Colonial Pipeline confirms it paid $4.4M to hackers

May 19 2021, by Cathy Bussewitz

Tanker trucks are parked near the entrance of Colonial Pipeline Company Wednesday, May 12, 2021, in Charlotte, N.C. The operator of the nation's largest fuel pipeline has confirmed it paid $4.4 million to a gang of hackers who broke into its computer systems. That's according to a report from the Wall Street Journal. Colonial Pipeline's CEO Joseph Blount told the Journal that he authorized the payment after the ransomware attack because the company didn't know the extent of the damage. Credit: AP Photo/Chris Carlson

The operator of the nation's largest fuel pipeline confirmed it paid $4.4 million to a gang of hackers who broke into its computer systems.

Colonial Pipeline said Wednesday that after it learned of the May 7 ransomware attack, the company took its pipeline system offline and needed to do everything in its power to restart it quickly and safely, and made the decision then to pay the ransom.

"This decision was not made lightly," but it was one that had to be made, a company spokesman said. "Tens of millions of Americans rely on Colonial – hospitals, emergency medical services, law enforcement agencies, fire departments, airports, truck drivers and the traveling public."

Colonial Pipeline's CEO, Joseph Blount, told The Wall Street Journal he authorized the payment because the company didn't know the extent of the damage and wasn't sure how long it would take to bring the pipeline's systems back.

The FBI discourages making ransom payments to ransomware attackers, because paying encourages criminal networks around the globe who have hit thousands of businesses and health care systems in the U.S. in the past year alone. But many victims of ransomware attacks, where hackers demand large sums of money to decrypt stolen data or to prevent it from being leaked online, opt to pay.

"I know that's a highly controversial decision," Blount told the Journal. "But it was the right thing to do for the country."

Blount said Colonial paid the ransom in consultation with experts who previously dealt with the group behind the attacks, DarkSide, which rents out its ransomware to partners to carry out the actual attacks.

Multiple sources had confirmed to The Associated Press that Colonial Pipeline had paid the criminals who committed the cyberattack a ransom of nearly $5 million in cryptocurrency for the software decryption key required to unscramble their data network.

A ransom payment of 75 Bitcoin was paid the day after the criminals locked up Colonial's corporate network, according to Tom Robinson, co-founder of the cryptocurrency-tracking firm Elliptic. Prior to Robinson's blog post, two people briefed on the case had confirmed the payment amount to AP.

Blount told the Journal the attack was discovered around 5:30 a.m. on May 7. It took Colonial about an hour to shut down the pipeline, which has 260 delivery points across 13 states and Washington, D.C., Blount said. That helped prevent the infection from potentially migrating to the pipeline's operational controls. But there are lingering issues. Blount said Colonial is still unable to bill customers following an outage of that system.

The pipeline system delivers about 45% of the gasoline consumed on the East Coast, and Colonial, which is based in Alpharetta, Georgia, halted fuel supplies for nearly a week. That led to panic-buying and shortages at gas stations from Washington, D.C. to Florida.

Colonial restarted its pipeline a week ago, but it took time to resume a full delivery schedule, and the panic-buying led to gasoline shortages. More than 9,500 gas stations were out of fuel on Wednesday, including half of the gas stations in D.C. and 40% of stations in North Carolina, according to Gasbuddy.com, which tracks fuel prices and station outages.