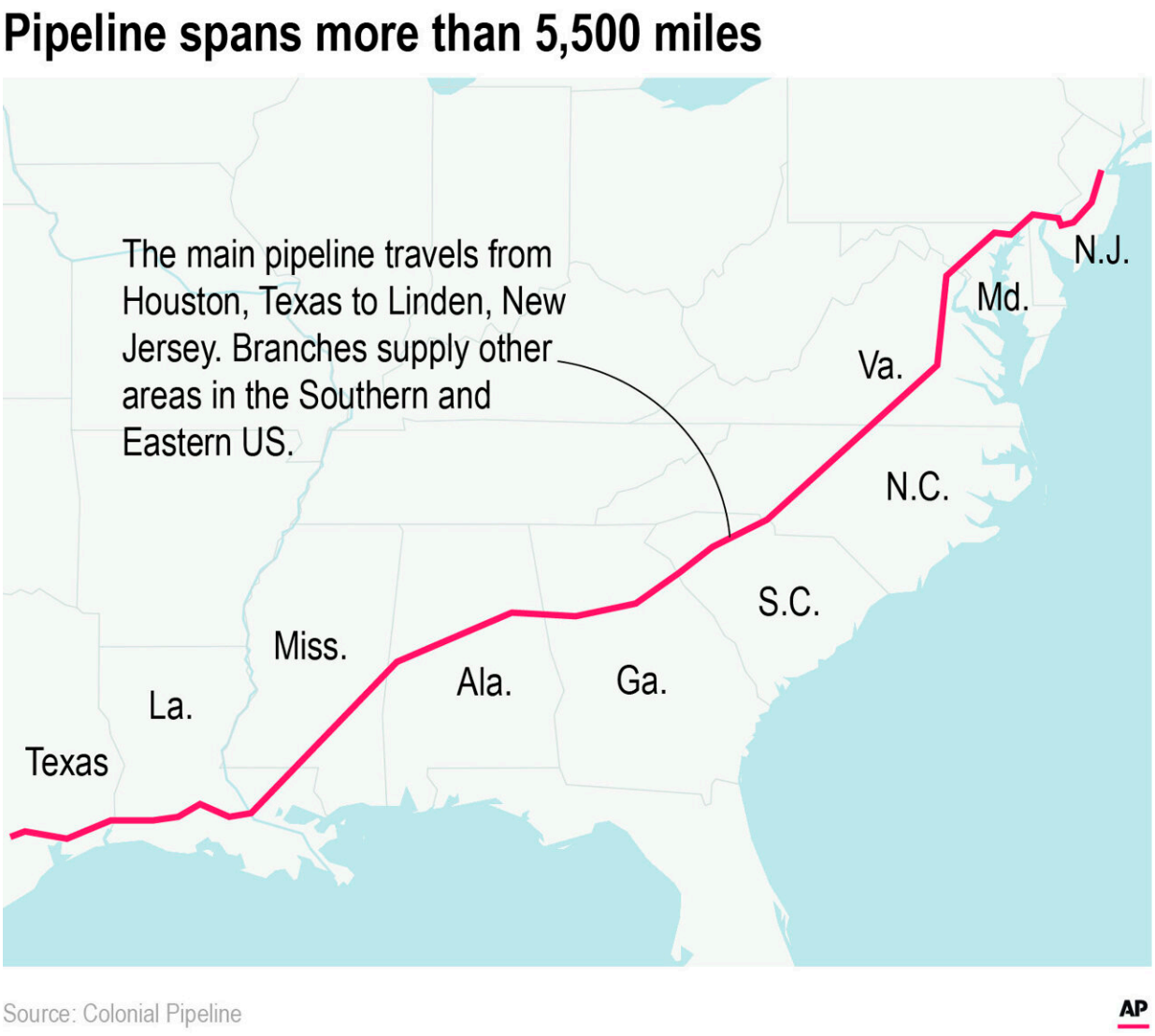
Major US pipeline halts operations after ransomware attack

May 8 2021, by Alan Suderman and Eric Tucker



A company that operates a major U.S. energy pipeline says it was forced to temporarily halt all pipeline operations following a cybersecurity attack.

The operator of a major pipeline system that transports fuel across the East Coast said Saturday it had been victimized by a ransomware attack and had halted all pipeline operations to deal with the threat. The attack is unlikely to affect gasoline supply and prices unless it leads to a prolonged shutdown of the pipeline, experts said.

Colonial Pipeline did not say what was demanded or who made the demand. Ransomware attacks are typically carried out by criminal hackers who scramble data, paralyzing victim networks, and demand a large payment to decrypt it.

The attack on the company, which says it delivers roughly 45% of fuel consumed on the East Coast, underscores again the vulnerabilities of critical infrastructure to damaging cyberattacks that threaten to impede operations. It presents a new challenge for an administration still dealing with its response to major hacks from months ago, including a massive breach of government agencies and corporations for which the U.S. sanctioned Russia last month.

In this case, Colonial Pipeline said the ransomware attack Friday affected some of its information technology systems and that the company moved "proactively" to take certain systems offline, halting pipeline operations. In an earlier statement, it said it was "taking steps to understand and resolve this issue" with an eye toward returning to normal operations.

The Alpharetta, Georgia-based company transports gasoline, diesel, jet fuel and home heating oil from refineries located on the Gulf Coast through pipelines running from Texas to New Jersey. Its pipeline system spans more than 5,500 miles, transporting more than 100 million gallon a day.

The White House said President Joe Biden was briefed Saturday morning and the federal government was working with the company to assess the implications of the attack, restore operations and avoid disruptions to the supply. The government is planning for various scenarios and working with state and local authorities on measures to mitigate any potential supply issues.

The private cybersecurity firm FireEye said it's been hired to manage the incident response investigation.

Oil analyst Andy Lipow said the impact of the attack on fuel supplies and prices depends on how long the pipeline is down. An outage of one day or two would be minimal, he said, but an outage of five or six days could cause shortages and price hikes, particularly in an area stretching from central Alabama to the Washington, D.C., region.

In this Sept. 8, 2008 file photo traffic on I-95 passes oil storage tanks owned by the Colonial Pipeline Company in Linden, N.J. A major pipeline that transports fuels along the East Coast says it had to stop operations because it was the victim of a cyberattack. Colonial Pipeline said in a statement late Friday that it "took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, and affected some of our IT systems." (AP Photo/Mark Lennihan, File)

Lipow said a key concern about a lengthy delay would be the supply of jet fuel needed to keep major airports operating, like those in Atlanta and Charlotte, North Carolina.

A leading expert in industrial control systems, Dragos CEO Robert Lee, said systems such as those that directly manage the pipeline's operation have been increasingly connected to computer networks in the past decade.

But critical infrastructure companies in the energy and electricity industries also tend to have invested more in cybersecurity than other sectors. If Colonial's shutdown was mostly precautionary—and it detected the ransomware attack early and was well-prepared—the impact may not be great, Lee said.

While there have long been fears about U.S. adversaries disrupting American energy suppliers, ransomware attacks by criminal syndicates are much more common and have been soaring lately. The Justice Department has a new task force dedicated to countering ransomware attacks.

The attack "underscores the threat that ransomware poses to

organizations regardless of size or sector," said Eric Goldstein, executive assistant director of the cybersecurity division at the federal Cybersecurity Infrastructure and Security Agency.

"We encourage every organization to take action to strengthen their cybersecurity posture to reduce their exposure to these types of threats," Goldstein said in a statement.

Ransomware scrambles a victim organization's data with encryption. The criminals leave instructions on infected computers for how to negotiate ransom payments and, once paid, provide software decryption keys.

The attacks, mostly by criminal syndicates operating out of Russia and other safe havens, reached epidemic proportions last year, costing hospitals, medical researchers private businesses, state and local governments and schools tens of billions of dollars. Biden administration officials are warning of a national security threat, especially after criminals began stealing data before scrambling victim networks and saying they will expose it online unless a ransom is paid.

In this Sept. 20, 2016 file photo vehicles are seen near Colonial Pipeline in Helena, Ala. A major pipeline that transports fuels along the East Coast says it had to stop operations because it was the victim of a cyberattack. Colonial Pipeline said in a statement late Friday that it "took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, and affected some of our IT systems." (AP Photo/Brynn Anderson, File)

Average ransoms paid in the United States jumped nearly threefold to more than $310,000 last year. The average downtime for victims of ransomware attacks is 21 days, according to the firm Coveware, which helps victims respond.

U.S. law enforcement officials say some of these criminals have worked with Russia's security services and that the Kremlin benefits by

damaging adversaries' economies. These operations also potentially provide cover for intelligence-gathering.

"Ransomware is the most common disruptive event that organizations are seeing right now that would cause them to shut down to prevent the spread," said Dave White, president of cybersecurity firm Axio.

Mike Chapple, teaching professor of IT, analytics and operations at the University of Notre Dame's Mendoza College of Business and a former computer scientist with the National Security Agency, said systems that control pipelines should not be connected to the internet and vulnerable to cyber intrusions.

"The attacks were extremely sophisticated and they were able to defeat some pretty sophisticated security controls, or the right degree of security controls weren't in place," Chapple said.

Brian Bethune, a professor of applied economics at Boston College, also said the impact on consumer prices should be short-lived as long as the shutdown does not last for more than a week or two. "But it is an indication of how vulnerable our infrastructure is to these kinds of cyberattacks," he said.

Bethune noted the shutdown is occurring at a time when energy prices have already been rising as the economy reopens further as pandemic restrictions are lifted. According to the AAA auto club, the national average for a gallon of regular gasoline has increased by 4 cents since Monday to $2.94.

Anne Neuberger, the Biden administration's deputy national security adviser for cybersecurity and emerging technology, said in an interview with The Associated Press in April that the government was undertaking a new effort to help electric utilities, water districts and other critical

industries protect against potentially damaging cyberattacks. She said the goal was to ensure that control systems serving 50,000 or more Americans have the core technology to detect and block malicious cyber activity.

Since then, the White House has announced a 100-day initiative aimed at protecting the country's electricity system from cyberattacks by encouraging owners and operators of power plants and electric utilities to improve their capabilities for identifying cyber threats to their networks. It includes concrete milestones for them to put technologies into use so they can spot and respond to intrusions in real time.