Analysis of Recent Ransomware Attacks and Preventable Measures

Nadika Bandara[a], Larissa Marques[a], Mawuli Martey[a] and Akalanka Mailewa[b]

[a]Department of Information Systems, St. Cloud State University, St. Cloud, MN, United States

[b]Department of Computer Science and Information Technology, St. Cloud State University, St. Cloud, MN, United States

Abstract

This research paper explores the growth and impact of ransomware attacks on organizations. The paper defines ransomware as malicious software that encrypts or corrupts data or files with the intention of extorting money from the targeted victim. The paper first provides an overview of common types of ransomware attacks, their scale, and the increasing frequency of attacks. The paper then delves into the evolution of ransomware and strategies for preventing future attacks. In conclusion, the paper highlights the importance of proactively safeguarding information assets in the face of growing and sophisticated ransomware attacks. The security of information confidentiality, integrity, and availability requires a thorough understanding of ransomware attacks and strategies for prevention. Despite the potential for innovative technologies to improve the detection of attacks, ransomware is expected to persist as a threat in the future. As such, organizations must prioritize strengthening and investing in their information security to mitigate potential harm.

Keywords: Ransomware, Cryptocurrency, IoT, Policy, Detection, Prevention

1. Introduction

Ransomware is a malicious software that encrypts or corrupts data or files with the intention of extorting money from the targeted victim. The victim is promised access to their data again if they pay the ransom [1]. The objective of this research paper is to examine the growth of ransomware attacks over time and the damaging effects they have had on organizations. To better understand these attacks, this paper will first provide an overview of the common types of ransomwares, their scale, and the increasing frequency of attacks. The paper will then explore into the evolution of ransomware and strategies for preventing future attacks.

2. Common Ransomware Attacks

Government and corporate institutions, businesses, and internet of things devices have seen an increase in the number of new malware attacks such as ransomware in recent times. About 966 government, educational, and healthcare organizations in the United States of America alone have witnessed ransomware attacks, causing about 7.5 billion dollars in financial losses in 2019 [7]. As a result of widespread ransomware attacks, many user systems and online businesses have recently suffered significant damage. Recent ransomware attacks have not only resulted in massive financial losses but have also posed a significant threat to human lives. Patients' appointments and medical procedures have been canceled, and some have been diverted to different medical facilities. Many businesses and data centers have been knocked out as a result of ransomware attacks.

2.1 Types of Ransomwares

Based on its activity, ransomware can be categorized into four groups from one point of view. These types include ransomware, crypto-ransomware, scareware, and locker ransomware [7]. Crypto ransomware basically encrypts targeted data and files. Crypto ransomware is one of the most perilous types of

ransomwares. When crypto ransomware successfully encrypts their target sources, regaining access to infected data becomes difficult, unless the ransomware has a weak algorithm [9] Scareware ransomware typically uses social engineering techniques to coerce victims into paying a ransom and displays phony alerts requesting payment. Locker ransomware goes to the extreme by locking down computer systems and any targeted devices while restricting victims from accessing them. Locker ransomware normally locks computer systems and Internet of Things devices without encrypting or locking the files and data stored on them. Data and files stored are not affected when malware is successfully removed [22]. If ransomware cannot be removed, storage devices or media are moved to different computer systems to recover the data stored on them. Hence, locker ransomware is typically ineffective at extorting huge amounts of money from victims. However, crypto ransomware encrypts files and data stored on computer systems; hence, information or data is affected even if the ransomware is removed. It was difficult for ransomware attackers to receive payment in the late 1990s through 2005, before the emergence of online payment and cryptocurrency. Recently, it has been difficult to track payments made to ransomware attackers because of the use of cryptocurrency. Attackers most often request payment in bitcoin.

2.2 Why Ransomware is More Common Now

The advancement in technology has increased information and data exchange rapidly, making data and information security management challenging. One of the challenges associated with the increase in technology and data usage is the use of computer programs to disrupt information and data management processes. Ransomware has become the most used computer program or malware by attackers to cause harm to information systems and data centers or servers [20]. Both novice and advanced ransomware attackers have significantly benefited from the advancement in technology and products in computer engineering and programming. Also, the advancement in technology, computer programming, and cryptography has created many opportunities for novice attackers to use open-source code and drag-and-drop platforms to develop dangerous and effective ransomware. The most popular type of limitation used today is encryption, which effectively allows an attacker to keep system data or user data hostage [4]. One of the common ways ransomware is spread is through files with the DOC and PDF extension and icon, files with the screensaver extension (.SCR), macros included in text files, and files with the crypt extension (.js). Recently, the variety has increased and now includes ransomware as a service (RaaS), whitelisting, live chat, high-quality design, and more [20].

2.3 Attacks Scalability

The first instance of ransomware appeared in the late 1980s, and it has been resurfacing since 2013. Ransomware was originally designed to attack personal or individual computers at home, but industries and government institutions have been harder hit than individual entities. Recent major ransom cyberattacks have severely damaged many user computers and online businesses.

In the two years between 2013 and 2014, the number of new crypto-ransomware families increased by 250%, according to Symantec [5]. In just a few days in May 2017, WannaCry spread to more than 150 countries and 200,000 computers, severely disrupting several commercial and residential networks. Additionally, specifically targeted ransomware like Crysis disrupted numerous small and large businesses around the world; for instance, Trend Micro found that the Crysis family exclusively targeted firms in Australia and New Zealand in September 2016 [26]. Compared to late 2016, the number of these targeted ransomware assaults increased in January 2017. Additionally, 10% of all ransomware attacks have targeted IoT (Internet of Things) devices because of the lack of attention paid to security. According to research, between 25% and 30% of all ransomware attacks will be on IoT devices [26]. Remote Desktop Protocol and phishing emails are currently the most frequent attack vectors [5]. The average ransomware payment grew by more than 60% in the second quarter of 2020, reaching more than $170,000 per incident. current high-profile hacks like the Wastedlocker, where it is suspected that the ransom has been paid [5].

Traditional ransomware was frequently distributed randomly and without actual targets through host testing or network monitoring, thus, it is simple to spot them by keeping an eye out for unusual host actions such as root filesystem processes and network activity. In recent times, ransomware attacks have

become increasingly targeted. According to the Kaspersky Security Bulletin, targeted attacks have taken over as one of the main ways for several well-known ransomware groups to proliferate in. Besides basic security protocols, many firms struggle with security because they have many old systems and they frequently lack an organizational culture that places a high priority on information security, which has left many businesses unsure of how to deal with ransomware attacks [10][11]. It is estimated that the damages and costs to be incurred as a result of ransomware attacks will range from $7.5 billion to $200 billion soon.

3. Evolution of Ransomware Attacks

The first known ransomware attack is believed to have occurred in 1989 with the "AIDS" Trojan, also known as "PC Cyborg" or "AIDS Info Disk" [25]. The malware was distributed on a floppy disk and claimed to be a program that could cure AIDS. When executed, the malware encrypted the hard drive's file names and demanded a payment in exchange for the decryption key [21]. This attack is the first instance of ransomware, although it was not called as such at the time. Joseph Popp, a Harvard-educated biologist who created this ransomware used it to raise awareness and funding for the AIDS epidemic [21]. Even though the first instance of ransomware was done for a good cause, most of the ransomware attacks carried out after that were mal intentional.

3.1 Ransomware Attacks During 90s

After the first ransomware attack, there were only a few notable ransomware attacks that happened during the 1990s. This was mostly due to the difficulties of distributing ransomware. With the world not being interconnected with the internet like today, the distribution of malware needed to be done using physical media distribution methods such as floppy disks and CDs. Another factor that limited large scale distribution of ransomware was the lack of payment methods. Unlike the digital payment methods that are available now such as online payment gateways and digital cryptocurrencies such as Bitcoin, it was difficult for an attacker to get payments. They had to use cashier's checks or money orders like in the case of the "AIDS" Trojan ransomware [25].

3.2 Ransomware Attacks After Internet

With the internet becoming mainstream during the late 1990s and early 2000s, ransomware attacks started having a second life. During the 90s, malware was primarily implemented and experimented on by hobbyist hackers. However, with the boom of the internet, malware became profitable and scalable [12]. This applied to ransomware as well. Advances in communication methods over the internet, such as emails, peer-to-peer messaging, web forums, and the ability to transfer larger files, made it easy and cheap to spread malware, including ransomware. Another reason for its widespread use during this time was the advancement of encryption technologies. An example of this is the Gpcode ransomware, discovered in 2006. It spread via infected email attachments and used an advanced RSA-1024 algorithm to encrypt files on the victim's hard drive and any mapped network drives [6].

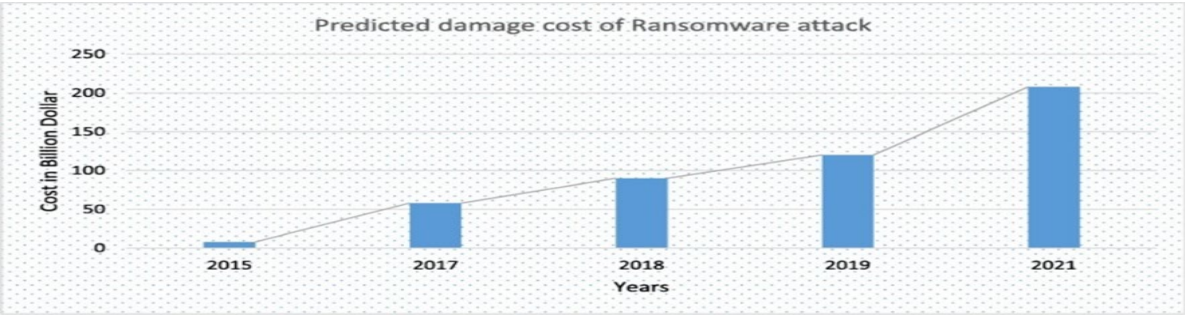

Figure 1. Cost of ransomware attacks from 2015 to 2021 [14]

3.3 Ransomware Attacks & Cryptocurrencies

Cryptocurrencies such as Bitcoin gained popularity in the late 2010s. They are digital, decentralized currencies that are maintained without a central authority or third-party intermediaries, unlike traditional currencies. Due to their decentralized nature and the difficulty of tracing transactions, cryptocurrencies are often used for criminal activities and monetary transactions. Ransomware, being a type of malware, requires a reliable and untraceable method to collect ransom payments from victims. As a result, cryptocurrencies have become the preferred payment method for many largescale ransomware attacks in recent years. For instance, the WannaCry ransomware attack used Bitcoin payments, providing victims with a Bitcoin wallet address and instructions on how to use cryptocurrencies. Once the ransom was received, the decryption was done manually [18]. More recently, ransomware attacks have started to use more sophisticated payment and decryption methods, leveraging the smart contract feature on the Ethereum cryptocurrency. Each victim receives a unique wallet address to send the ransom to, and the smart contract automatically decrypts the victim's files once the payment is received [18].

3.4 IoT Ransomware and COVID-19

Figure 1. Cost of ransomware attacks from 2015 to 2021 [14]. Ransomware attacks on Internet of Things (IoT) devices have become a growing concern. This is mostly due to the exponential growth of IoT device usage over the past decade. Ransomware attacks on IoT devices can deny access to critical systems, disrupt organization operations and compromise sensitive data. Compromised IoT devices can make other systems in the network vulnerable [14]. The COVID-19 pandemic has been a major contributor to the evolution of ransomware attacks. As a result of social distancing measures, many organizations have shifted to remote work, which involves the use of personal devices, access to company data outside of VPN, online data sharing, and collaboration tools. This shift has introduced vulnerabilities that attackers can exploit [23].

Since the inception of ransomware in 1989, ransomware attacks have progressed significantly. The widespread adoption of the internet, the development of cryptocurrencies, the increasing usage of IoT devices, and the remote working environment brought about by the COVID19 pandemic were the major external factors contributing to the evolution of ransomware attacks. Technologically, major advancements in encryption and communication technologies also played a role in the growth of ransomware attacks. As depicted in Figure 1, the financial harm caused by ransomware attacks from 2015 to 2021 clearly relates to these causes which were prevalent during that time.

4. Assessment Measures & Policies

The number of ransomware attacks is not only increasing, but they are also becoming more sophisticated with significant operational and financial consequences. Currently, the existing defense mechanisms are struggling to control these threats, and many need to be updated to keep pace with the evolving nature of ransomware [16].

Prevention and detection are two measures used when analyzing ransomware attacks. Prevention focuses on reducing the likelihood of an attack through actions such as system updates, installing security applications, and creating backup files to eliminate vulnerabilities. Detection, on the other hand, involves using various mechanisms to identify an attack with the objective of minimizing its impact on the system, as detection only alerts of the attack but does not prevent it from happening [13].

At some point, ransomware attacks were making headlines every day, with victims ranging from individuals to colleges, hospitals, government offices, and more. Around 2017, news coverage picked up on organizations being targeted, leading to a surge in attacks by criminals seeking to exploit the increased awareness of crypto viruses in the media. For instance, California passed a new law addressing ransomware after the attack on Hollywood Presbyterian Medical Center, which paid a ransom of $17,000 to recover from the incident [28].

As advanced and sophisticated threats like phishing and pharming become more prevalent, organizations are increasingly worried about information security and the potential misuse of IT departments leading to

violations of privacy. Hence, it's crucial for every business to safeguard the confidentiality, integrity, and availability of their information.

For years, companies have focused on reactive security, responding to attacks rather than proactively preventing them. In the pursuit of staying ahead of the competition with innovative technology, organizations risk exposing their information assets to security threats in the digital world. Encryption algorithms can protect these assets, but they can also be used by malicious attackers to cause harm. For example, the recent ransomware attack on JBS, the world's largest beef supplier, resulted in the company having to pay $11 million to regain control of its computer systems [2].

Ransomware is a new form of malware that poses significant threats to information assets. Research by Luo and Liao says, "ransomwares are induced through Internet like other computer virus such as Trojan horse, worms, and spyware" [27]. It involves hijacking and encrypting users' files, then demanding payment in exchange for the decryption key. The attackers hold the users' files until they agree to pay, often through a transfer to a specific online currency account.

To prevent ransomware attacks, all stakeholders should take several preventive measures. Upper-level management should provide security technologies for all company users and limit each personnel's access. Sharing admin credentials should be avoided, and software systems should be installed with administrator rights to increase protection. Acting against ransomware is simpler than restoring damage after an attack. IT staff should install up-to-date antivirus for all users, check all downloaded files, and format hacked files to remove damage. Backups of encrypted files should be created in case they can be decrypted later, and up-to-date backups should be stored in separate locations. End users should be cautious when handling spam emails, links, or attachments, remove unused access, and not pay ransom if they are attacked as it is not guaranteed their files will be accessible [17].

The financial incentives for companies to pay ransoms have been increased by the rapid growth of cyber-insurance, which can cover ransoms with a lower deductible. Companies see this as a cost-saving measure, as paying a ransom is cheaper than restoring their systems. This increases the likelihood that attackers will receive their demands. Organizations often rely on cyberinsurance policies to determine the cost of ransom payments or recovery [3]. However, they should prioritize implementing measures to prevent ransomware attacks in the first place.

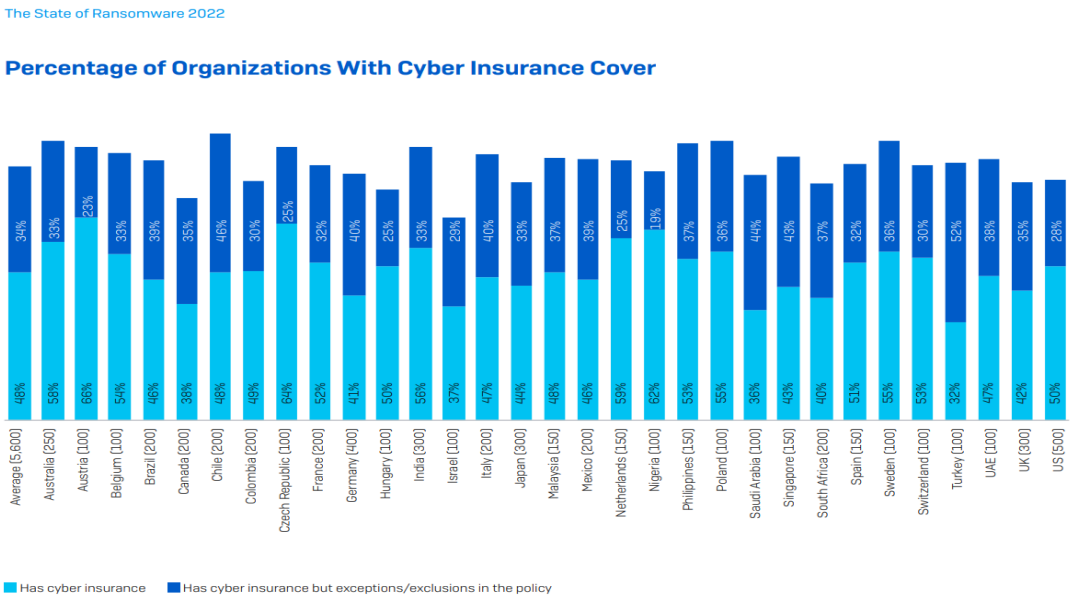

Figure 2. Organizations with Cyber Insurance Based on Countries [24]

4.1 Policies and Regulations

It is crucial to include measures to manage ransomware in the information security and privacy policy to mitigate this malicious threat. Some of the key questions that need to be addressed are:

- Do we have the capability to detect ransomware attacks?
- In case of a ransomware attack, how can we assist our users in decrypting their files?
- How quickly can we address a system vulnerability once it is identified?
- In the event of a suspected ransomware attack, how should we report it and notify the authorities while maintaining confidentiality?

An effective policy with clear procedures can serve as a guide for inexperienced staff and users. However, the policy needs upper management support and enforcement for it to be implemented effectively. According to Jelley, it is vital to have a plan in place for dealing with ransomware attacks, both during and after an attack [15]. Some of the action steps that may be taken include:

- Contacting the national reporting center for cybercrime.
- Disconnecting infected computers from all network connections.
- Reviewing cybersecurity policies to determine the support available.
- Checking if backups are unaffected to restore them.
- Resetting passwords and implementing Multi-Factor Authentication.

4.2 Access Control and Management

Large corporations typically have multiple layers of security that can prevent ransomware from infecting the network by identifying and addressing system vulnerabilities. However, small businesses should implement measures such as using firewalls to regulate access to information, maintaining updated antivirus software, regularly updating systems and software with the latest security upgrades, avoiding downloads from unfamiliar websites, and regularly backing up computer files.

Challenges in mitigating the impact of ransomware on businesses include the limitations of intrusion detection systems (IDS), antivirus, and firewalls. These systems rely on known cyberattack signatures in metadata, making them inappropriate for detecting ransomware or other types of cyberattacks. Ransomware traffic patterns may not be distinguishable from regular traffic patterns, leading to potential misunderstandings of changes in business activity as attacks if proper detection is not done. It can also take time to find the right balance between reducing false alarms and improving detection. Maimó et al. say, "a high false alarm rate can be rather frustrating for the administrator, and a low detection rate can make the system ineffective" [8].

According to Luo and Liao, access control and management are attained with "a centralized IT structure where multi-layer prevention solutions can be efficiently managed by IT professionals" [27]. These professionals will be responsible for maintenance, including updating, troubleshooting, and repairing. They are also authorized to impose ransomware prevention policies to prevent risks.

4.3 Education, Training and Awareness (ETA)

Several industries, such as retail and banking, should implement awareness initiatives to educate customers on how to secure and protect their confidential information online. In addition, organizations should take steps to raise employee awareness, such as having employees acknowledge security guidelines and standards. It's crucial to educate employees on the potential impact of ransomware incidents, such as loss of customers and reduced stock value, to show them why it's important to follow security policies and procedures. By understanding the consequences of their actions, employees are more likely to take the necessary steps to protect the company, customers, and themselves.

According to Landgraf, employees should receive simulated phishing emails from the IT department as a way to increase awareness of the potential risks of opening unknown attachments and links [19]. Other measures may include conducting security system audits and restricting staff from using third-party

applications. Employees should also be mindful of the harmful consequences their emails could have on the company.

4.4 Actionable Practices

There are several specific actionable practices that companies can implement to protect themselves from ransomware attacks:

- Backup data regularly: Regular backups ensure that in the event of a ransomware attack, companies can restore their data without paying the ransom.
- Keep software up to date: Regularly update software with the latest security patches to ensure that known vulnerabilities are not exploited.
- Implement multi-factor authentication: Require employees to use multi-factor authentication (MFA) when accessing sensitive systems or data to prevent unauthorized access in case an employee's credentials are compromised.
- Monitor for suspicious activity: Use monitoring tools to detect suspicious activity in network traffic. This can help to identify a ransomware attack early.
- Develop a disaster recovery plan: Develop a comprehensive disaster recovery plan as a guideline with steps to take in the event of a ransomware attack or other security breach.

These actions can help organizations protect themselves from ransomware attacks and other cybersecurity threats.

5. Conclusion

In conclusion, with the growing prevalence and sophistication of ransomware attacks, organizations must take proactive measures to safeguard their information assets. Ensuring the security of information confidentiality, integrity, and availability requires a thorough understanding of the various types of ransomware attacks and their evolution over time, as well as strategies for prevention. Unfortunately, cybersecurity experts anticipate that ransomware will continue to be a persistent threat in the future. While innovative technologies may improve the ability to detect attacks, cyber attackers are always seeking new methods of causing harm and extorting ransoms [29][30][31]. Thus, it is essential for organizations to prioritize the strengthening and investment in their information security to mitigate the potential for substantial harm.

References

[1] Khan, Muhammad Maaz Ali, Enow Nkongho Ehabe, and Akalanka B. Mailewa. "Discovering the Need for Information Assurance to Assure the End Users: Methodologies and Best Practices." In 2022 IEEE International Conference on Electro Information Technology (eIT), pp. 131-138. IEEE, May 2022. (DOI:10.1109/eIT53891.2022.9813791)
[2] Best Practices for Preventing Business Disruption from Ransomware Attacks. (2021). Seybold Report: Analyzing Publishing Technologies, 21(13), 2–3.
[3] Blessing, J., Drean, J., & Radway, S. (2022). Survey and analysis of U.S. policies to address ransomware.
[4] Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. Network Security, 2016(9), 5–9. https://doi.org/10.1016/S1353- 4858(16)30086-1
[5] Davies, S. R., Macfarlane, R., & Buchanan, W. J. (2021). Differential area analysis for ransomware attack detection within mixed file datasets. Computers & Security, 108, 102377– .https://doi.org/10.1016/j.cose.2021.102 377
[6] Emm, D. (2008). Cracking the code: The history of Gpcode. Computer Fraud & Security, 2008(9), 15-17.
[7] Faghihi , F., & Zulkernine, M. (2021). RansomCare: Data-centric detection and mitigation against smartphone cryptoransomware. Elsevier, 191, 1-10. https://doi.org/10.1016/j.comnet.2021.10 8011
[8] Fernández Maimó, L., Huertas Celdrán, A., Perales Gómez, Á. L., García Clemente, F. J., Weimer, J., & Lee, I. (2019). Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments. Sensors (14248220), 19(5), 1114. https://doi.org/10.3390/s19051114
[9] Fernando, D. W., & Komninos, N. (2022). Feature selection architecture for ransomware detection under concept drift. Elsevier, 116, 1-13. https://doi.org/10.1016/j.cose.2022.1026 59
[10] Frenz, C. M., & Diaz, C. (2016, March 15). Anti-Ransomware Guide [OWASP open Web Application Security Project]. https://owasp.org/www-pdfarchive/Anti-RansomwareGuide.pdf
[11] Jairu, Pankaj, and Akalanka B. Mailewa. "Network Anomaly Uncovering on CICIDS-2017 Dataset: A Supervised Artificial Intelligence Approach." In 2022 IEEE International Conference on Electro Information Technology (eIT), pp. 606-615. IEEE, May 2022. (DOI:10.1109/eIT53891.2022.9814045)
[12] Hampton, N., & Baig, Z. A. (2015). Ransomware: Emergence of the cyberextortion menace.
[13] Herrera Silva, J. A., Barona López, L. I., Valdivieso Caraguay, Á. L., & Hernández-Álvarez, M. (2019). A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters. Remote Sensing, 11(10), 1168. https://doiorg.scsuproxy.mnpals.net/10.3390/rs111 01168
[14] Khan, Saad, and Akalanka B. Mailewa. "Discover Botnets in IoT Sensor Networks: A Lightweight Deep Learning Framework with Hybrid Self-Organizing Maps." Microprocessors and Microsystems (2023): 104753. (DOI: https://doi.org/10.1016/j.micpro.2022.104753).
[15] Jelley, G. (2022). Ransomware attacks - how to deal with them. Education Journal, 501, 27.
[16] Jethva, B., Traoré, I., Ghaleb, A., Ganame, K., & Ahmed, S. (2020). Multilayer ransomware detection using grouped registry key operations, file entropy and file signature monitoring. Journal of Computer Security, 28(3), 337–373. https://doiorg.scsuproxy.mnpals.net/10.3233/JCS191346
[17] Kara, I., & Aydos, M. (2022). The rise of ransomware: Forensic analysis for windows based ransomware attacks. Expert Systems with Applications, 190, N.PAG. https://doi.org/10.1016/j.eswa.2021.1161 98
[18] Kshetri, N., & Voas, J. (2017). Do crypto-currencies fuel ransomware?. IT professional, 19(5), 11
[19] Landgraf, G. (2018). When Ransomware Attacks: How three libraries handled cyberextortion. American Libraries, 49(6), 20–23.
[20] Lee, J. K., Moon, S. Y., & Park, J. H. (2017). CloudRPS: a cloud analysis based enhanced ransomware prevention system. The Journal of Supercomputing, 73(7), 3065–3084. https://doi.org/10.1007/s11227-016- 1825-5
[21] O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. Iet Networks, 7(5), 321-327.
[22] Richardson, R., & North, M. (2017). Ransomware: Evolution, Mitigation and Prevention. International Management Review, 13(1), 10–.
[23] Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabaee, S., Choo, K. K. R., & Al-Qirim, N. (2022). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. Digital Communications and Networks.
[24] Sophos. (2022). The State of Ransomware 2022.

[25] Rozendaal, Kyle, and Akalanka Mailewa. "Neural Network Assisted IDS/IPS: An Overview of Implementations, Benefits, and Drawbacks." International Journal of Computer Applications 975: 8887. (DOI:10.5120/ijca2022922098)

[26] Wang, Z., Liu, C., Qiu, J., Tian, Z., Cui, X., & Su, S. (2018). Automatically Traceback RDP-Based Targeted Ransomware Attacks. Wireless Communications and Mobile Computing, 2018, 1–13. https://doi.org/10.1155/2018/7943586

[27] Xin Luo, & Qinyu Liao. (2007). Awareness Education as the Key to Ransomware Prevention. Information Systems Security, 16(4), 195–202. https://doi.org/10.1080/10658980701576 412

[28] Young, A. L., & Yung, M. (2017). Privacy and Security Cryptovirology: The Birth, Neglect, and Explosion of Ransomware: Recent attacks exploiting a known vulnerability continue a downward spiral of ransomware-related incidents. Communications of the ACM, 60(7), 24–26. https://doi.org/10.1145/3097347

[29] Greengard, S. (2021). The Worsening State of Ransomware: Sophisticated, dangerous ransomware is the new normal ... and there is no simple fix. Communications of the ACM, 64(4), 15–17. https://doi.org/10.1145/3449054

[30] Mailewa, Akalanka, and Kyle Rozendaal. "A Novel Method for Moving Laterally and Discovering Malicious Lateral Movements in Windows Operating Systems: A Case Study." Advances in Technology (2022): 291-321, ISSN 2773-7098. (DOI:10.31357/ait.v2i3.5584)

[31] Mazi, Hilary, Foka Ngniteyo Arsene, and Akalanka Mailewa Dissanayaka. "The influence of black market activities through dark web on the economy: a survey." In The Midwest Instruction and Computing Symposium.(MICS), Milwaukee School of Engineering and Northwestern Mutual, Milwaukee, Wisconsin. 2020.