

Colonial Pipeline attributes ransomware claims to ‘unrelated’ third-party data breach


 therecord.media/colonial-pipeline-attributes-ransomware-claims-to-unrelated-third-party-breach



Image: Unsplash+

[Jonathan Greig](#)

October 15th, 2023

Colonial Pipeline said there has been no disruption to pipeline operations or their systems after a ransomware gang made several threats on Friday afternoon.

The company – which runs the largest pipeline system for refined oil products in the U.S. – addressed claims made by the Ransomed.vc gang that data had been stolen from their systems.

“Colonial Pipeline is aware of unsubstantiated claims posted to an online forum that its system has been compromised by an unknown party. After working with our security and technology teams, as well as our partners at CISA, we can confirm that there has been no disruption to pipeline operations and our system is secure at this time,” a spokesperson for the company said.

“Files that were posted online initially appear to be part of a third-party data breach unrelated to Colonial Pipeline.”

When asked further questions about what third party was attacked, whether that incident involved ransomware and if the situation had been contained, a spokesperson directed Recorded Future News to CISA, which did not respond.

The gang runs a Telegram channel where they boast of attacks, and claimed on Friday afternoon that they attempted to extort Colonial Pipeline unsuccessfully. They shared a zip file with stolen documents that security researchers said had documents related to Colonial Pipeline.

The post also includes a photo of Rob Lee, CEO of incident response firm Dragos. Lee was closely involved in the response to a 2021 ransomware attack on Colonial Pipeline. The company did not respond to requests for comment, but on Twitter Lee said the claims of data theft were fictitious.

PSA: Criminal groups lie. Yes even, and especially, ransomware group ones.
Exhausting but pointless.

— Robert M. Lee (@RobertMLee) October 13, 2023

“When we wouldn’t pay their extortion attempt they’ve been pretty ticked off since. Have drug my name and the firm every chance they get,” he said.

The 2021 ransomware attack on Colonial Pipeline is largely considered one of the most consequential ransomware attacks in history, shutting down their operations for five days and paralyzing gas stations throughout the East Coast.

The company operates about 5,500 miles of pipeline that delivers gasoline, diesel, jet fuel, home heating oil, and other refined oil products throughout the Southern and Eastern U.S. Colonial Pipeline ended up paying a \$5 million ransom.

The attack made ransomware a household topic and kickstarted a push at all levels of government to address the attacks and the groups behind them. Several new cybersecurity regulations governing pipelines were instituted following the attack.

In June, the U.S. government confirmed that it used controversial digital surveillance powers to identify the individual behind the crippling ransomware attack and to claw back a majority of the millions of dollars in bitcoin the company paid to restore its systems.

Russia arrested one of the people behind the attack in 2022 but it is unclear whether the person was ever convicted of a crime.

Ransomed.vc recently made waves after threatening victims with the prospect of European data breach fines if ransoms for stolen data are not paid. It defaced a Hawai’i state government website last month, and two weeks ago Japanese manufacturing giant Sony told Recorded Future News that it was investigating data theft claims by the group.

But the group's legitimacy has been questioned, considering none of the victims added to the group's leak site since it emerged on August 15 have reported incidents. It is still unclear if the group actually uses ransomware.

The group claimed to have attacked U.S. credit agency TransUnion – which denied its systems were ever breached but noted that the data being offered for sale may have “come from a third party.”

- [Cybercrime](#)
- [Industry](#)
- [News](#)

Get more insights with the
Recorded Future

Intelligence Cloud.

[Learn more.](#)

No previous article

No new articles

Jonathan Greig



Jonathan Greig is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.