Cyberattack on US pipeline is linked to criminal gang

May 9 2021, by Mae Anderson and Frank Bajak

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)

The cyberextortion attempt that has forced the shutdown of a vital U.S. pipeline was carried out by a criminal gang known as DarkSide that cultivates a Robin Hood image of stealing from corporations and giving a cut to charity, two people close to the investigation said Sunday.

The shutdown, meanwhile, stretched into its third day, with the Biden administration loosening regulations for the transport of petroleum products on highways as part of an "all-hands-on-deck" effort to avoid disruptions in the fuel supply.

Experts said that gasoline prices are unlikely to be affected if the pipeline is back to normal in the next few days but that the incident—the worst cyberattack to date on critical U.S. infrastructure—should serve as a wake-up call to companies about the vulnerabilities they face.

The pipeline, operated by Georgia-based Colonial Pipeline, carries gasoline and other fuel from Texas to the Northeast. It delivers roughly 45% of fuel consumed on the East Coast, according to the company.

It was hit by what Colonial called a ransomware attack, in which hackers typically lock up computer systems by encrypting data, paralyzing networks, and then demand a large ransom to unscramble it.

On Sunday, Colonial Pipeline said it was actively in the process of restoring some of its IT systems. It says it remains in contact with law enforcement and other federal agencies, including the Department of Energy, which is leading the federal government response. The company has not said what was demanded or who made the demand.

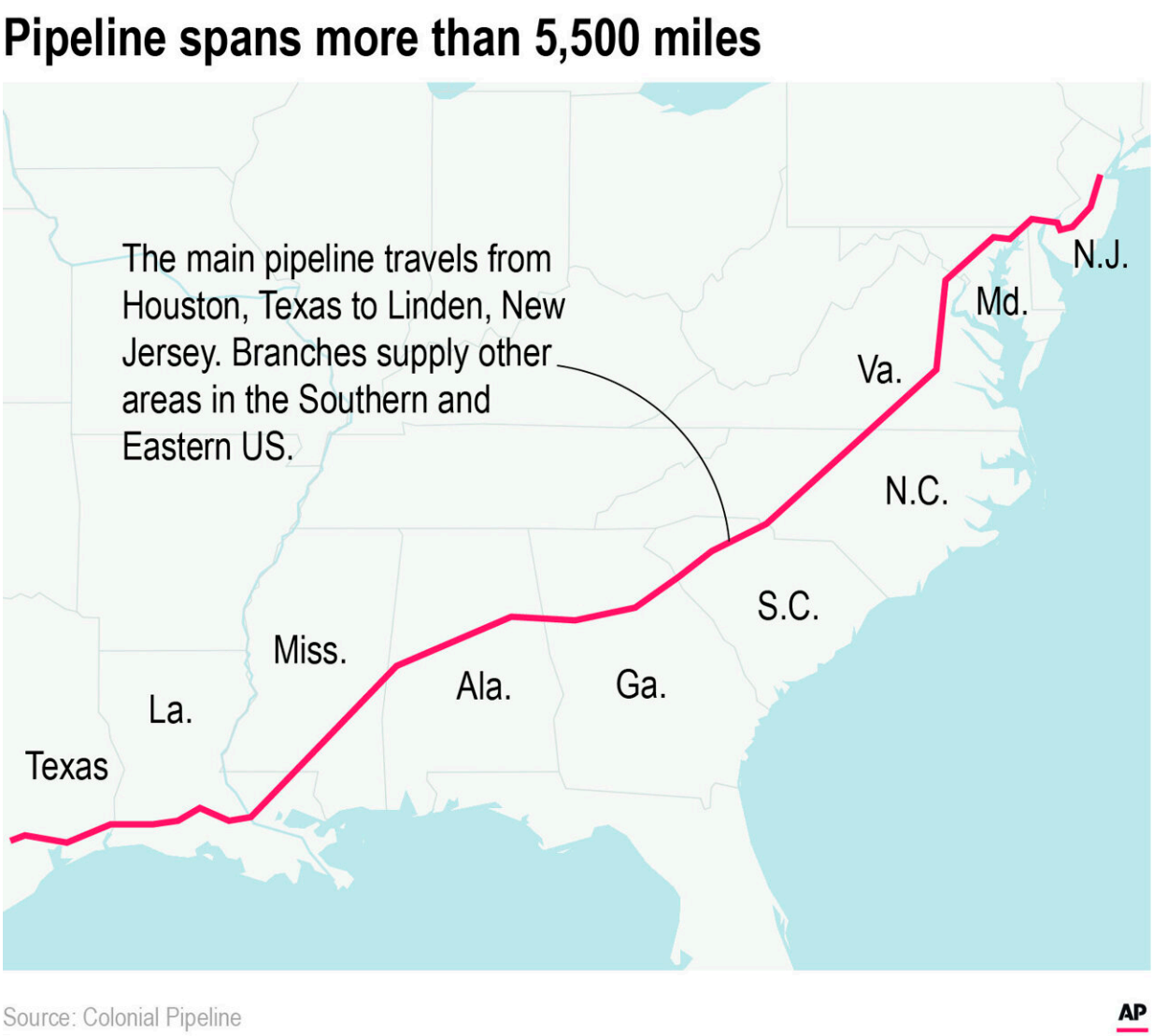
However, two people close to the investigation, speaking on condition of anonymity, identified the culprit as DarkSide. It is among ransomware gangs that have "professionalized" a criminal industry that has cost Western nations tens of billions of dollars in losses in the past three

years.

DarkSide claims that it does not attack hospitals and nursing homes, educational or government targets and that it donates a portion of its take to charity. It has been active since August and, typical of the most potent ransomware gangs, is known to avoid targeting organizations in former Soviet bloc nations.

Colonial did not say whether it has paid or was negotiating a ransom, and DarkSide neither announced the attack on its dark web site nor responded to an Associated Press reporter's queries. The lack of acknowledgment usually indicates a victim is either negotiating or has paid.

On Sunday, Colonial Pipeline said it is developing a "system restart" plan. It said its main pipeline remains offline but some smaller lines are now operational.



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

"We are in the process of restoring service to other laterals and will bring our full system back online only when we believe it is safe to do so, and in full compliance with the approval of all federal regulations," the company said in a statement.

Commerce Secretary Gina Raimondo said Sunday that ransomware attacks are "what businesses now have to worry about," and that she will work "very vigorously" with the Department of Homeland Security to address the problem, calling it a top priority for the administration.

"Unfortunately, these sorts of attacks are becoming more frequent," she said on CBS' "Face the Nation." "We have to work in partnership with business to secure networks to defend ourselves against these attacks."

She said President Joe Biden was briefed on the attack.

"It's an all-hands-on-deck effort right now," Raimondo said. "And we are working closely with the company, state and local officials to make sure that they get back up to normal operations as quickly as possible and there aren't disruptions in supply."

The Department of Transportation issued a regional emergency declaration Sunday, relaxing hours-of-service regulations for drivers carrying gasoline, diesel, jet fuel and other refined petroleum products in 17 states and the District of Columbia. It lets them work extra or more flexible hours to make up for any fuel shortage related to the pipeline outage.

One of the people close to the Colonial investigation said that the attackers also stole data from the company, presumably for extortion purposes. Sometimes stolen data is more valuable to ransomware criminals than the leverage they gain by crippling a network, because some victims are loath to see sensitive information of theirs dumped online.

Security experts said the attack should be a warning for operators of critical infrastructure—including electrical and water utilities and energy and transportation companies—that not investing in updating their

security puts them at risk of catastrophe.

Ed Amoroso, CEO of TAG Cyber, said Colonial was lucky its attacker was at least ostensibly motivated only by profit, not geopolitics. State-backed hackers bent on more serious destruction use the same intrusion methods as ransomware gangs.

"For companies vulnerable to ransomware, it's a bad sign because they are probably more vulnerable to more serious attacks," he said. Russian cyberwarriors, for example, crippled the electrical grid in Ukraine during the winters of 2015 and 2016.

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)

Cyberextortion attempts in the U.S. have become a death-by-a-thousand-cuts phenomenon in the past year, with attacks forcing delays in cancer treatment at hospitals, interrupting schooling and paralyzing police and city governments.

Tulsa, Oklahoma, this week became the 32nd state or local government in the U.S. to come under ransomware attack, said Brett Callow, a threat analyst with the cybersecurity firm Emsisoft.

Average ransoms paid in the U.S. 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.

David Kennedy, founder and senior principal security consultant at TrustedSec, said that once a ransomware attack is discovered, companies have little recourse but to completely rebuild their infrastructure, or pay the ransom.

"Ransomware is absolutely out of control and one of the biggest threats we face as a nation," Kennedy said. "The problem we face is most companies are grossly underprepared to face these threats."

Colonial transports gasoline, diesel, jet fuel and home heating oil from refineries on the Gulf Coast through pipelines running from Texas to New Jersey. Its pipeline system spans more than 5,500 miles (8,850 kilometers), transporting more than 100 million gallons (380 million

liters) a day.

Debnil Chowdhury at the research firm IHSMarkit said that if the outage stretches to one to three weeks, gas prices could begin to rise.

"I wouldn't be surprised, if this ends up being an outage of that magnitude, if we see 15- to 20-cent rise in gas prices over next week or two," he said.

The Justice Department has a new task force dedicated to countering ransomware attacks.

While the U.S. has not suffered any serious cyberattacks on its critical infrastructure, officials say Russian hackers in particular are known to have infiltrated some crucial sectors, positioning themselves to do damage if armed conflict were to break out. While there is no evidence the Kremlin benefits financially from ransomware, U.S. officials believe President Vladimir Putin savors the mayhem it wreaks in adversaries' economies.

Iranian hackers have also been aggressive in trying to gain access to utilities, factories and oil and gas facilities. In one case in 2013, they broke into the control system of a U.S. dam.