Cybersecurity and Infrastructure Security Agency
Integrated Operations Division

Situation Report

Colonial Pipeline Suffered Ransomware Attack – Alpharetta, GA - 05-10-21 - INC10337231

Date As Of: 05/10/2021 20:19:06	**Sitrep Update #:** Init
Incident Start Time: 05/07/2021 **Incident End Time:** Ongoing	**Incident Location:**
Impacted Sectors: Energy, (Oil), Transportation Systems, (Pipeline Systems)	**Reported Cause of Incident:** Ransomware Attack
Interagency Coordination:	**On Scene Agencies:** CISA, DOE
Owner/Operator(s) Involved: Colonial Pipeline	**Source of Information:** Open source, proprietor

Incident Summary:

The Colonial Pipeline halted all pipeline operations on May 7 after proactively taking certain systems offline to contain the threat from an ongoing cybersecurity incident. Colonial has hired a third-party cybersecurity firm and is working to return the pipeline to normal operation, but the timeline for full restoration is unknown at this time.
Colonial Pipeline is the main conduit of refined products from Gulf Coast refineries to the U.S. Atlantic Coast and into the New York Harbor. Colonial Pipeline's 5,550 miles of pipe serve major metropolitan areas including Birmingham, AL; Atlanta, GA; Charlotte, NC; Richmond, VA; Washington, DC; Baltimore, MD; Philadelphia, PA; and New York, NY.

Key Points:

- Colonial Pipeline reports mainlines 1 through 4 are offline, but some smaller lateral lines between terminals and delivery points are now operational.
- Colonial stated there are indications the malware was present up to a week prior to being executed.
- According to DOE, a shutdown lasting beyond May 12 would have widespread impacts on fuel supply in the Southeast and Central Atlantic markets
- The Colonial Pipeline is currently the sole source of supply to the Nashville, TN market as supply of refined product via barge on the Cumberland River has been limited due to a lock closure. Fuel markets in Hampton Roads, VA, Raleigh, NC, and southwestern Georgia are also largely dependent on supply received via the Colonial Pipeline.

RANSOMWARE

The suspected variant is termed “Darkside” and 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). This variant can encrypt files on fixed and removable hardware as well as network devices. Darkside has impacted numerous organizations across various sectors including manufacturing, legal, insurance, healthcare, and energy.

Darkside ransomware actors haven't previously targeted specific companies within the U.S. Energy Sector. The FBI has investigated Darkside since October 2020. Darkside most often exfiltrates victim data before encrypting it and then threatening to release the data if the ransom is not paid.

COLONIAL PIPELINE OVERVIEW

More than 250 pipeline shippers and 270 product storage terminal companies use the Colonial Pipeline system to

transport refined petroleum products to locations in 14 states. Colonial Pipeline is estimated to carry approximately 15-20% of U.S. pipeline shipments per company figures. For the East Coast, Colonial provides approximately 40% per company figures. There are limited alternatives to move refined petroleum products from the U.S. Gulf Coast without utilizing 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 the Colonial Pipeline, 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.

The Colonial Pipeline has direct connections to seven major airports and has transfer service to three airports in New York City area via an interconnection with the Buckeye Pipeline system.
• The seven major airports with direct connections are: Atlanta (ATL), Nashville (BNA), Charlotte (CLT), Greensboro (GSO), Raleigh-Durham (RDU), Washington-Dulles (IAD), and Baltimore-Washington (BWI)

WARNING: Information in this report is FOUO//TLP: GREEN. Recipients may only share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. This information may be circulated widely within a particular community but may not be released outside of the community, consistent with both the DHS policy relating to safeguarding FOUO information (link here) and with the Traffic Light Protocol, http://www.us-cert.gov/tlp. Information in this report is not customarily in the public domain and may be exempt from public release under the Freedom of Information Act (5 U.S.C. § 552). Further, this section may contain or be based upon commercial or financial information, which is privileged or confidential, law enforcement sensitive, or deliberative/pre-decisional material. DHS personnel are reminded of their obligations under DHS Form 11000-6, Non-Disclosure Agreement. Further dissemination of any of the information contained in this REPORT requires express consent from CISA Central.