The Colonial Pipeline Ransomware Attack: A Comprehensive Analysis

By: Colin Murphy

CYSE 280

April 18, 2024

Introduction

Every minute, thousands of cyberattacks are launched in various countries across the world. We do not notice because most of them have little to no effect on us thanks to the protective systems that are installed in our infrastructure. However, now and then, a cyber-attack is able to slip through the crack and can cause immense damage to the target and every device connected. The Colonial Pipeline Ransomware attack that hit the United States in May of 2021 is a textbook example of how a cyberattack can cripple or stall a part of our infrastructure and lead to a public and economic catastrophe. It has also been regarded as the most publicly disclosed cyberattack in U.S. history. In this paper, I hope to illustrate the background behind the attack, what software was used in the attack, and how it was conducted to effectively cripple one of our largest pipelines. I also hope to elaborate on the importance of teaching cyber awareness to workers in companies critical to our infrastructure so they can identify attacks and baits as well as how to take preventative measures to ensure an attack has no crippling damages.

History

The Colonial Pipeline Company is one of the largest oil pipeline companies in the United States. It is responsible for shipping refined oil throughout the states along the East Coast primarily to be used for gasoline. The attack was believed to have been conducted by a group referred to as “DarkSide.” They are a group of hackers are traced to Eastern Europe or

Russia however it has never been confirmed if they have ties to any government. According to an analysis by IEEE, the attack was initiated at the end of April of 2021. They hacked into an old account of the company that was still attached to their VPN and did not have any multifactor authentication preferences activated. This allowed them access to the company's entire database at their disposal. They launched a form of cyber-attack called "ransomware" which is a type of virus that holds the device hostage and prompts a transaction of an amount of currency the hackers demand or they will keep it locked down or wipe it. On May 7th, the ransomware was discovered by the pipeline staff, and this caused panic throughout the company and the US government. This led to the pipeline being completely shut down which caused widespread gas shortages from Texas to New York. The Pipeline Company was forced to pay the amount totaled to $4.4 million in cryptocurrency and was given the decryption key to gain back access to their systems. Thanks to the shutdown the pipeline was not damaged and resumed operations within a week. The Department of Justice was able to recover $2.3 million of the paid cryptocurrency in June of that year. (1)

The Ransomware

As stated before the malware used in the attack is called "ransomware," and it has been the backbone of many cyberattacks that have crippled many companies with heavy ties to infrastructure. Ransomware attacks have been growing in frequency since they were first developed in the early 2000s and they prove to be some of the most devastating methods of hacking in our current cyberspace. One of the most devastating ransomware attacks in history was targeted at Ukraine and it was called “NotPetya.” It was launched in June of 2017, and it targeted any computer in Ukraine it could spread to including devices from an advertising firm called “WPP,” a shipping company called Maersk, and Heritage Valley Health System. It also had an effect on more than sixty countries including the United States. The estimated total damages came close to $11 Billion. This specific attack used EternalBlue, a Microsoft Windows exploit that used the Server Message Block (SMB) protocol to remotely execute code on target computers. (2)

DarkSide’s attack on the pipeline was orchestrated a little differently. They found out the Colonial Pipeline Company issued encrypted remote access to employees who work from home or from afar. They were able to identify an unused account that was still connected to the company’s VPN. Not only that but the account had no two-factor authentication meaning with just the password they could access the account. They then stole 100 GB of data from the servers and left behind their program. (3)

Their ransomware was harder to break because of a private security firm. They are called Bitdefender, and they announced a flaw in the ransomware that DarkSide had used previously had been discovered by researchers Fabian Wosar and Michael Gillespie. The researchers never announced the discovery so that they could discretely help any victims who were affected by the attacks. By publicizing the vulnerability, DarkSide made quick work to reengineer their ransomware and “thanked” them for helping fix the issues. (4)

The Effects of the Attack

The biggest effect of the attack was the pipeline itself being shut down. Word carried around about the cyberattack and many people were unsure if the pipeline would be reactivated in a short amount of time. This led to a large number of people panic-buying their gasoline which led to a temporary increase in gas prices (5). It even caused many gas stations to shut down operations because of how depleted their supplies were. The attack also temporarily halted flights from airports as jet fuel was shorted as well. The attack also displayed how much of an effect a cyberattack could have on a major part of our infrastructure. Since the US has started to implement more advanced technologies to help operate different integral parts of our infrastructure this increases the need for cybersecurity and for people to be informed and trained on how to respond to an attack.

What We Learned

This attack brought to light the numerous amount of flaws that our infrastructure’s cybersecurity faces even to this day. Cybersecurity is not just the programs and software that go into protecting a corporation’s devices from attacks, it is also on each employee to understand how their systems work and how to properly secure them. It is important that corporations not only invest in cybersecurity systems and workers but also in company training sessions that illustrate the importance of cyber awareness. This includes the utilization of different tools such as multifactor authentication and password resets to help secure their accounts and devices, as well as learning how to identify scams. Another lesson that is important to learn is that breakthroughs in decrypting malware must not be widely disclosed as hackers are a part of the audience it would be informed too. People deserve to know the truth about the world, but it is also important that some information be withheld so no further damage can be caused by revised methods. Lastly, innovation and reengineering our systems and our policies will help us better ensure our cybersecurity remains strong. As the technology we use every day advances so do the methods hackers use to steal our data and cripple our infrastructure. That is why we must take persistent measures to ensure that our policies evolve with our technology. The U.S. government is also enacting cybersecurity policies and procedures that will help corporations and government agencies bolster their cybersecurity efforts and investments.

Conclusion

In conclusion, the Colonial Pipeline attack was one of the most notable cyberattacks of this decade. While it is economic effect was not long-lasting, its societal effect will help ensure we uphold our cyber initiatives and continue to educate the public about its importance. Understanding and studying this attack can help us understand better how hackers find ways to infiltrate our systems and force our hands to do their bidding. Research must continue to help develop tools and methods to help detect, erase, and decrypt malware. We were fortunate that this attack only had minor consequences, but we may not be so lucky the next time. A properly executed attack could send our nation back into the stone age and our way of life may never be the same again. We must take action to ensure that the public, businesses, and government agencies are properly educated on the basics of cybersecurity preparedness and the procedure for when an attack occurs. We may not be able to prevent these attacks, but we have the power to ensure that our way of life remains protected for years to come. (6)

References

(1) Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023). *A Review of Colonial Pipeline Ransomware Attack*. ieeeexplore.ieee.org. https://ieeexplore.ieee.org/abstract/document/10181159

(2) Fayi, S. (2018, January). What Petya/NotPetya Ransomware Is and What Its Remidiations Are. Retrieved 2024,.

(3) 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

(4) Dudley, R., & Golden, D. (2021, May 24). *The Colonial Pipeline Ransomware Hackers had a secret weapon: Self-promoting cybersecurity firms*. ProPublica. https://www.propublica.org/article/the-colonial-pipeline-ransomware-hackers-had-a-secret-weapon-self-promoting-cybersecurity-firms

(5) Tsvetanov, T., & Slaria, S. (2021, October 12). *The effect of the colonial pipeline shutdown on gasoline prices*. Economics Letters. https://www.sciencedirect.com/science/article/abs/pii/S0165176521003992

(6) Easterly, J. (2023, May 7). *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. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years