Exploring the Impact of Crypto-Ransomware on Critical Industries: Case Studies and Solutions

Austin Yee Meng Jun , Bryan Alexander Jinu , Lay Kah Seng , Muhamad Haris Firdaus Bin Zainol Maharaiq , Wadthanak Khongsuwan , Bryan Thong Khai Junn , Aidan Au Wen Hao , Siva Raja Sindiramutty *

Posted Date: 18 September 2024

doi: 10.20944/preprints202409.1325.v1

Keywords: Crypto Ransomware; Cybersecurity; Ransomware Attack; Cryptocurrency; Data Encryption

Article

Exploring the Impact of Crypto-Ransomware on Critical Industries: Case Studies and Solutions

Austin Yee Meng Jun, Bryan Alexander Jinu, Lay Kah Seng, Muhamad Haris Firdaus Bin Zainol Maharaiq, Wadthanak Khongsuwan, Bryan Thong Khai Junn, Aidan Au Wen Hao and Siva Raja Sindiramutty *

School of Computer Science Taylor's University Subang Jaya; austinyeemengjun@gmail.com, bryan.jinu04@gmail.com, alexlay9933@gmail.com, muhdharisfirdaus711@gmail.com, wadthanakkhongsuwan48@gmail.com, bryanthong88@gmail.com, Aidanawh04@gmail.com
* Correspondence: siva.sindiramutty@taylors.edu.my

Abstract: Crypto-ransomware has emerged as one of the most significant cybersecurity threats in recent years. Ransomware attacks, particularly those involving the encryption of data and demanding payment in cryptocurrency, have caused severe disruptions across various critical industries, including healthcare, energy, and finance. The proliferation of these attacks is largely attributed to the anonymity provided by cryptocurrency transactions and the increasing sophistication of cybercriminal tactics. The impact of ransomware extends beyond immediate financial losses, often leading to prolonged operational downtime, reputational damage, and even risks to public safety. In this research paper, we explore the growing threat of crypto-ransomware by examining real-life case studies in key industries, analyzing the countermeasures taken, and proposing additional solutions to mitigate the risk. The goal is to raise awareness and provide actionable insights for organizations to better protect themselves against this pervasive threat.

Keywords: crypto ransomware; cybersecurity; ransomware attack; cryptocurrency; data encryption

1.0. Background

1.1. Purpose

As technology has gotten more and more advanced, people's skills have also gotten much better. As a result, some resort to malicious activities for monetary gain and illegal access to data. Examples of those malicious activities are hacking and creating and releasing malware such as crypto malware. Therefore, this assignment is to raise awareness of the history, causes, prevention, and solution to overcoming crypto-ransomware. As technology advances, so too do the skills of those who engage in malicious activities for financial gain or illegal access to data. Among the most concerning of these activities is the creation and dissemination of crypto-ransomware, a form of malware that encrypts a victim's data and demands a ransom for its release. The purpose of this paper is to raise awareness about the history, causes, and potential solutions to the challenges posed by crypto-ransomware. Through the examination of real-world case studies, we aim to highlight the severity of this threat and to provide practical recommendations for preventing and responding to such attacks.

In 2013, the first case of crypto ransomware happened. This new breed of ransomware not only abused and exploited the power of Bitcoin currency transactions but implemented their actions with the use of encryption to block their victims from accessing their files and data. This first case of crypto-ransomware implemented 2048-bit RSA key pairs that are generated from a command-and-control server to encrypt their victim's files and data, further ensuring that they are not able to crack the code and retrieve their critical information without paying the ransom. This malicious act was performed by a group called Gameover Zeus. (CrowdStrike, 2021; Almoysheer et, al., 2021; Alsharif et, al., 2022)

1.3. Architecture Used

 doi:10.20944/preprints202409.1325.v1

The first known case of crypto-ransomware occurred in 2013, marking the beginning of a new era in cybercrime. This new breed of ransomware exploited the growing popularity and anonymity of Bitcoin transactions, coupled with advanced encryption techniques, to effectively hold victims' data hostage. The perpetrators of this attack, identified as the Gameover Zeus group, employed 2048-bit RSA key pairs generated from a command-and-control server to encrypt the files and data of their victims. The strength of this encryption made it virtually impossible for victims to recover their data without paying the demanded ransom. This incident not only highlighted the potential for cryptocurrency to be used for illicit purposes but also set the stage for the widespread adoption of crypto-ransomware by cybercriminals worldwide.

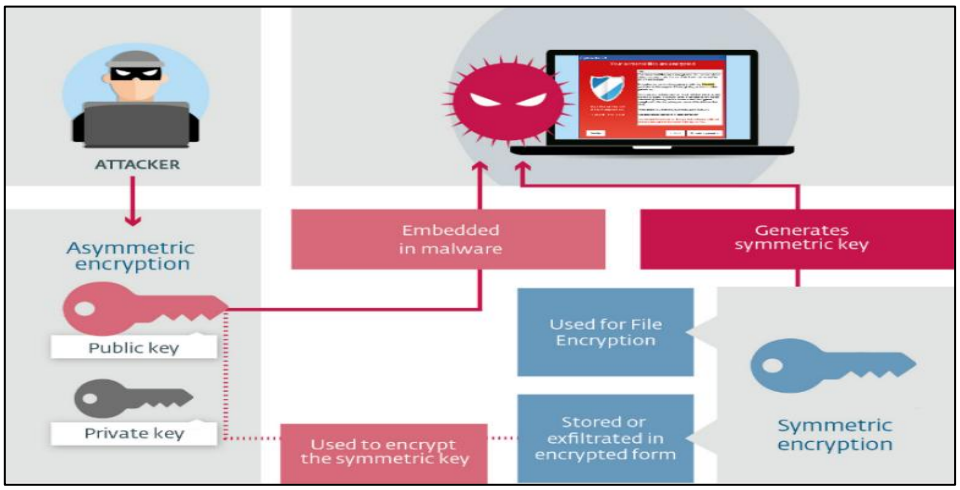

Figure 1. Schematic of dual encryption in crypto-ransomware.

1.4. Technology Used

The technologies used by crypto-ransomware attackers are commonly infection methods and encryption methods. The purpose of infection methods is to spread and send malware to the victims, whereas the purpose of encryption is to lock the victims from accessing their data and files.

1.4.1. Infection Methods

Phishing Emails: Email phishing infection method usually utilizes social engineering to deceive their victim to download their malware (Longtchi et al., 2024; Fatima-Tuz-Zahra *et al.*, 2020). The way they deceive their victims is by adding attachments that are infected with malware or contain malicious links that will redirect the victim to the website. They will also ensure that their attachments look convincing and real (Goenka, Chawla and Tiwari, 2023; Gaur et, al., 2023; H. Ashraf et, al., 2023 and 2022). There are also cases where the attackers implement spoofing by using the victim's acquaintance's name with an extra number or alphabet to make the victim further believe that the email is from that person. (Check Point Software, n.d.)

Malicious Websites: Websites are also another common way for attackers to attack their victims (Lim, Park and Kim, 2024; Humayun et al., 2022, and 2020). These malicious websites often have links that have an install function available alongside convincing "marketing" to lure the victim to install the malware (Kumari and Sharma, 2024; Javaid et, al., 2022; Jhanjhi et, al., 2020). Most of the time, these malicious websites include Trojan Horse, which is malware that dissimulates to be real software but is malware that will infect the user's computer. (Check Point Software, n.d.)

Compromised Accounts: Another way of spreading malware to victims is by using compromised accounts (Chimmanee and Jantavongso, 2024; Kok et, al., 2021 2019). This means after breaching or guessing the password of a legitimate user, the attacker will log into the account using an RDP (Remote Desktop Protocol) or VPN (Virtual Private Network) and message their victims. The attackers will then spread the malware through chats with the victims. (Check Point Software, n.d.)

 doi:10.20944/preprints202409.1325.v1

1.4.2. Encryption Methods

Symmetric Algorithms: Symmetric encryption is efficient for large volumes of encryption at one time, otherwise known as bulk encryption (SaberiKamarposhti, Ghorbani and Yadollahi, 2024). Ransomware uses this function to encrypt the victim's files and data to ensure it is not retrievable. (Check Point Software, n.d.)

Asymmetric Algorithms: Symmetric encryption keys are safeguarded by asymmetric encryption (Parekh et al., 2023; Gopi et al., 2021). Ransomware can use the public key if it is bundled with malware to encrypt files and store the symmetric key (Nagar, 2024; Lim et, al., 2019; Saeed et, al., 2020). After the ransom is paid, the attacker just needs the private key to decrypt the symmetric key. (Check Point Software, n.d.)

2.0. Crypto Ransomware Case Scenario

In this section, we will discuss and roughly elaborate on the details of the organizations that have been attacked by crypto-ransomware: Kaseya, Travelex, and the U.S. Colonial Pipeline.

2.1. Kaseya Case Scenario

On the 2nd of July 2021, Kaseya, which is an IT solution organization for companies, was invaded by ransomware in their product called VSA which enables small and medium-scale businesses to remotely observe and monitor their computer systems while providing an automatic routine responsible for the businesses' server maintenance and security updates. The attacker of this case is REvil, which is a group of cybercriminals. The ransomware utilized by REvil was sent to the customers and injected into the organization systems (Niveditha, Kunwar and Kumar, 2024; Alkinani et al., 2021; Sangkaran et, al., 2019 and 2020). This ransomware is used to encrypt their data, forcing victims to pay the ransom to retrieve their data. As of the 23rd of July 2021, REvil had demanded approximately $70 million in ransom through cryptocurrency (Allen, 2022; Shah et, al., 2024).

2.2. Travelex Case Scenario

On the 31st of December 2019, Travelex, which is a London-based foreign currency exchange, was unfortunately infiltrated by the cybercrime group Sodinokibi otherwise known as REvil. REvil injected ransomware that crippled the network and stole approximately 5GB worth of customer data, which included date of birth, credit card information and details of insurance. This attack was horrible for Travelex since their network and system were completely crippled, forcing all business operations to transition to pen and paper for the time being (Murphy, 2024; Dogra et al., 2021; Vijayalakshmi et, al., 2021). This meant that many high street banks that depended on their currency services had been impacted. According to reports, this ransomware attack by REvil had cost the organization approximately $30 million in losses and forced their parent company, Finablr, under large financial stress. Ultimately, the ransom to retrieve organization and customer data costs around $2.3 million. (Nish, A., Naumann, S. and Muir, J., 2022)

2.3. Colonial Pipeline Case Scenario

On May 7th, 2021, a ransomware attack occurred on the Colonial Pipeline, a major US fuel pipeline that carries over 2.7 million barrels a day and supplies eastern states with their fuel needs (Jacob, no date). The attack was from DarkSide, which is a criminal hacker organization. It was reported that the criminal organization intended to make money without creating problems for society. This attack had a massive impact not only on the state of the economy of the U.S. but also became the largest disruption in US energy Infrastructure. DarkSide demanded a ransom of $5 million in exchange for 100GB of stolen files (Stephens, 2021). Colonial Pipeline to this date has paid them over USD 4 million which is equivalent to 75 bitcoins to recover some of its data. The attack caused a disruption of fuel supply and increased fuel rates which showed the need for security throughout every part and detail of the infrastructure (Stephens, 2021).

 doi:10.20944/preprints202409.1325.v1

3.0. Crypto Ransomware Security Issues

In this section, we will analyze and discuss the security issues and vulnerabilities that enabled the attacks to happen.

3.1. Kaseya Case Security Issue

In the Kaseya Ransomware Attack, one of the major vulnerabilities and security issues was the outdated system software and lack of security patches implemented (Ispahany et al., 2024). Due to these vulnerabilities, REvil took the chance to exploit the system vulnerabilities and take advantage of the organization's information. As mentioned in the case scenario, Kaseya is an IT solution organization. This means Kaseya most likely has plenty of crucial and critical information and assets at the same time. These factors made Kaseya a favourable victim for the REvil cybercrime group.

The way REvil hacked the Kaseya system is by injecting malicious software into the organization's managed services provider (MSPs) worldwide without compromising the code of Kaseya's software codes (Hon, 2024; Usman et al., 2023; Zaman et, al., 2011). Instead, the platform that delivers its products and services to customers, which includes VSA, has been injected with ransomware. As the delivery of the VSA product occurs, the Kaseya VSA agent is deployed to Kaseya's customers through (MSPs) and then it will be deployed in the MSP customer's computer systems therefore spreading it to their customers as well. The cloud-based servers make it difficult for Kaseya to update the software in their systems, which can be set as an example for other organizations to update their software despite the nuisance it brings to ensure their security (Allen, 2022; Chesti et al., 2020). Moreover, SQL injection was also exploited by REvil, allowing them to bypass the authentication of the system and gain maximum access privileges (Pelliccione, 2021). As Kaseya did not run security patch updates frequently, REvil was able to compromise Kaseya's servers and workstations before the patches were implemented.

3.2. Travelex Case Security Issue

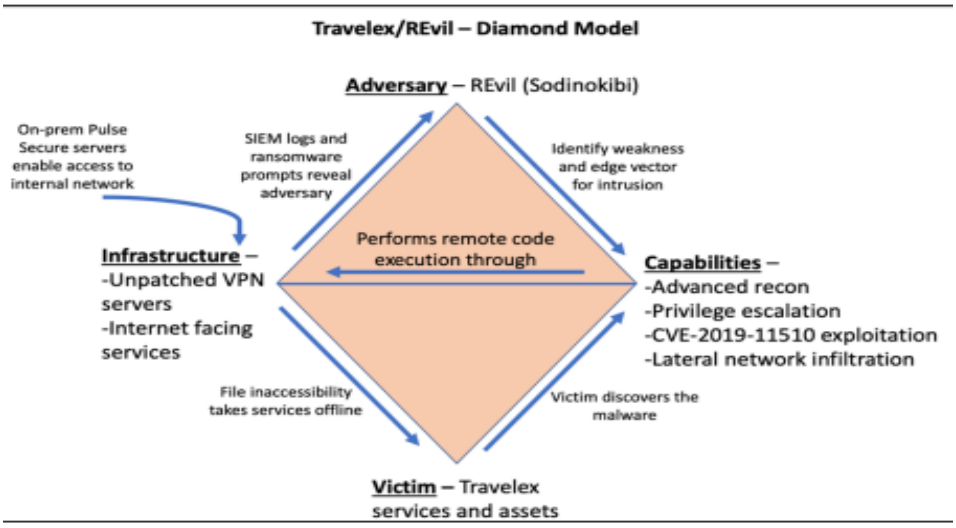

Figure 2. Travelex and REvil Diamond Model.

In the Travelex Ransomware Attack, REvil exploited the vulnerability of the system which is the Pulse Server vulnerability, and the specific medium that enabled REvil to inject the ransomware into the Travelex network (Caras, n.d.).

The pattern which enabled REvil to obtain the domain admin access is by using PsExec to install a Virtual Network Compute (VNC). The installation of VNC allowed the attackers to laterally traverse their target's network and disable endpoint security tools, which enables the exfiltration of data and the installation of REvil's malware (Caras, n.d.; Muzafar and Jhanjhi, 2020). Once the

 doi:10.20944/preprints202409.1325.v1

ransomware had been injected and installed in the Travelex network, REvil then demanded the ransom through Bitcoin as it is a decentralized block-chaining currency. The reason behind the utilization of cryptocurrency as the medium for ransom is due to the anonymity and capability to avoid alarming investigating officials (Caras, n.d.).

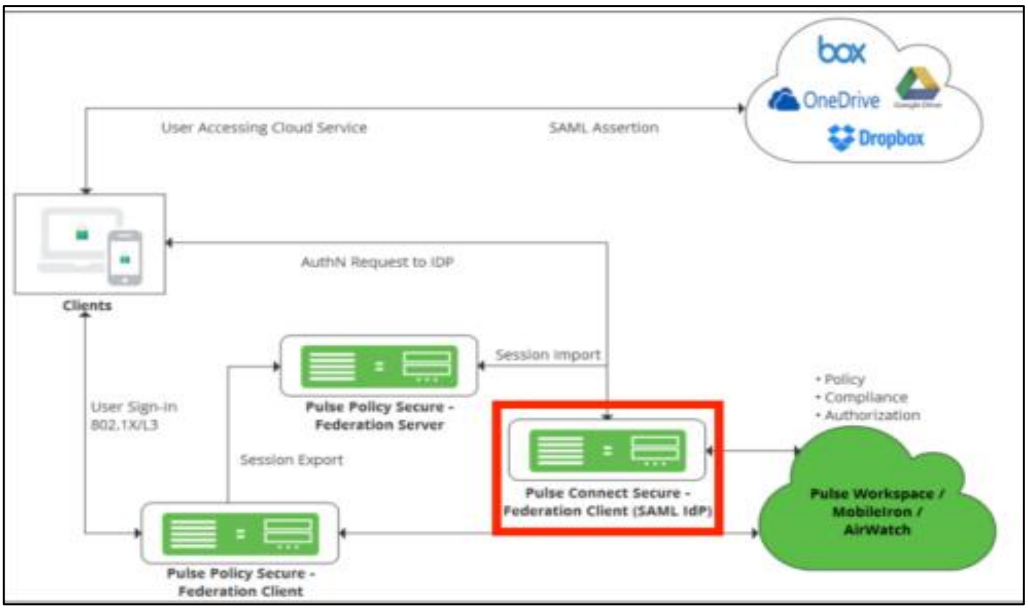

Figure 3. Travelex Vulnerability and Exploit Diagram.

Moreover, another vulnerability that was exploited by REvil was the unpatched and weak Pulse Connect Secure VPN that was implemented in the Travelex network. This weak and unpatched VPN allowed for malicious network infiltration of the ransomware strain, which enables the connectivity between the attacker and the victim. Travelex keeps their servers on-premises in the Travelex datacenter, however, the lack of diligence by the system administrators caused the affected servers to be left unpatched for over 8 months, allowing REvil to further deploy their malware which only increased the severity of the attack (Caras, n.d.).

3.3. Colonial Pipeline Ransomware Attack Security Issue

The cause of the Colonial Pipeline ransomware attack was a vulnerability in the system that has been spotted by hackers therefore seizing the opportunity to exploit it. A year before the Colonial Pipeline attack, another organization in the U.S. called SolarWinds also left an impact on the United States as it was also a case where hackers attacked federal departments and stole modified critical information (Lazarovitz, 2021; Alferidah and Jhanjhi, 2020). This case should have been a lesson for the Colonial Pipeline due to the adverse effects it left. The vulnerability of the Colonial Pipeline attack was their failing infrastructure and underwhelming security (Ford, 2021; Brohi et al., 2020).

Early evidence of compromised data was shown in reports on the 29th of April 2021 where the attackers had gained access to the organization's network through a legacy VPN and spoofed to pretend to be an employee using the employee's credentials. However, the organization did not implement simple preventive measures such as multifactor authentication when logging into the network, therefore it took little effort for the attacker to access the system and compromise the data (Ratnayake, 2021; Jhanjhi, Humayun and Almuayqil, 2021). Due to this mistake of not implementing preventive measures, the attacker could access and hack the system easily. This mistake also caused many citizens to experience fuel shortages as it forced the U.S. oil fuel pipeline to shut down. This case of the Colonial Pipeline Attack should be an example for other organizations to stay alert and aware of their security systems.

4.0. Crypto Ransomware Potential Threats

 doi:10.20944/preprints202409.1325.v1

In this section, we will discuss the potential threats and risks that will happen if no action or countermeasures are taken to mitigate the ransomware attacks.

4.1. Kaseya

The potential threats that Kaseya would face if they did not mitigate the ransomware attack are the loss of organizational reliability and trustability, loss of critical organizational data, and destruction of reputation.

As Kaseya is an IT solution company, it provides cybersecurity solutions and other IT-related services to other businesses. However, if Kaseya did not manage to properly mitigate and control the situation of the ransomware attack, their reliability and trustability from customers will be completely lost as they can't even provide a solution for their attacks. Besides, if Kaseya did not mitigate the ransomware attack, critical information such as customer data, organizational data, and so on would be in the hands of the attackers. This highly important data will be exploited by the attackers and more parties will be affected by the cybercrime group. Following all the previously stated threats, the reputation of Kaseya will be ruined and will lead the organization to go down a rabbit hole of failures.

4.2. Travelex

There are many potential threats and risks that Travelex would face if no mitigation techniques were implemented. When Travelex was attacked, there was potential for REvil to delete the shadow copies in the system which would have made it difficult for Travelex. Besides, REvil can exploit vulnerabilities in the servers and networks by utilizing remote launch attacks. This will enable REvil to take much more control over the company servers and networks.

Another threat that REvil could have caused is data leakage. This is because REvil has access to the victim's data and is capable of publishing those data. Moreover, REvil also could have potentially manipulated the victims into paying the ransom. This is because REvil could have lied to the victim to make them pay the ransom to keep their data private and retrieve it. Additionally, REvil could have saved a copy of all victim data after the ransom was paid as there is no guarantee that the retrieved data is safe (Deochakke and Tyagi, 2022).

REvil has a very high severity on the operating system such as Windows and Linux (S and Shanker, 2023; Wen et al., 2023). Therefore, another potential threat is the lack of expertise and basic understanding of operating systems might cause the organization to be intruded by ransomware. This is because most attacks that REvil carry out are targeted towards smaller and medium organizations. After the intrusion into the operating system, REvil can then inject its malware and collect data from the organizations (Datta and Acton, 2022).

4.3. Colonial Pipeline

Before we discuss the potential threats, let's first discuss what were the consequences of the ransomware attack. First, Colonial Pipeline had to shut down its operation for approximately five days which caused a shortage of gasoline, diesel fuel and jet fuel in local areas. Locals were filling bags with fuel, afraid of not being able to attend work or send their kids to school. Economically, fuel prices were at their all-time high in 7 years. Tsvetan Tsevetanov, associate professor of economics at the University of Kansas, discovered that the incident led to a 4 cents-per-gallon increase in average gasoline prices in affected areas. (KU News, 2021; Sindiramutty et al., 2024).

The potential threat of the possibility of a halt on the operation of the Colonial Pipeline if countermeasures weren't deployed is the decline of the state of the economy. In general, if any pipeline were to cease its operation due to an attack, it could cause fluctuation in the economy. Prices of gasoline, diesel fuel and jet fuel will increase as there is no new fuel coming. With that it could start a chain reaction, if a major pipeline such as the Colonial Pipeline ceases to operate, it can cause the value of cars to slowly fall. This will also lead to a loss of revenue for the vehicle industry.

 doi:10.20944/preprints202409.1325.v1

Another threat that may emerge is social consequences. Fuels are used to power transportation such as buses, cars and taxis. Being short on these resources will heavily impact citizens who rely on this transportation to get by such as work, school etc.

5.0. Crypto Ransomware Countermeasures

5.1. Kaseya

5.1.1. Kaseya Countermeasure

As the vulnerability in the unpatched software gave the cybercrime group REvil unauthorized access to the VSA system, it enabled them to encrypt the critical files and ensure that the organization would not be able to access it unless they paid the ransom (Ologunde, 2024). However, Kaseya did not end up paying the ransom as they had a countermeasure to this situation. On the 4th of July, Kaseya identified the root cause of the attack by analyzing the system and came up with a recovery and patch plan. After analyzing, Kaseya published a summary regarding the ransomware attack and what they did to mitigate it (Sharma et al., 2024; Sindiramutty, 2024). One of the ways Kaseya has mitigated the attack is by removing some VSA functionality out of caution. Moreover, Kaseya has implemented new security measures such as SaaS servers by FireEye and enablement of enhanced WAF capabilities to enhance the security and monitoring of the system (Osborne, 2021).

After that, Kaseya published two run books which are "VSA SaaS Startup Guide" and "On-Premises VSA Startup Readiness Guide" to help their customers prepare to return to the service and patch deployment. This process took a long time and had delays. However, on the 12th of July, Kaseya released a patch and worked on the on-premises customers to implement the security fix, enabling 100% of their SaaS customers to work live (Osborne, 2021; Sindiramutty, Tee, et al., 2024). Nevertheless, on the 22nd of July, Kaseya managed to secure the decryption key to the encrypted organizational and customer files. This decryption key was retrieved by a third-party organization and the decryption key and Kaseya denied paying for the decryption key (Osborne, 2021).

5.1.2. Proposed Countermeasure for Kaseya

In the case of a ransomware attack, an organization should never pay the ransom. As the attacker encrypts and steals data from the organization, there is a large possibility that the attacker has copied the critical organizational files and data that could be exploited. Therefore, the better way to approach the ransomware attack is to utilize BitDefender Anti-Ransomware tools (Muslim et al., 2019). Bitdefender Anti-Ransomware tools are crucial for providing full protection against crypto-ransomware as once the anti-ransomware software is run in the computer system and network, it detects and identifies any infections before the malware spreads to other files and computers in the network (Filiz et al., 2021; Sindiramutty, Tan, Lau, et al., 2024). Besides, the splash screen in the software will stop the infection sections running executing, therefore preventing it from spreading to other locations. Moreover, the anti-ransomware software will also turn on protection from the computer boot (Muslim et al., 2019).

Moving on, the Avast Anti-Ransomware tool could also be implemented to fight against ransomware as it is designed to detect and fight against malware and ransomware threats. Avastdecryptors is a free-of-charge tool that provides a decryption wizard which neutralizes the active ransomware after the users restart their PC. As the PC is restarting, Avast decryptors will decrypt organizational and customer data (blog.avast.com, n.d.).

5.2. Travelex

5.2.1. Travelex Countermeasure

The countermeasures Travelex has tried to implement which will mitigate the ransomware attack is by deploying a specialist team consisting of IT and computer externalist security experts. The specialist team were continuously working during New Year's Eve to exterminate the virus and have the affected system restored to its default. The chief executive of Travelex, Tony D'Souza, had

 doi:10.20944/preprints202409.1325.v1

informed users that Travelex had to temporarily halt their service to contain the virus and protect the data. This action has caused many inconveniences as Travelex provides services to multiple high street banks that depend on their currency.

Besides, Tony D'Souza, chief executive of Travelex mentioned to the public that contaminated and infected services must be stopped. The reason behind the stoppage of services is to contain the virus and protect the organizational data. However, Jake Davis, a computer security expert mentioned that the Travelex website and services are inconsistent as it would abruptly shut down (ComputerWeekly.com, n.d.).

Despite the discussions regarding countermeasures that would mitigate the ransomware attack, Travelex ended up paying the ransom which cost $2.3 million. After paying the ransom, Travelex was back to operating on the 17th of January 2020 (BleepingComputer, n.d.).

5.2.2. Proposed Countermeasure for Travelex

There are better measures that could have been taken by Travelex as they have paid the ransom. The measures that Travelex could have implemented include utilizing an intelligent ransomware protection called Lepide Data Security. This ransomware protection provides solutions that help organizations analyze and identify the symptoms of an attack that is in progress and act defensively against it. It works by a combination of multiple threat models, real-time threat responses and threshold alerting. Lepide helps the organization to also reduce the risk of the chance of a threat surface. Using Lepide can help you identify inactive users and enable you to remove all the users that are inactive in the system, as well as open shares and misconfiguration of the bad practices that the company has made involving the Active Directory. With all the features Lepide can give, it ultimately reduces the risk and damage of what a ransomware attack could do and remains compliant (Robinson, 2023).

In addition, Travelex has the option to do routine software, database server, and VPN patch updates to guarantee security. Additionally, Travelex might make use of Commvault, a well-known supplier of database management solutions with support for disaster recovery and backup. Moreover, Commvault gives businesses access to a cloud data management platform for data management. Users and companies can completely manage their data across files, applications, clouds, and hypervisors with Commvault (King, 2023).

5.3. Colonial Pipeline

5.3.1. Colonial Pipeline Countermeasure

A proper countermeasure was never performed as Colonial Pipeline had to pay a ransom worth more than USD 4 million in Bitcoin. Colonial Pipeline had to shut down the pipeline to avoid any more spread of the ransomware. Considering that it was during the COVID-19 era and most employees were working at home, it forced the organization to use unsecured networks and remote access tools such as VNC, Team Viewer etc. For enterprises, these unprotected distant connections pose a serious risk.

As Colonial Pipeline employees utilized unsecured networks and remote access tools, it is detrimental for employees to secure their endpoints such as mobile phones, laptops, desktops, etc. They connect to a computer network to exchange information. An unsecured endpoint poses a massive threat to the employee and their company, basically letting hackers easily attack you. This is because cybercriminals will highly likely target endpoints. After all, they act as the doorway to corporate data and are very vulnerable to attacks. By securing endpoints, the likelihood of getting breached and attacked will be slimmer.

5.3.2. Proposed Countermeasure for Colonial Pipeline

A countermeasure to prevent any ransomware attack from happening ever again is to enhance endpoint security. To do so, implementation of the Principle of Least Privilege (PoLP) can be done especially when employees are working remotely from home. PoLP is an information security

 doi:10.20944/preprints202409.1325.v1

concept that maintains the access of a user to specific data, resources and applications needed to complete a task. To implement PoLP, employees must have access to only the data, resources, applications, and application functionalities necessary to complete their tasks. The principle of least privilege strikes a balance between security and usability to safeguard sensitive information and systems. To do this, attack surfaces are decreased, cyberattacks are restricted, operational performance is improved, and the consequences of human error are minimized.

Another countermeasure that can be implemented is securing remote access through Privileged Access Management (PAM) and identity authentication. Privileged Access Management (PAM) is a cybersecurity strategy to control, monitor, audit and secure all privileged identities and activities across an IT environment. With this, the possibility of external attacks and insider threats can be lowered and even prevented.

Not only that, but it also enhances operational performance. Limiting privileges to the bare minimum required for a process to carry out an approved task lowers the possibility of system or application incompatibilities and helps with lowering the risk of downtime occurring. Implementing PAM also helps with achieving and proving compliance. PAM creates a less complex and more audit-friendly environment by curbing privileged activities. PAM offers many features that help with the security of an enterprise or a company such as Multifactor Authentication, a password vault that securely stores the privileged passwords, session tracking after privileged access has been granted to employees, audit logging tools that can help the organization to comply and automated provisioning and de-provisioning to reduce insider threats.

6.0. Conclusion

Crypto ransomware is a serious threat to today's digital environment as attackers are utilizing technology for destructive ends. Over the years, cybercrime groups began to use new encryption methods, making it more difficult for individuals to retrieve their data without paying a ransom. This attack architecture includes a range of penetration techniques, such as phishing emails and hacked accounts, underscoring the importance of broad cybersecurity precautions. To minimize the possibility of becoming a victim of ransomware attacks, avoidance strategies should be placed top of mind on secure data backups, user education, and strong security protocols.

Throughout this report, we have researched and studied the crypto-ransomware attacks on Kaseya, Travelex, and Colonial Pipeline. There were plenty of similar aspects between the three organizations that allowed the attacks to happen. It is concluded that these three organizations had critical security flaws and vulnerabilities in their system and network which enabled cybercrime groups to inject their ransomware into the system. The purpose behind the attacks is also similar, which is to access and lock critical organizational data. By having access to critical data, the attackers can send threats of leaking data to the organization which will make them consider paying the ransom. However, from this report, we have learnt that paying the ransom is not a good option in most cases. This is because the attackers may have downloaded a copy of the files and data, which doesn't ensure the security and privacy of the data.

In conclusion, throughout this report, we have learnt a lot about crypto-ransomware. With that said, we hope to raise awareness and alert digital users about the harm and danger that ransomware holds. The link to the video below is a guide for digital users to prevent themselves from getting into ransomware and malware attacks.

References

1. BleepingComputer. (n.d.). Travelex Reportedly Paid $2.3 Million Ransom to Restore Operations. [online] Available at: https://www.bleepingcomputer.com/news/security/travelex-reportedly-paid-23-million-ransom-to-restore-operations/.
2. blog.avast.com. (n.d.). Avast releases a free decryption tool for EncrypTile ransomware. [online] Available at: https://blog.avast.com/avast-releases-free-decryption-tool-for-encryptile-ransomware [Accessed 6 Jun. 2024].

3. Alauthman, M. et al. (2024) 'Malware Threats Targeting Cryptocurrency: A Comparative Study,' *2024 2nd International Conference on Cyber Resilience (ICCR)* [Preprint]. https://doi.org/10.1109/iccr61006.2024.10532846.
4. Alferidah, D.K. and Jhanjhi, N. (2020) 'Cybersecurity Impact over Bigdata and IoT Growth,' *2020 International Conference on Computational Intelligence (ICCI)* [Preprint]. https://doi.org/10.1109/icci51257.2020.9247722.
5. Alkinani, M.H. et al. (2021) '5G and IoT Based Reporting and Accident Detection (RAD) System to Deliver First Aid Box Using Unmanned Aerial Vehicle,' *Sensors*, 21(20), p. 6905. https://doi.org/10.3390/s21206905.
6. Allen, J. (2022, June 15). Kaseya Ransomware Attack Explained By Experts. PurpleSec. Retrieved November 15, 2022, from https://purplesec.us/kaseya-ransomware-attackexplained/#Responde
7. Almoysheer, Najd, Mamoona Humayun, and N. Z. Jhanjhi. "Enhancing Cloud Data Security using Multilevel Encryption Techniques." Turkish Online Journal of Qualitative Inquiry 12, no. 3 (2021).
8. Alsharif, Mohammed H., Abu Jahid, Anabi Hilary Kelechi, and Raju Kannadasan. "Green IoT: A review and future research directions." Symmetry 15, no. 3 (2023): 757.
9. Brohi, S.N. et al. (2020) 'Key Applications of State-of-the-Art Technologies to Mitigate and Eliminate COVID-19.pdf,' *Techrxiv* [Preprint]. https://doi.org/10.36227/techrxiv.12115596.v1.
10. Caras, C. (n.d.). Diamond Model of Intrusion Analysis -Travelex Ransomware Attack. [online] Available at: https://repository.gatech.edu/server/api/core/bitstreams/c57ffb71-bcb0-42da-bc85-977db9858952/content [Accessed 5 Jun. 2024].
11. Chesti, I.A. et al. (2020) 'Evolution, Mitigation, and Prevention of Ransomware,' *2020 2nd International Conference on Computer and Information Sciences (ICCIS)* [Preprint]. https://doi.org/10.1109/iccis49240.2020.9257708.
12. Chimmanee, K. and Jantavongso, S. (2024) 'Digital forensic of Maze ransomware: A case of electricity distributor enterprise in ASEAN,' *Expert Systems With Applications*, p. 123652. https://doi.org/10.1016/j.eswa.2024.123652.
13. ComputerWeekly.com. (n.d.). Suspected ransomware attack causes worldwide disruption for Travelex. [online] Available at: https://www.computerweekly.com/news/252476220/Suspected-ransomware-attack-causes-worldwide-disruption-for-Travelex.
14. CrowdStrike (2021). A Brief History of Ransomware | CrowdStrike. [online] crowdstrike.com. Available at: https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/.
15. Datta, P.M. and Acton, T. (2022) 'From disruption to ransomware: Lessons From hackers,' *Journal of Information Technology Teaching Cases*, 13(2), pp. 182–192. https://doi.org/10.1177/20438869221110246.
16. Deochakke, A. and Tyagi, A.K. (2022) 'Analysis of ransomware security on cloud storage systems,' in *Communications in computer and information science*, pp. 47–59. https://doi.org/10.1007/978-3-031-23724-9_5.
17. Dogra, V. et al. (2021) 'Analyzing DistilBERT for Sentiment Classification of Banking Financial News,' in *Lecture notes in networks and systems*, pp. 501–510. https://doi.org/10.1007/978-981-16-3153-5_53.
18. Fatima-Tuz-Zahra, N. et al. (2020) 'Proposing a Hybrid RPL Protocol for Rank and Wormhole Attack Mitigation using Machine Learning,' *2020 2nd International Conference on Computer and Information Sciences (ICCIS)* [Preprint]. https://doi.org/10.1109/iccis49240.2020.9257607.
19. Filiz, B. et al. (2021) 'On the Effectiveness of Ransomware Decryption Tools,' *Computers & Security*, 111, p. 102469. https://doi.org/10.1016/j.cose.2021.102469.
20. Ford, E. W. (2021). Cyber ransom in the information age: A call to arms against the hackers. Journal of Healthcare Management, 66(4), 243–245. https://doi.org/10.1097/jhm-d-21- 00161
21. Goenka, R., Chawla, M. and Tiwari, N. (2023) 'A comprehensive survey of phishing: mediums, intended targets, attack and defence techniques and a novel taxonomy,' *International Journal of Information Security* [Preprint]. https://doi.org/10.1007/s10207-023-00768-x.
22. Gopi, R. et al. (2021) 'Enhanced method of ANN based model for detection of DDoS attacks on multimedia internet of things,' *Multimedia Tools and Applications*, 81(19), pp. 26739–26757. https://doi.org/10.1007/s11042-021-10640-6.
23. Gouda, W. et al. (2022) 'Detection of COVID-19 based on chest x-rays using deep learning,' *Healthcare*, 10(2), p. 343. https://doi.org/10.3390/healthcare10020343.
24. Gaur, L. & Jhanjhi, N. Z. (Eds.). (2023). Digital Twins and Healthcare: Trends, Techniques, and Challenges. IGI Global. https://doi.org/10.4018/978-1-6684-5925-6
25. Ghani, Norjihan Binti Abdul, Suraya Hamid, Muneer Ahmad, Younes Saadi, N. Z. Jhanjhi, Mohammed A. Alzain, and Mehedi Masud. "Tracking Dengue on Twitter Using Hybrid Filtration-Polarity and Apache Flume." Comput. Syst. Sci. Eng. 40, no. 3 (2022): 913-926.
26. H. Ashraf, F. Khan, U. Ihsan, F. Al-Quayed, N. Z. Jhanjhi and M. Humayun, "MABPD: Mobile Agent-Based Prevention and Black Hole Attack Detection in Wireless Sensor Networks," 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2023, pp. 1-11, doi: 10.1109/ICBATS57792.2023.10111277.

27. H. Ashraf, M. Hanif, U. Ihsan, F. Al-Quayed, M. Humayun and N. Jhanjhi, "A Secure and Reliable Supply chain management approach integrated with IoT and Blockchain," 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2023, pp. 1-9, doi: 10.1109/ICBATS57792.2023.10111371
28. Hon, K.W. (2024) 'Security risks and concepts,' in Edward Elgar Publishing eBooks, pp. 141–157. https://doi.org/10.4337/9781803923918.00017.
29. Humayun, M. et al. (2022) 'A Transfer Learning Approach with a Convolutional Neural Network for the Classification of Lung Carcinoma,' Healthcare, 10(6), p. 1058. https://doi.org/10.3390/healthcare10061058.
30. Humayun, M., N. Z. Jhanjhi, B. Hamid, and G. Ahmed. "Emerging smart logistics and transportation using IoT and blockchain. IEEE Internet of Things Magazine, 3 (2), 58-62." (2020).
31. Humayun, M., Khalil, M. I., Alwakid, G., & Jhanjhi, N. Z. (2022). Superlative feature selection based image classification using deep learning in medical imaging. Journal of Healthcare Engineering, 2022(1), 7028717.
32. Ispahany, J. et al. (2024) 'Ransomware detection using machine learning: A review, research limitations and future directions,' IEEE Access, 12, pp. 68785–68813. https://doi.org/10.1109/access.2024.3397921.
33. Jacob, S. (no date) The Rapid Increase of Ransomware Attacks Over the 21st Century and Mitigation Strategies to Prevent Them from Arising. https://digitalcommons.liberty.edu/honors/1326/.
34. Javaid, Mohd, Abid Haleem, Ravi Pratap Singh, Shahbaz Khan, and Rajiv Suman. "An extensive study on Internet of Behavior (IoB) enabled Healthcare-Systems: Features, facilitators, and challenges." BenchCouncil Transactions on Benchmarks, Standards and Evaluations 2, no. 4 (2022): 100085.
35. Jhanjhi, N., Humayun, M. and Almuayqil, S.N. (2021) 'Cyber security and privacy issues in industrial internet of things,' Computer Systems Science and Engineering, 37(3), pp. 361–380. https://doi.org/10.32604/csse.2021.015206.
36. Jhanjhi, N. Z., Sahil Verma, M. N. Talib, and Gagandeep Kaur. "A canvass of 5G network slicing: Architecture and security concern." In IOP Conference Series: Materials Science and Engineering, vol. 993, no. 1, p. 012060. IOP Publishing, 2020.
37. King, T. (2023). The 28 Best Database Management Systems & Software for 2024. [online] Best Data Management Software, Vendors and Data Science Platforms. Available at: https://solutionsreview.com/data-management/the-best-database-management-systems-and-software-tools/ [Accessed 8 Jun. 2024].
38. KU News, Jon Niccum. (2021). Cyberattack on Colonial Pipeline affected gas prices far less than initially reported, study finds. Retrieved from https://news.ku.edu/news/article/2021/12/16/cyberattack-colonial-pipeline-affected-gas-prices-far-less-initially-reported-study-finds#:~:text=While%20in%20May%2C%20fuel%20prices,largest%20for%20refined%20oil%20products.
39. Kumari, A. and Sharma, I. (2024) 'Mitigating Malvertising Threats: An Exploration of Machine Learning Classification Algorithms for Effective Detection,' *2024 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC)* [Preprint]. https://doi.org/10.1109/assic60049.2024.10508033.
40. Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). A review of intrusion detection system using machine learning approach. International Journal of Engineering Research and Technology, 12(1), 8-15.
41. Lim, Marcus, Azween Abdullah, N. Z. Jhanjhi, Muhammad Khurram Khan, and Mahadevan Supramaniam. "Link prediction in time-evolving criminal network with deep reinforcement learning technique." IEEE Access 7 (2019): 184797-184807.
42. Lazarovitz, L. (2021). Deconstructing the solarwinds breach. Computer Fraud & Security, 2021(6), 17–19. https://doi.org/10.1016/s1361-3723(21)00065-8
43. Lim, K., Park, J. and Kim, D. (2024) 'Phishing Vs. Legit: Comparative Analysis of Client-Side Resources of Phishing and Target Brand Websites,' *ACM* [Preprint]. https://doi.org/10.1145/3589334.3645535.
44. Longtchi, T.T. et al. (2024) 'Internet-Based Social Engineering Psychology, Attacks, and Defenses: A survey,' *Proceedings of the IEEE*, pp. 1–37. https://doi.org/10.1109/jproc.2024.3379855.
45. Murphy, G.J. (2024) 'Conclusion: accessible moments and darkness on the edge of town,' in *Palgrave science fiction and fantasy*, pp. 93–112. https://doi.org/10.1007/978-3-031-56627-1_6.
46. Muslim, A.K., Dzulkifli, D.Z.M., Nadhim, M.H. and Abdellah, R.H. (2019). A Study of Ransomware Attacks: Evolution and Prevention. Journal of Social Transformation and Regional Development, [online] 1(1), pp.18–25. Available at: https://publisher.uthm.edu.my/ojs/index.php/jstard/article/view/5503/3327.
47. Muzafar, S. and Jhanjhi, N.Z. (2020) 'Success stories of ICT implementation in Saudi Arabia,' in *Advances in electronic government, digital divide, and regional development book series*, pp. 151–163. https://doi.org/10.4018/978-1-7998-1851-9.ch008.
48. Nagar, G. (2024) 'The Evolution of Ransomware: Tactics, techniques, and mitigation strategies,' *International Journal of Scientific Research and Management (IJSRM)*, 12(06), pp. 1282–1298. https://doi.org/10.18535/ijsrm/v12i06.ec09.
49. Nish, A., Naumann, S. and Muir, J., 2022. Enduring cyber threats and emerging challenges to the financial sector. Carnegie Endowment for International Peace..

50. Niveditha, V.S., Kunwar, R.S. and Kumar, K. (2024) 'Ransomware attacks on IoT devices,' in *Chapman and Hall/CRC eBooks*, pp. 124–147. https://doi.org/10.1201/9781003386926-7.
51. Ologunde, E. (2024) 'Ransomware,' *SSRN Electronic Journal* [Preprint]. https://doi.org/10.2139/ssrn.4823359.
52. Osborne, C. (2021). Updated Kaseya ransomware attack FAQ: What we know now. [online] ZDNet. Available at: https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/.
53. Parekh, A. et al. (2023) 'Multilayer symmetric and asymmetric technique for audiovisual cryptography,' *Multimedia Tools and Applications*, 83(11), pp. 31465–31503. https://doi.org/10.1007/s11042-023-16401-x.
54. Pelliccione, A. (2021, July 5). The ransomware threat rises to the next level: the Kaseya case, how it happened and how to defend yourself. Agenda Digitale. Retrieved 2022, from https://www.agendadigitale.eu/sicurezza/la-minaccia-ransomware-sale-di-livello-il-casokaseya-come-successo-e-come-difendersi
55. Robinson, P. (2023). What is REvil/Sodinokibi Ransomware. [online] Lepide Blog: A Guide to IT Security, Compliance and IT Operations. Available at: https://www.lepide.com/blog/what-is-revil-sodinokibi-ransomware/.
56. S, A.C. and Shanker, R. (2023) 'Zero Trust Resilience Strategy for Linux Crypto Ransomware Obviation and Recuperation,' *2023 3rd International Conference on Intelligent Technologies (CONIT)* [Preprint]. https://doi.org/10.1109/conit59222.2023.10205545.
57. S, K.P.D. and R, P.K.H. (2024) 'A Systematic Study on Ransomware Attack: Types, Phases and Recent Variants,' *2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)* [Preprint]. https://doi.org/10.1109/icicv62344.2024.00110.
58. SaberiKamarposhti, M., Ghorbani, A. and Yadollahi, M. (2024) 'A comprehensive survey on image encryption: Taxonomy, challenges, and future directions,' *Chaos Solitons & Fractals*, 178, p. 114361. https://doi.org/10.1016/j.chaos.2023.114361.
59. Saeed, Soobia, Afnizanfaizal Abdullah, N. Z. Jhanjhi, Mehmood Naqvi, Mehedi Masud, and Mohammed A. AlZain. "Hybrid GrabCut Hidden Markov Model for Segmentation." Computers, Materials & Continua 72, no. 1 (2022).
60. Sangkaran, Theyvaa, Azween Abdullah, and N. Z. Jhanjhi. "Criminal community detection based on isomorphic subgraph analytics." Open Computer Science 10, no. 1 (2020): 164-174.
61. Sangkaran, Theyvaa, Azween Abdullah, N. Z. JhanJhi, and Mahadevan Supramaniam. "Survey on isomorphic graph algorithms for graph analytics." International Journal of Computer Science and Network Security 19, no. 1 (2019): 85-92.
62. Shah, I. A., Jhanjhi, N. Z., & Ujjan, R. M. (2024). Drone Technology in the Context of the Internet of Things. In I. Shah & N. Jhanjhi (Eds.), Cybersecurity Issues and Challenges in the Drone Industry (pp. 88-107). IGI Global. https://doi.org/10.4018/979-8-3693-0774-8.ch004
63. Shah, I. A., Jhanjhi, N. Z., & Ray, S. K. (2024). Artificial Intelligence Applications in the Context of the Security Framework for the Logistics Industry. In M. Ghonge, N. Pradeep, N. Jhanjhi, & P. Kulkarni (Eds.), Advances in Explainable AI Applications for Smart Cities (pp. 297-316). IGI Global. https://doi.org/10.4018/978-1-6684-6361-1.ch011
64. Sharma, S. et al. (2024) 'Implementation Analysis of Ransomware and Unmanned Aerial Vehicle Attacks,' *Wiley*, pp. 165–211. https://doi.org/10.1002/9781394175512.ch9.
65. Sindiramutty, S.R. (2024) 'Autonomous Threat Hunting: a future paradigm for AI-Driven Threat intelligence,' *arXiv (Cornell University)* [Preprint]. https://doi.org/10.48550/arxiv.2401.00286.
66. Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Khan, N. A., Gharib, A. H., & Yun, K. J. (2024). Applications of Blockchain Technology in Supply Chain Management. In N. Jhanjhi & I. Shah (Eds.), Cybersecurity Measures for Logistics Industry Framework (pp. 248-304). IGI Global. https://doi.org/10.4018/978-1-6684-7625-3.ch009
67. Sindiramutty, S.R., Tan, C.E., Lau, S.P., et al. (2024) 'Explainable AI for cybersecurity,' in *Advances in computational intelligence and robotics book series*, pp. 31–97. https://doi.org/10.4018/978-1-6684-6361-1.ch002.
68. Sindiramutty, S.R., Tan, C.E., Tee, W.J., et al. (2024) 'Modern smart cities and open research challenges and issues of explainable artificial intelligence,' in *Advances in computational intelligence and robotics book series*, pp. 389–424. https://doi.org/10.4018/978-1-6684-6361-1.ch015.
69. Sindiramutty, S.R., Tee, W.J., et al. (2024) 'Explainable AI in healthcare application,' in *Advances in computational intelligence and robotics book series*, pp. 123–176. https://doi.org/10.4018/978-1-6684-6361-1.ch005.
70. Stephens, T. G. (2021). Lessons learned: The colonial pipeline ransomware attack. California C.P.A.
71. Usman, T.M. et al. (2023) 'Diabetic retinopathy detection using principal component analysis multi-label feature extraction and classification,' *International Journal of Cognitive Computing in Engineering*, 4, pp. 78–88. https://doi.org/10.1016/j.ijcce.2023.02.002.

 doi:10.20944/preprints202409.1325.v1

72. Vijayalakshmi, B., Ramar, K., Jhanjhi, N. Z., Verma, S., Kaliappan, M., & Vijayalakshmi, K. & Ghosh, U.(2021). An attention-based deep learning model for traffic flow prediction using spatiotemporal features towards sustainable smart city. International Journal of Communication Systems, 34(3), e4609.
73. Wen, B.O.T. et al. (2023) 'Detecting cyber threats with a Graph-Based NIDPS,' in Advances in logistics, operations, and management science book series, pp. 36–74. https://doi.org/10.4018/978-1-6684-7625-3.ch002.
74. Zaman, Noor, and Azween B. Abdullah. "Position responsive routing protocol (prrp)." In 13th International Conference on Advanced Communication Technology (ICACT2011), pp. 644-648. IEEE, 2011.