FBI: DarkSide group behind ransomware hacking of US Colonial Pipeline

May 10 2021

The largest oil pipeline in the eastern United States was shut down by ransomware hackers

The FBI said Monday that ransomware from the shadowy DarkSide group forced the shutdown of the Colonial Pipeline network, as the

major fuel supplier said it was beginning to resume operations after the three-day freeze.

Colonial said in a statement that it was moving toward a partial opening of its 5,500 miles (8,850 kilometers) of pipeline—the largest fuel network between Texas and New York— after hackers locked down its corporate IT systems on Friday, apparently demanding a significant amount of money in ransom.

At the White House, Deputy National Security Advisor Elizabeth Sherwood-Randall said President Joe Biden was being kept updated on the incident, which threatened to crimp supplies of gasoline, diesel fuel and jet fuel across much of the eastern United States.

"The president continues to be regularly briefed on the incident," she said.

Colonial said in a statement that "segments of our pipeline are being brought back online in a stepwise fashion."

Seeking ransom

It said the ransomware targeted its corporate computers systems and not the separate computer controls of its pipeline.

However, it said, "we proactively took certain systems offline to contain the threat, which temporarily halted all pipeline operations, and affected some of our IT systems."

"To restore service, we must work to ensure that each of these systems can be brought back online safely."

The company did not comment on how it was addressing the ransom

demand.

The Federal Bureau of Investigation separately identified DarkSide as the group which produced the ransomware used in the attack.

"We continue to work with the company and our government partners on the investigation," said in a statement.

DarkSide is an enigmatic group that surfaced last year with its corporate-style approach to inserting itself into a target's computers, locking them up and demanding payment in exchange for supplying the tools to digitally unfreeze them.

They focus on large corporate targets like Colonial, and reportedly ask for payments of between hundreds of thousands of dollars and the low millions of dollars to unlock the frozen systems.

They claim to be apolitical and strictly in the business of making money via extortion.

Nothing yet has tied them to any government, and they have indicated in statements that they will work with other hackers to use DarkSide hacking tools and to share the ransom.