# **Title**

Colonial Pipeline Cyberattack: A Ransomware Incident and its Impact on U.S. Fuel Supply

# **Introduction:**

Colonial Pipeline, a critical oil pipeline system in the U.S., faced a ransomware cyberattack on May 7, 2021.

# **Background:**

The pipeline system covers the transport of gasoline, diesel, and jet fuel from Texas to the Southeastern U.S., constituting 55% of East Coast fuel consumption.

Occurred amid heightened concerns about infrastructure vulnerability following the 2020 SolarWinds hack.

# **Incident Overview:**

Dates: May 6, 2021 (data stolen), May 7, 2021 (ransomware attack), May 12, 2021 (pipeline restarted).

Type: Cyberattack, data breach, ransomware.

Target: Colonial Pipeline.

Suspects: DarkSide hacking group.

# **Attack Method:**

Ransomware cyberattack impacting pipeline management systems.

DarkSide demanded a 75 Bitcoin ransom (approx. $4.4 million USD), paid within hours.

# **Impact:**

Halting of pipeline operations due to concerns about potential further attacks.

Primary target was the billing infrastructure, causing customer billing disruptions.

Attackers stole nearly 100 gigabytes of data, threatening release if the ransom was unpaid.

Panic buying led to widespread gasoline shortages and increased fuel prices.

# **Investigation:**

FBI oversaw the response; Department of Justice recovered 63.7 bitcoins (84% of the ransom) with decreased value due to Bitcoin crash.

# **Lessons Learned:**

One of the first high-profile corporate cyberattacks initiated from a breached employee's personal password found on the dark web.

# **Conclusion:**

Pipeline operations resumed, and a significant portion of the ransom was recovered.