Review

In-Depth Analysis and Countermeasures for Ransomware Attacks: Case Studies and Recommendations

Yap Jia Seng , Teo Yue Cen , Muhammad Amar Hakim bin Mohd Raslan , Miteshwara Rao Subramaniam , Lim Yi Xin , Say Jun Kin , Moh Shao Long , Siva Raja Sindiramutty *

Posted Date: 2 September 2024

doi: 10.20944/preprints202408.2261.v1

Keywords: ransomware; cybersecurity; case studies; security issues; countermeasures

Review

In-Depth Analysis and Countermeasures for Ransomware Attacks: Case Studies and Recommendations

Yap Jia Seng, Teo Yue Cen, Muhammad Amar Hakim bin Mohd Raslan, Miteshwara Rao Subramaniam, Lim Yi Xin, Say Jun Kin, Moh Shao Long and Siva Raja Sindiramutty *

School of Computer Science Taylor's University Subang Jaya; siva.sindiramutty@taylors.edu.my

ABSTRACT: Ransomware, a combination of "ransom" and "malware," is a type of malicious software designed to encrypt or block access to a victim's data or system, demanding a ransom for its release Initially targeting individuals, ransomware has evolved to attack businesses for greater financial gain. It mainly exists in two forms: encrypting ransomware, which holds data hostage, and non-encrypting ransomware, which blocks system access and displays a ransom note. The energy sector has been notably targeted by ransomware, exemplified by the 2021 attack on Colonial Pipeline by the DarkSide group, which led to a temporary shutdown and a significant fuel shortage on the US East Coast. Similarly, in 2023, Russian hackers using LockBit ransomware disrupted Royal Mail, halting international deliveries and incurring millions in recovery costs despite no ransom payment. These incidents underscore the need for comprehensive cybersecurity strategies that combine human vigilance with advanced technologies like AI and machine learning. By adopting a multi-layered protection approach, organizations can better prepare for and mitigate the risks posed by ransomware attacks safeguarding sensitive data and ensuring business continuity

Keywords: ransomware; cybersecurity; case studies; security issues; countermeasures

BACKGROUND

Ransomware is a portmanteau of 2 words which are ransom and malware respectively. It is malicious software that is used to block users from accessing its computer system or necessary data till a ransom is paid. Ransomware involves using encryption algorithms to encrypt the data of a targeted victim or block access of that user to accessing to its computer system (Cen et al., 2024; Ghosh et al., 2020), making him/her inaccessible to retrieve his/her information, then demanding the target victim to pay a ransom before reallow the victim to decrypt it (Raj et al., 2024). There are 2 types of ransomware where the most common type is encrypting ransomware where threat actors use locked data as hostages and demand ransom in return for the decryption key or non-encrypting ransomware (Cen et al., 2024; Sindiramutty et al., 2024) where its locked the victim's device by blocking access to its computer system and usually leads to the device displaying a screen that requests ransom.

Purpose

In the beginning, ransomware is used to target ordinary people. However, cybercriminals began to realize it as a chance for financial gain. Hence, they started to target businesses where they encrypt important data (Möller, 2023; Shahid et al., 2021). Then, these threat actors use the importance of the data they hold as hostages and force the owners of the businesses to pay the ransom. Usually, the ransom comes with a deadline and a threat of permanently deleting data if the ransom is not paid within the deadline (Teichmann, Boticiu, and Sergi, 2023; Sindiramutty, Tan, Lau, et al., 2024). However, not all ransomware is made for financial gain. At certain times, the objective of ransomware can be used for disruption, political or social activity, or cyber espionage.

 doi:10.20944/preprints202408.2261.v1

History Of Ransomware

The first ransomware can be dated back to 1989 where it's called the AIDS Trojan or PC Cyborg (Worrell, 2024). This ransomware was delivered via a floppy disk and demanded a ransom of $189 5o be delivered to a PO box in Panama. Since then, ransomware has become more and more advanced and has undergone evolution. Some notable revolutions of ransomware are such as Cryptolocker in 2013. It was found that this ransomware strain was using a sophisticated 2,048-bit RSA key, the most advanced ransomware to date at that time (Begovic, Al-Ali, and Malluhi, 2023; Singhal et al., 2020). Next was the WannaCry ransomware incident where it exploited the vulnerability of Microsoft Windows in 2017. This ransomware is also called ransomware and is spread through Eternal Blue vulnerability, an exploit leaked from the National Security Agency. has affected over 150 countries and it started on the Internet and then spread to schools, hospitals, and other public service industries (Shaikh et al., 2024; Humayun et al., 2022). Looking now, ransomware has evolved from commodity to targeted attacks via the Ransomware-as-a-Service (RaaS) model (Alqahtani and Sheldon, 2024; Sindiramutty, Tee, et al., 2024). Threat attackers now buy access from Initial Access Brokers (IABs) on the Deep Web and focus on high-revenue targets.

How does ransomware work (Architecture of ransomware)

Ransomware is being carried out in 5 stages involving infection, execution, discovery, lateral movement, deployment, and ransom demand.

- Stage 1: Infection- The infection is usually spread through a few notable methods such as email(malware) where this email contains trap attachments or links redirecting to malicious websites (Choi, Lee and Merizalde, 2023), spear phishing where the attacker impersonates as someone else which required you to click on some link via email where the email is a malware, social engineering where it uses the Trojan Horse Virus and lastly software vulnerability. These are the few common methods that will lead to infection.
- Stage 2: Execution- The execution method used is via command and control(C&C) server. Once this server is set up, the attackers will send encryption keys to the target system, download additional malware if needed facilitate the following progress, and give instructions.
- Stage 3: Discovery and lateral movement- This 2-step action involves where attackers familiarize themselves with the victim network structure, allowing them to seek out important data before launching the attack. In this stage, they will also spread the infection to other devices.
- Stage 4: Deployment- After identifying the targeted data, attackers will encrypt these data using an encryption algorithm and prevent the victim from accessing them lock the device screen and flood them with pop-ups, or disable the victim form using the computer.
- Stage 5: Ransom demand- A note will be then displayed to the victim demanding payment to regain access to its data or computer system in exchange for the decryption key.

Technologies Involved in Ransomware

Technologies used to deliver ransomware can be categorized into 3 different groups which are infection and execution, encryption, and ransom payments.

 doi:10.20944/preprints202408.2261.v1

- Infect and Execution- Attackers need a few tools to aid them in infecting and executing their attack. The tools are phishing tools, exploited kits, and commands to control servers. Phishing tools are used to create fake emails and websites that look legitimate to hook victims to click on them, while exploited kits are used to exploit vulnerabilities in the victim's system. (Öztürk. 2024), (Trendmicro. n.d.) Lastly, the command and control servers are used to obtain confidential information from a target network and issue commands to malware-infected systems. (Trendmicro. n.d.)
- Encryption- Advanced Encryption Standard (AES) and Rivest, Shamir, Adleman (RSA) are the 2 most common algorithms used for encrypting data. AES is a type of symmetric encryption algorithm that could quickly encrypt many files. (Murphy. 2023) RSA is client asymmetric encryption where there will be 2 keys- a public and a private key. RSA is used for a more secure key exchange however; it needs a much longer time to encrypt data. (Murphy. 2023)
- Ransom Payment- Payments are likely to be carried out via cryptocurrency due to its anonymity. The most common forms of cryptocurrency used for payment are Bitcoin and Monero. Bitcoin allows ease of transfer whereas Monero has been favored lately due to its enhanced security protocol which makes it harder to trace. (Gren. 2024; James, 2024)

DISCUSSION ON SECURITY ISSUES

Case 1 (Colonial Pipeline. 2021)

Figure 1. Colonial Pipeline. 2021.

Introduction

The IT network of Colonial Pipeline was subjected to a ransomware attack in May 2021 by a hacker collective known as DarkSide. Colonial Pipeline ceased operations to separate the compromised IT network from the operational technological systems, which resulted in an

 doi:10.20944/preprints202408.2261.v1

interruption in the East Coast's petroleum supply. The business paid a ransom of 75 Bitcoin, or about $4.4 million at the time, to reclaim control of its systems (Fox. 2023; Almusaylim, Zaman, and Jung, 2018, Ali, S., Hafeez, 2022). The attack shut down Colonial Pipeline's operations for approximately five days, causing localized shortages of gasoline, diesel fuel, and jet fuel (Wood. 2023; Gouda et al., 2022, Almoysheer et al., 2021, Alsharif et al.,2021). It had an impact on the airline sector, as numerous carriers, including American Airlines, saw a lack of jet fuel. Panic buying and lengthy lineups at gas stations were brought on by the fear of a petrol shortage in several states, including Florida, Georgia, Alabama, Virginia, and the Carolinas. Following the closure of the Colonial Pipeline, ordinary petrol prices at the pump also increased, reaching an all-time high of $3 per gallon (Kerner. 2022., Dogra, V., Singh et al., 2024).

Security Issues

Colonial Pipeline's IT network was successfully hacked by the DarkSide due to the deployment of an antiquated Virtual Private Network (VPN) infrastructure that lacked multifactor authentication. This implies that it may be accessed with a password alone, devoid of a second step like a text message—a typical security feature found in more modern applications (Kelly, S. & Resnick-adult. 2021; Sindiramutty, 2024; Ghani, Norjihan Binti Abdul, 2022). Furthermore, a major contributing factor to hacker success is weak password management. The perception that password security is not a concern stems from reports that the password used in the cyberattack was part of a batch of credentials that were hacked and posted on the dark web (Securelink. 2021, Gaur, L at al., 2023; H. Ashraf at el. 2023). Even though Colonial Pipeline Chief Executive Joseph Blount stated, "I want to be clear that it was a complex password. The password was not of the Colonial123 variety" (Kelly, S. & Resnick-adult. 2021; Sindiramutty, Jhanjhi, Tan, et al., 2024). However, it is still regarded as the primary cause of the DarkSide's successful hack of the IT network.

Potential Security Threats

Ransomware attacks on critical infrastructure can pose a variety of hazards, including Data Loss or Theft, Financial Loss, Operational Downtime, and so on.

Data loss or Theft: The group exploited an exposed VPN account with a reused password, stealing 100 gigabytes of data within two hours (Fox. 2023). This data could have included sensitive information such as operational details, customer data, and potentially confidential business information. Even if a ransom is paid, there is no guarantee that a threat actor will act benevolently and return the data (J.P. Morgan. 2024; Jayakumar, P., at el., 2021; Jhanjhi et. al 2020; Javaid, Mohd, Abid Haleem., at el., 2022; Kok, S. H., 2019).

Financial Loss: Ransomware is an unexpected cost, and it is expensive. In addition to the loss in revenue an organization may suffer, other costs may be obvious and some may not. More obvious costs include the cost of the ransom payment (if paid); the cost to remediate the incident, including new hardware, software, and incident response services; insurance deductibles; attorney fees and litigation; and public relations (J.P. Morgan. 2024; Lim Marcus et al., 2019). For this case, Colonial Pipeline paid a ransom of 75 bitcoins, which was approximately $4.4 million at the time, to regain control of its systems.

Operational Downtime: The attack shut down Colonial Pipeline's operations for approximately five days, causing localized shortages of gasoline, diesel fuel, and jet fuel (Wood. 2023; M Saleh, at.al, 2022; Shah at el., 2024). This resulted in operational downtime, affecting transportation and disturbing fuel along the East Coast. The shutdown led to fuel shortages, price spikes, and logistical challenges.

Lessons

What we have learned is the 'Importance of Multifactor Authentication (MFA)' and the 'Consequences of Poor Password Management'.

 doi:10.20944/preprints202408.2261.v1

For MFA, the company must ensure all systems, especially remote access points like VPNs, require multifactor authentication to enhance security. So that the technology that underpins the services that the system relies on every hour of every day is safe and secure (CISA. 2024; Sood et al., 2022). Further 'Consequences of Poor Password Management', the use of a reused or common password for accessing the VPN was a major security lapse. This highlights the need for strong password policies, including the use of unique, complex passwords and regular password changes.

Recommendations For Improving

Update legacy hardware and systems: Outdated hardware and software leave companies exposed to known vulnerabilities that make them easy targets for ransomware attacks. Keeping workplace software and devices updated eliminates vulnerabilities so that fraudsters have no entry point to break into your systems (Terranova Security. 2023; Tiwalade at. Et., 2023). Backup your data: Use a secure option to back up your data that cannot be compromised if a computer is infected with ransomware (Terranova Security. 2023). Limit administrative rights on computers: Whenever possible, reduce user privileges on endpoints and use policies that restrict access to critical systems (Terranova Security. 2023; Zaman at. El., 2011).

Routinely analyze your entire IT estate to ensure you're following best practices around the National Institute of Standards and Technology cybersecurity framework and CISA zero trust maturity model (Parsons & Knudtson and Reid. 2023).

Case 2 (Royal Mail, LockBit Ransomware. 2023)

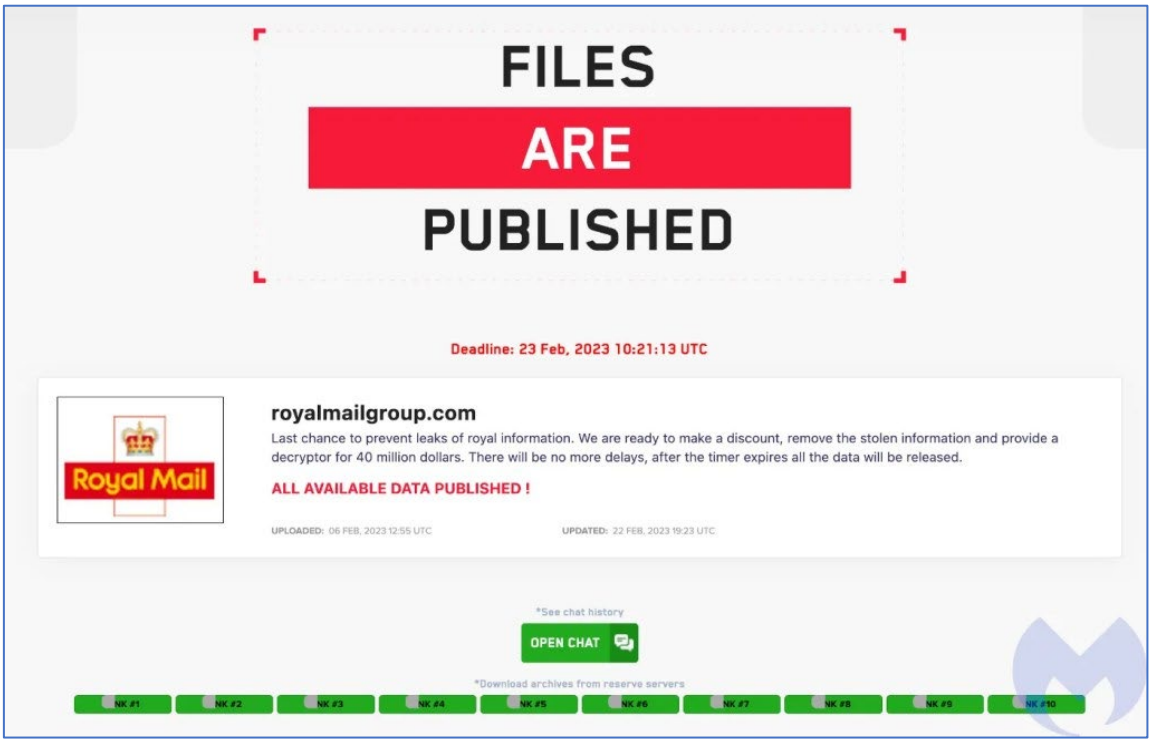

Figure 2. Royal Mail, LockBit Ransomware. 20Introduction.

Royal Mail experienced disruption in its overseas deliveries on January 12th due to a ransomware attack related to Russian criminals. The cyber-attack has compromised the computer systems essential for sending international mail, prompting Royal Mail to warn customers against sending letters and parcels abroad until the issue is resolved (Mark Sweney 2023; Fatima-Tuz-Zahra et al., 2020). The ransomware was identified as "LockBit". Attackers demanded an enormous amount of $80 million (RM342.84 million) **as** 0.5% of annual revenue from Royal Mail International, threatening to publish the stolen sensitive information if their demands were not met (Bachchas, 2024; Nayyar, Gadhavi and Zaman, 2021). However, Royal strongly disagreed with this demand,

 doi:10.20944/preprints202408.2261.v1

highlighting that it was not the substantial organization the hackers had claimed. The company explained that is a smaller subsidiary and lacked the resources that the hackers had assumed it possessed. Despite the pressure, Royal Mail stayed firm and did not pay the ransom (Rob. 2023). The efforts to remediate the January 2023 Royal Mail cyber-attack cost $12.4 million (RM54.963 million)**.** These expenses were associated with improving the **corporation's** Heathrow Worldwide Distribution Centre, which was the target of the attack (Connor. 2023). Post offices were eventually used to begin overseas delivery following the malware incident (Mark Sweney 2023).

Impact

The LockBit ransomware attack on Royal Mail in January 2023 had a massive negative financial and operational impact. The attack impacted not just the firm and its clientele but also the communications and overseas businesses of citizens. Royal Mail encountered significant disruption for six weeks after the cyberattack that restricted the company from sending certain parcels overseas at its 11,500 Post Office branches. An estimated $12.4 million would be spent on the recovery efforts, especially at the Heathrow Worldwide Distribution Centre. Royal Mail's overseas shipping operations were severely hampered by the cyberattack, which led to a 6.5% year-over-year drop in foreign revenue—a loss of $27 million. In addition, the incident caused a 5% decrease in international package volumes, which was exacerbated by poor macroeconomic circumstances and the aftermath of industrial action. IDS has lost $395.8 million over the last six months because of these delays (Connor. 2023; Humayun, Sujatha, et al., 2022).

Security Issue

LockBit attackers exposed critical vulnerabilities in Royal Mail's cybersecurity infrastructure. The Royal Mail's international shipping operations were halted when LockBit exploited security flaws to install ransomware, encrypting files and rendering them unusable. As printers at a Northern Ireland distribution facility started generating ransom notes, indicating a significant breach in Royal Mail's systems, the permeability of the hack was brought to light (Jasper. 2023).

The incident serves as a reminder of the significant security risks that modern businesses must deal with. As part of its reaction, Royal Mail notified the Information Commissioner's Office, the National Crime Agency, and the UK's National Cyber Security Centre of the breach. Depending on how serious the exposed data is and how extensive the attack was, one must decide whether to pay the ransom, which is typically requested in untraceable cryptocurrency. This attack emphasizes the necessity of robust cybersecurity defences and the value of being prepared to deal with sophisticated cyberattacks. It also serves as an example of the careful balancing act that organizations must perform when it comes to managing operational disruptions during such disasters and data protection (Niamh. 2023; Gopi et al., 2021).

Potential Security Threats

Operating Model: LockBit 3.0 also known as LockBit Black. It operates under a Ransomware-as-a-Service (RaaS) model. Its developers can rent out ransomware tools to other criminals, referred to as affiliates under this business model (Noone. 2023). These affiliates carry out criminal acts while distributing the developers a portion of the ransom payment. This commercial model makes ransomware a constant danger by increasing the frequency and reach of attacks as well as facilitating the quick spread and development of new methods (SOCRadar. 2023).

Data Breach: There are serious hazards associated with the threats of sensitive data leakage. A data breach may expose personal information, inflict damage to individuals, and result in long-term negative effects on the organization's reputation (Zulfikar. 2023). 44GB of purported Royal Mail data was made public by LockBit on their deep web blog in February 2023. The leaked data included HR records, salary and overtime payment information, network layout details, contracts with third parties, and files from an individual's OneDrive. Despite Royal Mail's confirmation that most of the

 doi:10.20944/preprints202408.2261.v1

exposed data was technical program files and administrative business data, devoid of any sensitive consumer information, there is still an enormous danger to the company's reputation. The leakage of sensitive employee information and internal documents can harm the organization's reliability and trustworthiness (Connor. 2023).

Ongoing Activity: LockBit is still in existence despite law enforcement's persistent attempts to disrupt its operations. Its resilience to the world of cybercriminals stems from its capacity for swift innovation and adaptation (Amaan. 2024).

Recommendations For Improvement

Strengthen network security, including firewalls, intrusion detection systems, and regular security audits (Fazzino. 2023). Implement robust access controls and user authentication mechanisms. Regularly update and patch software to prevent vulnerabilities. Educate employees about phishing emails, suspicious attachments, and safe online practices (Fazzino. 2023). Conduct regular security awareness training to prevent social engineering attacks. Develop and test an incident response plan to handle cyber incidents promptly (SecurityScorecard. 2024). Define roles, responsibilities, and communication channels during an attack. Backup and Recovery Strategy (Gatlan. 2023). Regularly back up critical data and systems. Test data restoration procedures to ensure quick recovery. Work closely with law enforcement agencies and cybersecurity experts. Share threat intelligence and collaborate on investigations.

DISCUSSION ON SECURITY COUNTERMEASURES

Security Countermeasures

Case 1 (Colonial Pipeline. 2021)

a) Antivirus and Antimalware

For the Colonial Pipeline case, the effectiveness of antivirus and antimalware solutions was evident in their ability to detect the ransomware attack early and mitigate its impact.

Implement Multi-Factor Authentication (MFA): The attack exploited a weak password stored on the dark web, which was linked to a VPN account. Enforcing MFA adds an extra layer of security, making it harder for unauthorized users to gain access, even if they have the password (PMA360. 2021).

Signature-Based Detection: Using signature-based detection, conventional antivirus software looks for recognized patterns or "signatures" of ransomware in files and processes. The program can erase or quarantine the threat once a match is discovered. Nevertheless, this technique is less successful against recently discovered or zero-day ransomware strains (Sergey. 2022).

Behaviour Monitoring: Behavioral monitoring is a feature of contemporary antivirus software that helps identify ransomware by keeping an eye out for odd system activity, like unannounced file encryption or connection with command-and-control servers. This method is a more proactive defensive strategy because it can detect ransomware even if it has never been seen before (Kyle. 2024).

b) Regular Backups

For Colonial Pipeline, while the exact details of their backup strategy were not disclosed, the ability to separate the compromised systems suggests they had a robust backup and disaster recovery plan in place. This approach enabled them to restore their systems once the ransom was paid and the threat actors lifted the encryption, minimizing the overall downtime and financial loss.

Secure Storage: Backups ought to be kept safe, preferably offline or in a cloud service that keeps older versions of the files and permits rollbacks to an unencrypted state. This stops malware from attacking the backup files directly (Larry. 2020).

Maintain Consistent Backups: Establish a consistent backup strategy that includes policies specifying the required frequency of backups for critical infrastructure and data. This ensures that you have a recent copy of your data that can be restored if needed (Ferdowsi. 2021).

 doi:10.20944/preprints202408.2261.v1

Protection Against Deletion: Strategies to safeguard backups can be informed by knowledge of how ransomware tries to erase them. For example, understanding that some ransomware variations target specific file types or disable the Volume Shadow Copy service can help determine where and how backups should be stored (CIS. 2023).

c) Patch Management

For Colonial Pipeline, the attackers likely exploited known vulnerabilities in their systems to gain access. The recommendation to regularly patch security vulnerabilities in operating systems and software is highlighted as a crucial measure to protect against such threats. Regular patch management ensures that these vulnerabilities are addressed promptly, reducing the window of opportunity for attackers to exploit them.

Proactive Vulnerability Management: Implement a proactive approach to managing vulnerabilities by regularly scanning systems for known vulnerabilities and applying patches as soon as they become available. This reduces the window of opportunity for attackers to exploit known vulnerabilities (Rothschild. 2021; Alkinani et al., 2021).

Preventing Initial Access: Ransomware attackers often target systems that lack the latest security patches. Software vendors release these patches to address known vulnerabilities that attackers could exploit. By consistently applying patches, organizations can greatly reduce their risk of ransomware attacks, as it limits attackers' opportunities to exploit these vulnerabilities (NLC. 2023).

Enhancing System Stability and Performance: Applying updates regularly improves the stability and performance of systems while also securing them. Patches often include enhancements and bug fixes that improve the general effectiveness and health of the system. This dual advantage emphasizes how crucial patch management is to preserving a reliable and effective computer environment (Intel. 2023).

d) Security Awareness Training

In the Colonial Pipeline case, the attack was facilitated through a weak password policy, where a reused or simple password was used for VPN access. This highlights the importance of security awareness training in educating employees about the dangers of reusing passwords and the significance of choosing complex, unique passwords. Employees should be trained to recognize and avoid phishing attempts, which are common vectors for delivering ransomware.

Implement Cybersecurity Awareness Training with Simulated Phishing Attacks: Hacking groups often use social engineering techniques, especially phishing, to compromise systems. Training programs that simulate these attacks can significantly enhance employees' ability to recognize and avoid falling victim to such tactics. This hands-on approach helps in building a culture of vigilance towards phishing attempts and other common cyber threats (TealTech. 2024).

Employee Empowerment: Employees who complete training programs will be equipped with the information and abilities needed to recognize and counteract ransomware threats. This entails seeing phishing emails, spotting dubious links and attachments, and being aware of the consequences of clicking on harmful content (Terranova Security. 2023).

Behavioural Change: Through fostering a culture of security consciousness, companies encourage their staff to adopt safer practices. To achieve this, people should be urged to carefully read emails, attachments, and adverts before responding to them. The likelihood of unintentionally clicking on harmful content is reduced in such a culture since caution is emphasized over convenience (Neko and Robert. 2021).

e) Network Segmentation

Network segmentation refers to separating a larger network into smaller sub-networks with limited connections between each sub-network. Limited access between the sub-networks results in restricted access for attacker lateral movement, network segmentation prevents unauthorized users from accessing the organization’s intellectual property and data.

Since the Colonial Pipeline network was segmented, they were able to defend against the ransomware using strong firewalls at each endpoint. (Chin, 2024). The unusual activity was also

 doi:10.20944/preprints202408.2261.v1

detected since the segmented networks provided more insights into the network's activity. (Intelligence, 2024). Faster detection allows for quicker response and prevention of infection spread, reducing the impact on the system. (Intelligence, 2024).

Case 2 (Royal Mail, LockBit Ransomware. 2023)

a) Antivirus and Antimalware

In the Royal Mail case, antivirus and antimalware solutions would have been instrumental in detecting the LockBit ransomware and alerting the IT team to the potential threat. Organizations can implement many tactics, derived from the ransomware assault and overall cybersecurity best practices, to avert events such as the Royal Mail ransomware attack by utilizing antivirus and antimalware solutions:

Implement Application Allowlisting Platforms: Application allowlisting platforms, such as PC Matic Pro, prevent unknown applications from executing on endpoints or networks. This significantly reduces the risk of ransomware infections by ensuring only approved applications run on the system (Buikema. 2023).

Real-Time Scanning: By monitoring files and processes in real-time, antivirus and anti-malware software can identify and thwart ransomware attacks before they have a chance to take effect. This ability allows one to stop ransomware before it has an opportunity to encrypt files (Mimecast, 2023).

Blocking Suspicious Email and Web Traffic: These programs scan email and online traffic for signs of ransomware assaults, like malware downloads or phishing emails. They can stop ransomware from ever infecting the user's machine by filtering potentially harmful content (Sergey. 2022).

b) Regular Backups

The Royal Mail's response to the LockBit ransomware attack involved focusing on restoring their systems and operations. Although the specifics of their backup strategy were not detailed, the fact that they were able to resume overseas deliveries through post offices indicates they had measures in place to recover from the attack. Suggesting that backups and recovery plans were instrumental in quickly returning to normal operations despite the significant disruption process.

Data Recovery: Organizations can avoid paying the ransom by using regular backups to restore their systems to a condition before the ransomware attack. This is important because paying the ransom includes risks such as inciting more assaults and does not guarantee data decryption (Nick. 2019).

Verification and Testing: To make sure they work properly, it is crucial to confirm the integrity of backups and evaluate the restoration procedure. This proactive strategy lowers the chance of depending on flawed backups in an emergency by assisting in the early detection of any problems with the backup process (Larry. 2020).

c) Patch Management

For Royal Mail, although the specific details of their patch management practices leading up to the attack are not explicitly mentioned, the emphasis on enhancing cybersecurity measures, including regular software updates and patches, is applicable. Ensuring that all software, including those running on servers and workstations, is kept up-to-date is fundamental to preventing unauthorized access and exploitation of vulnerabilities by malicious actors.

Avoiding Permanent Data Loss: The danger of data loss rises in the absence of adequate patch management because of vulnerabilities that may result in system malfunctions or breaches. An organization's ability to recover from possible assaults and lessen the impact of data loss is ensured by effective patch management in conjunction with data backup and disaster recovery procedures (Amanda. 2023).

Automating Patch Deployment: Automating the deployment of patches across all systems and devices within the network is crucial. Automation ensures that patches are applied consistently and efficiently, minimizing the risk of manual errors and delays. This approach helps in maintaining a

 doi:10.20944/preprints202408.2261.v1

secure environment by addressing vulnerabilities as soon as patches are available (CM-Alliance. 2024).

Testing Patches in a Controlled Environment: Before deploying patches across the entire network, they should be tested in a controlled environment to ensure compatibility and stability. This step helps prevent unintended disruptions to operations and ensures that patches do not introduce new issues (CM-Alliance. 2024).

d) Security Awareness Training

In the Royal Mail case, while specific details on security awareness training are not provided, the attack underscores the need for comprehensive cybersecurity education among employees. Given the sophistication of the LockBit ransomware and its operation under a Ransomware-as-a-Service (RaaS) model, employees need to be aware of the evolving tactics used by cybercriminals.

Regular Updates and Simulations: Regular phishing attack simulations and ongoing training can significantly reduce the chance of ransomware infection. Employee vigilance and familiarity with attacker techniques can be increased by regular simulated attacks and the integration of training into the business culture (James. 2020).

Technical Measures Support: Human factors-focused Security Awareness Training complements technological measures such as installing anti-spam filters to prevent dangerous file types (.exe,.vbs, and. scr), applying the least privilege principle, and keeping an eye on networks for strange activity. These actions come together to create a multi-layered defense against ransomware (Jones. 2023).

Simulate Threats and Conduct Training Workshops: Implement simulated phishing and ransomware attacks as part of the training curriculum. This hands-on approach helps employees recognize and avoid falling victim to such tactics, thereby strengthening the organization's defenses against real-world threats (Avey. 2024).

e) Network Segmentation

In the Royal Mail case, it's stated that only the overseas deliveries were disrupted this is proof of network segmentation without proper network segmentation more of their network would have been vulnerable. Network segmentation refers to separating a larger network into smaller sub-networks with limited connections between each sub-network. Limited access between the sub-networks results in restricted access for attacker lateral movement, network segmentation prevents unauthorized users from accessing the organization’s intellectual property and data (Reuters. 2023).

Each sub-network should have its security controls, firewalls, and unique access to prevent ransomware from reaching target data. This way the spread of an infection can be prevented from spreading across the whole network. (Chin, 2024)

Smaller, segmented networks are easier to monitor. Suspicious activities such as ransomware attacks are easily spotted in a segmented network. (Intelligence, 2024). Faster detection allows for quicker response and prevention of infection spread, reducing the impact on the system. (Intelligence, 2024).

PROPOSED COUNTERMEASURES

Case 1 (Colonial Pipeline. 2021)

a) Implementation of Advanced VPN Security:

Change the old VPN technology with newer systems that have better security features. Multifactor Authentication (MFA) should be used for all VPN access to add an extra layer of security. An OTP sent to a mobile device is one example of MFA.

b) Enhanced Password Management:

 doi:10.20944/preprints202408.2261.v1

Establish rules that require complicated passwords that are changed often. Follow the rules that say you must use a mix of letters, numbers, and special characters. Password managers can help you make and keep safe complicated passwords. You should either encourage or require people to use them. Do regular checks to make sure that credentials that have been compromised are quickly updated.

c) Network Segmentation and Zero Trust Architecture:

Ensure strict segregation between IT and OT networks to limit the spread of malware. Adopt a zero-trust security model where each access request is verified, regardless of its origin within or outside the network.

d) Regular Security Audits and Penetration Testing:

Perform periodic security audits to detect and address system vulnerabilities. Conduct regular penetration tests to mimic attacks and detect vulnerabilities before they may be taken advantage of by malevolent individuals.

e) Incident Response and Backup Strategy:

Create and consistently maintain a thorough incident response plan that encompasses specific protocols for managing ransomware threats. Establish a resilient backup plan that includes regular, encrypted backups stored offline or in a secure cloud environment to guarantee prompt recovery without the need to pay ransoms.

f) Threat Intelligence and Monitoring:

Employ complex threat detection technologies to continuously monitor network traffic in real-time for indications of hostile behaviors. Engage in industry threat information exchange initiatives to remain updated on developing threats and techniques for mitigating them.

Case 2 (Royal Mail, LockBit Ransomware. 2023)

a) AI-Driven Threat Detection

Royal Mail was not able to detect they were about to be attacked by the lock bit ransomware. This could have been avoided if they were equipped with AI-driven threat detection. This enhancement enables multi-layered AI detection of suspicious files, improving the detection of unknown threats. AI can also accurately identify Lock Bit ransomware which in this case would have saved Royal Mail millions of dollars and avoided. As ransomware attacks are more complex now, AI tools are becoming more effective to counter these attacks. These developments can be utilized to protect software and applications from these ransomware attacks.

An example where AI can help detect threats is by using AI to help detect phishing emails technology can make use of machine learning to scan through larger amounts of data to detect anomalies or threats. These include detecting corrupted files or other indicators of compromise hidden in the emails before they can harm the network. (Hurley, 2023)

Utilizing AI-based security solutions also helps with threat detection. An example of an AI security solution is XDR. It can detect threats in real time within hours where it may take weeks without AI assistance. (Hurley, 2023)

AI tools can analyze current and past trends and predict potential security threats and attacks. Therefore, AI can proactively take measures to prevent these attacks.

Royal Mail was not able to detect they were about to be attacked by the lock bit ransomware. This could have been avoided if they were equipped with AI driven threat detection. This enhancement enables multi-layered AI detection of suspicious files, improving the detection of unknown threats. AI can also accurately identify Lock Bit ransomware which in this case would have saved Royal Mail millions of dollars and avoided.

b) Dynamic Analysis of Malware

 doi:10.20944/preprints202408.2261.v1

Dynamic analysis of malware involves executing malware in a controlled environment and monitoring its effect on the system whether it's trying to send data to a remote server, spreading the malware to other devices or does it make changes to the system. This analysis helps to learn how the malware operates and how to neutralize the threat of the malware to the system. Dynamic analysis of malware helps to fight against ransomware attacks on multiple fronts:

Ransomware is a type of malware that prevents the user from accessing their computer. Analysis of malware helps the organization to prepare for ransomware attacks as they know how to neutralize attacks of such. Royal Mail wouldn't have such a long downtime if they were prepared for the lock-bit ransomware attack as they would have been prepared for that attack with dynamic malware analysis. (Anon., n.d.)

Providing rapid attack response, not only ensures IT specialists can react quickly but also prevents major damage to the network or damage to any other device in the network. Dynamic malware analysis is handy when it comes to reacting quickly and provides rapid incident response which is crucial in any network so that data from the network does not also get spread publicly. (Anon., n.d.)

Understanding the malware helps to understand attackers' methods to encrypt the data and develop better backup and recovery strategies. Organizations can make sure their backups are safe, and recovery methods are effective in securing the data.

By leveraging dynamic malware analysis, Royal Mail can turn their expensive lesson with lock bit ransomware into actionable intelligence, by enhancing their defense capabilities against similar attacks in the future.

c) Automated Patching and Updates

Automated patch management refers to the automation of the entire patch management such as scanning all networked systems to identify missing patches, testing new patches, and periodic reports on patch deployment status. Automated patching and updates are vital as attackers actively look for networks that do not have the new patches. Many organizations lack the manpower to keep up with continuous updates from vendors. In this situation, automated patching and updates can be very helpful and cost-efficient. How does automated patching help in the battle against ransomware attacks:

Minimizes endpoint security risks: Modern malware spreads very fast through the whole network. Therefore, organizations must keep every endpoint of the network secure. Most organizations have segmented networks that help against the spread of malware but without a secure endpoint, there is no benefit of the segmented network. (Liongard, 2023)

Eliminates human error, an organization's security is a complex design, and keeping it up to date with security features is a day-to-day process. Even a manual patching wizard is known to leave some vulnerabilities open to attack. Some of the most common mishaps when patching and updating a network are missing out on a failed update notification, and deploying the wrong version of the patch. Automated patch and update deployment does not make those human errors (Stockley. 2023).

CONCLUSION

In conclusion, ransomware uses complex and difficult-to-break encryption techniques to hijack files and demand a large ransom which is a significant and evolving threat to cybersecurity. From the 1989 AIDS Trojan to now ransomware has evolved to targeted attacks via the Ransomware-as-a-

 doi:10.20944/preprints202408.2261.v1

Service (RaaS) model, this evolution illustrates the increasing sophistication and targeting of ransomware (PKTech. 2024).

Ransomware's journey began with relatively simple attacks on individuals. These early forms of ransomware were often spread through email attachments or malicious websites, and they typically demanded modest sums of money for the release of encrypted files. However, as cybersecurity defenses improved and attackers sought greater financial gain, ransomware evolved into a more complex and targeted threat. Encrypting ransomware and non-encrypting ransomware are the two main categories under which modern ransomware falls. As the name implies, encryption ransomware encrypts the victim's files and demands a ransom to unlock them. Conversely, non-encrypting ransomware prevents users from accessing the system and shows a notice requesting money to allow users to again. Both individuals and businesses are susceptible to the disastrous impacts of both types of ransomware.

Based on case study scenario 1&2, we can identify that the main reason for ransomware to occur is due to the vulnerability in the cybersecurity infrastructure. In case 1(Colonial Pipeline), it was caused by an outdated version of VPN where the multifactor authentication is not used. Besides weak password management is another key factor that allows the ransomware to be carried out easily. Looking into case 2(Royal Mail), similarly, the attack occurred due to vulnerable infrastructure however, it is where LockBit attackers exploited a loophole in its system leading to the attack. From these attacks, both companies have been facing operational disruption, financial loss, and data breaches. Hence, various improvements are being made to these attacks. The first is regarding hardware and software systems. Companies must upgrade them to date to prevent them from having exploited loopholes. Besides, robust security measures such as firewalls and intrusion detection systems should be implemented. Furthermore, regarding sensitive data, MFA should be compulsory to enhance the security system and prevent data leaks. Education and training for all employees are also crucial. With such training, employees can raise awareness, decrease in risk of getting phishing and other cyber threats, and understand the importance of strong complex passwords to prevent the password from being hacked. Regular security check-ups should be conducted together with cybersecurity experts to ensure that the system is safe and can further increase security enhancement as prevention for cyberattacks. Finally, data backups must be done regularly to ensure data can be restored when it’s needed instead of depending on paying ransom to obtain back the necessary data. This will also aid in operation to be performed safely without much disruption (Secureworks. 2024).

The incidents involving Royal Mail and Colonial Pipeline highlight the necessity of strong security protocols to stop and lessen ransomware attacks. Using thorough antivirus and antimalware software can assist Colonial Pipeline in identifying and thwarting ransomware before it has a chance to infiltrate the system. By regularly backing up important data, businesses may ensure that they can restore their systems without having to pay the ransom in the case of a ransomware attack. The security of remote connections can be improved and unwanted access can be stopped by putting multifactor authentication into contemporary VPN solutions. Organizations can also lessen the risk of lateral movement within the network and restrict the spread of ransomware by segmenting the network and implementing a Zero Trust strategy.

The progression of ransomware, exemplified by the advanced Ransomware-as-a-Service (RaaS) model and the 1989 AIDS Trojan, demonstrates the growing intricacy and focused character of these assaults. RaaS broadens the threat landscape by enabling attackers to rent out ransomware to affiliates, hence democratizing access to sophisticated malware. This strategy has led to an increase in attacks by making it simpler for attackers with less technical expertise to start ransomware campaigns. To counteract the increasing threat of ransomware, enterprises need to have a multilayered and proactive cybersecurity strategy. This entails making investments in cutting-edge security technologies, putting best practices for network security into practice, and encouraging an

 doi:10.20944/preprints202408.2261.v1

employee culture of cybersecurity knowledge. Frequent training and awareness campaigns can assist staff members in identifying phishing attempts and other typical ransomware attack routes.

Collaborative efforts between the public and private sectors are indispensable in combating the ransomware crisis. Governments can significantly influence the fight against ransomware by implementing strict cybersecurity laws, fostering information exchange, and allocating resources to bolster organizational defenses. Global teamwork is also vital, given that ransomware attacks frequently involve perpetrators from various countries. By embracing a proactive and unified strategy, entities can fortify their defenses against ransomware and safeguard their vital assets from this persistent menace. The continuous struggle against ransomware highlights the necessity for constant alertness, creativity, and partnership in striving for a safer digital environment.

REFERENCES

1. 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.
2. Almusaylim, Z.A., Zaman, N. and Jung, L.T. (2018) 'Proposing A Data Privacy-Aware Protocol for Roadside Accident Video Reporting Service Using 5G In Vehicular Cloud Networks Environment,' *2018 4th International Conference on Computer and Information Sciences (ICCOINS)* [Preprint]. https://doi.org/10.1109/iccoins.2018.8510588.
3. Ali, S., Hafeez, Y., Humayun, M., Jhanjhi, N. Z., & Le, D. N. (2022). Towards aspect based requirements mining for trace retrieval of component-based software management process in globally distributed environment. *Information Technology and Management*, *23*(3), 151-165.
4. 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).
5. 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.
6. Alqahtani, A. and Sheldon, F.T. (2024) 'EMIFS: a normalized hyperbolic ransomware deterrence model yielding greater accuracy and overall performance,' *Sensors*, 24(6), p. 1728. https://doi.org/10.3390/s24061728.
7. Amaan, R. (2024). LockBit Ransomware Creator's Face Revealed and Sanctioned [online]. Available from: https://www.techworm.net/2024/05/lockbit-ransomware-creator-face-revealed.html [accessed 16 May 2024].
8. Amanda, S. (2023). What Is a Countermeasure in Computer Security. Available from: https://www.comptia.org/blog/what-is-a-countermeasure-in-computer-security [accessed 15 May 2024].
9. Anastasia (2024) Ransomware goes political and other extortion activity of 2023, Analyst1. Available from: https://analyst1.com/ransomware-goes-political-and-other-extortion-activity-of-2023/ [Accessed: 17 May 2024].
10. Anon (n.d.) A guide to ransomware [internet]. Available from: https://www.ncsc.gov.uk/ransomware/home. [Accessed: 17 May 2024].
11. Anon (n.d.) Exploit Kit [Internet]. Available from: https://www.trendmicro.com/vinfo/us/security/definition/exploit-kit [Accessed: 17 May 2024].
12. Avey, C. (2024). Essential steps to prevent a ransomware attack. Available from: https://www.bcs.org/articles-opinion-and-research/essential-steps-to-prevent-a-ransomware-attack/ [accessed 26 May 2024].
13. Bachchas, K S. (2024). The rise of ransomware: Strategies for prevention. Available from: https://cybersecurity.att.com/blogs/security-essentials/the-rise-of-ransomware-strategies-for-prevention [accessed 28 May 2024].
14. Begovic, K., Al-Ali, A. and Malluhi, Q. (2023) 'Cryptographic ransomware encryption detection: Survey,' *Computers & Security*, 132, p. 103349. https://doi.org/10.1016/j.cose.2023.103349.
15. Buikema, N. (2023). International Deliveries in Limbo – How Royal Mail Could Have Avoided Ransomware Attack. Available from: https://www.pcmatic.com/blog/international-deliveries-in-limbo-how-royal-mail-could-have-avoided-ransomware-attack/ [accessed 26 May 2024].
16. Cen, M. *et al.* (2024) 'Ransomware early detection: A survey,' *Computer Networks*, 239, p. 110138. https://doi.org/10.1016/j.comnet.2023.110138.
17. Chin, K., 2024. How to Prevent Ransomware Attack: Top 10 Best Practices. [Online] Available at: https://www.upguard.com/blog/best-practices-to-prevent-ransomware-attacks [Accessed 18 5 2024].
18. Choi, K.-S., Lee, C.S. and Merizalde, J. (2023) 'Spreading viruses and malicious codes,' in *Edward Elgar Publishing eBooks*, pp. 232–250. https://doi.org/10.4337/9781800886643.00024.

19. CIS. (2023). 7 Steps to Help Prevent & Limit the Impact of Ransomware. Available from: https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware [accessed 15 May 2024].
20. CM-Alliance. (2024). Ransomware Resilience: Prevention and Recovery in 2024. Available from: https://www.cm-alliance.com/cybersecurity-blog/ransomware-resilience-prevention-and-recovery-in-2024 [accessed 26 May 2024].
21. Connor, J. (2023). LockBit leaks 44GB of Royal Mail's data and sets fresh £33 million ransom [online]. Available from: https://www.itpro.com/security/ransomware/370124/lockbit-leaks-44gb-royal-mails-data-sets-fresh-ps33-million-ransom [accessed 16 May 2024].
22. Cybersecurity & Infrastructure Security Agency (CISA). (2024). The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. [online] Available from: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years [accessed 14 May 2024].
23. Dogra, V., Singh, A., Verma, S., Kavita, Jhanjhi, N.Z., Talib, M.N. (2021). Analyzing DistilBERT for Sentiment Classification of Banking Financial News. In: Peng, SL., Hsieh, SY., Gopalakrishnan, S., Duraisamy, B. (eds) Intelligent Computing and Innovation on Data Science. Lecture Notes in Networks and Systems, vol 248. Springer, Singapore. https://doi.org/10.1007/978-981-16-3153-5_53
24. Edwards, L., Iqbal, M.Z. and Hassan, M. (2024) 'A multi-layered security model to counter social engineering attacks: a learning-based approach,' *International Cybersecurity Law Review*, 5(2), pp. 313–336. https://doi.org/10.1365/s43439-024-00119-z.
25. 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.
26. Fazzino. (2023). Cybersecurity Defense-in-Depth Using AI and ML. Available from: https://www.jackhenry.com/fintalk/cybersecurity-defense-in-depth-using-ai-and-ml [accessed 28 May 2024].
27. Ferdowsi, O. (2021). Lessons from Colonial Pipeline- How Your Company Can Avoid Ransomware Attacks. Available from: https://www.comtechlocation.com/blog/lessons-from-colonial-pipeline-how-your-company-can-avoid-ransomware-attacks [accessed 26 May 2024].
28. Fox, J. (2023). 11 Biggest Ransomware Attacks in History. [online] Available from: https://www.cobalt.io/blog/11-biggest-ransomware-attacks-in-history [accessed 13 May 2024].
29. Gatlan, S. (2023). LockBit ransomware gang claims Royal Mail cyberattack. Available from: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-claims-royal-mail-cyberattack/ [accessed 28 May 2024].
30. 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
31. 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.
32. Ghosh, G. *et al.* (2020) 'Secure surveillance system using chaotic image encryption technique,' *IOP Conference Series Materials Science and Engineering*, 993(1), p. 012062. https://doi.org/10.1088/1757-899x/993/1/012062.
33. 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.
34. 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.
35. Humayun, M., Ashfaq, F., *et al.* (2022) 'Traffic management: Multi-Scale vehicle detection in varying weather conditions using YOLOV4 and spatial pyramid pooling network,' *Electronics*, 11(17), p. 2748. https://doi.org/10.3390/electronics11172748.
36. Humayun, M., Sujatha, R., *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.
37. 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.
38. 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).
39. 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.

40. Hurley, A., 2023. How AI is changing ransomware and how you can adapt to stay protected. [Online] Available at: https://blog.barracuda.com/2023/11/13/ai-ransomware-adapt-stay-protected [Accessed 26 5 2024].
41. Intel. (2023). What Is Patch Management. Available from: https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/patch-management.html [accessed 15 May 2024].
42. Intelligence, T., 2024. Network Segmentation and How it Can Prevent Ransomware. [Online] Available at: https://www.threatintelligence.com/blog/network-segmentation [Accessed 26 5 2024].

43. Jayakumar, P., Brohi, S. N., & Jhanjhi, N. Z. (2021). Artificial intelligence and military applications: Innovations, cybersecurity challenges & open research areas.

44. 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.

45. 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.
46. J.P. Morgan. (2024). The Potential Impacts of Ransomware. [online] Available from:https://www.jpmorgan.com/technology/news/the-potential-impacts-of-ransomware [accessed 13 May 2024].
47. James, A T. (2024). From Origins to Double-Extortion: The Evolution of Ransomware Tactics. Available from: https://www.spiceworks.com/it-security/vulnerability-management/guest-article/evolution-of-ransomware-tactics/ [accessed 28 May 2024].
48. James, M. (2020). How to Deal with Ransomware Attacks. Available from: https://www.metacompliance.com/blog/cyber-security-awareness/how-to-deal-with-ransomware-attacks [accessed 15 May 2024].
49. Jasper, J. (2023). Royal Mail ransomware attackers threaten to publish stolen data [online]. Available from: https://www.theguardian.com/business/2023/jan/12/royal-mail-ransomware-attackers-threaten-to-publish-stolen-data [accessed 13 May 2024].
50. Jones, C. (2023). Royal Mail's recovery from ransomware attack will cost business at least $12M. Available from: https://www.theregister.com/2023/11/16/royal_mail_recovery_from_ransomware/ [accessed 28 May 2024].
51. Kelly, S. & Resnick-ault, J. (2021). One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators. [online] Available from: https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/ [accessed 13 May 2024].
52. Kerner, S.M. (2022). Colonial Pipeline hack explained: Everything you need to know. [online] Available from: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know [accessed 13 May 2024].

53. 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.
54. Kyle, C. (2024). How to Prevent Ransomware Attacks: Top 10 Best Practices. Available from: https://www.upguard.com/blog/best-practices-to-prevent-ransomware-attacks. [accessed 15 May 2024]
55. LaPorte, B. (2024). History of Ransomware: The Evolution of Attacks and Defense Mechanisms. Available from: https://blog.morphisec.com/ransomware-history-evolution-of-attacks-and-defenses [accessed 28 May 2024].
56. Larry, G. (2020). Ransomware Response Safeguards and Countermeasures. Available from: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/ransome-response-safeguards-and-countermeasures [accessed 15 May 2024].
57. Liongard, 2023. Using Security Automation to Protect Business from Ransomware. [Online] Available at: https://www.linkedin.com/pulse/using-security-automation-protect-business-from-ransomware-liongard/ [Accessed 31 3 2024].

58. 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.
59. Mark Sweney. (2023). Royal Mail resumes overseas deliveries via post offices after cyber-attack [online]. Available from: https://www.theguardian.com/business/2023/feb/21/royal-mail-international-deliveries-cyber-attack-ransom-strikes [accessed 14 May 2024].

60. M. Saleh, N. Jhanjhi, A. Abdullah and R. Saher, "IoTES (A Machine learning model) Design dependent encryption selection for IoT devices," *2022 24th International Conference on Advanced Communication Technology (ICACT)*, PyeongChang Kwangwoon_Do, Korea, Republic of, 2022, pp. 239-246, doi: 10.23919/ICACT53585.2022.9728960.
61. Mark, S. (2023). Royal Mail resumes overseas deliveries via post offices after cyber-attack [online]. Available from: https://www.theguardian.com/business/2023/feb/21/royal-mail-international-deliveries-cyber-attack-ransom-strikes [accessed 15 May 2024].
62. Mimecast. (2023). Ransomware prevention is a critical priority. Available from: https://www.mimecast.com/content/ransomware-prevention/#:~:text=Antispam%2C%20antivirus%20and%20anti-malware,block%20new%20and%20emerging%20threats [accessed 15 May 2024].
63. Möller, D.P.F. (2023) 'Ransomware Attacks and Scenarios: cost factors and loss of reputation,' in *Advances in information security*, pp. 273–303. https://doi.org/10.1007/978-3-031-26845-8_6.
64. Nayyar, A., Gadhavi, L. and Zaman, N. (2021) 'Machine learning in healthcare: review, opportunities and challenges,' in *Elsevier eBooks*, pp. 23–45. https://doi.org/10.1016/b978-0-12-821229-5.00011-2.
65. Neko, P and Robert, S. (2021). Countermeasures for Ransomware. Available from: https://www.proofpoint.com/us/blog/security-awareness-training/countermeasures-ransomware [accessed 15 May 2024].
66. Niamh, L. (2023). Royal Mail cyber-attack carried out by Russian-linked ransomware gang [online]. Available from: https://news.sky.com/story/royal-mail-cyber-attack-carried-out-by-russian-linked-ransomware-gang-12785685 [accessed 13 May 2024].
67. Nick, C. (2019). Protect backups from ransomware and other security risks. Available from: https://www.techtarget.com/searchdatabackup/feature/Protect-backups-from-ransomware-and-other-security-risks [accessed 15 May 2024].
68. NLC. (2023). Patching: A Necessity in a World of Ransomware. Available from: https://www.nlc.org/article/2023/11/29/patching-a-necessity-in-a-world-of-ransomware/#:~:text=Once%20inside%20your%20system%2C%20they,that%20attackers%20could%20otherwise%20exploit [accessed 15 May 2024].
69. Noone, G. (2023). Royal Mail spent £10m on cybersecurity after LockBit ransomware attack. Available from: https://techmonitor.ai/technology/cybersecurity/royal-mail-spent-10m-on-cybersecurity-after-lockbit-ransomware-attack [accessed 28 May 2024].
70. Parsons, M. & Knudtson, B. and Reid, A. (2023). Is cybersecurity doing enough to prevent the next Colonial Pipeline attack? [online] Available from: https://www.cybersecuritydive.com/news/colonial-pipeline-anniversary/649532/ [accessed 14 May 2024].
71. PKTech. (2024). Ransomware in 2024: Trends, Tactics, and Prevention Strategies. Available from: https://www.pktech.net/2024/04/ransomware-in-2024-trends-tactics-and-prevention-strategies/ [accessed 28 May 2024].
72. PMA360. (2021). The Colonial Pipeline Ransomware attack: Lessons for cybersecurity teams. Available from: https://blogs.manageengine.com/corporate/manageengine/pam360/2021/06/15/the-colonial-pipeline-ransomware-attack-lessons-for-cybersecurity-teams.html [accessed 15 May 2024].
73. Raj, A. *et al.* (2024) 'Modern ransomware: Evolution, methodology, attack model, prevention and mitigation using multi-tiered approach,' *Security and Privacy* [Preprint]. https://doi.org/10.1002/spy2.436.
74. Reuters. (2023). Royal Mail faces threat from ransomware group LockBit. Available from: https://www.reuters.com/technology/lockbit-ransomware-group-threatens-publish-stolen-royal-mail-data-techcrunch-2023-02-07/ [accessed 28 May 2024].
75. Rob, D. (2023). 'All we have had is losses': Royal Mail dismisses 'absurd' $80m ransom demand [online]. Available from: https://www.theguardian.com/business/2023/feb/15/under-no-circumstances-will-we-pay-that-absurd-amount-royal-mail-tells-hackers [accessed 14 May 2024].
76. Rothschild, M. (2021). Colonial Pipeline Ransomware Attack: How to Reduce Risk in OT Environments. Available from: https://www.tenable.com/blog/colonial-pipeline-ransomware-attack-how-to-reduce-risk-in-ot-environments [accessed 26 May 2024].

77. Saeed, S., Haron, H., Jhanjhi, N. Z., Naqvi, M., Alhumyani, H. A., & Masud, M. (2022). Improve correlation matrix of discrete fourier transformation technique for finding the missing values of mri images. *Mathematical Biosciences and Engineering*, *19*(9), 9039-9059.

78. 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.

79. 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).
80. 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.
81. SecureLink. (2021). Back to Basics: A Deeper Look at the Colonial Pipeline Hack. [online] Available from: https://www.govtech.com/sponsored/back-to-basics-a-deeper-look-at-the-colonial-pipeline-hack [accessed 13 May 2024].
82. Secureworks. (2023). Ransomware Evolution. Available from: https://www.secureworks.com/research/ransomware-evolution [accessed 28 May 2024].
83. SecurityScorecard. (2024). Proactive Strategies to Prevent Ransomware Attacks. Available from: https://securityscorecard.com/blog/proactive-strategies-to-prevent-ransomware-attacks/ [accessed 28 May 2024].
84. Sergey, B. (2022). Can Antivirus Protect Against Ransomware? Available from: https://spin.ai/blog/does-antivirus-protect-against-ransomware/ [accessed 15 May 2024].
85. Shahid, H. *et al.* (2021) 'Energy Optimised Security against Wormhole Attack in IoT-Based Wireless Sensor Networks,' *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, 68(2), pp. 1967–1981. https://doi.org/10.32604/cmc.2021.015259.

86. Shah, I. A., Jhanjhi, N. Z., & Brohi, S. N. (2024). Use of AI-Based Drones in Smart Cities. In I. Shah & N. Jhanjhi (Eds.), *Cybersecurity Issues and Challenges in the Drone Industry* (pp. 362-380). IGI Global. https://doi.org/10.4018/979-8-3693-0774-8.ch015

87. 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

88. 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
89. Shaikh, M.U.R. *et al.* (2024) 'Fortifying Against Ransomware: Navigating Cybersecurity Risk Management with a Focus on Ransomware Insurance Strategies,' *International Journal of Academic Research in Business and Social Sciences*, 14(1). https://doi.org/10.6007/ijarbss/v14-i1/20566.
90. 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.
91. Sindiramutty, S.R., Jhanjhi, Noor Zaman, Tan, C.E., Tee, W.J., *et al.* (2024) 'IoT and AI-Based Smart Solutions for the Agriculture Industry,' in *Advances in computational intelligence and robotics book series*, pp. 317–351. https://doi.org/10.4018/978-1-6684-6361-1.ch012.
92. 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.
93. 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.
94. Sindiramutty, S.R., Tee, Wee Jing, Balakrishnan, S., Kaur, S., *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.
95. Singhal, V. *et al.* (2020) 'Artificial Intelligence Enabled Road Vehicle-Train Collision Risk Assessment Framework for Unmanned railway level crossings,' *IEEE Access*, 8, pp. 113790–113806. https://doi.org/10.1109/access.2020.3002416.
96. SOCRadar. (2023). Dark Web Profile: LockBit 3.0 Ransomware [online]. Available from: https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/ [accessed 16 May 2024].

97. Sood, M., Angra, P., Verma, S., & Jhanjhi, N. Z. (2022). Efficient feature grouping for IDS using clustering algorithms in detecting known/unknown attacks. In *Information security handbook* (pp. 103-116). CRC Press.
98. Stockley, M. (2023). Royal Mail schools LockBit in leaked negotiation. Available from: https://www.threatdown.com/blog/royal-mail-schools-lockbit-in-leaked-negotiation/ [accessed 28 May 2024].
99. TealTech. (2024). Lessons from the Colonial Pipeline Ransomware Hack. Available from: https://tealtech.com/blog/lessons-from-the-colonial-pipeline-ransomware-hack/ [accessed 26 May 2024].

100. Teichmann, F., Boticiu, S.R. and Sergi, B.S. (2023) 'The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate?,' *International Cybersecurity Law Review*, 4(3), pp. 259–280. https://doi.org/10.1365/s43439-023-00095-w.
101. Terranova Security. (2023). 6 Things to Learn from the Garmin Security Breach. [online] Available from: https://www.terranovasecurity.com/blog/garmin-security-breach. [accessed 14 May 2024].
102. Terranova Security. (2023). How To Prevent Ransomware. Available from: https://www.terranovasecurity.com/blog/how-to-prevent-ransomware#:~:text=To%20prevent%20ransomware%2C%20companies%20need,can%20have%20on%20the%20company [accessed 15 May 2024].

103. Tiwalade Modupe Usman, Yakub Kayode Saheed, Djitog Ignace, Augustine Nsang, Diabetic retinopathy detection using principal component analysis multi-label feature extraction and classification, International Journal of Cognitive Computing in Engineering, Volume 4, 2023,
104. Pages 78-88, ISSN 2666-3074, https://doi.org/10.1016/j.ijcce.2023.02.002.

105. 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.

106. Wood, K. (2023). Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack. [online] Available from: https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/#_ftn1 [accessed 13 May 2024].
107. Worrell, J.L. "Jamey" (2024) 'A SURVEY OF THE CURRENT AND EMERGING RANSOMWARE THREAT LANDSCAPE,' *EDPACS*, pp. 1–11. https://doi.org/10.1080/07366981.2024.2315639.

108. 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.
109. Zulfikar, H. (2023). Mengenal Ransomware LockBit 3.0 yang Diduga Serang BSI dan Cara Kerjanya [online]. Available from: https://tekno.kompas.com/read/2023/05/15/12450037/mengenal-ransomware-lockbit-30-yang-diduga-serang-bsi-dan-cara-kerjanya [accessed 16 May 2024].

 doi:10.20944/preprints202408.2261.v1