

Ransomware attack on Colonial Pipeline disrupts fuel supplies across Southeast US

Kevin Reed
11 May 2021

Shortages of gasoline, jet fuel and diesel are mounting in the Southeastern region of the US and prices are rising across the eastern half as supply was disrupted from the shutdown of the 5,500-mile Colonial Pipeline by a cyberattack late last week.

Media reports on Tuesday said that hundreds of filling stations in the Southeast ran out of gas or moved to restrict sales as buying surged amid concerns that supplies would run out. GasBuddy noted on Monday that demand was 40 percent greater in Georgia, Florida, South Carolina, North Carolina and Virginia than it was one week earlier.

Andy Lipow, president of Lipow Oil Associates, said jet fuel is a concern because it is only stored at airports. “They’re at risk of running out of jet fuels, and airlines have to make alternative plans, loading up aircraft before they fly into those airports, making sure they have supplies before they go to their next destination.”

In response to the shortages, American Airlines announced it was adding stops to the long-haul flights from Charlotte to Honolulu and from Charlotte to London in order to conserve fuel at its North Carolina hub.

The AAA automobile group reported that the national average for a gallon of regular gasoline rose 6 cents in one week and increased an average of nearly 13 cents in South Carolina and 17 cents in Georgia during the same period.

Colonial Pipeline—based in Alpharetta, Georgia—reported on Saturday that it learned of the ransomware attack the previous day. In response, the company said, “we proactively took certain systems offline to contain the threat, which has temporarily halted all pipeline operations.”

Ransomware is a computer virus that renders a targeted system inoperable by encrypting all data and

demanding ransom in exchange for decryption. Ransomware attacks typically include information about how the ransom—sometimes in the millions of dollars—can be paid, including in the form of cryptocurrency. Sometimes the hackers will also threaten to leak confidential data as part of their extortion tactics.

The privately owned Colonial Pipeline manages the largest transport system for refined oil products in the US that stretches from Texas to New Jersey and carries up to 3 million barrels of fuel each day. The main lines of the 5,500-mile system are made up of two pipes—one is 40 inches, and the other is 36 inches in diameter—the first carrying primarily gasoline and the other carrying petroleum distillate products, such as aviation fuel, diesel and home heating oil.

Energy analysts have said that the problem is not a shortage of refined fuel as much as it is products stuck in the wrong places. CNBC reported on Tuesday afternoon that while there are refining facilities across the Gulf Coast, “[M]oving it requires a hodgepodge of solutions, and analysts say it will be impossible to meet demand without the pipeline.”

While some corporate media sources are saying the crisis will be short lived, CNBC warned of the ripple effects of a prolonged shutdown. “If the Colonial Pipeline is not back in business by the weekend, prices could continue to rise at the pump, and there will be broader localized fuel shortages across the Southeast and mid-Atlantic regions.”

Michael Tran, energy analyst at Royal Bank of Canada, raised a more alarming prospect. “Given the size and the direction of the pipeline and the market that it feeds, the Colonial Pipeline is the single most important artery moving refined products in the country. This is already an earthquake, and the

magnitude of the earthquake just grows by the day.”

Concerned about the possibility of a run on fuel supplies prior to the increase in travel expected during the Memorial Day holiday, White House Press Secretary Jen Psaki released a short statement saying President Biden is “continually assessing the impact of this ongoing incident on fuel supply for the East Coast. We are monitoring supply shortages in parts of the Southeast and are evaluating every action the Administration can take to mitigate the impact as much as possible.”

Biden’s Energy Secretary Jennifer Granholm also attempted to downplay the crisis by saying that federal agencies are working around the clock to help the pipeline return to normal operations and that she held “several conversations with the CEO of Colonial and who has indicated that by close of business tomorrow, Colonial will be in a position to make the full restart decision. But even after that decision is made, it will take a few days to ramp up operations.”

Meanwhile, Republican Georgia Governor Brian Kemp signed an executive order on Tuesday suspending gasoline taxes through Saturday, which amounts to roughly 20 cents a gallon. Kemp said this decision would “help level the price for a little while” and cautioned against panic buying, which he said was unnecessary. Democratic Governors Roy Cooper of North Carolina and Ralph Northam of Virginia declared states of emergency in order to suspend some fuel transport rules, such as lifting hours of service limitations and tanker weight restrictions.

Colonial Pipeline issued a press release on Monday saying it was working with “third-party cybersecurity experts, law enforcement and other federal agencies to restore pipeline operations quickly and safely.” The statement went on to say that the company was “executing a plan that involves an incremental process that will facilitate a return to service in a phased approach.”

Although Colonial Pipeline did not disclose any details about its plan or the extent of the malware infection of its systems, it is typical for ransomware attacks to gain access to one unsecure computer within an organization and then replicate itself on all the other systems on the network. Since restoration of operability is never guaranteed with a ransom payment, many organizations opt to replace their entire IT

infrastructure from scratch.

On Monday, the FBI confirmed in a short statement that the hacking group DarkSide was responsible for the ransomware attack on Colonial Pipeline. The Biden administration wasted no time attempting to connect the attack to the Russian government, with Deputy National Security Adviser for Cyber and Emerging Technologies Anne Neuberger saying that DarkSide was “a criminal actor,” and the US government was looking for any nation-state ties that the group might have.

President Biden then also said that although there was no evidence from US intelligence officials that Russia was involved, “There is evidence that the actors’ ransomware is in Russia. They have some responsibility to deal with this.”



To contact the WSWWS and the
Socialist Equality Party visit:

wsws.org/contact