NORTH CAROLINA'S INFORMATION SHARING AND ANALYSIS CENTER ISAAC

SITUATIONAL AWARENESS BULLETIN

UNCLASSIFIED//FOR OFFICIAL USE ONLY

May 11, 2021

Impact of Colonial Pipeline Cyber Attack

This information has been compiled by NC Emergency Management.

(U) OVERVIEW

(U//FOUO) On May 7, 2021, Colonial Pipeline Company learned it was the victim of a cybersecurity attack and it has since determined that the incident involved the Darkside ransomware group. Quickly after learning of the attack, Colonial proactively took certain systems offline to contain the threat. These actions temporarily halted all pipeline operations and affected some of its IT systems. The threat group who caused Colonial Pipeline to shut down on Friday May 7, 2021, began their attack against the company approximately one day prior, stealing a large amount of data before locking computers with ransomware and demanding payment.

(U) EVENT DETAILS

(U//FOUO) The Darkside ransomware group took nearly 100 gigabytes of data out of the company's network in two hours on Thursday May 6, 2021. The attack employed a double-extortion scheme that is common among cyberattacks committed by the Darkside ransomware group and others like it. Colonial was threatened that the stolen data would be leaked to the internet while the information that was encrypted would remain locked unless it paid a ransom. It is not yet clear how much money the attackers have demanded, or whether Colonial intends to comply with those demands.

(U) THREAT ACTOR

(U//FOUO) The FBI has been investigating the Darkside ransomware group since October 2020. Darkside is a ransomware-as-a-service (RaaS) variant, in which criminal affiliates conduct the attacks and the proceeds are shared with the ransomware developer(s). Darkside has impacted numerous organizations across various sectors including manufacturing, legal, insurance, healthcare, and energy. According to information provided by the Darkside ransomware group, they mainly target large corporations who they determine are more likely to comply with ransom demands. The group also states that based on their principles they do not target organizations in the following industries: medicine, funeral services, education, non-profit, and government.

(U//FOUO) According to the FBI, Darkside can encrypt files on fixed and removable hardware as well as network devices. Darkside encrypts files using Salsa20 encryption with an RSA-1024 public key and affiliates can use Darkside in both Windows and Linux environments.

(U//FOUO) Darkside actors are encouraged by the ransomware developers to use Monero1 in their demands, as cyber actors believe that cryptocurrency provides additional anonymity and security. Darkside affiliates use an administrative panel over The Onion Router (TOR) to access communications with the victims and manage administration of the ransomware. The Darkside website includes a landing page with possible victims and descriptions of data taken.

(U) COLONIAL PIPELINE COMPANY

(U//FOUO) The Colonial Pipeline Company, founded in 1962, connects refineries – primarily located in the Gulf Coast – with customers and markets throughout the Southern and Eastern United States through a pipeline system that spans more than 5,500 miles. The company delivers refined petroleum products such as gasoline, diesel, jet fuel, home heating oil, and fuel for the U.S. Military. It is the largest refined products pipeline in the United States, transporting more than 100 million gallons or 2.5 million barrels per day. Colonial transports approximately 45 percent of all fuel consumed on the East Coast, providing refined products to more than 50 million Americans.

(U//FOUO) More than 250 shippers and 270 terminals use the Colonial Pipeline system to transport refined petroleum products to locations in 14 states. Major markets served include Birmingham, AL; Atlanta, GA; Nashville, TN; Charlotte, NC; Norfolk and Richmond, VA; Washington, D.C.; Philadelphia, PA; and the New York City area. Colonial also feeds other pipeline systems such as the Buckeye system, which supplies products across Pennsylvania and upstate New York, as well as to Long Island and New York City airports.

(U//FOUO) Markets in the Southeast are highly dependent on the Colonial Pipeline for petroleum product supply. Colonial delivers more than 70% of the transportation fuels supply to Georgia, South Carolina, North Carolina, Tennessee, and Virginia. Colonial also provides 30% to 70% of the fuel supply to Alabama, and Maryland. The Plantation pipeline system, and to a lesser extent receipts at coastal ports, make up the balance of supply in these states. Colonial also supplies less than 30% of the fuel in Mississippi and to the U.S. Northeast.

(U) RESPONSE

(U//FOUO) The U.S. Department of Transportation (USDOT) announced May 9, 2021, that as part of the federal government's efforts to actively assess the implications of the Colonial Pipeline incident and to avoid disruption to supply, that the USDOT's Federal Motor Carrier Safety Administration (FMCSA) is taking steps to create more flexibility for motor carriers and drivers. FMCSA is issuing a temporary hours of service exemption that applies to those transporting gasoline, diesel, jet fuel and other refined petroleum products to Alabama, Arkansas, District of Columbia, Delaware, Florida, Georgia, Kentucky, Louisiana, Maryland, Mississippi, New Jersey, New York, North Carolina, Pennsylvania, South Carolina, Tennessee, Texas and Virginia.

(U//FOUO) Reports from the American Petroleum Institute suggest the system was full upon shutdown so fuel should likely be available more quickly upon system restart. While the (FMCSA) issued an hours of service waiver on May 9, 2021, North Carolina is unaware of any additional fuel waiver requests at this time.

(U//FOUO) As of May 10, 2021 7:55PM, the Colonial Pipeline Company reports "that Line 4, which runs from Greensboro, N.C., to Woodbine, Md., is operating under manual control for a limited period of time while existing inventory is available. As previously announced, while our main lines continue to be offline, some smaller lateral lines between terminals and delivery points are now operational as well. We continue to evaluate product inventory in storage tanks at our facilities and others along our system and are working with our shippers to move this product to terminals for local delivery." Updated press releases can be monitored at the following site: Media Statement: Colonial Pipeline System Disruption (colpipe.com)

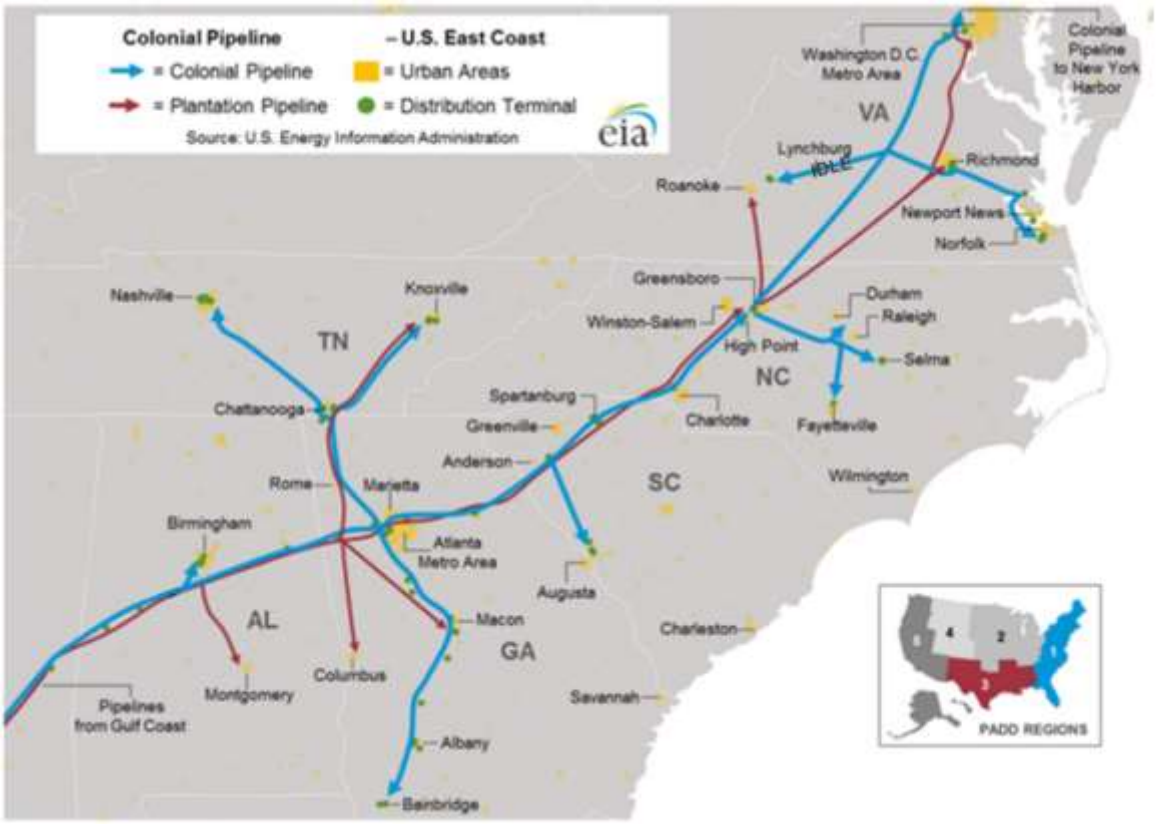
(U) SHUTDOWN CONCERNS

(U//FOUO) There are limited alternatives to the Colonial Pipeline system, particularly for markets in the U.S. Southeast. The much smaller, 700,000 b/d Plantation Pipeline runs a similar route to Colonial, but it does not supply markets further north than the Washington, D.C. area, and likely has minimal ability to increase volumes above their normal supply.

(U//FOUO) During an extended outage, Central Atlantic markets such as New York and Philadelphia would likely increase marine imports to offset losses from Colonial. However, additional import cargos may take extended time to arrive on the East Coast to support immediate supply issues. For some markets in the Southeast, product would need to either be trucked directly from Gulf Coast refineries or shipped by marine vessel to coastal ports (Wilmington, Savannah, Charleston, Jacksonville, and Mobile, etc.) and then trucked to inland markets (e.g., Atlanta, Charlotte, Raleigh, etc.).

(U//FOUO) Some markets may be more significantly impacted. The Colonial Pipeline is currently the sole source of supply to the Nashville, TN market as barge supply on the Cumberland River has been limited due a lock closure. Markets in the Hampton Roads, VA, Raleigh, NC, and southwestern Georgia are also predominantly dependent on Colonial Pipeline supply.

(U//FOUO) Media stories about the cyber incident may promote a spike in consumer purchases of gasoline in areas served by the line, further limiting supply.



(U) TERMINALS

(U//FOUO) Non-Colonial owned terminals supplied by the Colonial systems can operate using existing supplies.

(U//FOUO) Fuel marketers operating in the Southeast have reportedly started allocating fuel volumes available to their customers. Unbranded distributors may experience disruptions as major suppliers provide contracted supply to branded dealers.

(U) REFINERIES

(U//FOUO) With the loss of Colonial as a takeaway option, Gulf Coast refiners may need to reduce runs or shut-in operations if production builds up in tankage and marine loadings cannot be quickly arranged. Stocks of diesel and gasoline in the Gulf Coast Region (PADD 3) were high as of April 30, limiting storage options for refineries from a prolonged shutdown. At least one Gulf Coast refiner has booked a foreign-flagged oil products' tanker for storage in the Gulf of Mexico to increase storage capacity, per industry sources. The chartered tanker would provide up to 330,000 barrels of potential storage.

(U) MARINE IMPORTS

(U//FOUO) At least five tankers carrying a total of 2.3 million barrels of gasoline are reportedly destined for New York Harbor after loading in Saudi Arabia. The tankers are scheduled to discharge fuel through June 4. An additional three tankers chartered to carry 1.5 million barrels of Mideast Gulf gasoline to the U.S. Atlantic Coast are loading this week for future delivery.

(U//FOUO) An import vessel with 370,000 barrels of gasoline has reportedly been diverted to Yorktown, VA from New York Harbor to help supply the Hampton Roads, Virginia area. The vessel is likely 2-3 days away from delivery.

(U//FOUO) At least six tankers have been booked for U.S. destinations from Europe on a provisional basis, according to media reports.

(U) AIRPORTS

(U//FOUO) Some major airports along the Colonial system only have a few days of jet fuel supply in onsite storage and may be particularly vulnerable to a multi-day supply outage. Airlines may adjust to shortages by refueling aircraft at other airports whenever possible.

(U//FOUO) Colonial directly serves seven airports. Three of these also have access to jet fuel from Plantation. Additional airports are served indirectly by Colonial, including airports in Norfolk and Richmond, VA.

(U//FOUO) Airports in the New York metropolitan region (JFK, LaGuardia, and Newark) are supplied with jet fuel from the Buckeye Pipeline system, which can be supplied via Colonial Pipeline. However, Buckeye Pipeline can also receive fuel from refineries in New Jersey and Pennsylvania, providing some alternative fuel supply during the Colonial disruption.

(U//FOUO) Notably, three of the seven airports directly supplied by the Colonial Pipeline Company are in North Carolina and highlighted below:

Airports Directly Supplied by Colonial Pipeline			
Airport Name (Code)	**Metropolitan Region Served**	**Supply Pipelines**	**2020 Jet Fuel Consumption (b/d)**
Hartsfield-Jackson (ATL)	Atlanta, GA	Colonial and Plantation	36,000
Charlotte Douglas (CLT)	Charlotte, NC	Colonial and Plantation	19,000
Dulles (IAD)	National Capital Region	Colonial and Plantation	14,000
Baltimore-Washington (BWI)	Baltimore, MD	Colonial	13,000
Nashville (BNA)	Nashville, TN	Colonial	5,000

Raleigh-Durham (RDU)	Raleigh, NC	Colonial	4,000
Piedmont Triad (GSO)	Greensboro, Winston-Salem, and High Point, NC	Colonial	No data available

(U) ADDITIONAL CONSIDERATIONS

- North Carolina has an approximate 5-day fuel supply in the state. For planning purposes, 5 days expires Wednesday, May 12th.
- Western NC is more heavily dependent on the Colonial Pipeline
- Fuel suppliers are waiting until Colonial Pipeline releases an estimated time of restoration before deciding if they will request an Hours of Service or Weight Waiver.
- Fuel suppliers are hesitant to request a waiver due to the likelihood that this request will trigger a State of Emergency. This may result in increased customer volume at local gas stations which will significantly affect current state fuel supply.
- With increased media interest, a run on the pumps may begin to occur. Public information may want to prepare messaging to help avoid this type of situation.
- If this event continues into the week, traffic control and security will be a concern at terminals in Selma, Greensboro, Charlotte, and Port of Wilmington.
- The Port of Wilmington may see significantly higher quantities of product than normal.
- A bulk fuel transportation plan was being implemented in the Charlotte Area by Colonial Pipeline to supply fuel to the area as well as to the Airport.
- The Aviation ISAC has an inbound request to the FAA (DOE has awareness) for current planned or underway mitigation actions to ensure the seven directly connected airports to the Colonial Pipeline maintain fuel supplies.
    - The Monroe Refinery in Chester, PA (owned by Delta Airlines) is an alternative source of production for Jet-A aircraft fuel and if needed, it could be trucked to close by airports to maintain operation
- Impacts to fuel supply within North Carolina may occur. Organizations should review their fuel contingency planning and be postured in the chance of a shortage. If so, it will likely have a greater impact to organizations that have unbranded distributors.
- Fuel supply shortages are likely to have multiple downstream cascading impacts to include but not limited to: aviation, shipping/essential resource distributions (food, water, livestock, etc.), public safety organizations (rely heavily on gasoline and diesel fuel for Hospitals, Fire, EMS, LEO, etc.), and individual citizens.
- Open sources suggest the following locations in North Carolina are reporting “out of gas” and/or experiencing “fuel shortages”: Asheville, Clinton, Vanceboro, Robbinsville, Chocowinity, Hendersonville, Ocean Isle Beach, Jacksonville, Fayetteville, and Washington.

(U) If you have any information to share, please contact the NCISAAC at ncisaac@ncsbi.gov.