2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW) | 979-8-3503-0208-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/CCGridW59191.2023.00017

A Review of Colonial Pipeline Ransomware Attack

Jack Beerman, David Berent, Zach Falter, Suman Bhunia
Department of Computer Science and Software Engineering, Miami University, Oxford, Ohio, USA 45056
Email: beermajt@miamioh.edu, berentdm2@miamioh.edu, falterzt@miamioh.edu, bhunias@miamioh.edu

***Abstract*—In April, 2021 a ransomware attack occurred on Colonial Pipeline. The details of this attack point to the hacking group DarkSide taking advantage of the design flaws in the Colonial Pipeline network. After extensive research, the specificity of this attack was related to VPN access through an unused account. In order to regain control of their systems, Colonial Pipeline paid the attackers. This act has only created an incentive for similar attacks across the nation. The events of this attack have impacted both the United States, where the company is located and the world in a very negative way. This paper analyzes the attack with published data and provides a detailed attack methodology. From the attack methodology the focus then shifts into the impacts that an attack of this caliber had, on both the company, the United States, and the world. We then outline possible defense strategies against this type of ransomware attack, analyzing what could have been done to prevent this attack from happening. In addition, we also detail how companies can prevent future attacks of this caliber. Finally we wrap up or findings and detail the key takeaways of the entire attack.**

***Index Terms*—Colonial Pipeline, Ransomware, DarkSide (Hacking Group), Virtual Private Network (VPN), Dark Web**

I. Introduction

The Colonial Pipeline Co. is the biggest oil pipeline company in the United States, making it one of the most important companies in the U.S.. Anything to happen to this company would affect oil movement across the United States, causing massive problems in every aspect of the economy. On April 29, 2021 the Colonial Pipeline Co. was hit by a ransomware attack. The company was blackmailed by the hackers for cryptocurrency on May 7, roughly a week after the ransomware attack began. It began with an employee receiving a message at 5 a.m. telling him to pay $4.4 million in cryptocurrency to those responsible for the hack. Upon receiving the message the employee sent the message up to his supervisors, who then shut the plant down. The company opted to eventually pay the hackers much to the dismay of most of the cyber world. After paying the hackers the company started an extensive search to determine how the actual hack took place and found some interesting things. Luckily, through the shutdown, the pipeline was not damaged at all.

The findings for looking into the routing of the hackers lead the researchers to find the exact entry place. There was an old account that was no longer in use that was attached to the virtual private network (VPN) as can be seen in Fig. 5. Through this old account, the password was either compromised through human blackmail (ex-employee), or through the finding of a doubly used password and then used on the website [1]. It is also possible that the password to the account was guessed, but it is almost impossible to determine the exact way in which the hackers found the way into the account with so many options.

Normally just entering an account would not be a problem, but the VPN for which the account was connected to did not have multi-factor authentication, meaning that as soon as they got in there was no holding back. The password and username were all that was needed. After entering the account, and therefore having full access to the VPN, the hackers were able to access the entire network of Colonial Pipeline Co. It is not known yet whether any back doors were left, but the network damages seemed to have been kept to a minimal amount. The team who looked into the attack installed “alarms” so that if the hackers reached certain points in the network from now on without the correct permissions the company would be notified rather than allowing the hackers to have free reign over the network. This is illustrated in Figure 1 and will be discussed further in Attack Methodology.

The Colonial Pipeline fell under the category of “Critical Infrastructure vulnerable to attack” which detailed that should the pipeline ever become compromised that it could be shut down “for days to weeks”. While the East Coast certainly saw a gasoline shortage for a couple of weeks, however, a bigger discussion is being held on how the government involves itself in the protection of assets that it deems as ‘Critical Infrastructure’. Furthermore, because Infrastructure is no longer protected by the traditional borders as was the case in the past, another discussion has yet to be held on how private IT and OT may have a role to play in the National Security Systems [2].

The systems to defend such assets exist, but the synergy of assets is not being utilized to the extent that they could be. For instance, legislation has been proposed that would bolster CISA’s involvement in the defense of critical infrastructure and how it detects and mitigates said threats. Furthermore, changes have been proposed to CISA’s model of approach by potentially making it more team-oriented to defend America’s infrastructure from within. Lastly, the establishment of the Cyber Safety Review Board would document and review lessons learned from cybersecurity incidents [3].

The Colonial Pipeline Hack was a wakeup call to the concerned authorities and vulnerabilities that exist within our infrastructure. The intrusion tactics utilized by Darkside could have been easily prevented, but the preventative measures were not put in place and the consequences were predictable. The East Coast suffered a temporary shortage of gasoline and Darkside got their ransome, but the real implications involved

979-8-3503-0208-0/23/$31.00 ©2023 IEEE
DOI 10.1109/CCGridW59191.2023.00017

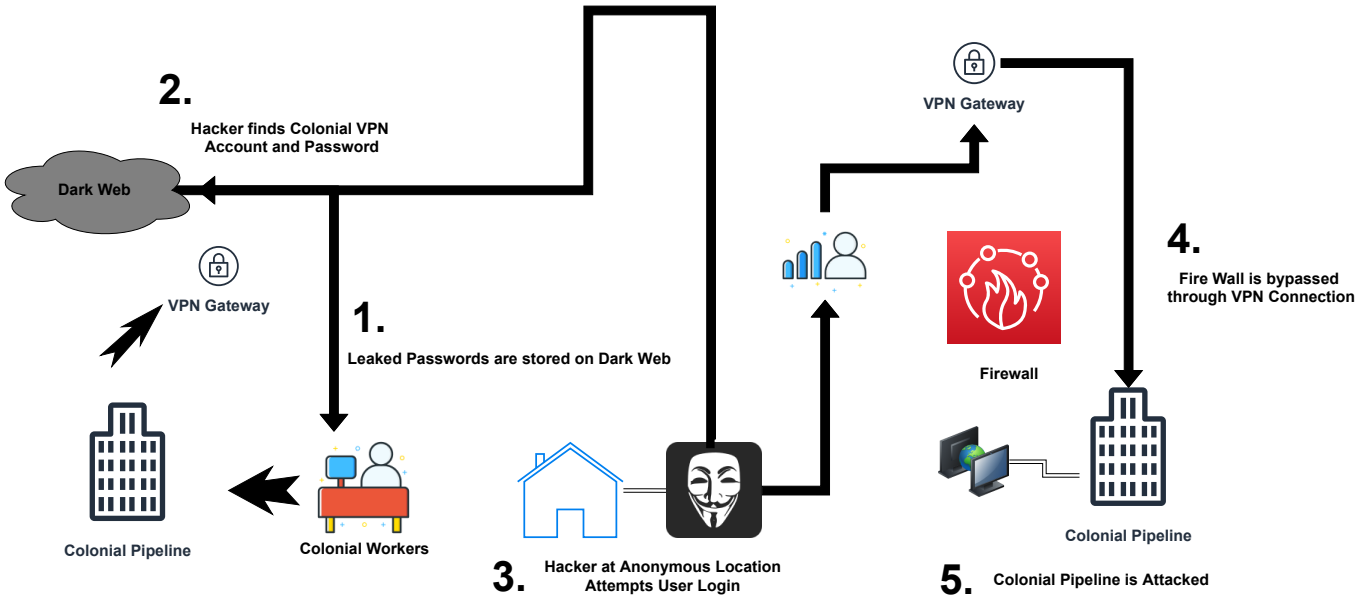

Fig. 1: Process of Access to Colonial Pipeline Infrastructure

what the cybersecurity vulnerabilities might entail for other aspects of the United States Critical Infrastructure. However, there's no better time to plan for future attacks than the present, as long as those plans are executed as well. The promise of proposed changes gives hope that we'll be able to turn the threat of cyberattacks around on those who perpetuate them.

As you read through section II, we illustrate the information regarding the extent of the Colonial Pipeline as a company and an introduction to the hacker group Darkside in the Background. Section III transitions to the Attack Methodology. This section details how the actual hack took place, an in depth look into what methods were used in entering the networks, and the timelines involved. After reviewing the attack, the section IV details the implications of the Attack and summarizes these in Impact.These are direct results in relation to the failure of security on the Colonial Pipeline network. We then propose potential remedies in the section V. The paper depicts proposed ways in which this incident could have been prevented, or future events may be prevented. Lastly, we summarize our work in the section VI and detail drawn out thoughts on how the Colonial Pipeline attack has affected both the company and the world, and a brief touch on all previous topics. Furthermore, we detail possible work for the future. .

II. Background

Before diving into the attack methodology, in this section, we provide a brief background of the Colonial Pipeline's history, the importance of the Colonial Pipeline in the East Coast region, and a simplistic overview of how the pipeline was attacked. Furthermore, we will discuss how the Colonial Pipeline is structured along the East Coast to help convey the extensive impact of the cyber attack. Lastly, we will go into detail as to who DarkSide is, when their cyber activities were first noticed, and how they operate as an organization.

A. History of Colonial Pipeline

The Colonial Pipeline is a major mover of gasoline, diesel, and jet fuel throughout the eastern seaboard [4]. The pipeline starts in Houston, Texas by the Gulf Coast and travels along the eastern seaboard to go as far north as Linden, New Jersey. The Colonial Pipeline, initially called the Suwannee Pipeline Company, was started in 1961 by eight major oil companies for the purpose of building a refined products pipeline from the Gulf Coast to the East Coast. In 1962, the pipeline was renamed to the Colonial Pipeline as we know today, and construction began with the addition of Mobil as the ninth owner of the pipeline. Two years after construction began the construction of the pipeline was completed. In 1967, the Colonial Pipeline underwent a major expansion to increase capacity to 1 million barrels/day. In 1972, the looping project increased the Pipeline's capacity to 1.6 million barrels/day. Today, the Colonial Pipeline is owned by six companies: Kock Industries, South Korea National Pension Service and KKR through Keats Pipeline Investors, Caisse de depot et placement de Quebec (CDPQ), Shell Pipeline, and Industry Funds Management. Currently, the pipeline transports 3 million barrels/day [5].

B. Design of Physical Pipeline

Currently the Colonial Pipeline is composed of 4 main lines (Figure 3):

- **Line 1 -** A 40 inch line moving 1.5 million barrels/day of gasoline from Houston to Greensboro, NC
- **Line 2 -** A 36 inch line moving 1.2 million barrels/day of middle distillates (diesel, heating oil, jet fuel) from Houston to Greensboro, NC

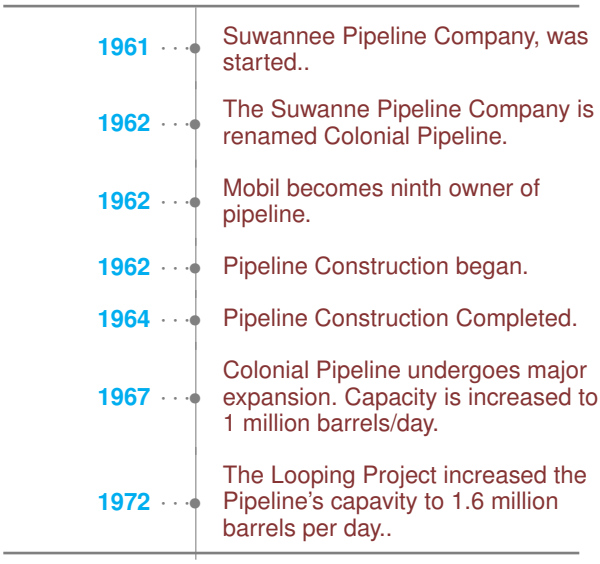

Fig. 2: Background History of Colonial Pipeline.

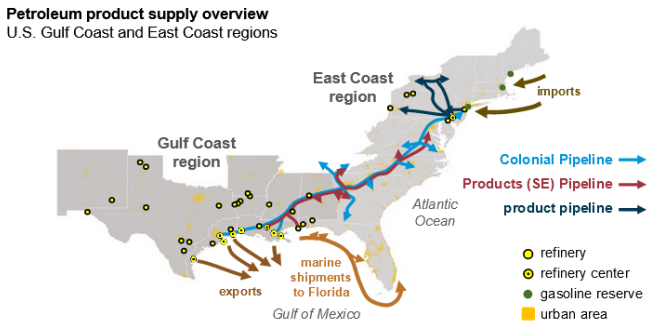

Fig. 3: Gas Lines of Colonial Pipeline

- **Line 3 -**An 885 thousand barrels/day line moving all products (gasoline, diesel, heating oil, jet fuel) from Greensboro, NC to Linden, NJ
- **Line 4 -**A 32 inch line moving 700 thousand barrels/day from Greensboro, NC to Baltimore

In addition to the main lines there are major spurs that branch off to more inland parts of the United States near the eastern seaboard. These major spurs include:

- Atlanta to Southern Georgia
- Atlanta to Tennessee (Chattanooga, Nashville, Knoxville)
- Greensboro to Raleigh/Durham, NC
- Mitchell (central Virginia) to Richmond, Norfolk, and Roanoke

Furthering the Colonial Pipeline's reach and partial control of the fuel supply, the Colonial Pipeline is also connected to a number of other pipelines located in the Northeast:

- **Laurel pipeline (Buckeye) -** Connects in Philadelphia and moves product west through Pennsylvania to Pittsburgh
- **IHT -** Connects in Linden and moves product across the surrounding New York and New Jersey area

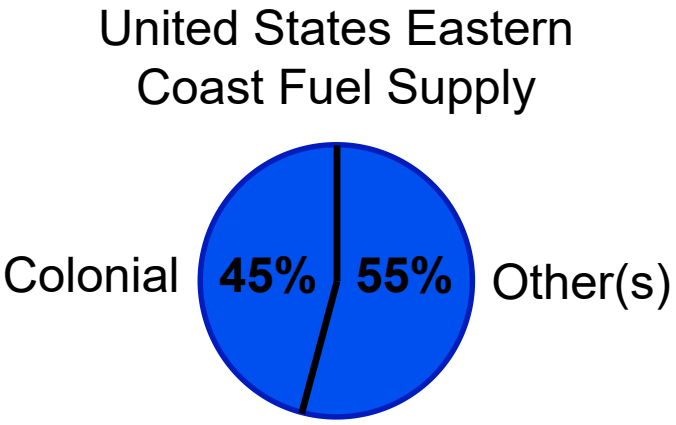

Fig. 4: Colonial Pipeline Gas Percentage

- **Long Island pipeline (Buckeye) -** Connects in Linden and moves product across Long Island
- **Buckeye East System -** Connects in Linden and moves product west to Eastern Pennsylvania, where there is a connection to the Laurel pipeline and lines moving north into Northeastern Pennsylvania and upstate New York [6]

When taking into account the Colonial Pipeline's reach along the eastern seaboard, it should come as no surprise that the pipeline controls 45% of the fuel supplied to the East Coast as depicted in Figure 4. It is due to its large share of fuel control within the region that made the Colonial Pipeline a critical target to the hacker group DarkSide to use the pipeline as a hostage. DarkSide was able to infiltrate the Information Technology network and make-off with 100 gigabytes of data, but there was no any indication that DarkSide was able to gain access to the Operational Technology Systems, which controls the flow of gasoline and gas related products through the pipeline.

C. Ransomware group DarkSide

DarkSide is a relatively new hacker group that has been hacking U.S. and European companies since August of 2020. According to a Boston-based cybersecurity firm, Cybereason, DarkSide follows a "ransomware-as-a-service" model, where DarkSide develops and sells the ransomware for other cyber actors to use [7]. Other analysts have compared DarkSide's ransomware model to "franchising", where those who buy and use the ransomware can use DarkSide's name in association with their attack [8]. It has been noted that DarkSide runs a somewhat professional operation where they have a press room, mailing list, and even a hotline for their victims listed on their website. Also published on DarkSide's website, they have their code of ethics open to the public, which states that they "will never attack hospitals, schools, universities, non-profit organizations, and government agencies" [7]. In regards to the Colonial Pipeline hack, New York City-based cyber intelligence firm, Flashpoint, assessed the hack and concluded with a moderate-strong degree of confidence that the cyber attack was not intended to cause damage to the nation's

infrastructure, but rather to extort payment from an entity who could afford to pay a large sum [9]. DarkSide likes to act as a 'Robin Hood' entity where a portion of their extorted money is donated to charities of their choice. Analysts are stumped by DarkSide's charitable giving and what their intended end-game is for doing so [10]. It should be noted that DarkSide only targets English speaking countries while avoiding former Soviet countries.

III. Attack Methodology

In this section, we will touch on typical hacker activity with the five basic steps most hackers utilize when performing an attack. In addition, we will discuss how DarkSide hacked the Colonial Pipeline, what they were able to access, and how the Colonial Pipeline company responded when they found out. Lastly, we will discuss what the U.S. government did to help the situation.

A. Chronological steps of the attack

The basic steps of hacking are [11]:

1) Reconnaissance
2) Scanning
3) Gaining Access
4) Maintaining Access
5) Clear Tracks/Leave Back Doors

The hacker group most likely started with reconnaissance into how secure the systems were on the Colonial Pipeline network. Simply by monitoring the employee list of Colonial Pipeline on LinkedIn may have lead to them seeing that an employee was going to no longer be with the company. After scanning ports and figuring out the account that would be vulnerable, the question was just finding the password to login.

After the employee's retirement the group DarkSide simply acquired the password to the VPN account that was no longer in use by anyone, but still had access to the VPN network [12]. The investigation as to how the password knowledge came out is still ongoing and nothing has officially been released on how this information was obtained by anyone outside of the company. Some theories are a key-logger, disgruntled employee, or an actual login check into the account. Whichever one it was, the password ended up with others in a leaked password batch on the dark web [13].

B. DarkSide access through VPN

The hacker group obtained the leaked password from the dark web, and gained access. From entering into the account, although they may not have known it previously, once in, they had access to the entire network. The earliest found tampering on the network was found to be on April 29, but access to the account could have come much earlier than that, allowing for lots of planning from DarkSide [14]. Since there was no two-factor authentication, they were immediately able to access the Colonial Pipeline network. VPN services are perfect for blocking unwanted access, however they have a fatal flaw, once into the VPN there is no stopping the amount of access someone has.

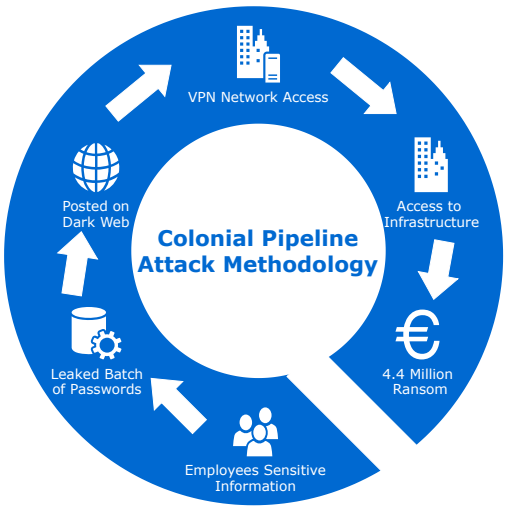

Fig. 5: Attack Methodology

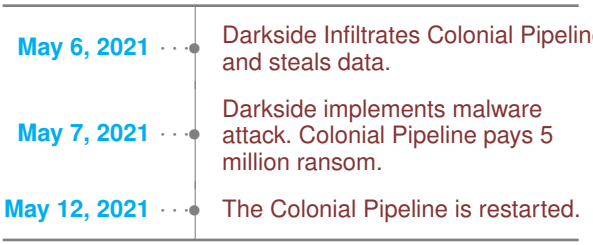

Fig. 6: Attack Timeline

As shown in Figure 5 after access into the VPN network was granted they were able to perform a chained attack on all infrastructure within the network. It is thought that after access to infrastructure was granted the hackers chose to bide their time and wait, or the step of maintaining access. The presence of the hacker group was not noticed for the week they were hacked into the network, leading to them being able to acquire everything they wanted to. Finally, on May 7 at 5 a.m., DarkSide left a ransom note on one of the computer screens, and was found by an employee [14]. In just one hour the whole pipeline and associated network were shut down.

C. Ransom Request

The hacker group, on the ransom note, demanded a payment of 4.4 million dollars to release the network from their grasp [15]. Additionally they stole over 100 gigabytes of data while remaining stagnant in the network, for the one week they were inside, and threatened to leak that if the payment total was not met. Once the payment went through DarkSide released their hold and threat on the company, but most likely still have the stolen information. Upon exiting the network, they cleaned shop and it is still not known the exact methodologies of data collection, and network trafficking used by the group, they they successfully covered all their tracks.

The effectiveness of this methodology is proven through the payment that went all the way through to the DarkSide group.

In almost every case of cyber attacks it is not recommended to negotiate or concede, as it only promotes the behavior [16]. Although the company may have remained down for some small time longer, the money may not have been forced to be payed, and those responsible may have been found [17], [3]. The information that was stolen remains to be found, and could in the future be used again, in theory, to threaten the company. Since this point, Colonial Pipeline claims to have changed VPN services which should fix the first issue that the company had.

In total, DarkSide cost Colonial Pipeline company:

- 4.4 million dollars in ransom money
- Over 100 gigabytes of data breached
- Professional standing as a company
- Knowledge to other hacker groups that their network was vulnerable
- Millions in product that had to stop moving during shutdown

The Justice Department was able to seize $2.3 million from the group DarkSide after the seizure was authorized by the the Honorable Laurel Beeler, U.S. Magistrate Judge for the Northern District of California. The seizure of the cryptocurrency payment was carried out by the Special Prosecutions Section and Asset Forfeiture Unit of the U.S. Attorney's Office for the Northern District of California. [18]

These impacts will be elaborated on in the following section.

IV. Impact

Having discussed how DarkSide was able to hack the Colonial Pipeline, we will be discussing the ramifications of said hack in this section. Similar to other massive data breaches in the last couple of years, the attack on pipeline has havoc impact on the society [19]–[23]. As an overview, this section will describe what exactly happened as a result of the hack, the economic impact it had on American citizens, and concerns the U.S. military has moving forward.

A. Shutdown of Colonial Pipeline

The Attack Methodology described above and its implementation resulted in many ramifications for a multitude of parties such as the United States economy, and military [24]. These impacts are depicted in Fig. 7. First and foremost, the Colonial Pipeline Hack caused the shut down of the Colonial Pipeline for the first time in fifty-seven years.The attack did not directly shutdown the pipeline, but the attack forced the operator of the system to initiate a complete shutdown. The operator of the system took this action because of the uncertainty of what was comprised with the attack. The shutdown lasted for five days and operations did not return to normal for many days even after the pipeline was restarted. The Colonial Pipeline initiated a restart protocol on May 12, 2021 and stated that their delivery supply chain would slowly recover.

B. Economic Effect

As a result rippling effects were sent across the United States Economy. The Colonial Pipeline operates the largest gas system across North America and includes over 5,500 miles of pipelines in the United States. These pipelines are essential to supplying an estimated 100 million gallons of fuel a day and support nearly forty-five percent of the United State's Eastern Coast. In addition, the United States has seven airports that directly get their jet fuel from the Colonial Pipeline. When these pipelines were shutdown, many consumers suffered drastically. Consumers were unable to amass enough fuel for day to day operations. Gas prices slowly began to rise and creep closer to three dollars a gallon. Furthermore, it was reported that "80 percent of gas stations are without fuel, according to the latest data from GasBuddy. In North Carolina 63 percent of stations are short, in Georgia and South Carolina more than 40 percent, and in Virginia 38 percent." These percentages are illustrated in Fig. 8 The United States suddenly began to arrive at the realization that cyber attacks could have detrimental impacts.

In order to restart the pipeline, Joseph Blount, the CEO of Colonial Pipeline, decided to pay the Darkside hackers over 4.4 million dollars [25]. This amount was requested from the malicious group and in return the organization would regain access to the pipeline. Paying a ransom is an act that the Federal Bureau of Investigation has adamantly advised against. By controversially resolving the issue through payment, Joseph Blount stated, "I believe with all my heart it was the right choice to make... I believe that restoring critical infrastructure as quickly as possible, in this situation, was the right thing to do for the country..." [26]. These statements occurred while being scrutinized by numerous government officials in the United States Senate.

C. Military Concerns

Lastly, the United States government, United States military, businesses, and other countries are constantly learning from the attack on the Colonial Pipeline. In fact, this attack was referred to as "Cybersecurity's Pearl Harbor" [27] of modern day. In addition, in June of 2021, Jennifer Granholm, the United States' Energy Secretary admitted that cyber attacks have the full potential and capability to impact the United States' electricity grid [28]. In response, many organizations, the United States' government, and United States military are bolstering their defense systems and spreading awareness of cyber vulnerabilities. As the United States has recovered from the attack and other countries have watched their recovery, many malicious groups have continued to launch additional cyber attacks and increase their frequencies of attack. These attacks create the need for effective and efficient defense solutions as discussed in the following section.

V. Defense Solution

After examining how the attack occurred, there are methodologies that could have been utilized to prevent said attack. In this section, we will discuss the various technologies

Fig. 7: Impact of Colonial Pipeline Hack

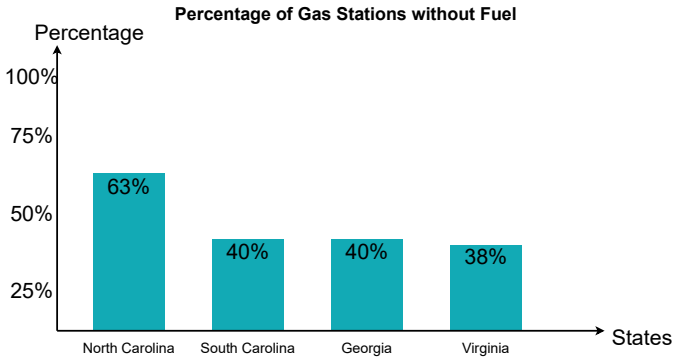

Fig. 8: Gas Stations Impacted by Attack

and techniques that can be used to prevent such an incident from happening again, such as, a 'Zero-trust' network model, Internal Review System, and Secure User Authentication.

The process by which DarkSide was able to infiltrate the Colonial Pipeline's Systems was not trivial and rather perplexing to many investigating the event. Virtual Private Networks are secure networks that cannot be broken up to having only the necessary access they need to the network. Either those who use a VPN on a network have complete access to the network, or they have none at all. A VPN's 'all-or-nothing' approach violates a recently enacted executive order meant to enhance government cybersecurity called the 'Zero Trust' model. The 'Zero Trust' model implements low-tiered privilege access/authentication to users where the user can only access the necessary hosts, ports, and applications designated. Furthermore, VPNs prevent organizations on the shared network to monitor and audit third-party vendor activity, meaning there is no log view of VPN sessions to see where certain issues may have arisen.

A. Resistant Internal Review System

To help alleviate these problems, a Internal Review System can be utilized to mitigate the risk of an inactive VPN account being used by an unspecified user, as was the case in this attack. How the internal review system works is an automated review system audits the access permissions of users and then flags unauthorized access of those marked users. The IRS helps to "provision or de-provision users who could be inactive, terminated from the organization or no longer in need of the system license." If the VPN that was used by the hackers had been flagged and de-provisioned based on its inactivity, then the hackers would not have been able to gain access to the system.

B. Secure User Authentication

Another solution that could have helped prevent the attack is the use of Multi-factor Authentication. Multi-factor authentication was listed in the previously mentioned executive order's list of mandates, but its effectiveness is still overlooked. Multi-factor authentication operates through a series a steps the user must take to authenticate that they are the appropriate user trying to access the designated private, and/or sensitive information. Typically, multi-factor authentication works in 3 steps:

1) Enter password into space provided
2) Receive a push notification or passcode to be externally verified
3) Enter choice to confirm or deny the push notification, or enter the passcode into the designated space

Most of the time, the push notification will be received via email from the entity that operates the multi-factor authentication. This helps tie the login attempt to the correct users, since

TABLE I: Proposed remedies

Internal Review System	Automated Audit System that checks for unauthorized access privileges of user accounts and provisions/de-provisions accounts accordingly
Multi-factor Authentication	User must authenticate that they are the authorized user of the space/information they are trying to access by entering a passcode or opening a push notification tied to the authorized user's email
Zero-Trust network model	Users are granted low-tier privileges with access to applications, hosts, and ports

only the user should have access to the designated passcode or email address to access the push notification.

C. Future Protection

In summary, to best protect against malicious activity as described in this paper is to:

- Implement a Zero-trust network model
- Perform a role based user access review
- Utilize practical security measures, such as: Use strong passwords, mandate multi-factor authentication, etc.

Other practical solutions involve backing up your data so that way a system can be restored if the information is compromised, such as the case with DarkSide. The Colonial Pipeline could have avoided paying the ransom if they had backed up their systems so that they could have restored their system [29].

Overall, these defense remedies could have potentially prevented the attack on the Colonial Pipeline. The business would have saved itself from paying a ransom to DarkSide and the economy would not have suffered. It is vital that organizations, governments, and device users understand the implications of unsecure software/hardware and defend their devices accordingly.

VI. Conclusion

Cyber threats continue to advance each year with new exploits being tried and tested at exponential rates. However, the real test will not be how to defend against these new attacks but rather how to respond. whether intentional or not, the current message that's understood within the hacking community is that companies will pay any ransom to free their networks from being held hostage. Although Colonial Pipeline paid the ransom to limit their losses and free up the pipeline, they may have enabled future cyber actors to take their chance at halting operations in the hopes of being paid as well. With hacker groups now expecting a payout by holding networks and operational systems hostage, it might become commonplace for these types of attacks to occur more frequently. However, just because hacking attempts may become more frequent does not mean that vulnerable and critical companies will just wait around to be hacked, but rather invest in their own network infrastructure. The Colonial Pipeline hack was the alarm bell sounding off for companies that control other aspects of critical infrastructure to examine their own network security practices and policies to make the necessary proactive changes that prevent cyber actors from wreaking havoc.

References

[1] W. Turton and K. Mehrotra, "Hackers Breached Colonial Pipeline Using Compromised Password." https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

[2] P. Parfomak, "Colonial Pipeline: The Darkside Strikes." https://crsreports.congress.gov/product/pdf/IN/IN11667.

[3] J. Monken, "THE COLONIAL PIPELINE HACK SHOWS WE NEED A BETTER FEDERAL CYBERSECURITY ECOSYSTEM." https://mwi.usma.edu/the-colonial-pipeline-hack-shows-we-need-a-better-federal-cybersecurity-ecosystem/.

[4] P. Coy, "Here's How the Colonial Pipeline Carries Multiple Fuels at Once." https://www.bloomberg.com/news/articles/2021-05-12/here-s-how-the-colonial-pipeline-carries-multiple-fuels-at-once.

[5] J. Panettieri, "Colonial Pipeline Ransomware Attack: Timeline and Status Updates." https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/.

[6] "Colonial Pipeline." https://www.mckinseyenergyinsights.com/resources/refinery-reference-desk/colonial-pipeline/.

[7] E. Palmer, "What is DarkSide?." https://www.newsweek.com/darkside-hacker-group-russia-colonial-pipeline-1590352/.

[8] E. DeCiccio, "Hacker group DarkSide operates in a similar way to a franchise." https://www.cnbc.com/2021/06/02/hacker-group-darksides-operates-in-a-similar-way-to-a-franchise-new-york-times-reporter-says.html/.

[9] "A closer look at the DarkSide ransomware gang." https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/.

[10] J. Tidy, "Mysterious 'Robin Hood' hackers donating stolen money." https://www.bbc.com/news/technology-54591761/.

[11] A. Sahni, "5 Phases of Hacking." https://www.geeksforgeeks.org/5-phases-hacking/.

[12] CyberTalk.org, "Colonial Pipeline Co. attack: What really happened. . . ." https://www.cybertalk.org/2021/06/09/colonial-pipeline-co-attack-what-really-happened/.

[13] "Back to Basics: A Deeper Look at the Colonial Pipeline Hack." https://www.govtech.com/sponsored/back-to-basics-a-deeper-look-at-the-colonial-pipeline-hack.

[14] W. S. Journal, "Colonial Pipeline Hack Sparks Questions About Oversight." https://www.aesolutions.com/post/colonial-pipeline-hack-sparks-questions-about-oversight?_vsrefdom=adwords&gclid=Cj0KCQjwkbuKBhDRARIsAALysV6fn3f3dtNBb3SYX_fPF-l_DpU1s0PQqCMDTZZDJSka4Mi_W1GmfE8aAvXGEALw_wcB.

[15] D. G. R Dudley, "The Colonial pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms." /.

[16] R. Martin, "'You Can't Just Concede.' How One Expert Explains Negotiating With Cybercriminals." https://www.npr.org/2021/05/18/997549334/you-cant-just-concede-how-one-expert-explains-negotiating-with-cybercriminals.

[17] C. S. B Fung, "What it's really like to negotiate with ransomware attackers." https://www.cnn.com/2021/07/13/tech/ransomware-negotiations/index.html.

[18] P. A. Office, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside." https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[19] M. H. Nguyen Ba, J. Bennett, M. Gallagher, and S. Bhunia, "A Case Study of Credential Stuffing Attack: Canva Data Breach," in *International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021.

[20] L. Sterle and S. Bhunia, "On SolarWinds Orion Platform Security Breach," in *2021 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, 2021.

[21] J. Huddleston, P. Ji, S. Bhunia, and C. Joel, "How VMware Exploits Contributed to SolarWinds Supply-chain Attack," in *International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021.
[22] B. Gibson, D. Lewis, S. Townes, and S. Bhunia, "Vulnerability in Massive API Scraping: 2021 LinkedIn Data Breach," in *International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021.
[23] J. Rudie, Z. Katz, S. Kuhbander, and S. Bhunia, "Technical analysis of the nso group's pegasus spyware," in *International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021.
[24] C. M. Holdridge, "Leveraging Cyberspace." https://mca-marines.org/wp-content/uploads/Leveraging-Cyberspace.pdf.
[25] J. Ainsley and K. Collier, "Colonial Pipeline paid ransomware hackers 5 million, U.S. official says." https://www.nbcnews.com/tech/security/colonial-pipeline-paid-ransomware-hackers-5-million-u-s-official-n1267286.
[26] C. Eaton and D. Volz, "Colonial Pipeline CEO Tells Why He Paid Hackers a 4.4 Million Ransom." https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636.
[27] J. R. Reeder, "Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack." https://www.gtlaw.com/-/media/files/insights/published-articles/2021/08/cybersecuritys-pearl-harbor-moment.pdf.
[28] D. C. Smith, "Cybersecurity in the energy sector: are we really prepared?." https://doi.org/10.1080/02646811.2021.1943935.
[29] S. Clarke, "Lessons Learned from the Colonial Pipelines Cyber Attack: What You Need to Know." https://www.menark.com/lessons-learned-from-the-colonial-pipelines-cyber-attack/.