UNIVERSITI MALAYA

Centre for Continuing Education

MASTER IN DATA SCIENCE

GROUP ASSIGNMENT

COURSE CODE : WQD7010

COURSE TITLE : NETWORK & SECURITY

TOPIC : THE COLONIAL PIPELINE RANSOMWARE ATTACK IN 2021

LECTURER : DR. SAAIDAL RAZALLI BIN AZZUHRI

GROUP MEMBERS:

1) SHAMEEN BINTI IZWAN ANTHONYSAMY (S2180659)
2) NUR HIDAYAH BINTI AHMAD SHAFII (22120931)
3) HANISAH ZULAIKHA BINTI ZULKIFLI (23072436)
4) HU LIANGLIANG（S2164046)
5) ILI NURIZZATI BINTI HANIM (17070213)

Contents

1 ABSTRACT

The 2021 ransomware attack on one of the United States' largest refined product pipelines revealed serious cybersecurity vulnerabilities. Due to this attack, there was significant operational disruption, temporary shutdown and highlighting the possibility for severe economic and environmental impacts. Our study explores the details of the Colonial Pipeline incident and examines the attack methodology from the first breach to execution and response. By providing in-depth insights into cyber threats, this comprehensive analysis can fill gaps in the existing literature. In this study, the implications of the attack to the organization, the United States, and international markets which underscore the extensive impact of the attack are studied. Apart from providing recommendations to enhance cybersecurity in critical sectors, the paper also outlines potential defense strategies that might minimize the impact of the cyberattack. Our findings highlight the importance of establishing strong and proactive cybersecurity measures in place to avoid future ransomware attacks and improve the dependability of the security system.

2 INTRODUCTION

In the digital age, cyberattack causes a significant concern particularly for the energy industry the risk of cyberattacks. Cyberattacks on pipelines have various effects on the environment in addition to disrupting operations. Both individuals and organizations are vulnerable to various forms of attacks such as malware, phishing, and ransomware if there are no proper security measures. The primary objective of ransomware attacks is to take over a network and make all information, services, and data inaccessible unless a ransom is paid. As a result, a company's reputation can suffer and users will lose trust in it. Over time, these attacks have increasingly targeted organizations for larger ransoms rather than individuals [1].

The shutdown of the Colonial Oil Pipeline, one of the United States' largest refined products pipelines, in 2021 is one of the real-world examples of the caused by a massive ransomware attack. The company was founded in 1961 and pipeline construction began in 1962. It spans over 5500 miles of pipeline and transports more than 100 million gallons of fuel daily[2]. The huge pipeline network links the refineries on the Gulf Coast to distribution centres across the East Coast, as shown in Figure 1.1. This extensive network is crucial in providing gasoline, diesel, jet fuel, and other refined products to markets from Texas to New Jersey. It is a vital component of the nation's energy infrastructure.

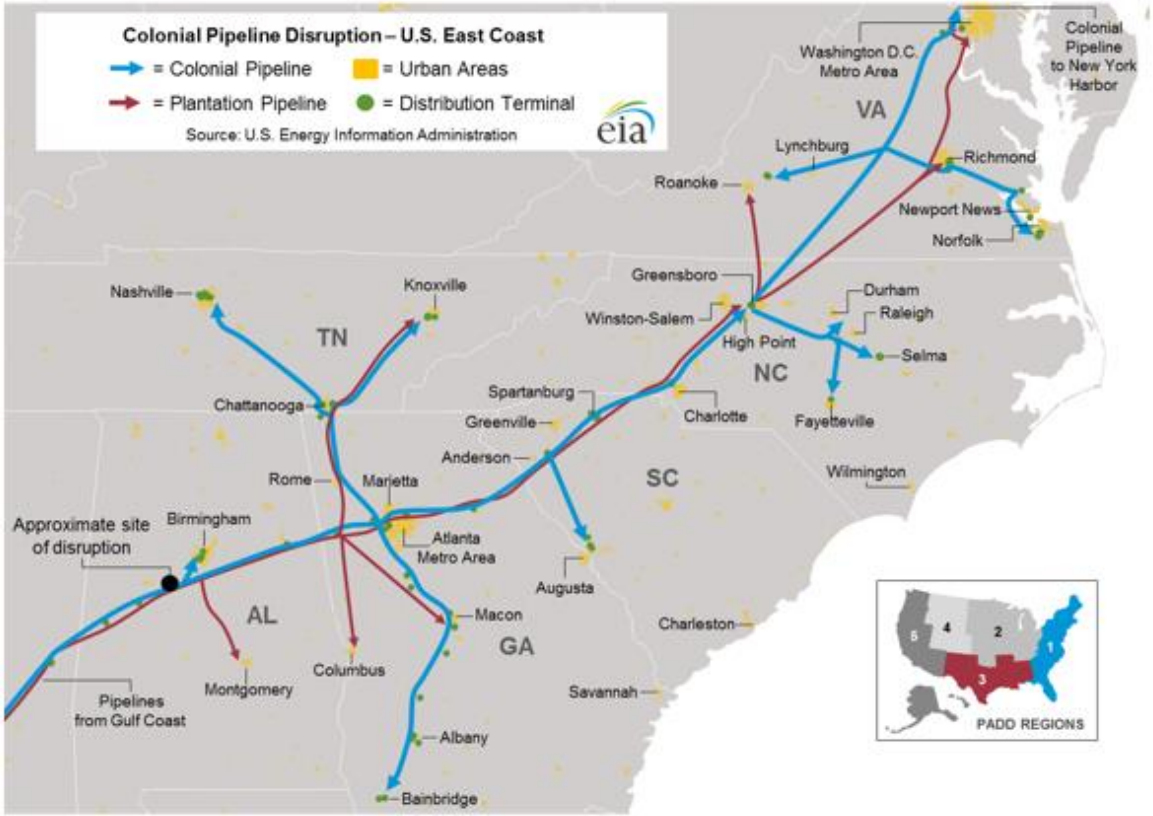


Figure 1.1 The Colonial Pipeline Network [2]

The 2021 Colonial Pipeline ransomware attack shows the vulnerabilities present in network security systems and the potential consequences of a successful breach. This resulted in major disruptions in the fuel distribution network and fuel shortages which increased fuel prices [3], [4]. It eventually causes national security concerns. This attack received a lot of attention from the media and was seen as one of the most important ransomware events in recent history. The Colonial Pipeline attack highlighted the benefits of strong cybersecurity protocols to avoid cyber threats and mitigate their consequences on critical sectors. Ultimately, this incident provides further evidence of the necessity for businesses to prioritize cybersecurity as a critical component of risk management by making investments in strong defences and proactive steps toward addressing new cyber threats.

The scope of this study covers Colonial Pipeline’s cyber-attack incident in 2021. For an in-depth study, this paper will provide a detailed analysis of the incident, implications of cyberattack, repercussions and preventive measures. The study also considered Colonial Pipeline’s cybersecurity practices, incident timeline and the tactics used in the attack. The study also discusses policy implications and proposes preventive strategies for future threats.

This study has potential limitations. Some information might not be reviewed because of the restrictions on public disclosure. Next, we also face challenges in gaining reliable information due to a lack of previous literature research as most of the information was from media outlets rather than the company's official statement. Hence, there might be a media bias in the available sources. Despite these limitations, this term paper seeks to provide valuable information to improve the cybersecurity system and protect critical infrastructure against cyberattacks.

3 LITERATURE REVIEW

3.1 Evolution of Ransomware Attack

Ransomware, a major threat to file access, demands payment to regain control and is acknowledged as a global crisis affecting various businesses [5]. Ransomware attacks, motivated by financial gain, are executed worldwide using vectors such as email, spam, and phishing. Understanding the history of ransomware reveals conflicting accounts regarding its origins and spread. Some attribute it to Russia and Eastern Europe, while others present different timelines and origins. This creates a nuanced narrative that underscores its evolution from unsophisticated attacks to sophisticated, targeted operations, highlighting the need for a comprehensive understanding of its historical context [6]. The inception of ransomware marked a shift in cybercriminal tactics, such as luring users to malicious websites and encrypting files for extortion. Table below shows the evolution of ransomware attacks throughout the last 10 years.

Name	Type	Main Agenda	Year
Maze	Crypto	Exploit kits, Phishing emails, Remote desktop	2019
REvil		Oracle WebLogic vulnerabilities, remote desktop, Password cracking	2019
Locky		Pishing emails	
WannaCry		Worm	2016
Bad		Drive by downloads	2017
Rabbit		Pishing emails	
Ryuk		Pishing emails	2018
Troldesh		Pishing emails	2014

Concurrently, ransomware strategies evolved to target financially robust businesses regionally. Criminal groups began strategically focusing on specific sectors, using malware encryption and data exfiltration to compel companies to weigh hefty ransom payments against the risk of exposing sensitive information [7]. This underscores the urgent need for robust cybersecurity measures and proactive strategies to combat the increasing sophistication and financial repercussions of ransomware attacks.

3.2 The Colonial Incident

On May 7, 2021, Colonial Pipeline was targeted by a cybercriminal known as DarkSide, which uses ransomware-as-a-service (RaaS) tactics to extort organizations for financial gain. According to [8], attackers stole 100 gigabytes of data within a two-hour window in Colonial Pipeline's network infrastructure. The CEO of the pipeline company stated that the hackers likely exploited Colonial’s computer through an unsecured VPN connection from the unused account. However, it remained unclear how valid user credentials were obtained [9]. The hacker successfully accessed its systems, encrypting vital data and effectively disrupting its operations to avoid further disruption and infection with the ransomware.

The Colonial Pipeline cyberattack had a significant impact after a shutdown of its operations for six days, thereby preventing further fuel transportation. Panic-buying spread along the East Coast due to consumer fears of fuel shortages. Additionally, there was a 4 cents-per-gallon increase in the average gas prices in the affected region following the pipeline shutdown when fuel demand was already rising due to the relief of COVID-19 restrictions, economic recovery, and holiday travel. Consumers faced long lines at gas stations and limited availability of fuel, leading to heightened uncertainty and volatility in the market [4], [10]. A study by [10] mentioned that the Colonial company paid 75 Bitcoin, approximately $4.4 million to the hacker before shutting down its operation for six days to restore affected systems and data.

President Joe Biden declared a state of emergency in response to the Colonial Pipeline shutdown and issued an interagency order to mitigate the immediate fallout. The government agencies, including the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), collaborated with Colonial Pipeline and other stakeholders to investigate the attack and provide technical assistance. One of the solutions in response to the incident is the new task force of the justice department was able to find the digital address of the wallet and recover 64 Bitcoin ransom paid by Colonial Pipeline [8], [10], [11].

3.3 Motivations of Cyber Attackers

Cyber attackers are often motivated by several factors that can be broadly categorized as financial gain, political goals, ideological beliefs, and personal gratification, with financial gain remaining the primary motivation for cyber attacks [12]. The ransomware attack on Colonial Pipeline is a typical example, where the attackers encrypted critical data and demanded a ransom to release it. Cryptocurrencies such as bitcoin facilitated these transactions while maintaining the anonymity of the attackers, making them difficult for law enforcement to track [13]. The DarkSide organization claimed that their attacks were not politically motivated but purely for financial gain, suggesting that their main goal was to extort money from their victims without any political considerations [14]. In addition, we can learn that they know how to create a sense of urgency to maximize the pressure on victims to pay the ransom. Exploiting vulnerabilities in critical infrastructure to maximize economic gain. The rapid increase in fuel prices caused by the attack and the subsequent panic buying that occurred on the East Coast. [15] created urgent pressure on Colonial Pipeline to comply with the ransom demand.

3.4 Ransomware

The [16] emphasized that there are two types of ransomware which are Crypto Ransomware and Locker Ransomware. Crypto ransomware focuses solely on encrypting the user's sensitive files but does not interfere with basic computer functions. Both symmetric and asymmetric data encryption techniques are used in this ransomware attack [17]**.** On the other hand, Locker Ransomware is designed to prevent the user's access to the computer and only permit interaction with the ransomware to make payments [1], [17]. [1] mentioned that spreading ransomware involves spam emails containing malicious attachments, which encrypt files. The finding is supported by a study by [1] which highlights phishing emails are the highest primary vector for ransomware infection at 33%, followed by Exploit kits at 15%, malicious applications at 13%, and drive-by-download at 10%. Additionally,[1]show that the lack of integrated cryptographic frameworks and appropriate fundamental management techniques in the early years of the cryptographic ransomware family contributed to the prevalence of locker ransomware variants between 2009 and 2013. Both ransomwares require the victim to pay a ransom to regain regular access to the computer. In some cases, the attacker will neither send a decryption key nor unlock the device even after receiving the ransom payment.

3.5 Ransom Payment

According to the [18], the emergence of cryptocurrencies like Bitcoin increases the rate of ransomware attacks. Criminals typically demand ransom payments in Bitcoin, then obscure the funds using methods like chain-hopping, mixing services, or demanding payments in privacy coins like Monero. Studied by [19] found that cryptographic ransomware strains mostly use cryptocurrencies as their payment method. The payments are difficult to attribute to individuals and often flow through multiple financial entities. Hence, these tactics make tracking and identifying criminals [17], [18]. In addition, ransomware attackers increasingly will use "double extortion" or "data exfiltration," threatening to publicly disclose sensitive data to pressure victims into paying, which adds to the strain on victims who are already struggling to recover operational capacity and safeguard their information.

Several studies have suggested that ransom payment is not recommended for several reasons. Firstly, no guarantee paying ransom will solve the problem. Also, the decryption processes often encounter numerous complications. On the other hand, the decryptor provided by cybercriminals may not receive as much attention as the encryption software. Hence, data recovery is impossible in the worst-case scenario. Paying a ransom will only motivate cybercriminals to look for new approaches to breaking into systems and target more victims [16], [17].

3.6 The Impact of Ransomware Attack

The ransomware attack on Colonial Pipeline in May 2021, as discussed by [20] exemplifies the evolving threat landscape posed by malware, particularly ransomware, to critical infrastructure. This literature review examines the impact of ransomware attacks on industries and social infrastructure, focusing on the agents and characteristics of such attacks and the response strategies that can be employed to mitigate their impact. One of the impacts is a direct financial loss where [21] discuss the direct financial costs of ransomware, including ransom payments and recovery expenses. Their study provides a comprehensive analysis of the economic burden on businesses and individuals, highlighting the significant financial drain caused by ransomware.

Other than that,[22] examines the operational disruptions caused by ransomware attacks. The research underscores how extended downtimes can lead to substantial financial losses, particularly for organizations heavily reliant on continuous operations. His findings also reveal how ransomware not only encrypts data but also can lead to permanent data loss, affecting business continuity and data reliability. This is also added by [23] in their study discussing how ransomware attacks erode customer trust and damage organizational reputation. Their research shows that businesses often face long-term reputational challenges, which can result in a loss of customers and revenue.

3.7 Cybersecurity Measures

The field of cybersecurity relies on established measures and standards to enhance the security of digital systems and protect against cyber-attacks. The study [11] examines key defensive concepts and best practices focusing on software testing, regular updates, and secure processes. These measures, along with security standards such as ISO 27001, provide a framework for increasing cybersecurity and can be leveraged by informed citizens to advocate for improved legislation.

[24] in their study emphasizes the importance of user education awareness in mitigating ransomware risks. For example, training employees to recognize phishing attempts and unsafe online behaviors as part of cyber security measures can significantly reduce the likelihood of ransomware infections. Other than that, [23] highlight the critical role of timely software updates in preventing ransomware. Their research demonstrates that robust patch management practices can close vulnerabilities that ransomware exploits. Moreover, one of the techniques for cyber security measure monitoring is network traffic to detect ransomware which has been discussed by

[25]. Their study shows how anomaly detection methods can be employed to identify suspicious data flows associated with ransomware attacks.

3.8 Forecasting and Identifying Ransomware

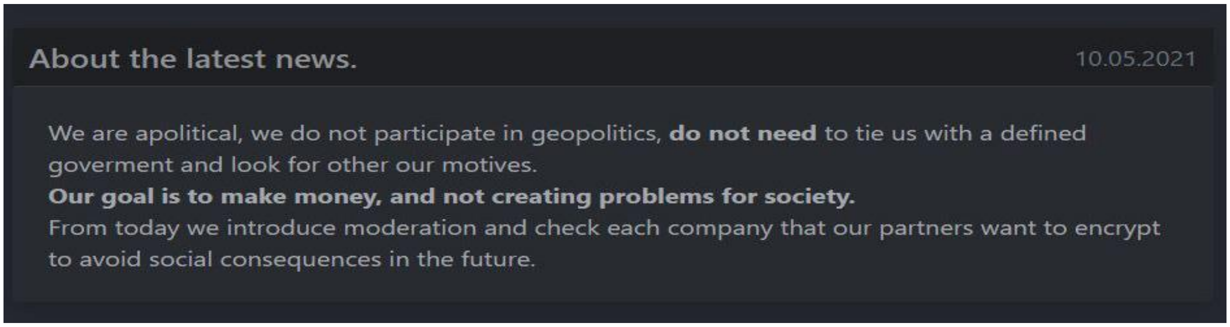
Situational awareness for protection against ransomware attacks goes beyond organizational and managerial factors. It also encompasses the operational parameters of the system. By integrating data from the ransomware's behavior during execution with organizational and managerial data, the model becomes capable of predictive analysis. This holistic approach allows the model to anticipate future attacks by considering the evolving behavior of ransomware alongside the vulnerabilities within the system. Consequently, the model can dynamically adjust to changes in both the operational behavior of the ransomware and the targeted system. Numerous research endeavors have explored the utilization of intelligent prediction engines to anticipate potential malware and ransomware threats. In one such investigation cited as [26], a Generative Adversarial Network (GAN) was harnessed to predict forthcoming malware variations. This involved the generation of novel malware samples based on existing ones, achieved by scrutinizing existing malware signatures and producing analogous signatures derived from static malware payload analysis.

Another important model, MalDeepNet was developed to forecast malware behavior and fabricate synthetic patterns representing the evolution of malware activity [27]. These newly created patterns were integrated into the existing malware dataset, subsequently employed to train a cluster-based detection system. Likewise, MalGAN functions as a GAN-based malware generator aimed at crafting black-box attacks [28]. MalGAN utilizes a generator to generate malware samples and a substitute detector to refine the black-box malware detection system. Through training a generative network, the aim is to minimize the number of generated adversarial samples required to trigger specific malicious probabilities predicted by the substitute detector. According to [29], researchers conducted a behavioral analysis of the ransomware attack process and devised a model to forecast the future actions of the malware. This study relied on various data sources, including information of the attack process, file system, persistence, and network activities. Employing supervised machine learning techniques, the model was constructed to observe, learn, and predict how the malware would evolve to accomplish its objectives with minimal data input.

4 DISCUSSIONS

4.1 Timeline Review

- On May 6, 2021, the DarkSide hacker group successfully compromised Colonial Pipeline's network systems through phishing emails or by exploiting unpatched system vulnerabilities.
- On May 7, 2021, DarkSide hackers planted ransomware in Colonial Pipeline's systems and encrypted the company's computers and data. The Company was forced to shut down portions of its systems to prevent the ransomware from spreading and halted operations throughout the pipeline.
- On May 8, 2021, Colonial Pipeline, a U.S. fuel pipeline company, made a notice on its website claiming to have learned of the hacking on the 7th and contacted third-party cybersecurity experts, law enforcement, and other federal agencies to activate an emergency response, which was determined to involve ransomware. The activation of the emergency response halted all pipeline operations and shut down certain systems to avoid further attacks.
- On May 9, 2021, several East Coast states experienced long lines for gasoline due to fuel supply disruptions, with many gas stations running out of fuel supplies. Consumers begin a panic rush to buy fuel.
- On May 9, 2021, the Federal Motor Carrier Safety Administration (FMCSA) issued a Regional Emergency Declaration announcing the emergency activation of motor vehicles to transport fuel due to the disruption of fuel shipments as a result of a cyber-attack on Colonial Pipeline, Inc. in an effort to address the fuel needs of the 18 affected U.S. states.
- On May 9, 2021, Colonial Pipeline's official website was updated with a notice stating that the company's operations staff is currently working on a plan to restart the system, and that while the main pipeline remains offline, the smaller pipeline between the terminal and the delivery point is operational.
- On May 10, 2021, the DarkSide group issued a certification stating that the attack against Colonial Pipeline was launched by its RaaS partners and that the attack was intended solely to make money and was not politically motivated.



About the latest news. 10.05.2021

We are apolitical, we do not participate in geopolitics, **do not need** to tie us with a defined goverment and look for other our motives.
Our goal is to make money, and not creating problems for society.
From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future.

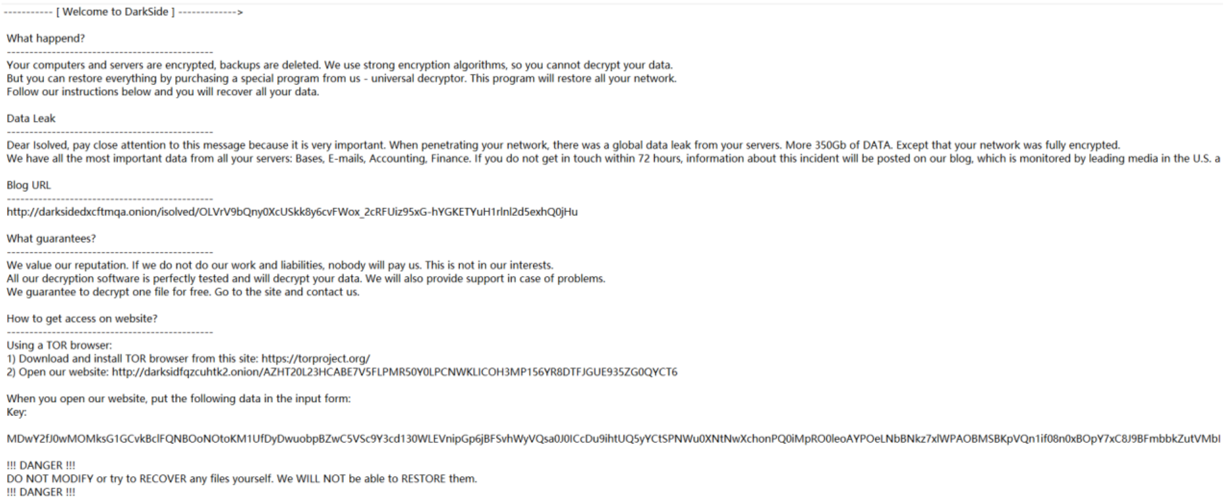
- On May 11, 2021, Colonial Pipeline decided to pay a ransom of approximately $5 million to obtain decryption tools to recover the encrypted data. However, even with access to the decryption tools, data recovery remains very slow and incomplete.

- May 12, 2021: Colonial Pipeline gradually resumes operations, but fuel shortages continue. Fuel prices across the region rise due to tight supply.
- May 13-14, 2021: The U.S. government issued a number of new cybersecurity directives and recommendations that require critical infrastructure operators to strengthen protections to prevent similar cyberattacks from happening again.

4.2 Attack Methodology

The DarkSide hacker group emerged in August 2020 and operates on a ransomware-as-a-service (RaaS) business model, consisting of a combination of ransomware developers and operators and distributors recruited by them, respectively, with the distributors carrying out the attacks and the core developer-operators being responsible for the development of the ransomware and negotiating with the victims to collect the ransom payments. The core team claims that healthcare, education, non-profit organizations and government are not among its targets, and in addition to encrypting the victim's system files, it also steals the victim's system data, evaluates the information obtained from the victim, and then determines the amount of money that needs to be paid for the decryption, and writes in its introduction that it has already made millions of dollars in profit.

DarkSide ransomware exists for both Windows and Linux platforms and can be customized through a visual panel, which includes encrypted directories, encryption modes, persistence methods, access operations, network interactions, cryptocurrency payment types, and more. It has been found that customized executables/software are created for specific targets, encrypting files with a SALSA20 key and re-encrypting that key with an RSA-1024 key in the executable. Eight pseudo-randomly defined lowercase hexadecimal characters are used as the encrypted file suffix.DarkSide ransomware leaves a ransom note on the victim's machine containing the amount of stolen data, data type, and a link to the data compromise site. If the ransom payment is not received within a specified period of time, the stolen information will be made public.



```
----------- [ Welcome to DarkSide ] ------------->

What happend?
----------------------------------------------
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.

Data Leak
----------------------------------------------
Dear Isolved, pay close attention to this message because it is very important. When penetrating your network, there was a global data leak from your servers. More 350Gb of DATA. Except that your network was fully encrypted.
We have all the most important data from all your servers: Bases, E-mails, Accounting, Finance. If you do not get in touch within 72 hours, information about this incident will be posted on our blog, which is monitored by leading media in the U.S. a

Blog URL
----------------------------------------------
http://darksidedxcftmqa.onion/isolved/OLVrV9bQny0XcUSkk8y6cvFWox_2cRFUiz95xG-hYGKETYuH1rlnl2d5exhQ0jHu

What guarantees?
----------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.

How to get access on website?
----------------------------------------------
Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://darksidfqzcuhtk2.onion/AZHT20L23HCABE7V5FLPMR50Y0LPCNWKLICOH3MP156YR8DTFJGUE935ZG0QYCT6

When you open our website, put the following data in the input form:
Key:

MDwY2fJ0wMOMksG1GCvkBclFQNBOoNOtoKM1UfDyDwuobpBZwC5VSc9Y3cd130WLEVnipGp6jBFSvhWyVQsa0J0ICcDu9ihtUQ5yYCtSPNWu0XNtNwXchonPQ0iMpRO0leoAYPOeLNbBNkz7xlWPAOBMSBKpVQn1if08n0xBOpY7xC8J9BFmbbkZutVMbl

!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
!!! DANGER !!!
```

DarkSide’s Ransomware Interface

In the colonial pipeline ransomware attack in 2021 incident, we summarize the methodology by darkside as follows:

A. Initial access and vulnerability exploitation:
   Attackers gained initial access to the Colonial Pipeline network through technical means such as phishing emails, unpatched system vulnerabilities, or credential stuffing. The specific access methods have not been fully disclosed, but in general, phishing emails and exploiting vulnerabilities in older software versions are common initial intrusion methods.

B. Privilege elevation and lateral movement:
   Once inside a system, attackers gain higher system privileges through elevation of privilege techniques (e.g., exploiting a local boost vulnerability or stealing credentials from a high-privileged account). This allows them to move laterally across the network to access more systems and data.

C. Deploying ransomware:
   After gaining sufficient privileges, the attackers deploy the DarkSide ransomware. It spreads over the network and encrypts critical data and files on the target system. After the encryption is complete, the victim's system displays a ransom message demanding a ransom payment for a decryption tool.

D. Data theft and threats:
   In addition to encrypting data, the DarkSide organization also steals a large amount of data. They claim to have stolen a large amount of sensitive data and threaten to make it public if the ransom is not paid.

E. Ransom Negotiation and Payment:
   After realizing that the system had been attacked, Colonial Pipeline began negotiating with the attackers. The initial ransom demand was approximately $7.5 million, but the final negotiation resulted in the payment of a ransom of approximately $5 million in Bitcoin. After the ransom was paid, the attackers provided decryption tools, but the recovery process was very slow and incomplete.

4.3 Impact of Attack

i. Economic Effect:

Colonial Pipeline paid a Bitcoin ransom of approximately $5 million to unlock the encrypted data, a cost that directly increased the company's financial burden . As a result of the pipeline shutdown, several East Coast states experienced severe fuel shortages. Yet prior to this the pipeline delivered about 2.5 million barrels of gasoline, diesel, and jet fuel per day, or 45% of the East Coast's fuel supply. Fuel shortages have led to dramatic increases in fuel prices, affecting a wide range of consumer groups, from the average driver to the airlines.

ii. Social Impacts:

The fuel shortage triggered panic buying, with long lines at many gas stations and even some running out of fuel. The supply crisis was exacerbated by consumers stockpiling fuel. Public transportation and emergency services were also affected in some areas, leading to a reduction in the efficiency of social functioning.

iii. Political and policy implications:

In the wake of the incident, the United States Government took swift action to strengthen cybersecurity protection for critical infrastructure. The Joint Cyber Defence Cooperative was established, new cybersecurity directives and recommendations were issued, and defences against similar attacks were upgraded. Promoted a reassessment and realignment of cybersecurity legislation and regulation to ensure the security of critical infrastructure.

This has also led industries to pay more attention to cybersecurity, especially the protection of critical infrastructure. Enterprises began to invest more resources in improving their cyber defense capabilities. Enterprises and government departments are prompted to improve technical measures, such as updating and patching system vulnerabilities on time and using stronger authentication mechanisms and monitoring tools to prevent the recurrence of similar attacks.

Overall, the Colonial Pipeline ransomware attack not only had a significant impact on an economic and social level, but also drove significant changes in the cybersecurity field and increased the focus on critical infrastructure protection.

4.4 Preventive Measures

The ransomware attack on the Colonial Pipeline by the Dark Side criminal group in May 2021 underscored the vulnerabilities of critical infrastructure to cyber threats. The attack, which resulted in the exfiltration of 100 gigabytes of proprietary data and software, disrupted operations and led to the pipeline's shutdown, impacting fuel supply to the Northeastern states. The response by Colonial Pipeline's IT staff, including the shutdown of servers supporting business and financial software, highlights the challenges faced by organizations in mitigating the attacks with the need to maintain critical business operations. The need to quickly identify and contain the attack while minimizing disruption requires a coordinated and well-prepared incident response plan. The Colonial Pipeline attack also drew significant public and government attention, leading to increased scrutiny of cybersecurity practices in critical infrastructure sectors. It also prompted calls for improved cybersecurity standards and regulations to better protect essential services from cyber threats.

One of the key implications of the Colonial Pipeline attack is the importance of robust cybersecurity practices, particularly in the areas of virtual private network (VPN) security and password hygiene. The attack was suspected to have originated from a latent vulnerability in the VPN used by Colonial Pipeline, highlighting the need for organizations to regularly update and secure their VPN infrastructure. Additionally, the discovery of the VPN password on the Dark Web among previously leaked credentials raises concerns about the reuse of passwords and underscores the importance of strong, unique passwords for all systems. This incident underscores the importance of implementing strong, unique passwords and regularly updating them to prevent unauthorized access to systems. Continuous monitoring of VPN usage and password activity can help organizations detect and respond to unauthorized access attempts promptly. This can help prevent attackers from exploiting vulnerabilities or using stolen credentials to access sensitive systems.

The attack underscored the crucial role of robust authentication practices in safeguarding critical infrastructure. In cases where attackers have acquired usernames and passwords through methods like phishing or data breaches, two-factor authentication, 2FA can mitigate the risk of unauthorized access. Two-factor authentication provides an additional layer of security beyond just a password. By requiring a second form of verification, such as a code sent to a mobile device, 2FA makes it significantly harder for attackers to gain unauthorized access, even if they have obtained login credentials. By having two-factor authentication in place, unauthorized access to Colonial Pipeline's systems might have been prevented. This highlights the importance of organizations continually updating their cybersecurity protocols to provide an additional layer of security. Implementing 2FA aligns with best practices and can help organizations comply with regulatory requirements.

Colonial Pipeline's response to the attack, including the shutdown of operational technology, highlights the difficulties organizations encounter in mitigating ransomware attacks on critical infrastructure. This incident underscores the necessity for organizations to develop and maintain comprehensive incident response plans to promptly detect and manage cyber threats. The involvement of cybersecurity experts, such as Mandiant, was important in understanding the attack vector and identifying potential vulnerabilities. Mandiant's forensic analysis provided valuable insights into how the attack occurred and how it could be prevented in the future. This highlights the importance of organizations partnering with cybersecurity experts to enhance their incident response capabilities.

Collaboration between organizations and law enforcement agencies enables the sharing of critical information related to cyber threats. In the case of the Colonial Pipeline, sharing information with the FBI likely facilitated a faster and more effective response to the attack. Law enforcement agencies, such as the FBI, bring legal expertise to cybercrime investigations. They can help navigate legal issues related to cyber-attacks, such as obtaining warrants, and ensure that investigations are conducted following the law.

5. RESULT

The Colonial Pipeline ransomware attack of 2021 had went through intense consequences, emitting a long shadow over censorious infrastructure and changing the cybersecurity industry. The event was planned by a hacker group called the DarkSide hacker group which aimed at the Colonial Pipeline's most important fuel transportation network, which then had started a chain of events that led to a bunch of disturbances across the whole United States

Due to the instant effect of the attack that was so impactful, the Colonial Pipeline was forced to stop the operations in order to control and to prevent any other continuous and bigger defects. The airline industry was one of the sectors that was seriously infected which extended beyond fuel supply Its ramifications extended beyond fuel supply. Americal Airlines had to indure fuel shortages which then impacted major airports such as Atlanta and Nashville. The after-math then created panic-buying across states that include Florida, Georgia, Alabama, Virginia, and the Carolinas . They were afraid of the gas shortage that was happening. The fear of a gas shortage triggered panic-buying across several states, including Long lines formed at gas stations, and the average price at the pump surged, with regular gas prices exceeding $3 per gallon in the aftermath of the Colonial Pipeline shutdown.

Without having any other choice, Colonial Pipeline had to make a choice, which ended up them responding to the hackers to pay the ransom that has been forced upon them. In the ended, the company chose to surrender to the extortion which they transfered millions of dollars in Bitcon to get back the access of their systems. Some say this desicion was controversial but it marks a harsh reminder to all the organizations of the awarness of cyberattacks.

The consequence from the Colonial Pipeline ransomware attack resonated far beyond the limits of the energy industry, encouraging a multifaceted response from government, industry, and cybersecurity experts. Investigations were launched, emergency regulatory waivers were issued, and cybersecurity measures were strengthen to build up defenses against future threats. The attack served as an impulse for awarness fostering a better emphasis on cybersecurity awareness, information sharing, and technological innovation.

After the immediate aftermath subsided, the impact of the Colonial Pipeline ransomware attack persevered, acting as a reminder of the vulnerability of digital infrastructure and highlighting the need for resilience in challenging circumstances. The lessons learned from this watershed moment continue to inform strategies for fortifying critical infrastructure, enhancing cybersecurity readyness, and safeguarding the integrity of digital ecosystems.

6. RECOMMENDATIONS

The analysis portrayed that the information required to doubt myths regarding the Colonial Pipeline incident which was only present in a small number of articles. Furthermore, the article's content and presentation largely ignored a few uncontroversial points, such as the idea that businesses should be in charge of securing their systems. This affects public opinion since varying accounts of the event can result in varying conclusions about the proper course of action.

Secondly, given the serious consequences of ransomware attacks, citizens must be prepared to assess such situations critically. Citizens should also critically assess public incident reporting, considering potential political ramifications such as new legislation or diplomatic initiatives. The analysis suggests that the public may not be adequately prepared for these conversations due to the current delivery of news and education.

Next, most articles presented Colonial as an innocent victim of Russian hackers, creating a more narrative framework for the incident. However, readers can analyze this story analytically and see how many of the details are unusual for ransomware incidents by realizing the suggested fallacies. This inspires readers to look up additional information and participate actively in political discussions regarding cybersecurity. As a result, it is necessary to have a public conversation about the significance of structured instruction about ransomware attacks and appropriate defences. It appears that the information required for intelligent public discourse is missing from both official education and unofficial sources, such as news articles.

For future work, the importance of incorporating relevant technical knowledge into formal education to effectively counter these misconceptions has been underlined. Academicians can use this information to better plan their lessons and emphasize key ideas. Future research must examine the real-world prevalence of these false beliefs among the general public and journalists covering these incidents. This analysis will help shape more comprehensive approaches and allow for a better understanding of the problem's scope.

7. CONCLUSION

This article analysed the reporting on the Colonial Pipeline incident. In this paper, it states that most case study articles focused on the consequences of the shutdown, rather than the attack, even if focusing solely on the articles that introduced the concept of ransomware attacks. For many years, policymakers have acknowledged the need to recognize financial institutions as systemically important however other sectors such as energy, healthcare, transportation and many others are not well versed. Additionally, several crucial aspects such as technical countermeasures were introduced only in a handful of articles. Thus, the need to gather more background information is crucial for further awareness and a reduced number of cyber-related cases similar to the ransomware attack.

8. REFERENCE

[1] A. K. Muslim, D. Z. Mohd Dzulkifli, M. H. Nadhim, and R. H. Abdellah, ‘A Study of Ransomware Attacks: Evolution and Prevention’, *Journal of Social Transformation and Regional Development*, vol. 1, no. 1, Jun. 2019, doi: 10.30880/jstard.2019.01.01.003.

[2] ‘The Anatomy of a Pipeline Accident: The Colonial Pipeline Spill | by Planet | Planet Stories | Medium’. Accessed: Jun. 07, 2024. [Online]. Available: https://medium.com/planet-stories/the-anatomy-of-a-pipeline-accident-the-colonial-pipeline-spill-d30bb2a5941d

[3] J. Niccum, ‘Cyberattack on Colonial Pipeline affected gas prices far less than initially reported by Jon Niccum’, 2021.

[4] T. Tsvetanov and S. Slaria, ‘The Effect of the Colonial Pipeline shutdown on gasoline prices’, *Econ Lett*, vol. 209, p. 110122, Dec. 2021, doi: 10.1016/J.ECONLET.2021.110122.

[5] M. Muniandy, N. A. Ismail, A. Y. Yahya Al-Nahari, and D. N. L. Yao, ‘Evolution and Impact of Ransomware: Patterns, Prevention, and Recommendations for Organizational Resilience’, *International Journal of Academic Research in Business and Social Sciences*, vol. 14, no. 1, Jan. 2024, doi: 10.6007/ijarbss/v14-i1/19803.

[6] A. K. Maurya, N. Kumar, A. Agrawal, and R. A. Khan, ‘Ransomware Evolution, Target and Safety Measures’, *International Journal of Computer Sciences and Engineering*, vol. 6, no. 1, pp. 80–85, Jan. 2018, doi: 10.26438/ijcse/v6i1.8085.

[7] M. Ozer, S. Varlioglu, B. Gonen, and M. Bastug, ‘A prevention and a traction system for ransomware attacks’, in *Proceedings - 6th Annual Conference on Computational Science and Computational Intelligence, CSCI 2019*, Institute of Electrical and Electronics Engineers Inc., Dec. 2019, pp. 150–154. doi: 10.1109/CSCI49370.2019.00032.

[8] E. Thakran and Ankita, ‘Impact of “Ransomware” on critical infrastructure due to pandemic’, *In Proceedings of the International Conference on Innovative Computing & Communication (ICICC)*, 2019, [Online]. Available: https://ssrn.com/abstract=4361110

[9] A. Greubel, D. Andres, and M. Hennecke, ‘Analyzing Reporting on Ransomware Incidents: A Case Study’, *Soc Sci*, vol. 12, no. 5, May 2023, doi: 10.3390/socsci12050265.

[10] I. Kilovaty, ‘Cybersecuring The Pipeline’, p. 605, 2023, [Online]. Available: https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline

[11] A. Greubel, D. Andres, and M. Hennecke, ‘Analyzing Reporting on Ransomware Incidents: A Case Study’, *Soc Sci*, vol. 12, no. 5, May 2023, doi: 10.3390/socsci12050265.

[12] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, and P. Laplante, ‘Dimensions of cyber-attacks: Cultural, social, economic, and political’, *IEEE Technology and Society Magazine*, vol. 30, no. 1, pp. 28–38, Mar. 2011, doi: 10.1109/MTS.2011.940293.

[13] A. Robinson, C. Corcoran, and J. Waldo, ‘New Risks in Ransomware Supply Chain Attacks and Cryptocurrency’, 2022. [Online]. Available: www.belfercenter.org/stpp

[14] ‘The Colonial Pipeline Ransomware Hackers Had a Secret Weapon: Self-Promoting Cybersecurity Firms — ProPublica’. Accessed: Jun. 07, 2024. [Online]. Available:

https://www.propublica.org/article/the-colonial-pipeline-ransomware-hackers-had-a-secret-weapon-self-promoting-cybersecurity-firms

[15] J. Beerman, D. Berent, Z. Falter, and S. Bhunia, ‘A Review of Colonial Pipeline Ransomware Attack’, in *Proceedings - 23rd IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing Workshops, CCGridW 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 8–15. doi: 10.1109/CCGridW59191.2023.00017.

[16] ‘Ransomware: Measures for Preventing, Limiting and Recovering from a Ransomware Attack.’, National Cyber Security Center. Accessed: Apr. 30, 2024. [Online]. Available: https://english.ncsc.nl/binaries/ncsc-en/documenten/factsheets/2020/june/30/factsheet-ransomware/71059_NCSC_FS+Ransomeware+EN_WEB.pdf

[17] M. Humayun, N. Z. Jhanjhi, A. Alsayat, and V. Ponnusamy, ‘Internet of things and ransomware: Evolution, mitigation and prevention’, *Egyptian Informatics Journal*, vol. 22, no. 1, pp. 105–117, Mar. 2021, doi: 10.1016/j.eij.2020.05.003.

[18] ‘Combating Ransomware’, Institute for Security and Technology. Accessed: Apr. 30, 2024. [Online]. Available: https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf

[19] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, ‘A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions’, *ACM Comput Surv*, vol. 54, no. 11s, Sep. 2022, doi: 10.1145/3514229.

[20] J. S. Kim and K. W. Park, ‘Ransomware Classification Framework Using the Behavioral Performance Visualization of Execution Objects’, *Computers, Materials and Continua*, vol. 72, no. 2, pp. 3401–3424, 2022, doi: 10.32604/cmc.2022.026621.

[21] Md Haris Uddin Sharif and Mehmood Ali Mohammed, ‘A literature review of financial losses statistics for cyber security and future trend’, *World Journal of Advanced Research and Reviews*, vol. 15, no. 1, pp. 138–156, Jul. 2022, doi: 10.30574/wjarr.2022.15.1.0573.

[22] D. P. F. Möller, ‘Ransomware Attacks and Scenarios: Cost Factors and Loss of Reputation’, *Advances in Information Security*, vol. 103, pp. 273–303, 2023, doi: 10.1007/978-3-031-26845-8_6.

[23] T. August, D. Dao, and M. F. Niculescu, ‘Economics of Ransomware: Risk Interdependence and Large-Scale Attacks’, *Manage Sci*, vol. 68, no. 12, pp. 8879–9002, Dec. 2022, doi: 10.1287/mnsc.2022.4300.

[24] A. Bello and A. Maurushat, ‘Technical and Behavioural Training and Awareness Solutions for Mitigating Ransomware Attacks’, *Advances in Intelligent Systems and Computing*, vol. 1226 AISC, pp. 164–176, 2020, doi: 10.1007/978-3-030-51974-2_14.

[25] R. Moussaileb, N. Cuppens, J.-L. Lanet, H. Le Bouder, and andHéì ene Le Bouder, ‘Ransomware Network Traffic Analysis for Pre-Encryption Alert’, 2019, doi: 10.1007/978-3-030-45371-8_2ï.

[26] H. Treiblmaier, ‘A comprehensive research framework for Bitcoin’s energy use: Fundamentals, economic rationale, and a pinch of thermodynamics’, *Blockchain: Research and Applications*, vol. 4, no. 3, Sep. 2023, doi: 10.1016/j.bcra.2023.100149.

[27] Z. Moti, S. Hashemi, and A. Namavar, ‘Discovering future malware variants by generating new malware samples using generative adversarial network’, in *2019 9th International Conference on Computer and Knowledge Engineering, ICCKE 2019*, Institute of Electrical and Electronics Engineers Inc., Oct. 2019, pp. 319–324. doi: 10.1109/ICCKE48569.2019.8964913.

[28] W. Hu and Y. Tan, ‘Generating Adversarial Malware Examples for Black-Box Attacks Based on GAN’, Feb. 2017, [Online]. Available: http://arxiv.org/abs/1702.05983

[29] N. K. Popli and A. Girdhar, ‘Behavioural Analysis of Recent Ransomwares and Prediction of Future Attacks by Polymorphic and Metamorphic Ransomware’, in *Advances in Intelligent Systems and Computing*, Springer Verlag, 2019, pp. 65–80. doi: 10.1007/978-981-13-1135-2_6.