The Colonial Pipeline's Vulnerabilities and Consequences

Robert Sullivan Timmons

School of Cybersecurity, Old Dominion University

CYSE300: Introduction to Cybersecurity

Dr. Joseph Kovacic

January 12th, 2023

The modern digital world is fraught with cyber-attacks. On a daily basis, data breaches and cyber-attacks occur. A majority of these attacks are minor, but in some cases, cyber attacks can garner national attention. A recent example of this would be the cyber-attack on the Colonial Pipeline Company, which owns and operates the Colonial Pipeline. The Colonial Pipeline is a petroleum and gas pipeline that runs through the majority of the east coast, providing a sizeable portion of gasoline and other oil products to the region. After the cyber-attack, the company was forced to temporarily shut down its pipeline, resulting in a major loss of gas transportation in the energy sector. This research paper will cover the vulnerabilities that led to the attack, the threats that took advantage of the vulnerabilities, and the repercussions of the incident. With a proper understanding of the situation and the events that made the attack possible, this paper will conclude with what could've been done differently to prevent the attack. Before continuing, the author would like to establish that he is not an expert on all things cyber-related and that the situation is extremely complex. The goal is to relay his findings on what caused the breach, who took advantage of the situation, and the repercussions to the reader, finishing up with cyber practices that could've hampered the attack.

Though the Colonial Pipeline delivers such a vital resource to the United States economy, the breach that brought down the company and its pipeline was relatively simple. Despite spending "…$200 million over the last five years in its IT systems…" (Kelly & Resnick-ault, 2021), one of the company's passwords was leaked and sold on a dark web forum. The CEO further disclosed that the company was utilizing a legacy VPN, with no Multi-Factor Authentication, otherwise known as MFA. This lack of MFA as well as the stolen password allowed access to the company's systems. The organization that exploited the system was a hacker group known as Darkside. Tom Uren, a writer at the Australian Strategic Policy Institute,

also known as ASPI, explains that the Darkside group is based in Russia, and the organization "…operates on a 'ransomware as a service' business model…" (Uren, 2021). After Darkside's malware was detected within Colonial Pipeline systems, the pipeline was shut down to prevent the further spread to more systems, stopping pipeline operations. No matter how much money is spent on cyber-related security services, the colonial pipeline hack proves that if simple vulnerabilities aren't taken care of, they can be devastating.

The repercussions of the Colonial Pipeline hack were twofold. The company was forced to pay 4.4 million dollars in bitcoin to Darkside to save their systems. After the attack, the federal government was able to return a majority of the stolen cryptocurrency. Due to crypto markets, however, the returned coins had lost value, incurring a loss to the Colonial Pipeline Company. More devastating was the shutdown of the pipeline. According to Cyber News, the pipeline "…supplies around 45% of the gas to the East Coast…". (Gaskell 2022) This shutdown led to a rise in prices, as well as market uncertainty and panic. Media coverage didn't assuage public panic either. This national event cost millions of dollars, not only to the colonial pipeline company but to the average American consumer.

Studying the breach brings to light some key takeaways that could be used to prevent further attacks. One way to mitigate an attack such as this would be password security. Though the CEO of the Colonial Pipeline Company stated that "It was a complicated password…" (Kelly & Resnick-ault, 2021 and "It was not a Colonial123-type password." (Kelly & Resnick-ault, 2021), the protection of the password was lacking. As with ODU MIDAS identification passwords, the company could have utilized expiring passwords, so that passwords and codes cannot be stored away and sold at later dates. Basic authenticators like Multi-Factor Authentication should have been standard practice in the company to avoid the entire breach.

This is pointed out by govtech, who state in their deep dive of the colonial pipeline hack, “This simple, yet extremely effective, security measure serves as the ultimate gatekeeper for those trying to access private networks…” (Securelink, 2021) Another technique that could have mitigated the attack would be the decentralization of the colonial pipeline’s systems. As reported by ASPI, “The hackers did not target the pipeline’s industrial control systems to deliberately stop the oil flow. Colonial itself shut down systems to prevent further spread of malware.” (Uren, 2021) If there were air gaps or separation between these systems, there may have not been the need for a shutdown of the pipeline’s systems. To be clear, the author of this paper is not an expert, and this issue is extremely complex, but with these basic techniques previously mentioned, there may have been proper counters to Darkside’s hack.

The Colonial pipeline hack was devastating to millions of Americans. Without basic password protection and multifactor authentication, the hacker group Darkside was able to compromise a part of the Colonial Pipeline company’s systems. To combat the spread of the malware, the company completely shut down oil transportation, leading to market uncertainty, public panic, and outrage. After explaining the situation, the paper suggested automatic password expiration dates, as well as decentralization, which could have prevented the breach or softened its consequences. The Colonial Pipeline hack is a painful example of how if critical infrastructure is not properly defended, it can easily be compromised and cause mayhem.

References

Person, & Stephanie Kelly, J. R.-ault. (2021, June 9). *One password allowed hackers to disrupt colonial pipeline, CEO tells senators*. Reuters. Retrieved January 16, 2023, from https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/

Uren, T. (2021, May 26). *US pipeline Hack exposes major vulnerabilities*. The Strategist. Retrieved January 16, 2023, from https://www.aspistrategist.org.au/us-pipeline-hack-exposes-major-vulnerabilities/

GovTech. (2021, July 8). *Back to basics: A deeper look at the colonial pipeline hack*. GovTech. Retrieved January 16, 2023, from https://www.govtech.com/sponsored/back-to-basics-a-deeper-look-at-the-colonial-pipeline-hack

The colonial pipeline hack affected gas prices less than we thought. (n.d.). Retrieved January 16, 2023, from https://cybernews.com/security/the-colonial-pipeline-hack-affected-gas-prices-less-than-we-thought/