Largest U.S. pipeline shuts down operations after ransomware attack

By Lawrence Abrams

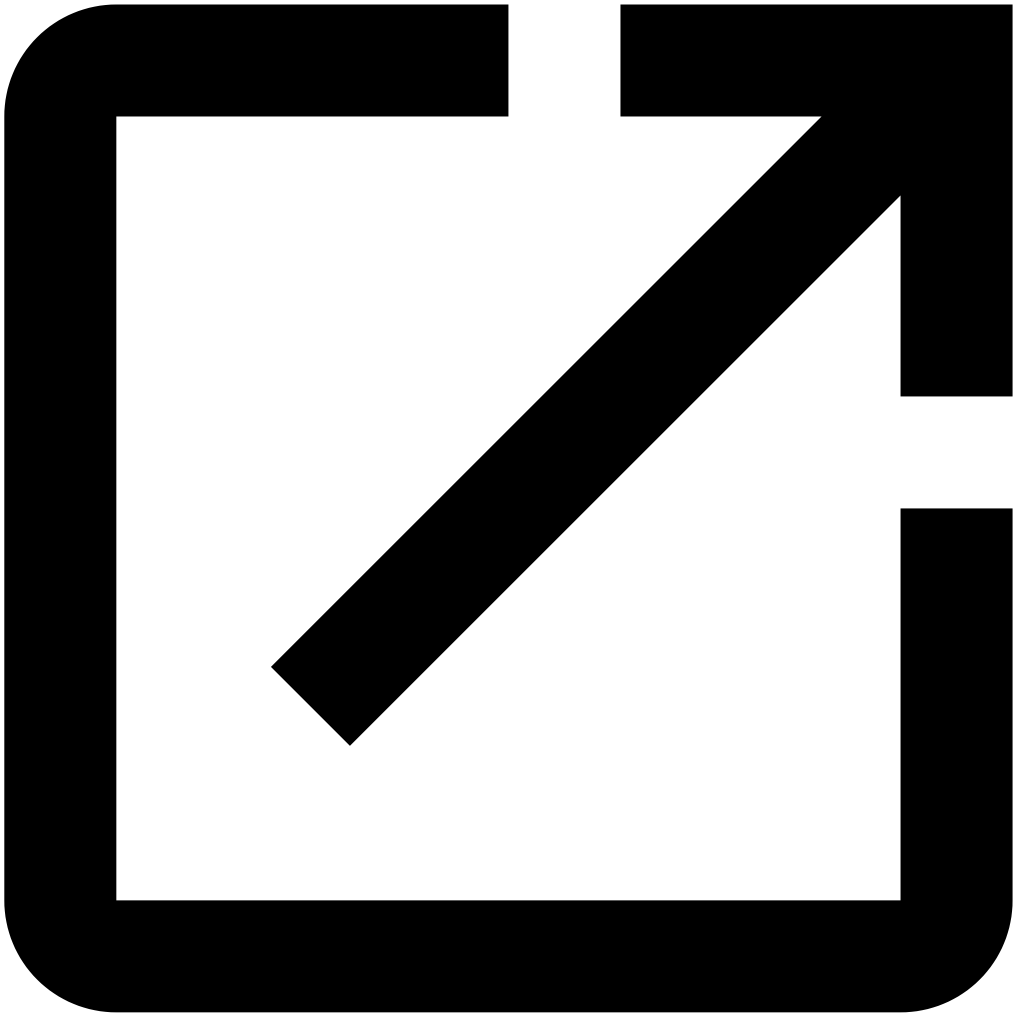
Published: 2021-05-08 · Archived: 2026-04-05 15:09:32 UTC

Update: Added new statement from Colonial Pipeline at the end of the article.

Colonial Pipeline, the largest fuel pipeline in the United States, has shut down operations after suffering what is reported to be a ransomware attack.

Colonial Pipeline transports refined petroleum products between refineries located in the Gulf Coast and markets throughout the southern and eastern United States. The company transports 2.5 million barrels per day through its 5,500 mile pipeline and provides 45% of all fuel consumed on the East Coast.


DIE LINKE.
0:00



Colonial Pipeline system map

According to a report by CNBC, Colonial Pipeline suffered a ransomware attack yesterday that forced them to shut down their entire network to prevent the spread of the malware.

Today, Colonial Pipeline issued a statement confirming the attack and stated that they temporarily shut down their pipeline operations while responding to the attack.

"On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack. In response, we proactively took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, and affected some of our IT systems."

"Upon learning of the issue, a leading, third-party cybersecurity firm was engaged, and they have already launched an investigation into the nature and scope of this incident, which is ongoing," Colonial Pipeline said in a statement.

DarkSide ransomware believed to be responsible

A US official has told the Washington Post that it is believed that the DarkSide ransomware operation is behind the attack.

BleepingComputer was the first to report about the DarkSide ransomware operation, which launched in the middle of August 2020.

Like other enterprise-targeting ransomware operations, when DarkSide gains access to a corporate network, they will quietly spread to other devices while gathering credentials and stealing unencrypted documents.

Once they gain access to Windows domain credentials, they will deploy the ransomware throughout the network to encrypt devices.

If DarkSide conducted the attack, the threat actors likely stole data, which will be used to extort Colonial Pipeline in their ransom demands.

High profile attacks previously conducted by the DarkSide gang include CompuCom, Discount Car and Truck Rentals, Brookfield Residential, and Brazil's Companhia Paranaense de Energia (Copel).

Update 5/8/21: The FBI today confirmed that the Colonial Pipeline cyberattack was conducted by the DarkSide ransomware operation.

Colonial Pipeline also issued an updated statement explaining that they are working with the US Department of Energy to slowly bring segments of the pipeline back online.

> "Colonial Pipeline continues to dedicate vast resources to restoring pipeline operations quickly and safely. Segments of our pipeline are being brought back online in a stepwise fashion, in compliance with relevant federal regulations and in close consultation with the Department of Energy, which is leading and coordinating the Federal Government's response.
>
> Restoring our network to normal operations is a process that requires the diligent remediation of our systems, and this takes time. 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. To restore service, we must work to ensure that each of these systems can be brought back online safely.
>
> While this situation remains fluid and continues to evolve, the Colonial operations team is executing a plan that involves an incremental process that will facilitate a return to service in a phased approach. This plan is based on a number of factors with safety and compliance driving our operational decisions, and the goal of substantially restoring operational service by the end of the week. The Company will provide updates as restoration efforts progress.
>
> We continue to evaluate product inventory in storage tanks at our facilities and others along our system and are working with our shippers to move this product to terminals for local delivery. Actions taken by the Federal Government to issue a temporary hours of service exemption for motor carriers and drivers transporting refined products across Colonial's footprint should help alleviate local supply disruptions and we thank our government partners for their assistance in resolving this matter.
>
> Our primary focus continues to be the safe and efficient restoration of service to our pipeline system, while minimizing disruption to our customers and all those who rely on Colonial Pipeline. We appreciate the patience of the traveling public and the support we have received from the Federal Government and our peers throughout the industry."

***5/8/21**: Added possible attribution to DarkSide ransomware*
***5/10/21**: FBI confirmed DarkSide ransomware attack and Colonial Pipeline update their statement.*

Source: https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/