Overview of the Colonial Pipeline Attack of 2021

Gavin L Williams

Old Dominion University

CS 462: Cybersecurity Fundamentals

Susan Zehra

4/14/2024

Introduction

America’s Colonial Pipeline serves as a crucial piece of infrastructure in the country's fuel supply chain. Spanning over 5,500 miles from Texas to New York, it makes up 45% of the East Coast's fuel supply. In May 2021, this vital asset fell victim to a sophisticated cyberattack, which halted operations. With the progression of technology, the frequency of cyberattacks is increasing. Therefore, it is crucial that we learn as much as possible from such incidents. This post aims to analyze the event by exploring its implications and important lessons learned. By examining the details of the attack, the response, and its broader consequences, we can use our past mistakes as opportunities to strengthen our systems for the future.

Background Information

The Colonial Pipeline, which stretches over 5,500 miles from Houston, Texas to the Port of New York, is the largest refined oil pipeline system in the United States. It distributes refined petroleum products to businesses and communities in the country's eastern and southern regions. Kimberly Wood (2023) states that without the oil from the Colonial Pipeline, there would be no gasoline for transportation, jet or diesel fuel, or home heating oil. Additionally, the pipeline supports many major airports and military bases along its route. Therefore, maintaining the integrity of the pipeline’s operations is crucial not only for commercial purposes but also for national security. Historically, damaging such significant infrastructure required physical force; however, with the advancement of technology and networked systems, cyberattacks have become an increasingly prominent threat. Previous attacks on infrastructure, such as those on Ukraine’s power grid in 2015 and the NotPetya attack in 2017, demonstrate the potential of cyberattacks to cause physical disruptions that can halt the operations of critical infrastructure

(Wood, 2023). These incidents highlight the importance of strong cybersecurity measures and swift incident response strategies to protect vital systems from harm.

Details of the Attack

According to Renee Dudley and Daniel Golden (2021), On January 11, an antivirus company by the name of Bitdefender made a prominent breakthrough in the realm of cybersecurity. They were able to find a flaw with the ransomware systems created by a large hacking gang known as DarkSide. DarkSide had been selling ransomware as a service to anyone who was able to pay for it. This would allow individuals the ability to attack just about anyone using the sophisticated malware developed by DarkSide. However, companies facing demands from this gang could simply download a tool created by Bitdefender that would bypass the ransomware. Consequently, through publishing this tool, "Bitdefender alerted DarkSide to the lapse, which involved reusing the same digital keys to lock and unlock multiple victims. The next day, DarkSide declared that it had repaired the problem, and that "new companies have nothing to hope for"" (Dudley and Golden, 2021, p. 2). DarkSide even went so far as to thank Bitdefender for finding the vulnerability in their malware. Shortly after this event, as Joe Reeder (2021) mentioned, on Friday, May 7, 2021, at around 5:00 AM, employees of Colonial Pipeline discovered a ransom note demanding millions of dollars in Bitcoin be paid to recover their locked systems. With this discovery, the colonial pipeline immediately shut down, halting services that extended the entire 5,500 miles of the pipeline. After the pipeline was shut down, rather than look for ways around the ransomware, they decided to simply pay the ransom of $4.4 million in exchange for a key to unlock its files. As written within Dudley and Golden's (2021) article, "CEO Joseph Blount told The Wall Street Journal, "I will admit that I wasn't comfortable seeing money go out the door to people like this"" (Dudley and Golden, 2021, p. 3).

The technical details of the colonial pipeline attack showed a combination of sophisticated tactics from the attackers and a major security oversight by the pipeline company. DarkSide was able to bypass the security of the company through a compromised password found online. The attackers used this password to connect to an old VPN account that lacked multi-factor authentication. Kerner (2022) noted that, once the attackers were able to get access to the network, they utilized typical ransomware tactics. They escalated their privileges and moved laterally through the network, moving from one machine to another to collect valuable data while aiming to increase their permissions. Then they encrypted the files and broadcast a ransom message demanding for money to be paid in order to get the key to unencrypt the files. Additionally, they threaten to leak sensitive information as another form of blackmail (Kerner, 2022). An advisory written by the Cybersecurity and Infrastructure Security Agency (2021) reports that "DarkSide actors have previously been observed gaining initial access through phishing and exploiting remotely accessible accounts and systems and Virtual Desktop Infrastructure (VDI) (*Phishing* [T1566], *Exploit Public-Facing Application* [T1190], *External Remote Services* [T1133]).[5],[6] DarkSide actors have also been observed using Remote Desktop Protocol (RDP) to maintain *Persistence* [TA0003]" (CISA, 2021).

Impact of the Attack

The shutdown of the Colonial Pipeline had significant economic ramifications, leading to sudden fuel shortages across several states. This disruption caused gasoline prices to spike, affecting airline operations and other industries that rely on frequent fuel deliveries. The news of the attack prompted many citizens to engage in panic buying, escalating the fuel shortage. Consequently, the federal government had to intervene to alleviate the crisis, highlighting the national scale of the disruption. Media coverage of the incident also significantly influenced the

public's distress. Many news stations exaggerated the severity of the attack, escalating the public's concern to outright panic. Furthermore, the extensive reporting shed light on potential vulnerabilities in our infrastructure, creating a sense of distrust.

Response

Sean Kerner (2022) notes that the initial response to the attack was an immediate shutdown of the pipeline's operations upon detecting the DarkSide ransomware, aimed at preventing the malware from spreading further and minimizing damage. Following the shutdown, Colonial Pipeline collaborated with leading cybersecurity experts and the FBI to determine how DarkSide gained access to the system, how to contain the ransomware's spread, and how to begin system recovery and data restoration. Subsequently, they decided to pay the ransom of $4.4 million, which amounted to 75 Bitcoin at the time. This decision was highly controversial because not only does paying the ransom potentially encourage future cyberattacks; furthermore, in many ransomware cases, the decryption key is not provided even after the ransom is paid. A few days following the attack, President Biden suggested that while the Russian government was not directly involved, there was a belief that the attackers were based in Russia. After which, the FBI confirmed that DarkSide was responsible for the ransomware attack, and a joint cybersecurity advisory was issued by CISA and the FBI regarding the ransomware. To mitigate damage caused by the sudden shutdown of the pipeline, various federal responses were initiated, such as directives from the Department of Transportation and other measures to assist states disrupted by the fuel shortage. After six days from the initial shutdown, they began restarting systems. It took a couple of days for operations to stabilize, and with all systems reporting back to normal, the Colonial Pipeline was announced and fully operational (Kerner, 2022). According to Renee Dudley and Daniel Golden (2021), after this incident

"President Joe Biden issued an executive order to improve cybersecurity and create a blueprint for a federal response to cyberattacks" (p. 2). Upon hearing this, "DarkSide said it was shutting down under U.S. pressure" (p. 2); however, they most likely disbanded and re-formed with a new name to avoid attention (Dudley and Golden, 2021, p. 2).

Lesson Learned

This incident highlighted the critical need for enhanced cybersecurity measures across all critical infrastructure. Key lessons include the importance of rapid incident response, the benefits of robust backup systems, and the need for ongoing cybersecurity education. Following the attack, Colonial Pipeline and other similar entities have implemented stricter cybersecurity protocols and increased collaboration with governmental cybersecurity agencies. As for specific improvements, we know that, as stated by John Shier (2021), "it was confirmed that the initial entry point into the Colonial Pipeline network was a single stolen password" (Shier, 2021). Specifically, the attackers were able to use this password without issue since the account failed to set up multi-factor authentication (MFA). MFA is a fairly simple security procedure, but it does an excellent job of strengthening password security. As Shier (2021) mentions, the password leak could have been the result of a past data breach that was not accounted for in the recovery stage post attack. It is critical to remember that older breaches can have a lasting impact; thus, it is crucial to continuously monitor and audit past and present security measures to prevent old vulnerabilities from resurfacing in future systems. Moreover, as Shier (2021) writes, "According to the investigators, the earliest indicator that the attackers were in the network was April 29, 2021. This means the attackers were in the Colonial Pipeline network for at least eight days prior to the ransomware attack on May 7, 2021" (Shier, 2021). The CEO of Colonial Pipeline later explains that if they were able to detect the malware sooner, they most likely would not have had

to shut down operations. This highlights the importance of improved detection systems and constant network monitoring to stop threats, as they appear to minimize damage done. Additional mitigation techniques, as mentioned by the Cybersecurity and Infrastructure Security Agency (2021), include filtering network traffic, limiting access to resources over the network, "deploying signatures to detect and block connections from Tor exit nodes, and other similar services" creation of demilitarized zones that hold/block irregular communications, and the implementation of application allowlisting (CISA, 2021).

Conclusion

The Colonial Pipeline incident highlights the significant impact cyberattacks can have on national infrastructure and the broader economy. This event not only disrupted fuel distribution across a significant portion of the United States but also highlighted the vulnerabilities in critical infrastructure systems to sophisticated cyber threats. The rapid response by Colonial Pipeline, in collaboration with federal agencies, mitigated what could have been a much more severe crisis, though the decision to pay the ransom remains controversial. From this incident, we can take away several key lessons: the necessity of robust cybersecurity measures, the importance of quick and coordinated incident response, and the critical role of government and industry collaboration in safeguarding national interests. Enhanced measures, such as the implementation of multi-factor authentication and continuous monitoring for breaches, experiences, such as this one, serve as a critical reminder of the ongoing and evolving challenges posed by cyber threats. They stress the need for continual improvement of defense techniques, regular security audits, and further cybersecurity education and awareness, ensuring readiness and resilience against future attacks.

Citations

Darkside ransomware: Best practices for preventing business disruption from ransomware attacks: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2024, February 29). https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a. Access 4/13/2024.

Dudley, R., & Golden, D. (2021). The colonial pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms. *ProPublica (24 May 2021)*. https://energyrights.info/sites/default/files/artifacts/media/pdf/the_colonial_pipeline_ransomware_hackers_had_a_secret_weapon_self-promoting_cybersecurity_firms_-_propublica.pdf. Accessed 4/12/2024.

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. Accessed 4/13/2024.

Reeder, J. R., & Hall, T. (2021). Cybersecurity's pearl harbor moment. *The Cyber Defense Review*, *6*(3), 15-40. https://www.jstor.org/stable/48631153?seq=3. Accessed 4/12/2024.

Shier, J. (2021b, June 28). What IT security teams can learn from the colonial pipeline ransomware attack. Sophos News. https://news.sophos.com/en-us/2021/06/28/what-it-security-teams-can-learn-from-the-colonial-pipeline-ransomware-attack/. Accessed 4/13/2024.

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/#:~:text=The%20pipeline%20network%20was%20vulnerable,to%20private%20sector%20entities%20themselves. Accessed 4/11/2024.