of the data was not retrieved from the hackers, but by leveraging the attackers' use of intermediary servers within the United States to store the stolen information.

In response to the attack, private sector companies worked with US agencies to take a key server offline as recently as Saturday, disrupting the cyberattacks against the pipeline operator, CNN previously reported.

But the company only accessed the backups with the help of outside security firms and US government officials after it had already paid the ransom and realized the decryption tool provided by DarkSide was inefficient, according to Bloomberg.

On Wednesday, White House press secretary Jen Psaki referred to the FBI guidance on whether to pay ransoms. "Of course, the guidance from the FBI is not to do that," she said.

The US government had not been providing advice to Colonial Pipeline on whether to pay the ransom or not, said another source.

Related Article: Biden warns gas station owners: 'Do not try to take advantage of consumers' during fuel crunch

Helping efforts to restore the pipeline is the fact that there are "no indications that the threat actor moved laterally" to the company's operational networks, the Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation said on Tuesday.

Colonial also said late Wednesday that it initiated the restart of pipeline operations but acknowledged "it will take several days for the product delivery supply chain to return to normal."

New details emerging about decision to shut pipeline

Meanwhile, new details are emerging about Colonial's decision to proactively shut down its pipeline last week, a move that has led to panic buying and massive lines at gas pumps.

The company halted operations because its billing system was compromised, three people briefed on the matter told CNN, and they were concerned they wouldn't be able to figure out how much to bill customers for fuel they received.

One person familiar with the response said the billing system is central to the unfettered operation of the pipeline. That is part of the reason getting it back up and running has taken time, this person said.

Asked about whether the shutdown was prompted by concerns about payment, the company spokesperson said, "In response to the cybersecurity attack on our system, we proactively took certain systems offline to contain the threat, which temporarily halted all pipeline operations, and affected some of our IT systems."

At this time, there is no evidence that the company's operational technology systems were compromised by the attackers, the spokesperson added.

Government working to identify individual hackers

In order to hold them accountable.

In a joint federal government alert issued Tuesday night, CISA and the FBI confirmed that DarkSide was used as a "ransomware-as-a-service," in which developers of the ransomware receive a share of the proceeds from the cybercriminal actors who deploy it, known as "affiliates."

The "affiliate" in this case was likely Russian, according to sources familiar with the investigation. The affiliate could be a single individual, one of the sources said.

Related Article: Colonial Pipeline is restarting but the gas crisis isn't over

There are also indications that the individual actors that attacked Colonial, in conjunction with DarkSide, may have been inexperienced or novice hackers, rather than well-seasoned professionals, according to three sources familiar with the Colonial investigation.

David Kennedy, the president of the cybersecurity firm TrustedSec, noted that DarkSide's business model is to provide attackers with limited skills the funding and resources they need to actually launch the attacks, providing a platform that both parties can profit off of.

Among the signs that the hackers were novices is the fact that they chose a high-risk target that deals in a low-margin business, meaning the attack was unlikely to yield the kind of payout experienced ransomware actors are typically looking for, the sources told CNN.

"This was a gross miscalculation on the hackers' part," a source previously told CNN, noting the hackers likely had not anticipated that their attack would lead to the shutdown of one of the US' largest refined products pipeline system, spurring emergency White House meetings and a whole-of-government response.

CORRECTION: An earlier version of this story said Colonial Pipeline was not likely to pay a ransom. The headline and story have been updated to reflect new reporting that they did pay and clarify the data recovery process.