# Colonial Pipeline Ransomware Attack

-By Ch. Akhil Sampath Vinay

I am currently a third-year B. Tech student in the Cyber Security department at Vignana Bharathi Institute of Technology. I am writing this article for Abhedhya club.

On May 6th, 2021, Colonial Pipeline was hit by a ransomware attack, causing a six-day shutdown of pipeline operations. The pipeline is responsible for transporting gasoline, diesel, and jet fuel from Texas to New York, and the East Coast relies on it for 55% of its fuel. The ransomware attack targeted the billing infrastructure, and while the oil pumping systems were unaffected, the pipeline was shut down as a precaution. The company paid a ransom of nearly 75 Bitcoin ($4.4 million USD) to the hackers, who also stole close to 100 gigabytes of data and threatened to release it on the internet if the ransom was not paid.

Colonial Pipeline is a major fuel pipeline operator in the United States, responsible for transporting gasoline, diesel, and jet fuel along the East Coast. The pipeline system spans from Texas to New Jersey and supplies a substantial portion of the fuel consumed in the eastern part of the country. In May 2021, Colonial Pipeline fell victim to a ransomware attack carried out by a hacking group called Darkside, which is believed to have operated from Russia or Eastern Europe. The attackers used ransomware to encrypt the company's computer systems and data, effectively disrupting its operation. As a result of the attack, Colonial Pipeline was forced to shut down its pipeline operations as a precaution to prevent the malware from spreading further and to assess the extent of the damage. As the pipeline operations were shut the country was affected by the Fuel shortage, Transportation disruptions, and Economic Impact.

The primary target of the attack was the billing infrastructure of the company. The actual oil pumping systems were still able to work. Colonial Pipeline reported that it shut down the pipeline as a precaution due to a concern that the hackers might have obtained information allowing them to carry out further attacks on vulnerable parts of the pipeline. The day after the attack, Colonial could not confirm at that time when the pipeline would resume normal functions. The attackers also stole nearly 100 gigabytes of data and threatened to release it on the internet if the ransom was not paid. It was reported that within hours after the attack the company paid a ransom of nearly 75 Bitcoins ($4.4 million USD) to the hackers in exchange for a decryption tool, which proved so slow that the company's business continuity planning tools were more effective in bringing back operational capacity. On May 9, Colonial stated, they planned to substantially repair and restore the pipeline's operations by the end of the week. U.S. President Joe Biden declared a state of emergency on May 9, 2021.

Biden signed Executive Order 14028. on May 12, increasing software security standards for sales to the government, tightening detection and security on existing systems, improving information sharing and training, establishing a Cyber Safety Review Board, and improving incident response. The United States Department of Justice also convened a cybersecurity task force to increase prosecutions. The Department of State issued a statement that a $10,000,000 reward would be given out in case of information leading to the arrest of DarkSide members DarkSide released a statement on May 9 that did not directly mention the attack, but claimed that "our goal is to make money, and not creating problems for society.

The Colonial Pipeline restarted operations on May 12 after a six-day shutdown. However, intermittent service interruptions may continue in some markets. The company is moving fuel as safely as possible until markets fully recover. By May 15, all systems had returned to normal. Gasoline prices rose to over $3.04 a gallon, the highest in six years, with some southern states experiencing even higher prices. The FBI has retrieved 63.7 Bitcoins worth $2.3 million by possessing the private key of the ransom account. U.S. Department of Justice issued a press release on June 7, 2021, but did not disclose how they obtained the private key.

The Colonial Pipeline ransomware attack sparked discussions about cyber security, critical infra-structure protection, and the need for stronger measures to prevent and respond to such attacks. It also emphasized the importance of private sector entities developing strategies to mitigate the risk of future attacks.