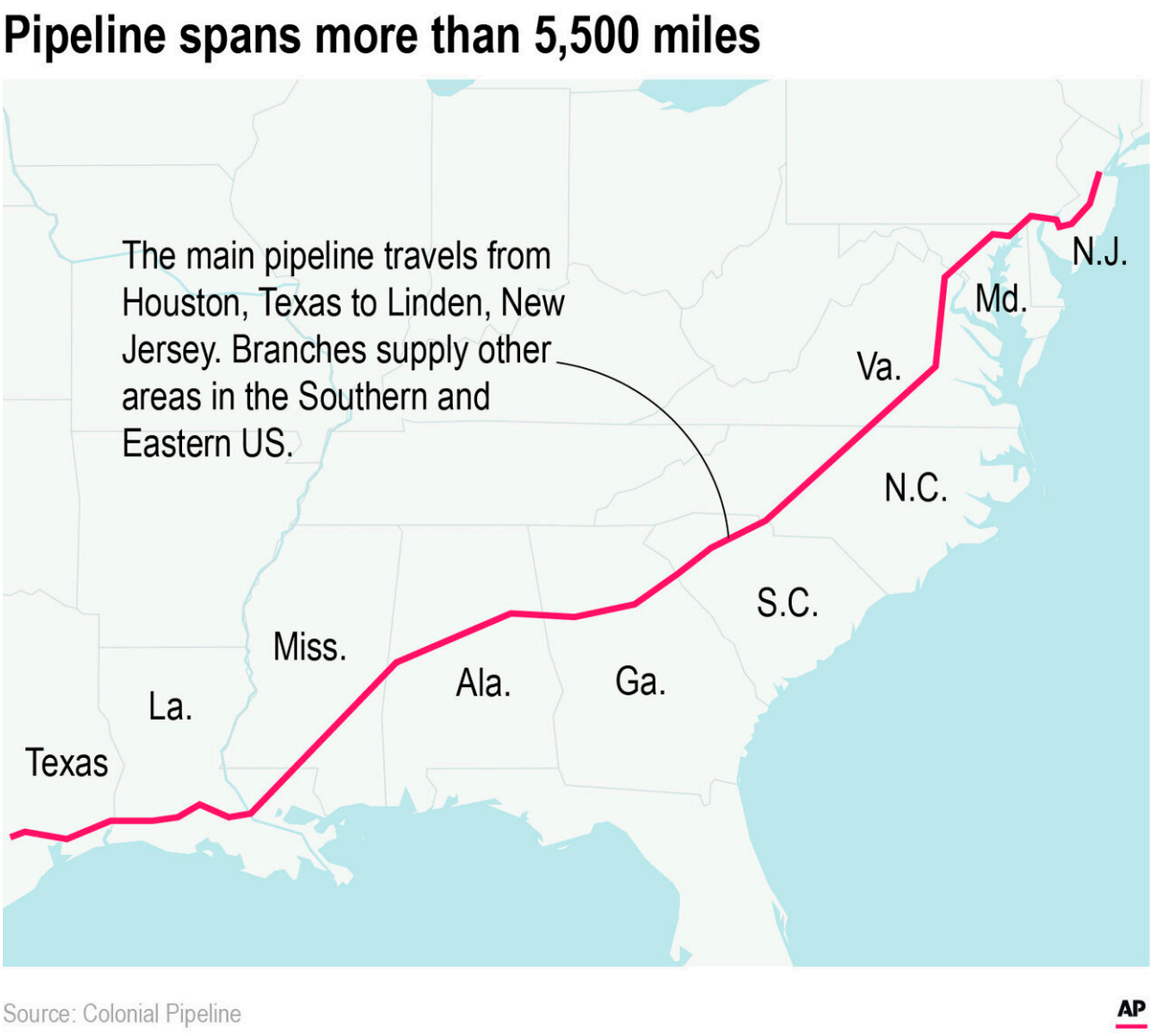
FBI names pipeline cyberattackers as company promises return

May 11 2021, by Eric Tucker, Cathy Bussewitz and Alan Suderman



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

Hit by a cyberattack, the operator of a major U.S. fuel pipeline said Monday it hopes to have services mostly restored by the end of the week as the FBI and administration officials identified the culprits as a gang of criminal hackers.

U.S. officials sought to soothe concerns about price spikes or damage to the economy by stressing that the fuel supply had so far not experienced widespread disruptions, and the company said it was working toward "substantially restoring operational service" by the weekend.

The White House said in a statement late Monday that it was monitoring supply shortages in parts of the Southeast and that President Joe Biden had directed federal agencies to bring their resources to bear.

Colonial Pipeline, which delivers about 45% of the fuel consumed on the East Coast, halted operations last week after revealing a ransomware attack that it said had affected some of its systems.

Nonetheless, the attack underscored the vulnerabilities of the nation's energy sector and other critical industries whose infrastructure is largely privately owned. Ransomware attacks are typically carried out by criminal hackers who scramble data, paralyzing victim networks, and demand large payments to decrypt it.

The Colonial attack was a potent reminder of the real-world implications of the burgeoning threat. Even as the Biden administration works to confront organized hacking campaigns sponsored by foreign governments, it must still contend with difficult-to-prevent attacks from cybercriminals.

"We need to invest to safeguard our critical infrastructure," Biden said

Monday. Energy Secretary Jennifer Granholm said the attack "tells you how utterly vulnerable we are" to cyberattacks on U.S. infrastructure.

The attack came as the administration, still grappling with its response to massive breaches by Russia of federal agencies and private corporations, works on an executive order aimed at bolstering cybersecurity defenses. The Justice Department, meanwhile, has formed a ransomware task force designed for situations just like Colonial Pipeline, and the Energy Department on April 20 announced a 100-day initiative focused on protecting energy infrastructure from cyber threats. Similar actions are planned for other critical industries, such as water and natural gas.

Despite that, the challenge facing the government and the private sector remains immense.

In this case, the FBI publicly assigned blame Monday by saying the criminal syndicate whose ransomware was used in the attack is named DarkSide. The group's members are Russian speakers, and the syndicate's malware is coded not to attack networks using Russian-language keyboards.

Anne Neuberger, the White House deputy national security adviser for cyber and emerging technology, said at a briefing that the group has been on the FBI's radar for months. She said its business model is to demand ransom payments from victims and then split the proceeds with the ransomware developers, relying on what she said was a "new and very troubling variant."

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)

She declined to say if Colonial Pipeline had paid any ransom, and the company has not given any indication of that one way or the other. Though the FBI has historically discouraged victims from making payments for fear of promoting additional attacks, she acknowledged "the very difficult" situation that victims face and said the administration needs to look "thoughtfully at this area" of how best to deter

ransomware.

"Given the rise in ransomware, that is one area we're definitely looking at now to say, 'What should be the government's approach to ransomware actors and to ransoms overall?'"

Speaking later in the day at a conference on national security, Neuberger said the administration was committed to leveraging the government's massive buying power to ensure that software makers make their products less vulnerable to hackers.

"Security can't be an afterthought," Neuberger said. "We don't buy a car and only then decide if we want to pay for seatbelts and airbags."

The U.S. sanctioned the Kremlin last month for a hack of federal government agencies, known as the SolarWinds breach, that officials have linked to a Russian intelligence unit and characterized as an intelligence-gathering operation.

In this case, though, the hackers are not known to be working at the behest of any foreign government. The group posted a statement on its dark web site describing itself as apolitical. "Our goal is to make money, and not creating problems for society," DarkSide said.

Asked Monday whether Russia was involved, Biden said, ""I'm going to be meeting with President (Vladimir) Putin, and so far there is no evidence based on, from our intelligence people, that Russia is involved, although there is evidence that the actors, ransomware, is in Russia.

"They have some responsibility to deal with this," he added.

U.S. officials have sought to head off anxieties about the prospect of a lingering economic impact and disruption to the fuel supply, especially

given Colonial Pipeline's key role in transporting gasoline, jet fuel, diesel and other petroleum products between Texas and the East Coast.

Colonial is in the process of restarting portions of its network. It said Monday that it was evaluating the product inventory in storage tanks at its facilities. Administration officials stressed that Colonial proactively took some of its systems offline to prevent the ransomware from migrating from business computer systems to those that control and operate the pipeline.

In response to the attack, the administration loosened 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.

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)

"The time of the outage is now approaching critical levels and if it continues to remain down we do expect an increase in East Coast gasoline and diesel prices," said Debnil Chowdhury, IHS Markit Executive Director. The last time there was an outage of this magnitude was in 2016, he said, when gas prices rose 15 to 20 cents per gallon. The Northeast had significantly more local refining capacity at that time.

The pipeline utilizes both common and custom technology systems, which could complicate efforts to bring the entire network back online, according to analysts at Third Bridge.

Granholm, the Energy Secretary, said "Cyber attacks on our critical infrastructure—especially energy infrastructure—is not going away."

"This is a serious example of what we're seeing across the board in many places and it tells you that we need to invest in our systems, our transmission grid for electricity. We need to invest in cyber defense in these energy systems," she told Bloomberg TV.

The attack has not affected the supply of gasoline, she said, "but if it goes on too long, of course that will change."

Gasoline futures ticked higher Monday. Futures for crude and fuel, prices that traders pay for contracts for delivery in the future, typically

begin to rise anyway each year as the driving season approaches. The price you pay at the pump tends to follow.

The average U.S. price of regular-grade gasoline has jumped 6 cents over the past two weeks, to $3.02 per gallon, which is $1.05 higher than a year ago. The year-ago numbers are skewed somewhat because the nation was going into lockdown due to the pandemic.

The attack on the Colonial Pipeline could exacerbate the upward pressure on prices if it is unresolved for a period of time.