The Colonial Pipeline Ransomware Attack

Samantha Riggs

Old Dominion University

CS462: Cybersecurity Fundamentals

Susan Zehra

August 2nd, 2025

Introduction

The seemingly exponential growth and development of technology, along with the expansion of the online world, has provided many benefits to society as a whole. Enhanced communication, improved access to information, and better healthcare methods are just a few examples. However, with this growth comes a corresponding growth of opportunities for malicious attackers to find and exploit vulnerabilities. In order for attackers to formulate their means of attack, they have to decide upon a variety of variables and components. For example, there are multiple different forms and means of these attacks such as phishing fraud schemes, worms, and viruses, each of which have their own complexities.

One form a cyber attack can take that is particularly malicious is the creation and subsequent deployment of ransomware. A recent case of ransomware being utilized in a large-scale attack is the Colonial Pipeline attack in 2021. Within this paper, I will explore the background of the attack, how it was carried out, the technology involved, the impact that followed, and the broader implications brought on by the attack.

Background

The Colonial Pipeline Company is a private company in charge of a pipeline that transports the fuel needed to provide energy to around half of the citizens of the United States. The pipeline's own website states that it "transports over one hundred million gallons of fuel every day on a system stretching from Houston to the New York Harbor" and it is the largest refined fuel pipeline by volume currently present within the nation. The company is just one example of a wide variety of companies involved in the United States's critical infrastructure systems.

In order for an industry to be considered part of a critical infrastructure sector, the Cybersecurity and Infrastructure Security Agency (CISA) states that it must have "assets, systems, and networks, whether physical or virtual, that are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." There are sixteen identified sectors by CISA, but in this case, the Colonial Pipeline Company falls under the Energy Sector. Due to how integral a role that critical infrastructure systems are to maintaining the efficiency of systems within the United States, these systems are particularly appealing to cyber attackers searching to infiltrate, cause damage, and aim for monetary gain.

The Attack Itself

This attack was carried out by a group who identified themselves as DarkSide. This group successfully hacked into the pipeline's systems and rendered them unusable by encrypting the data present. Then, the group demanded money from the company in order for the company to regain access to their own systems. In other words, the group held the company's systems for ransom, which is the main goal of ransomware attacks. DarkSide held both the encrypted data hostage and threatened to release the sensitive information contained within the data if the ransom was not paid.

The specific type of ransomware that DarkSide used was known for its ability to efficiently evade detection and operated as Ransomware as a Service (RaaS). An RaaS model allows an individual or a group to develop a specific script or other malicious program and then sell it off or even lease it to other criminals who can replicate the attacks done and then share the profits afterwards. Approximately $5 million in ransom was ultimately paid to the attackers.

Access to Colonial Pipeline's systems was revealed to have been achieved through an exposed password for a VPN account. Many companies, especially those that deal with sensitive or critical information, will often have company-regulated VPNs that are required for employees to use. What is thought to have happened in this case was that an employee used the same password for their VPN account for another service or website. This incident of password reuse becoming a vulnerability is a very common access point that users unknowingly present to attackers. If a user uses one password for one site, they are very likely to use that same password for another, or multiple other, websites. While having the same password across multiple accounts is convenient for the user, it presents a very large vulnerability. If password information is leaked from a website, attackers can attempt to use that password to access other accounts the user has. It is for this reason that attackers will sometimes target websites that have weak security in order to obtain login information and then attempt to use that information in more secure locations. It is likely that if this human vulnerability was not present, infiltration into such a secure system as a federal pipeline company's would be highly unsuccessful.

Impact, Response, and Remediation

In order to prevent the attack from spreading any further than it had already gotten, Colonial Pipeline was forced to completely shut down all of their systems, temporarily halting the movement of fuel across the country. The system stayed shut down for multiple days until the ransom was paid. After the decryption key was provided, it still took a couple more days for service to be fully restored. The resulting localized shortages of gasoline, diesel, and jet fuel caused by this downtime sparked panic-buying and multiple emergency declarations in several different states.

After the system was restored following the high-profile attack, both federal and state governmental agencies made efforts to ensure that oil and gas pipeline networks, as well as the electric grid, were secure. Even though initial access to these systems was achieved through an opening provided by password reuse, there was a secondary vulnerability present. Prior to this attack, government agencies left cybersecurity policies and strategies up to individual private companies and organizations. Prior to the attack, the Transportation Security Administration (TSA) had voluntary standards that were suggested to critical infrastructure sectors, but there was a lack of official guidelines or mandated policies.

The Colonial Pipeline attack elicited action by Congress and the Executive Branch, with President Joe Biden publishing an executive order that had already been drawn up in response to a separate cybersecurity incident prior to Colonial Pipeline's. Executive Order 14028 aims to address the security of the supply chain by working to remove the information barriers between government sectors and private sector entities concerning cybersecurity matters. The Bipartisan Infrastructure Law established assistance programs and grants that directly fund cybersecurity measures. Some additional measures were established were the State Energy Program to focus on energy security, the Cyber Response and Recovery Fund for the Cybersecurity and Infrastructure Security Agency to be used in the case of a cybersecurity incident, and the establishment of the Energy Sector Operational Support for Cyber Resilience Program to enhance the emergency response capabilities of the Department of Energy.

As far as consequences for the perpetrators, the DarkSide group was never publicly identified, arrested, or charged with a crime by United State authorities. However, approximately $2.3 million was able to be recovered by the United States Department of Justice. Later, Russia

(the country in which the attacker was thought be located) collaborated with the United States to arrest an individual suspect thought to be behind the attack.

Conclusion

This attack illustrated a large vulnerability present within private critical infrastructure sector in the United States, as well as highlighting just how detrimental the loss of these systems could be, even within a few days. Additionally, it highlighted the previously unseen growth of malicious cybersecurity attacks that target critical infrastructure systems rather than ones performed on information agencies or within the private sector. As a result of this attack and in response to the need for better cybersecurity awareness and policies not just for private companies but for government agencies as well, new strategies and legislation was passed to work to address the gap that was exposed through this attack.

References

Critical Infrastructure Sectors: CISA. Cybersecurity and Infrastructure Security Agency CISA. (n.d.-b). https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Colonial Pipeline Cyber Incident. Energy.gov. (n.d.). https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

Colonial Pipeline. (n.d.-b). https://www.colpipe.com/

Energy sector. Energy Sector | Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector

Holdsworth, J., & Kosinski, M. (2025, April 17). *What is Ransomware-as-a-service (raas)?*. IBM. https://www.ibm.com/think/topics/ransomware-as-a-service

Kerner, S. M. (2022, April 26). *Colonial pipeline hack explained: Everything you need to know*. WhatIs. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Lyngaas, S. (2022, January 14). *US officials believe Russia arrested hacker responsible for colonial pipeline attack | CNN politics*. CNN. https://www.cnn.com/2022/01/14/politics/us-russia-colonial-pipeline-hack-arrest

The attack on Colonial Pipeline: What we've learned & what we've done over the past two years: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2024, August 23).

https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Wood, K. (2023, March 7). *Cybersecurity policy responses to the Colonial Pipeline Ransomware attack*. Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack | Georgetown Environmental Law Review | Georgetown Law. https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack