# Colonial Pipeline paid hackers nearly $5 million in ransom

May 13 2021, by William Turton and Michael Riley, Bloomberg News

Credit: CC0 Public Domain

Colonial Pipeline Co. paid nearly $5 million to Eastern European hackers on Friday, contradicting reports earlier this week that the company had no intention of paying an extortion fee to help restore the

country's largest fuel pipeline, according to two people familiar with the transaction.

The company paid the hefty ransom in untraceable cryptocurrency within hours after the attack, underscoring the immense pressure faced by the Georgia-based operator to get gasoline and jet fuel flowing again to major cities along the Eastern Seaboard, those people said.

Once they received the payment, the hackers provided the operator with a decrypting tool to restore its disabled computer network. The tool was so slow that the company continued using its own backups to help restore the system, one of the people familiar with the company's efforts said.

A representative from Colonial declined to comment.

The hackers, which the FBI said are linked to a group called DarkSide, specialize in digital extortion and are believed to be located in Russia or Eastern Europe. On Wednesday, media outlets including the *Washington Post* and Reuters reported that the company had no immediate intention of paying the ransom. Those reports were based on anonymous sources.

Ransomware is a type of malware that locks up a victim's files, which the attackers promise to unlock for a payment. More recently, some ransomware groups have also stolen victims' data and threatened to release it unless paid—a kind of double extortion.

The FBI discourages organizations from paying ransom to hackers, saying there is no guarantee they will follow through on promises to unlock files. It also provides incentive to other would-be hackers, the agency says. Such guidance provides a quandary for victims who have to weigh the risks of not paying with the costs of lost or exposed records.

A report released last month by a ransomware task force said the amount

paid by ransomware victims increased by 311% in 2020, reaching about $350 million in cryptocurrency. The average ransom paid by organizations in 2020 was $312,493, according to report.

Colonial, which operates the largest fuel pipeline in the U.S., became aware of the hack around May 7 and shut down its operations, which led to fuel shortages and lines at gas stations along the East Coast.