
# CS571 Team Project
# Colonial Pipeline Hack Report

## Team Members:

Humberto Martínez

Justin Cabral

Jonathan Duran

Shary Llanos Antonio

March 23, 2022

# Table of Contents

# Executive Summary

On May 7th, 2021, the Colonial Pipeline Company discovered they had become a victim of Darkside ransomware. The Darkside group was a notorious hacking group known for developing sophisticated ransomware and they had targeted and compromised the networks of the Colonial Pipeline Company. The Darkside group exploited vulnerabilities in the company's legacy Virtual Private Network (VPN) and installed their ransomware on their network, causing a proactive shutdown of OT systems. The result was a complete shutdown of the pipeline and over 11,000 gas stations lacking supply to meet demand.

The case study is significant as it is a ransomware attack on critical infrastructure to the United States. The resulting gasoline shortages and impact on U.S. citizens allows us to investigate the security practices of private companies like the Colonial Pipeline Company, and how its role in the infrastructure of the United States affect their security standards.

The technical concerns for this incident include sophisticated ransomware developed by a group notorious for targeting high value organizations, and an outdated and compromised legacy VPN account that was still useable. The human behaviors that contributed to this incident involve the Darkside group officially announcing their intention to target high value companies with the means to pay off large ransom amounts and a US economy recovering from a recession and global pandemic, creating an environment for cybercrime to have a greater impact. The business decisions that had a significant impact on this incident include inadequate funding for IT security, delayed retirement of a legacy VPN to a new modern one, and use of a VPN without multi-factor authentication.

Insights from this case led to better understanding of the importance of maintaining and establishing better security defense measures to protect against intrusions and breaches. NIST (National Institute of Standards and Technology) has since published a risk management framework for organizations and critical infrastructure companies that helps them deal with and mitigating against ransomware attacks.[22]

Some lessons learned from this incident include, organizations must require better governance of user accounts, any accounts no longer in use should be disabled in a timely manner. All VPNs used by organizations should employ some form of additional factor authorization to access the network, simple username and password authorization opens an organization up to many vulnerabilities. Organizations should work to better segregate IT and OT networks in the event one comes under attack, this will increase chances services can remain operational and risk remains segregated. Better methods to monitor networks and detect breaches and intrusions should be implemented, the faster threats can be identified can result in faster response and minimized impact from attacks.

# Introduction

## Target of Attack

Colonial Pipeline, the major refined products pipeline in the United States, moving daily more than 100 million gallons of fuel (gasoline, diesel, and jet fuel) from Houston, Texas, to the New York Harbor [1]. The attacker was the Darkside group, which developed ransomware-as-a-service (RaaS) and received a share of the proceeds.[3][4]

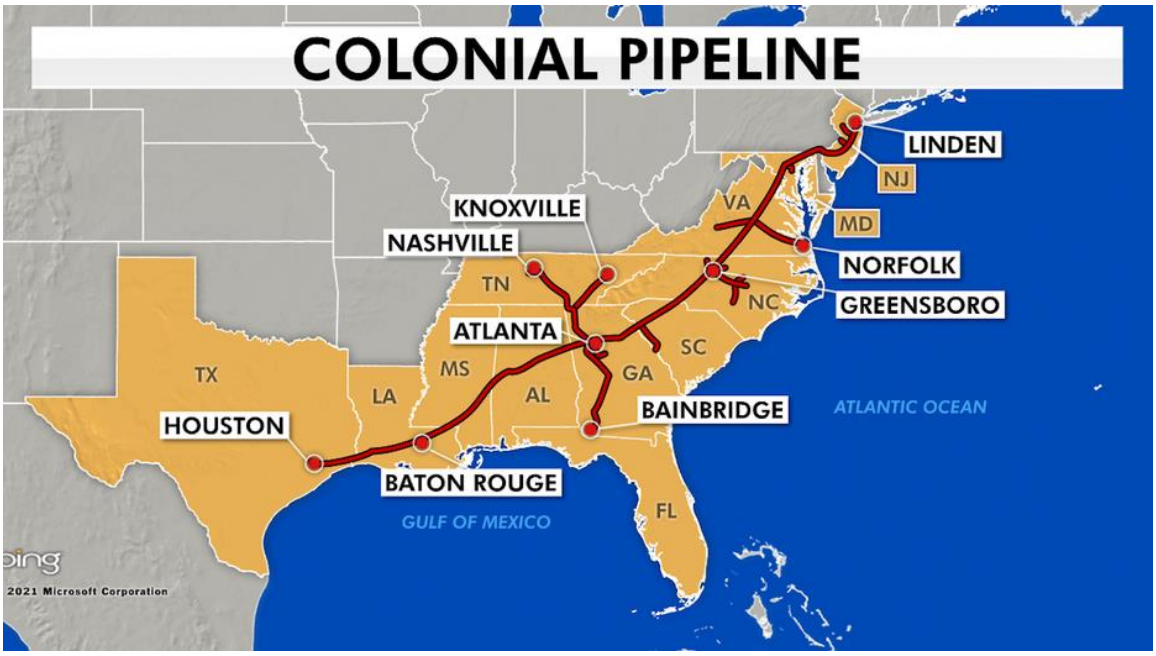


Figure 1. Colonial Pipeline system goes from Houston, Texas, to the Southeastern United States. Image taken from BING Images

## Timeline

*Table 1* summarizes the timeline for the Colonial Pipeline hack. Between May 7 and May 12, 2021. On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack, and on May 13, they safely restarted the entire pipeline.[2] Colonial paid $4.4 million in ransom just after the attack. Regardless, due to the slow decryption rate and integrity verification of the rest of its IT components. Colonial did not begin restarting the system until five days later, Wednesday, May 12, 2021. [4] On June 7, The DOJ seized $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside. [6]

| Activity | Dates | Description |
|---|---|---|
| Attack | May 7 | DarkSide Ransomware |
| Discovery | May 7 | 5:30 am – Ransomware note on employee computer |
| Payment | May 8 | 75 Bitcoins totaling around $4.4 million |
| Decryption | May 8-11 | Using Dark Side's decryption software after payment was too slow, forcing a resort to backup systems to restore service. |
| Restart of operations | May 12 | Restarted pipeline operations at around 5:00pm ET. |
| Seized partial payment | June 7 | Department of Justice Ransomware and Digital Extortion Task Group successfully recovered around 64 of the 75 bitcoins that were paid to the hackers. |

*Table 1: Timeline for the Colonial Pipeline Cyber Attack*

## Summary of Incident and Impact

Due to the use of a legacy VPN without two-factor authentication, the hackers were able to access the Colonial Pipeline network and deploy the Darkside ransomware, causing the proactive

shutdown of certain OT systems.[7][2] The shutdown affected more than 5,500 miles of refined oil pipeline between Texas and New York.[8] Various gas stations in affected states were unable to meet demand, with around sixteen thousand stations having no gasoline to sell.[5]

Following the hackers being paid 75 bitcoins, they sent the decryption software to Colonial Pipeline company. Due to the slow speed of the decryption software, the company used its own backups of the stolen data to restore service.[8] The pipeline was operational five days following the discovery of the ransomware. [2] In an effort by the department of justice to recover the paid ransom, the FBI was able to obtain the private key to the crypto wallet that stored the ransom payment. With this private key they were able to recover around 64 bitcoins of the 75 paid, which amounted to around $2.3 million dollars.[6]

### Case Study Significance

The Colonial Pipeline case is significant as a ransomware attack on the critical infrastructure of the United States. It raises technical concerns about cybersecurity hygiene, as the attackers used a leaked password to access their network through a legacy VPN system that did not have multi-factor authentication implemented [7].

Additionally, it allows us to analyze how the private/public partnership between the federal government and private companies affects their security practices. Furthermore, it lets us see if the federal government holds high-security standards for the private companies that it depends on to distribute energy around the country.

## Method of Attack

### How Attack Occurred

Hackers gained entry to the company's networks on **April 29, 2021**, by exploiting a Virtual Private Network (VPN) account that was no longer in use but still active to access the company's network. A cybersecurity expert hired by Colonial Pipeline, Charles Carmarkal, stated that they did not find “evidence of phishing for the employee whose credentials were used” nor other evidence of “attacker activity before April 29” [10].

Colonial Pipeline Co. first learned about the cybersecurity attack on **May 7, 2021**. They brought on a third-party cybersecurity firm, launched an investigation, and contacted law enforcement and other federal agencies. Once they determined it was a ransomware attack, they proactively took certain systems offline to contain the threat, halting all pipeline operations [2].

On Saturday, **May 8, 2021**, the victim reported the attack, which took down a major fuel pipeline in the country and led to shortages across the East Coast.

Colonial Pipeline Chief Executive Joseph Blount said to Reuters that the hack used a legacy VPN system that lacked multifactor authentication. Meaning hackers could access it with just the password alone, with no need for a second step like a text message, a standard security feature in newer software. Blount said. "It was a complicated password; I want to be clear on that. It was not a Colonial123-type password." [7]

Moreover, the password was later discovered in a dark web batch of leaked passwords. This might indicate that a Colonial Pipeline employee has used the same password on another previously hacked account. However, it is not certain that is how hackers obtained the password, and investigators may never know for sure how it was obtained. [10]

Colonial's CEO Joseph Blount also said in an interview that early (5 am), on May 7, a Colonial Pipeline's control room employee saw a ransom note requiring cryptocurrency appear on a computer. An operations supervisor was notified and immediately started shutting down the pipeline. By 6:10 am, the entire pipeline was shut down, Blount said. The first time in its 57-year history. [10] (See Fig. 1 for a representation of how the attack occurred)

Colonial Pipeline paid the ransomware (4.4 million dollars) in cryptocurrency. [17] Then the hackers provided a decrypting tool, but it was too slow, so the company used their own backups to restore the system. [10]

On **May 12**, **2021**, the Colonial Pipeline was back up and running within a few days, but not before over 11,000 gas stations closed due to fuel shortages. The Pipeline, which goes from Texas to New Jersey, carries up to 45 percent of the East Coast's gas. And while stalls and slow-downs in delivery contributed to shortages, consumer "panic-buying" played a major part in the scarcity of gas. [11]

On Monday, June 7, 2021, the Justice Department recovered 60 of the 75 bitcoins paid in ransom by Colonial Pipeline. As the value of the cryptocurrency had dropped between when Colonial Pipeline paid and when the government recovered it, the total amount in dollars fell short of what the company’s initial paid. The reported amount recovered in dollars was $2.3 million dollars [7].

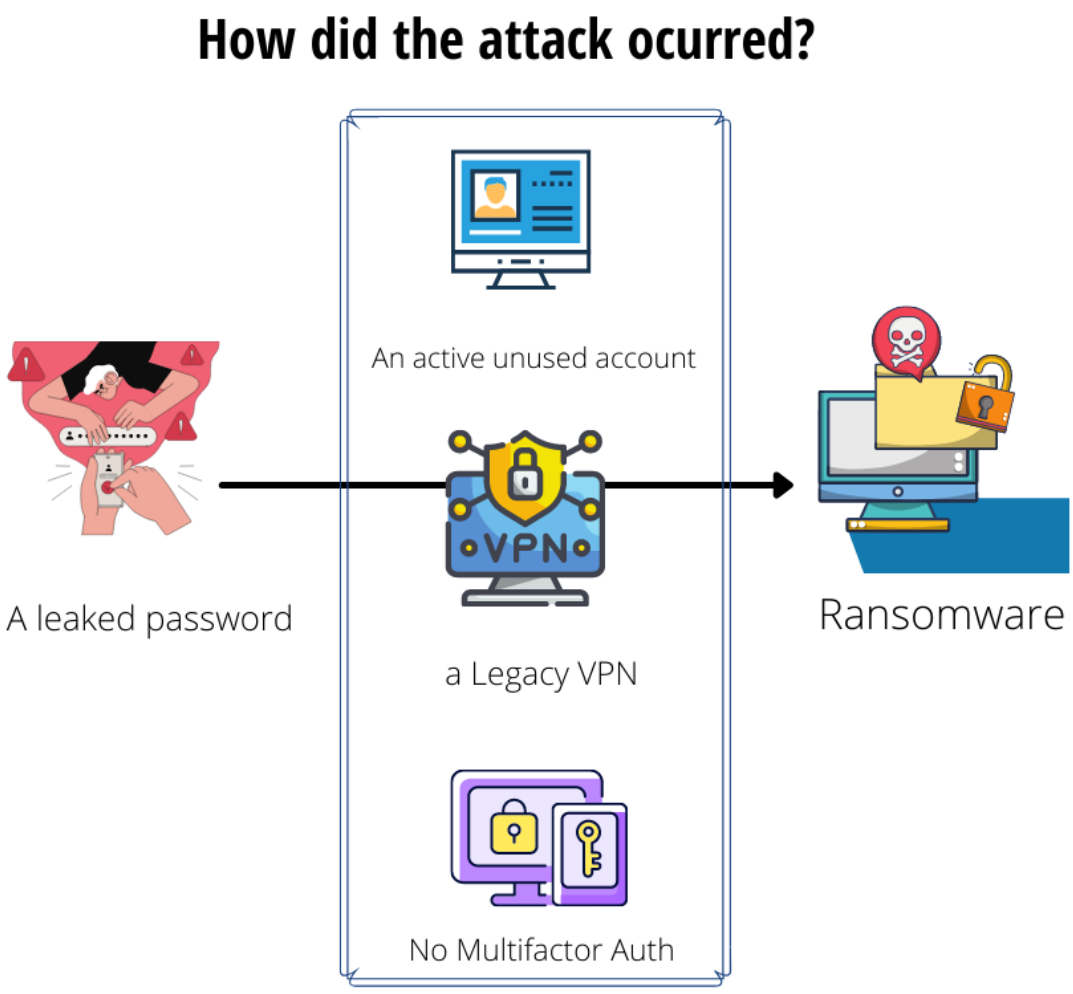


Figure 2. Represents how the attack occurred.

## Vulnerabilities Exploited

The hackers exploited the following vulnerabilities

- Legacy Virtual Private Network
- Lack of Multi-Factor Authentication for VPN
- VPN account with leaked credentials available on dark web

The Darkside hacker group used an account with access to the company's VPN to install ransomware. The account was no longer in use by an employee at the Colonial Pipeline, but the account still had access to the company's VPN. The account's password was later found on the dark web. [11]

The primary vulnerability exploited was the lack of Multi-Factor Authentication. Without MFA implemented, any other accounts with access to the VPN could have been exploited to carry out the same attack. Use of MFA for accessing networks remotely is essential, as without MFA any

actor with the password to an account can access the network from anywhere undeterred. If MFA had been implemented, the leaked password would have lost a lot of utility, as any hacker trying to access the network would have needed an additional factor to gain access.

The security firm Mandiant concluded that there was no evidence of phishing for the employee's password. The employee's password was found on the dark web following the attack. Mandiant believes one possibility is the employee used the same password for various accounts and had been previously hacked in a separate occasion. [11]

# Incident Contributors

## Technical Concerns

The technical concerns contributing to this incident include:

- The Darkside group had installed their custom ransomware software inside the Colonial Pipeline's information technology internal system.
- The attackers gained access to the Pipelines network through a vulnerable and compromised VPN account that was not being actively used or maintained.

The Darkside group had been notorious for developing sophisticated ransomware that they sold to other organized cyber criminals and benefited financially from any successful use of the malware. This group knew how to effectively exploit and install ransomware on systems, which aided in their attack on this high-level target.[11]

This group of attackers had a history of exploiting organizations, systems, and networks through mostly remote system vulnerabilities. In this case they had gained access by compromising a VPN account that was not being used or handled by the target company. They had extensive knowledge and expertise in this form of exploitation, and they used a familiar vector of attack to breach the pipeline's company IT network. [11][3]

## Human Behavior

The human behaviors contributing to this incident include:

- The attackers had previously announced their attraction and preference to target higher value organizations and companies that have the resources to pay larger sums of money.
- The US economy was amid recovering from a recession and a global pandemic, which created a vulnerable environment for organized cybercrime to have a greater impact on the US infrastructure and organizations that manage it.

In terms of human behavior, the fact that this group had a tendency and inclination towards attacking organizations that had greater levels of financial wealth meant a pipeline company such as the Colonial Pipeline company, that controlled one of six major pipelines in the US had a higher probability of being selected for an attack.[5]

The US economy in general was still in a delicate state during the earlier parts of 2021, which had fostered conditions that would cause attacks on critical infrastructure to be seen as more catastrophic and harming then during other stable periods. The country was preparing for an

increase in drivers as the summer months were approaching and COVID restrictions were beginning to loosen, this meant that any disruption to gasoline and oil production would cause social panic and concern to its potential availability.[3]

## Business Decisions

The business decisions contributing to this incident include:

- Underfunded cyber security policies for an I.T. department of $200 million
- Lagged on updating from a legacy VPN system to a modern one
- Lack of multi-factor authentication enforcement

During the previous 5 years before the pipeline cyber-attack, Colonial invested over $200 million dollars in its IT systems. However, when pressed by a congressional panel about its cyber security budget, the CEO repeated the amount of total investment, not the exact amount dedicated to cyber security. Since the company did not allocate an accounted budget directly to cyber security, he was not obligated to report a number to congress.[18] This type of accounting trick shows how the business decision of underfunding cyber security policies was kept in place. The CEO is allowed to point to their overall investment in IT systems as continued progress in the safety of its technology, but really, it is used as a shield to hide behind.

Another significant contributor to the incident was the business decision to be behind the rest of the industry on adopting a modern VPN system which included multi-factor authentication, which could have prevented the attack. Modern VPN systems use multi-factor authentication which requires more than just a password to log into an account. [19] The legacy VPN system in use by Colonial Pipeline was one that was ripe for exploitation when the Covid-19 pandemic hit, because it meant more of their top employees would be working remotely. There should have been a greater emphasis on updating legacy systems but due to the underfunding of cyber security policies discussed earlier, they were unable to defend against this type of attack.

The business decisions that lead to the attack speak to monetary negligence on behalf of Colonial Pipeline when it comes to funding the correct cyber security policies. If proper policies were in place, this entire attack may have been avoided.

## Most Significant Contributor

While all the factors discussed previously have contributed to the attack, the most significant contributor to this incident was the business decisions. For a company with a net worth that was estimated to be $100 billion dollars, it significantly underfunded its IT systems' cyber security policies. This company manages and operates a vital part of the United States critical infrastructure, there should have been a greater deal of emphasis placed on updating cyber security policies for the modern working environment.[20] Covid-19 caused the U.S (United States). workforce to shift from a more in-person work environment to an environment that allowed a lot of position to be remote or online, and knowing this, they intentionally chose not to spend the funds needed to research and implement policies to update their systems. While most scrutiny should be placed at the feet of the Colonial Pipeline Company, we should

question ourselves if there should be a role for the government to play in ensuring its private infrastructure partners are held to a certain standard of cyber security.

# Case Study Conclusions

## Lessons Learned

The Colonial Pipeline cyberattack caused significant disruption to critical infrastructure in the United States. It demonstrated the importance of having a cybersecurity strategy with key partnerships and an effective incident response plan.

The following lessons learned represent recommendations that apply to the Colonial Pipeline organization and its systems:

- Require better IT governance of user accounts
- Require updated VPNs (Virtual Private Network) that use multi-factor authentication
- Establish greater segregation of OT and IT networks
- Establishing methods to monitor systems to detect and prevent intrusions and breaches
- The costs associated with a breach can be significant
- Once a breach has been successful many other types of attacks can follow

**Require better IT governance of user accounts:** The attack on the Colonial Pipeline was carried out using a legacy profile that was not intended to be in use. Not only was this account dormant, but the single username/password combination granted access to the operational part of the Colonial Pipeline network. The lesson learned here is that there must be formal, standard procedures for decommissioning user accounts no longer in active use.[21] Governance over user profiles should be required for a company with vital operational technologies such as Colonial Pipeline. With the amount of security gained from a small amount of effort, there is no excuse for why this should not be implemented.

**Require updated VPNs that use multi-factor authentication:** The virtual private network that Colonial Pipeline used did not require the use of multi-factor authorization. This meant that if an attacker gained access to a user/password combination from a data leak, there was no alternate way for the system to prove the authenticity of the user. The attacker's barrier to entry was much lower than it should have been. The lesson learned here is that for a company with the scale and responsibility that Colonial Pipeline has, it must be a requirement that all users must enable multi-factor authentication to access any of their OT or IT systems. With the federal government's dependence on private companies to supply critical services for the nation, this is something that should be required by law as well.

**Establish greater segregation of OT and IT networks:** The energy sector of the economy uses both operational technology and information technology networks to a great extent. As the interdependence between both continues to grow, the cyber risk will escalate as well. During this attack, Colonial shut down most of their operational systems because they did not know

who was attacking or what the motives could be. The lessons learned here is that the segregation of OT and IT networks can help contain risk. As integrations continue, it is essential for companies such as Colonial to build security and auditing into their infrastructure from day one.[21] This type of planning can significantly reduce the impact of an attack and help keep OT systems operational. Since an OT attack can put lives at risk, companies such as Colonial must do their best to always keep them operational.

**Establishing methods to monitor systems to detect and prevent intrusions and breaches:** In the days before the attack the attackers had gained access to the company's internal network, where they began to steal a vast amount of data. They also began prepping to execute their ransomware attack by beginning to encrypt many of the systems they had gained access to. If there tools in place to monitor unusual and suspicious behavior within the organization's network the attackers might have been discovered earlier in the attack process and may have not had the time to encrypt many of the essential systems that they did. Establishing these types of systems such as intrusion detection and prevention systems would give the potential victims of an attack, such as the colonial pipeline company, the ability to discover and defend against such incidents before many of the irreversible damage is done.[21]

**The costs associated with a breach can be significant:** The Colonial Pipeline company suffered huge financial and operational costs related to this attack. They gave into the attacker's demand to pay the ransom which amounted to 75 bitcoins, which were worth $4.4 million dollars. The FBI was able to recover a substantial portion of the bitcoins paid out, but by the time they had recovered them, the value of the coins had dropped drastically, thus the value of the recovered ransom was 2.3 million dollars. [21] Apart from the ransom costs, the company had to repair the damage that attackers had caused and restore their systems to restart business operations. Finally, the organization had now been infamously put into the spotlight and its reputation suffered from it.

**Once a breach has been successful many other types of attacks can follow:** As stated before the DarkSide group had been notorious for targeting larger corporations and using remote access tools and methods.[11] Once the public is made aware of successful attacks there may be others who wish to benefit from similar methods of attacks or may see the success of these attacks as a signal that the industry these companies are involved in have unsecure systems. After the attack on the Colonial Pipeline other organizations in the energy industry saw efforts to attack their systems as well.[21]

## Summary of Case Study

The 2021 Colonial Pipeline attack highlights the need for smarter business decisions and greater concern for cyber security practices. The attack was not overly sophisticated, as the group responsible for the attack, the Darkside group, merely took advantage of poor business decisions and practices by the Colonial Pipeline Company. The Darkside group used an account no longer in use by the company, but whose access to the company's Virtual Private Network was still valid,

and password available on the dark web. Without any multi-factor authentication policies in place, the network allowed the attackers unrestricted access. Once inside the network, the Darkside group were free to install their ransomware on Colonial Pipeline's data, grinding their operations to a halt once their attack was discovered on May 7th. Operations began again after six days once the Bitcoin ransom was paid, and the Colonial Pipeline Company restored their lost data. While the FBI was able to retrieve 64 of the 75 Bitcoin paid, the incident exposed the Colonial Pipeline Company's major security shortcomings. Their outdated and insecure VPN network was on full display. The attack highlighted the need for greater security measures, like Multi-Factor Authentication, and immediate revocation of access privileges to outdated accounts. Going forward, private companies, especially those doing business with the government, must recognize the need for stronger and more robust security policies. Higher standards, like mandatory MFA and segregated IT and OT networks, must be set for companies that operate vital infrastructure for the country.

**REFERENCES**

[1] About Us: Excellence in Everything We Do. Colpipe.com. (n.d.). Retrieved January 31, 2022, from https://www.colpipe.com/about-us

[2] Colonial Press Release. Colpipe.com. (2021, May 8). Retrieved January 31, 2022, from https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption

[3] Internet Crime Complaint Center (IC3). (2021, May 11). *Darkside Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*. [online] IC3.gov. Available at: https://www.ic3.gov/Media/News/2021/210520.pdf [Accessed 20 January 2022]

[4] FBI. (2021, May 10). *FBI statement on Compromise of Colonial Pipeline Networks.* [online]. Available at: https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks [Accessed 20 January 2022]

[5] Pyziur, M. and Pugliaresi, L., 2021. *Colonial Pipeline Hack Highlights - Growing Energy Security Risks - Infrastructure cyberattacks are a threat to national security*. Energy Policy Research Foundation, Inc. [online] eprinc.org Available at: https://eprinc.org/wp-content/uploads/2021/06/EPRINC-ColonialPipelineHack-Briefing-Version3-1.pdf [Accessed 31 January 2022].

[6] Department of Justice, Office of Public Affairs., 2021. *Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside*. [online] www.justice.gov Available at: https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside [Accessed 31 January 2022].

[7] Kelly, S., & Resnick-ault, J. (2021, June 8). *One password allowed hackers to disrupt colonial pipeline, CEO tells senators*. Reuters. [online]. Available at: from https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/ [Accessed 21 January 2022]

[8] Novison, M. (2021, May 13). *Colonial Pipeline Paid $5M To Darkside Hours After Attack: Report* [online]. Available at: https://www.crn.com/news/security/colonial-pipeline-paid-5m-to-darkside-hours-after-attack-report [Accessed 02 February 2022]

[9] Panettieri, J. (2021, June 7) *Colonial Pipeline Cyberattack: Timeline and Ransomware Attack Recovery Details.* [online]. Available at: https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/ [Accessed 10 February 2022]

[10] Turton, W. (2021, June 4) *Hackers breached Colonial Pipeline Using Compromised Password.* [online]. Available at: from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [Accessed 10 February 2022]

[11] Pedroja, C. (2021, June 4) *Colonial Pipeline Hackers Used Unprotected VPN to Access Network: Report*. [online]. Available at https://www.msn.com/en-us/news/us/colonial-pipeline-hackers-used-unprotected-vpn-to-access-network-report/ar-AAKIyfQ [Accessed 10 February 2022]

[12] Smith, M. and Monken, J., 2021. *The Colonial Pipeline Hack Shows We Need a Better Federal Cybersecurity Ecosystem - Modern War Institute*. [online] Modern War Institute. Available at: https://mwi.usma.edu/the-colonial-pipeline-hack-shows-we-need-a-better-federal-cybersecurity-ecosystem [Accessed 20 January 2022].

[13] Sanger, D. and Perlroth, N., 2021. *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity*. [online] Nytimes.com. Available at: https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html [Accessed 20 January 2022].

[14] Parfomak, P. W., & Jaikaran, C. (2021, May 11). *Colonial Pipeline: The Darkside strikes*. [online] Congressional Research Service (CRS) for the United States Congress. Available at: https://crsreports.congress.gov/product/pdf/IN/IN11667 [Accessed 20 January 2022]

[15] Shah, S. (2022, January 6). *The colonial pipeline attack eight months on*. [online] Info security Magazine. Available at: https://www.infosecurity-magazine.com/opinions/the-colonial-pipeline-attack-eight/ [Accessed 20 January 2022]

[16] FBI. (2021, May 10). *FBI statement on Compromise of Colonial Pipeline Networks.* [online]. Available at: https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks [Accessed 20 January 2022]

[17] Eaton, C., & Volz, *D. Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom* [online]. Available at: https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636 [Accessed 02 February 2022]

[18] Kelly, S. *One password allowed hackers to disrupt Colonial Pipeline* [online].

Available at: https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/ [Accessed 02 February 2022]

[19] *Grealish, G. Colonial Pipeline and VPN Vulnerabilities* [online]

Available at: https://www.zerotrustedge.com/blog/colonial-pipeline-and-vpn-vulnerabilities/ [Accessed 02 February 2022]

[20] Helman, C. *Cyber-Ransom Of $5m 'Nothing' To Colonial Pipeline, Which Has Paid Hundreds Of Millions In Dividends To Billionaire Koch Family* [online] Available at: https://www.forbes.com/sites/christopherhelman/2021/05/14/cyber-ransom-of-5m-nothing-to-colonial-pipeline-which-has-paid-hundreds-of-millions-in-dividends-to-billionaire-koch-family/?sh=5b71d2162e6e [Accessed 02 February 2022]

[21] ISA Cybersecurity. *Lessons Learned From The Colonial Pipeline Cyber Attack* [online] at: https://isacybersecurity.com/lessons-learned-from-colonial-pipeline-attack/ [Accessed 02 March 2022]

[22] William Barker (Dakota Consulting), William Fisher (NIST), Karen Scarfone (Scarfone Cybersecurity), Murugiah Souppaya (NIST). *Ransomware Risk Management: A Cybersecurity Framework Profile* [online] at: https://csrc.nist.gov/publications/detail/nistir/8374/final [Accessed 23 March 2022]