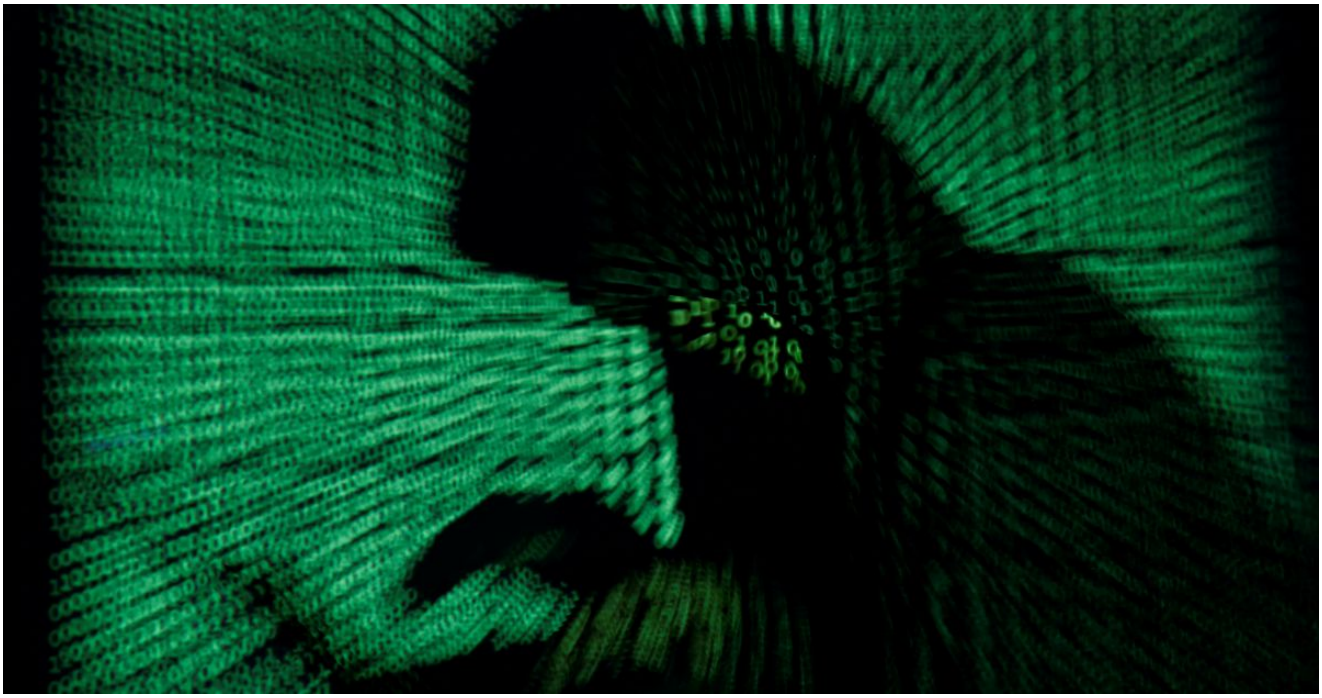
Cyber attack shuts down U.S. fuel pipeline ‘jugular,’ Biden briefed

reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

Christopher Bing, Stephanie Kelly



NEW YORK, May 8 (Reuters) - Top U.S. fuel pipeline operator Colonial Pipeline shut its entire network, the source of nearly half of the U.S. East Coast’s fuel supply, after a cyber attack on Friday that involved ransomware.

The incident is one of the most disruptive digital ransom operations ever reported and has drawn attention to how vulnerable U.S. energy infrastructure is to hackers. A prolonged shutdown of the line would cause prices to spike at gasoline pumps ahead of peak summer driving season, a potential blow to U.S. consumers and the economy.

"This is as close as you can get to the jugular of infrastructure in the United States," said Amy Myers Jaffe, research professor and managing director of the Climate Policy Lab. "It's not a major pipeline. It's the pipeline."

Colonial transports 2.5 million barrels per day of gasoline, and other fuels through 5,500 miles (8,850 km) of pipelines linking refiners on the Gulf Coast to the eastern and southern United States. It also serves some of the country's largest airports, including Atlanta's Hartsfield Jackson Airport, the world's busiest by passenger traffic.

The company said it shut down its operations after learning of a cyberattack on Friday using ransomware.

"Colonial Pipeline is taking steps to understand and resolve this issue. At this time, our primary focus is the safe and efficient restoration of our service and our efforts to return to normal operation," it said.

While the U.S. government investigation is in early stages, one former official and two industry sources said the hackers are likely a professional cybercriminal group.

The former official said investigators are looking at a group dubbed "DarkSide," known for deploying ransomware and extorting victims while avoiding targets in post-Soviet states. Ransomware is a type of malware designed to lock down systems by encrypting data and demanding payment to regain access.

Colonial said it had engaged a cybersecurity firm to help the investigation and contacted law enforcement and federal agencies.

The cybersecurity industry sources said cybersecurity firm FireEye (FEYE.O) was brought in to respond to the attack. FireEye declined to comment.

U.S. government bodies, including the FBI, said they were aware of the situation but did not yet have details of who was behind the attack.

President Joe Biden was briefed on the incident on Saturday morning, a White House spokesperson said, adding that the government is working to try to help the company restore operations and prevent supply disruptions.

The Department of Energy said it was monitoring potential impacts to the nation's energy supply, while both the U.S. Cybersecurity and Infrastructure Security Agency and the Transportation Security Administration told Reuters they were working on the situation.

"We are engaged with the company and our interagency partners regarding the situation. This underscores the threat that ransomware poses to organizations regardless of size or sector," said Eric Goldstein, executive assistant director of the cybersecurity division at CISA.

Colonial did not give further details or say how long its pipelines would be shut.

The privately held, Georgia-based company is owned by CDPQ Colonial Partners L.P., IFM (US) Colonial Pipeline 2 LLC, KKR-Keats Pipeline Investors L.P., Koch Capital Investments Company LLC and Shell Midstream Operating LLC.

A hooded man holds a laptop computer as cyber code is projected on him in this illustration picture taken on May 13, 2017. Top U.S. fuel pipeline operator Colonial Pipeline has shut its entire network after a cyber attack, the company said on Friday. REUTERS/Kacper Pempel/Illustration

"Cybersecurity vulnerabilities have become a systemic issue," said Algirde Pipikaite, cyber strategy lead at the World Economic Forum's Centre for Cybersecurity.

"Unless cybersecurity measures are embedded in a technology's development phase, we are likely to see more frequent attacks on industrial systems like oil and gas pipelines or water treatment plants," Pipikaite added.

PUMP PRICE WORRIES

The American Automobile Association said a prolonged outage of the line could trigger increases in gas prices at the pumps, a worry for consumers ahead of summer driving season.

A shutdown lasting four or five days, for example, could lead to sporadic outages at fuel terminals along the U.S. East Coast that depend on the pipeline for deliveries, said Andrew Lipow, president of consultancy Lipow Oil Associates.

After the shutdown was first reported on Friday, gasoline futures on the New York Mercantile Exchange gained 0.6% while diesel futures rose 1.1%, both outpacing gains in crude oil. Gulf Coast cash prices for gasoline and diesel edged lower on prospects that supplies could accumulate in the region.

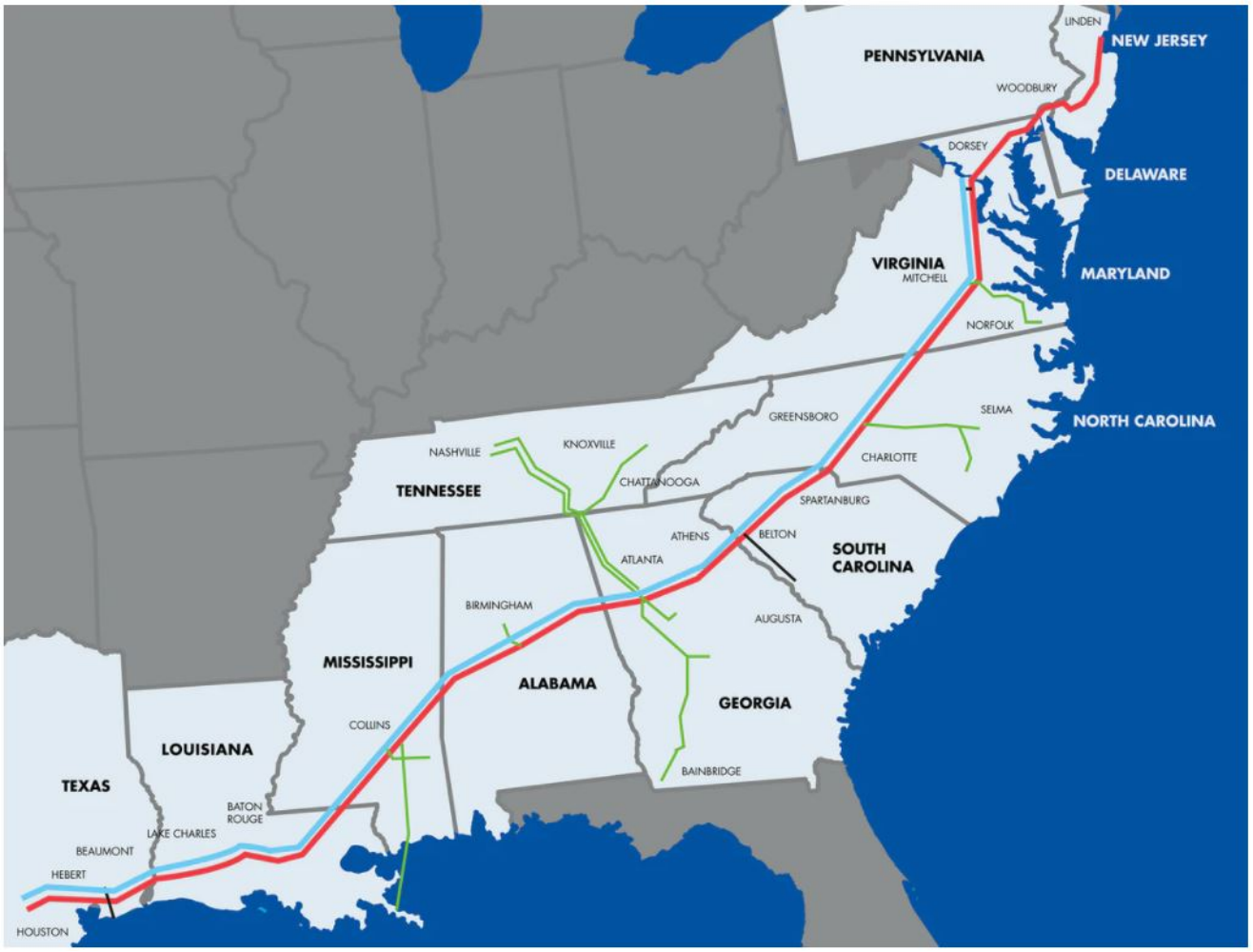
"As every day goes by, it becomes a greater and greater impact on Gulf Coast oil refining," said Lipow. "Refiners would have to react by reducing crude processing because they've lost part of the distribution system."

Oil refining companies contacted by Reuters on Saturday said their operations had not yet been impacted.

Kinder Morgan Inc (KMI.N), meanwhile, said its Products (SE) Pipe Line Corporation (PPL) serving many of the same regions remains in full service.

PPL is currently working with customers to accommodate additional barrels during Colonial's downtime, it said. PPL can deliver about 720,000 bpd of fuel through its pipeline network from Louisiana to the Washington, D.C., area.

Colonial Pipeline system map



The American Petroleum Institute, a top oil industry trade group, said it was monitoring the situation.

Ben Sasse, a Republican senator from Nebraska and a member of the Senate Select Committee on Intelligence, said the cyberattack was a wakeup call for U.S. lawmakers.

"This is a play that will be run again, and we're not adequately prepared," he said, adding Congress should pass an infrastructure plan that hardens sectors against these attacks.

Colonial previously shut down its gasoline and distillate lines during Hurricane Harvey, which hit the Gulf Coast in 2017. That contributed to tight supplies and gasoline price rises in the United States after the hurricane forced many Gulf refineries to shut down.

Reporting by Stephanie Kelly Editing by Shri Navaratnam

Our Standards: The Thomson Reuters Trust Principles.