Evaluating Modern Ransomware and Effective Data Backup and Recovery Solutions

Shivam Patel[1], Aditya Bhadouria[2], Kiran R Dodiya[3], Akash Khunt[4]
[1, 2] M. Sc Cyber security, NSIT-IFSCS (Affiliated to National Forensic Sciences University, Gandhinagar, Gujarat, INDIA)
[3, 4] Assistant Professor (Cyber Security & Digital Forensic) NSIT-IFSCS
(Affiliated to National Forensic Sciences University, Gandhinagar, Gujarat, INDIA)

Abstract- *Ransomware has become a severe cyber threat; recent attacks have been tremendously sophisticated and have shown the potential to encrypt vital data that can leave organisations crippled, only to be unlocked upon payment of exorbitant ransoms. The research investigates fresh ransomware variants and their newer strategies—double extortion and fileless attacks. It considers the most recent incidents to outline the vulnerabilities commonly targeted by attackers and proceeds to project the failures of classic security solutions. In particular, this research design considers strategies for data backup and recovery to respond to such complex threats. Again, it reviews different backup methodologies—full, incremental, and differential—for effectiveness against ransomware. Discussions on new solutions also include immutable storage and air-gapped systems while considering the role of artificial intelligence and machine learning in strengthening predictive and preventive measures. It proposes a step-by-step method for data recovery, citing that recovery plans are necessary for testing timely and updating to restore operations in case of an attack. It discusses the ethical deliberations involved in paying the ransom, pointing out broader implications on organisational reputation and security. This report will yield the necessary actionable knowledge and best practices to IT professionals and organisational heads to reinforce their data backup and recovery strategies and decrease the threat and impact of ransomware attacks.*

Keywords- Ransomware, Double Extortion, Fileless Attacks, Data Backup, Data Recovery, Immutable Storage

I. INTRODUCTION

1.1 Overview of Ransomware Threats

Since the targeted attacks on banks and financial institutions, ransomware has become an imminent threat to these industries. These highly skilled attacks encrypt standard financial information, disrupt the necessary processes, and often require big sums of money to unbolt access. On this, customer trust and regulatory compliance are at risk since many attackers have resorted to double extortion, demanding a ransom and leaking the data. Financial institutions remain under attack due to their vast accumulation of personal details, and the trend of shifting to fileless malware complicates guarding against such threats. Besides ransom demand, such breaches result in huge financial losses resulting from reputational damage, legal issues and massive disruption to operations.

1.2 Importance of Effective Data Backup and Recovery

The impacts of ransomware attacks can be minimised by implementing proper data backup and recovery for the banking and finance industries. This makes the practice of regular and secure backups important to guard crucial financial information, maintain customers' confidence and respond quickly to crises that may force the company to close shop without paying the ransom. Nonetheless, inadequate backup and recovery plans lead to more extended periods offline, missing critical financial data, and considerable suffering to economic health and reputation. Strong backup and recovery measures remain beneficial to safeguard businesses against ransomware attackers because, without them, organisations are likely to fail, attract fines, and lose clients' trust.

II. MODERN RANSOMWARE: EVOLUTION AND TACTICS

2.1 Historical Perspective and Recent Trends: In the past, relatively basic attacks targeting individual systems or organisations were considered the roots of ransomware; they occurred in banking and finances through phishing emails or malicious attachments. In these early attacks, files were encrypted, and the attackers demanded a small amount of money in exchange for the decryption key. Attack techniques evolved due to the growth of sophisticated digital platforms when financial institutions transitioned to a new level. They shifted from attacking random, worthless goals to the networks within enormous financial organisations with more sophistication and planning. This is because criminals have made it more profitable to target the financial industry as they have developed complex ways of exploiting vulnerabilities, disrupting operations, and asking for big money.

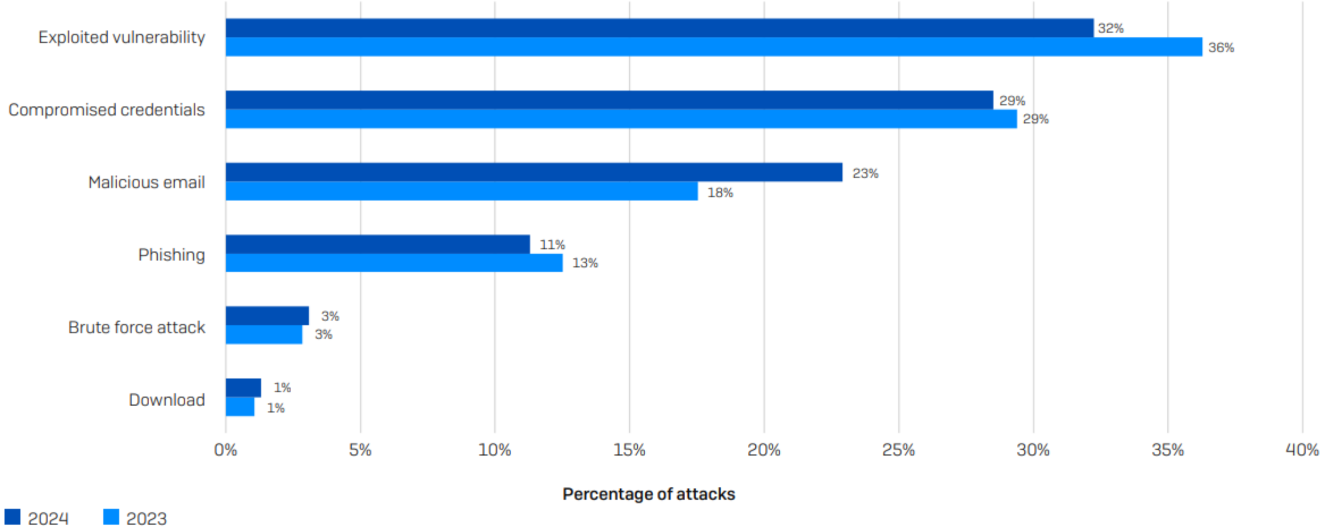

FIG. 1. The following graph displays the overall percentage for the sorts of cyberattacks in the years 2023 and 2024, where one can observe that the most utilised attacking ways were exploited vulnerabilities and suffice for credentials where we can see some difference between the two years.

2.2 New Ransomware Variants

2.2.1 Double Extortion

Blackmail can be defined as demanding someone or a group of individuals to do something or refrain from doing it, especially under the threat of harm or of revealing embarrassing information. The most common type of ransom has been identified in cyber extortion, of which ransomware is the most common, where the hackers hold personal data hostage, with the only way to access the information being to pay the required amount. Double extortion has been more prevalent recently, in which hackers encrypt data and threaten to make it publicly available, putting more pressure on victims to pay the ransom and prevent reputational harm.

2.2.2 Fileless Attacks

A cyberattack that does not depend on conventional malware files is a fileless attack. Rather, it takes advantage of pre-existing software, system utilities, or RAM, making detection and removal more difficult. Because fileless attacks leave no trace on the hard disk, they are highly dangerous and successful at getting past security measures because they are difficult to detect by typical antivirus software.

2.3 Case Studies of Recent Attacks

Young Consulting, now Connexure, recently notified 954,177 people of a data breach from an April 2024 BlackSuit ransomware attack. The Atlanta-based software provider, specialising in employer stop-loss insurance, discovered the breach three days later. Compromised data includes names, Social Security numbers, birthdates, and insurance claims. Affected individuals, including some Blue Shield of California members, are offered a year of free credit monitoring via Cyberscout. BlackSuit leaked the stolen data on its darknet extortion portal after failing to extort the company. Along with what was disclosed in the notices, BlackSuit claims to have leaked more sensitive information, including business contracts, employee passports, and financial records. The ransomware group, a rebrand of Royal, has caused significant financial damage in the U.S., with over $500 million in ransom demands in the past two years. The CDK Global outage is one of their most notable attacks.

Kootenai Health, Idaho's largest healthcare provider, disclosed a data breach affecting over 464,000 patients after a 3 AM ransomware attack. The breach, detected in early March 2024, allowed cybercriminals unauthorised access to Kootenai's systems from February 22, 2024. The investigation, completed on August 1, revealed that stolen data included names, birthdates, Social Security numbers, medical records, and other sensitive information. Although Kootenai Health has not reported any data misuse, it offers 12-24 months of identity protection services to affected individuals. The 3 AM ransomware gang, which operates a Rust-based strain linked to Conti and Royal ransomware, claimed responsibility and leaked a 22GB archive of the stolen data on its darknet portal.

The data is available for free of cost, raising problems about further attacks.

2.4 Common Vulnerabilities Targeted by Ransomware

Ransom variants often operate in weaknesses such as outdated operating systems, non-updated software, small or recycled passwords, and improper configurations enabling remote desktop services (RDS). In addition, phishing attacks are frequently employed using human errors, available open ports in networks, and vulnerabilities in third-party applications. The lack of sufficient email protection and the total lack of multi-factor authentication (MFA) provide ransomware attacks with straightforward vectors.

III. CHALLENGES OF CLASSIC SECURITY SOLUTIONS

3.1 Limitations of Traditional Antivirus and Anti-Malware

The effectiveness of earlier-generation antiviruses and other anti-malware tools is compromised when detecting and neutralising modern dangers. A large part of their discovery is based on signature signatures, which are completely ineffective against new or polymorphic strains of viruses and other malicious programs that change their code. Zero-day attacks can also exploit these tools, which exploit unknown vulnerabilities. Moreover, conventional approaches often lack in-depth behavioural examination, making them somewhat vulnerable to sophisticated attacks like ransomware, which can bypass common defences through fileless and encrypted calls.

3.2 Failures of Conventional Security Measures

The problem is that traditional protection methods are based on dated signature-based detection that cannot identify new or polymorphic threats and do not always protect against ransomware. All these shields may be insufficient in countering current ransomware because threat analysis and constant monitoring are not present, and the employed evasion strategies and zero-day vulnerabilities cannot be predicted. Therefore, ransomware may outcompete the reactive nature of traditional security solutions and penetrate networks, encrypt data, and disseminate in a relatively short time frame, exposing businesses to significant data and economic losses.

3.3 Need for Advanced Protection Mechanisms

Percussions are required beyond traditional security approaches, especially ransomware since the threats have evolved. Addressing new challenges and threats involves machine learning, behavioural analysis, and monitoring in near real-time to identify and contain issues before they become problematic. Risk management involves deploying layered security measures such as EDR, threat hunting, and zero-trust security. The following advanced solutions cannot be overemphasised to achieve information security and ensure secure organisational IT systems.

IV. DATA BACKUP AND RECOVERY STRATEGIES

4.1 Overview of Backup Methodologies

4.1.1 Full Backups

Full backups, the backups of the entire organisation's data at a specific time, are crucial for protecting against data loss due to ransom and malware attacks. This ensures that in the event of an attack, all data, programs and system settings are backed up and restored fully. Ransomware will help organisations reduce downtime and data loss and return to business by maintaining an up-to-date full backup and quickly cleansing an organisation from ransomware without paying any money to criminals.

4.1.2 Incremental Backups

One of the most effective ways of data protection is implementing an incremental backup approach, which works by copying only those files that may have been modified since the last incremental or full backup was done. Due to this method, a lot of disk space is conserved compared to complete backups, and backup times are also reduced. It is important to perform Incremental backups because they help in a sequential recovery process when a threat like ransomware hits. If one or several incremental backups were made, all the later incremental backups are added to the most recent full backup to get the complete backup of the system.

4.1.3 Differential Backups

Differential backups, on the other hand, make a well-balanced backup because they incorporate any changes made since the full backup was done to the full backup to offer data protection. Differential backups collect data so that all the changes made since the previous full backup are held in all backups, in contrast to incremental backups that only record the current changes. Since making a differential backup is less time-consuming than a full backup, this technique makes the restoration process much easier. It is a good strategy for responding to ransom or malware attacks.

4.2 Evaluating Backup Effectiveness Against Ransomware

The method of evaluating the speed and reliability of data retrieval during an attack is used when assessing the effectiveness of backups against ransomware. This involves verifying backups' speed and reliability, ensuring they are up to date, and testing their resistance to ransomware using methods such as making them immutable or storing them on air-gapped media. Reliable protection against ransomware-driven data loss demands frequent recovery rehearsals, anomaly detection, and non-similar backup techniques, including differential, incremental, and complete backups.

4.3 Immutable Storage Solutions

Another characteristic of immutable storage solutions is data protection, which makes them unalterable and nonhackable as soon as they are written. This feature ensures that the stored data cannot be manipulated through removal, overwriting, or change by ransomware or any other illicit user. Common in backup systems, the immutable storage protocols ensure that essential data is secure and available as and when required. It serves a crucial function in financial institutions and businesses, where it is employed to exclude data, adhere to regulations, and facilitate secure data retrieval whenever hackers attack a business entity.

4.4 Air-Gapped Systems

One important safety component of air-gapped systems is the isolation of backups from the principal network, which protects information from ransomware and other web threats. Thus, the chance of infecting backup files with malware is minimised because backup services are not exposed to the web or corporate networks or are connected/directly linked. In the case of ransomware assault, the air-gapped system provides a layer of security because this physical layer ensures that backups remain invulnerable and accessible for use successfully.

V. ROLE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

5.1 Predictive Capabilities of AI and ML

AI and machine learning analyse patterns and anomalies of network activity and data; they offer solid prediction capabilities in the war against ransomware. By detecting any deviation in the normal workflow, these technologies can identify signs of malicious activity, such as file access or attempts to encrypt. AI and ML increase threat discovery and response using vast data and efficient formulas. It allows preventive actions to be taken before ransomware can complete its attack, thereby strengthening the security overall.

5.2 AI-Driven Prevention and Detection

AI solutions in cybersecurity are changing the way of preventing and identifying malware because modern algorithms and machine learning can provide high accuracy. This analysis is conducted on a massive scale by the AI system, which also searches for indicators of malicious activity. This is helpful to them so that these new or unidentified forms of malware are detected and may not be detected by other traditional methods. AI-based solutions are real-time solutions based on constant learning of new threats and adaptation to evolving attacks. This makes the overall strategy more proactive than reactive regarding various complicated threats in cyberspace by increasing threat identification and self-administered countermeasures, reducing the time taken to address the threats.

5.3 Enhancing Backup and Recovery with AI

AI helps in the proper arrangement of data and also helps in the automatic process of creating backups and recovery of data. Starting with the most important information saves time to restore data, ensures more, including failure aspects, and makes more predictable backups accurate with intelligent scheduling. Using Artificial intelligence (AI) technology, restoration procedures can be made faster, problems existing in the backups can be identified and corrected quickly and adapt quickly to changing data conditions. AI significantly reduces the time when means are unavailable and enhances the speed of data retrieval with real-time control; it offers great resistance to data loss and system shutdowns.

VI. DEVELOPING A STRUCTURED DATA RECOVERY PLAN

6.1 Importance of Recovery Plans

When having a ransomware attack, it is crucial to have a recovery plan since it provides assurance on how essential data will be restored and the least time impact on the operations. A clear business recovery strategy will ensure that organisations avoid these or cut their financial losses, protect their image, or refrain from paying the attackers' demands. Further, it assists organisations to quickly resume normal business operations, preserving clients' confidence and enforcing the law. People need effective procedures for recovery to be able to beat ransomware attacks effectively.

6.2 Regular Testing and Updates

Since backup and recovery systems are critical cybersecurity strategies, it is crucial to check on them and update them regularly. Some of these systems can be tested for weaknesses by the organisation and corrected to ensure that data can be recovered in case of an attack within the shortest possible time. New software or new security protocols also help combat new and unknown threats. This preventive measure minimises potential risks, enhances the system's dependability, and ensures that recovery methods are always ready for implementation when required.

6.3 Step-by-Step Recovery Process

Every disaster must have a way of handling it, and data loss or a cyberattack is no exception; it needs a step-by-step recovery process. To begin with, the threat has to be identified and neutralised, and then an assessment of the severity of the incident takes place. Subsequently, identifying critical systems, minimising system outages, and starting points for data recoveries from verified backups should be performed. After the data restoration, it is important to check the operation and functionality of the system. To ensure that resistance is not encountered in the future, a post-recovery assessment will be conducted to identify weaknesses and develop ways of improving the recovery plan.

VII. ETHICAL CONSIDERATIONS AND ORGANIZATIONAL IMPACT

7.1 Ethical Dilemmas of Paying Ransoms

There are serious ethical issues with paying a ransom in the event of a ransomware attack. Inadvertent funding of illegal activity has the potential to incite other attacks and prolong the cycle of cybercrime. Furthermore, paying does not ensure that data will be recovered, and doing so could jeopardise an organisation's credibility with the public. Concerns about ethics also extend to the possible effects on other victims since clearing ransoms may create a precedent that leaves other people more open to similar extortion schemes.

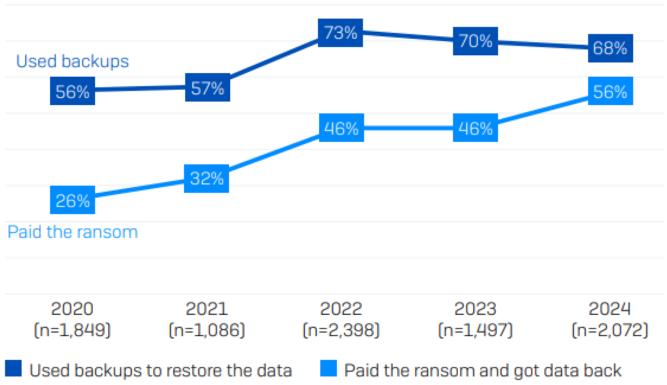

FIG. 2. The graph shows the trends from 2020 to 2024 in how organizations recovered data after a ransomware attack. It indicates that more organizations relied on backups over time while a decreasing proportion paid the ransom and successfully regained their data.

7.2 Impact on Organizational Reputation

The consequences of ransomware attacks also negatively impact the organisation's reputation, causing a drop in consumer trust and, accordingly, the company’s image and revenues. The attack can create doubts in consumers’ minds regarding the protection of the data and overall interruption of operations, which can reduce customers' loyalty and self-confidence in the company. Also, after the attack, an organisation has to work hard to repair the damage done after it has been featured on the news in a negative light or bent the regulatory agencies’ attention.

7.3 Broader Security Implications

Apart from resulting to immediate monetary loss, ransomware attacks have other security implications. They highlight some of the weaknesses in a company’s security architecture and open the company up to other forms of attack from other adversaries. Besides affecting the target company, the clients, partners and other stakeholders, such as the greater community, may also be fêted if a successful assault causes data leaks, IP theft and interruption of critical services. However, suppose the public loses confidence in digital security because of constantly recurring or massive data breaches. In that case, it may lead to stricter rules and regulations and higher compliance costs. The consequences of such events demonstrate the need for the existence and introduction of tight measures to prevent this from happening.

VIII. BEST PRACTICES FOR STRENGTHENING DATA BACKUP AND RECOVERY

8.1 Comprehensive Backup Strategies

The backup approaches must cover all these to restore the data and quickly commence operations in instances like ransomware attacks. To meet both storage capacity and recovery rate, these systems consist of Full backup, Incremental backup and Differential backup. There are offsite and cloud backups to guard data from local disasters, providing an added level of security. Backups are credible, first, because they are continually checked and tested. Moreover, using backup tools decreases the risk of errors, while combining shards with the ability to be tamper-proof and stored on air-gapped storage makes it more difficult for an attacker. They all combine to ensure the system has relatively heavy protection against downtime and data loss.

8.2 Incorporating Advanced Technologies

Identifying and responding to threats is much enhanced when cybersecurity tactics incorporate modern technologies such as artificial intelligence, machine learning, and automation. Before risks are fully manifested, AI and ML can identify patterns that lead to them. Compared to automation, there is a faster response to the queries made and little chance of human errors. Further, these technologies offer analysis of probable future occurrences, which help business entities prevent likely risks. These latter-generation technologies can help organisations build stronger and less reactive introductions to needs produced by changing cyber threats.

8.3 Regular Plan Reviews and Updates

Cyber security, therefore, has to be done to ensure constant assessments and improvements in the strategy. They help ensure that the recovery plans are as accurate and efficient as possible while considering the future changes in cyber threats and various organisational needs of the enterprise. Some dangers might still be in the future that can be covered by altering plans to address relevant threats, new technology, and new laws. They also give you a great opportunity to check the plan’s effectiveness, determine its weaknesses and make the necessary changes if necessary. Such an approach ensures the company is in a position to respond to emergencies in the most efficient manner possible.

IX. CONCLUSION

9.1 Summary of Key Findings

In conclusion, the review of twenty-four types of ransomware between 2015 and 2023 proves that threats in the field of cyber security are rather constant and diverse. Therefore, it is essential to have an effective defence system. As has been observed, every ransomware variation is unique in its way. They all affect different industries through various transmission mechanisms, which cause severe monetary losses and interruptions in business processes. The study also focuses on the need to enhance the understanding that it is crucial for the companies to come up with more enhanced global avoidance schemes that have to be beyond par usual safeguards. Data backup is one technique that needs to be employed, and various techniques, namely differential, incremental, and full backup, need to be employed. As for extra layers of protection, backup copies are kept immutable and stored in an air-gapped environment to prevent data manipulation in case of an attack.

Developing a comprehensive DR plan when creating a data recovery strategy is also important since it helps organisations continue business without paying the demanded ransom. This includes AI integration, enhancing the detection and reaction to threats, and regularly assessing backup and recovery measures. Therefore, the results demonstrate the need to have a proactive and dynamic security approach in terms of an organism experiencing changes in its security plan frequently and constant monitoring for threats to encounter ransomware. These advanced strategies can help businesses reduce the impacts of ransomware attacks, safeguard their data and ensure business continuity in an environment that has become more threatening with time.

9.2 Recommendations for IT Professionals and Organizational Heads

Both organisational decision-makers and IT professionals must pay significant attention to implementing comprehensive security solutions, including advanced threat identification tools and sound contingency plans. Please review the changes in data recovery to ensure they are up to date and in a position to be tested to withstand any new ransomware attack—Emphasise staff awareness of social engineering and phishing threats since most attacks first begin with the employees. Artificial intelligence-based technologies should also be employed to improve security and keep abreast of new threats. Developing an active and effective defence strategy against cyber threats is among the common goals that should be set by the company’s leadership and the IT systems departments.

9.3 Future Directions in Ransomware Defense

AI and machine learning are expected to play a larger role in any ransomware counteraction in the future, as these technologies can prevent these kinds of attacks from occurring. Analytic backups and recoveries will ensure the data can be restored quickly, which eliminates opening doors for interruption in access architectures through zero-trust concepts. Cybersecurity solutions should be advanced and combined with threat intelligence in real-time to sustain the unpredicted ransomware techniques and enhance the organisations' readiness level against such threats.

REFERENCES

[1] M. Ahmed, C. Pagutaisidro, A. Alexander Pike, Y. Yang, and A. S. Khan Pathan, “RansomCoin: A New Dataset for Analysing Cryptocurrency Transactions - Addressing a Gap in the Literature,” in IEEE INFOCOM 2023 - Conference on Computer Communications Workshops, INFOCOM WKSHPS 2023, 2023. doi: 10.1109/INFOCOMWKSHPS57453.2023.10225797.

[2] N. Kyurkchiev, A. Iliev, A. Rahnev, and T. Terzieva, “A new analysis of crypto locker ransomware and welches worm propagation behaviour. Some applications,” Communications in Applied Analysis, vol. 23, no. 2, 2019.

[3] L. Abrams, “Chemical distributor pays $4.4 million to DarkSide ransomware,” Bleepingcomputer.

[4] CISA and FBI, “Darkside Ransomware : Best Practices for Preventing Business Disruption from Ransomware Attacks,” Product ID: AA21-131A, vol. 21, no. 13, 2021.

[5] A. C. Wood and T. Eze, “The evolution of ransomware variants,” in European Conference on Information Warfare and Security, ECCWS, 2020. doi: 10.34190/EWS.20.027.

[6] G. O. Ganfure, C. F. Wu, Y. H. Chang, and W. K. Shih, “DeepWare: Imaging Performance Counters With Deep Learning to Detect Ransomware,” IEEE Transactions on Computers, vol. 72, no. 3, 2023, doi: 10.1109/TC.2022.3173149.

[7] D. Rendell, “Understanding the evolution of malware,” Computer Fraud and Security, vol. 2019, no. 1, 2019, doi: 10.1016/S1361-3723(19)30010-7.

[8] A. Oktaviani and M. Syafrizal, “GandCrab Ransomware Analysis on Windows Using Static Method,” Buletin Ilmiah Sarjana Teknik Elektro, vol. 3, no. 2, 2021, doi: 10.12928/biste.v3i2.4884.

[9] K. Komarov, S. Dursun, S. Erdin, and P. T. Ram, “NetWalker: A contextual network analysis tool for functional genomics,” BMC Genomics, vol. 13, no. 1, 2012, doi: 10.1186/1471-2164-13-282.

[10] J. Tidy, “How hackers extorted $1.14m from University of California, San Francisco - BBC News,” BBC News, 2020.

[11] R. L. P. Sai and T. P. Kumar, “Reverse engineering the behaviour of NotPetya ransomware,” International Journal of Recent Technology and Engineering, vol. 7, no. 6, 2019.

[12] J. Fruhlinger, “Petya ransomware and NotPetya malware: What you need to know now,” CSO Online. 2017.

[13] A. Dalvi, P. Kulkarni, A. Kore, and S. G. Bhirud, “Dark Web Crawling for Cybersecurity: Insights into Vulnerabilities and Ransomware Discussions,” in 2023 2nd International Conference for Innovation in Technology, INOCON 2023, 2023. doi: 10.1109/INOCON57975.2023.10101162.

[14] “Supply chain attack on Kaseya compromises hundreds of firms,” Computer Fraud & Security, vol. 2021, no. 7, 2021, doi: 10.1016/s1361-3723(21)00068-3.

[15] A. Hanel, “Big game hunting with ryuk: Another lucrative targeted ransomware,” Retrieved May, vol. 1, 2019.

[16] R. Surya Kusuma, R. Umar, and I. Riadi, “Network Forensics Against Ryuk Ransomware Using Trigger, Acquire, Analysis, Report, and Action (TAARA) Method,” Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 2021, doi: 10.22219/kinetik.v6i2.1225.

[17] O. Filipec and D. Plášilb, “THE CYBERSECURITY OF HEALTHCARE The Case of the Benešov Hospital Hit by Ryuk Ransomware, and Lessons Learned,” Obrana a Strategie, vol. 21, no. 1, 2021, doi: 10.3849/1802-7199.21.2021.01.027-052.

[18] K. Kraszewski, “SamSam and the Silent Battle of Atlanta,” in International Conference on Cyber Conflict, CYCON, 2019. doi: 10.23919/CYCON.2019.8757090.

[19] D. Palotay and P. Mackenzie, “SamSam ransomware chooses its targets carefully,” Sophos, 2018.

[20] Kaspersky Lab, “What is ‘WannaCry’ ransomware?,” AO Kaspersky Lab. 2021.

[21] Kaspersky, “Ransomware WannaCry: All you need to know,” AO Kaspersky Lab. 2022.

[22] J. Jones and N. Shashidhar, “Ransomware analysis and defence: WannaCry and the Win32 environment,” International Journal of Information Security Science, vol. 6, no. 4, 2017.

[23] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, “WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms,” Journal of Telecommunications and

Information Technology, no. 1, 2019, doi: 10.26636/jtit.2019.130218.

[24] C. S. Anand and R. Shanker, “Zero Trust Resilience Strategy for Linux Crypto Ransomware Obviation and Recuperation,” in 2023 3rd International Conference on Intelligent Technologies, CONIT 2023, 2023. doi: 10.1109/CONIT59222.2023.10205545.

[25] G. Kim, S. Kim, S. Kang, and J. Kim, “A method for decrypting data infected with Hive ransomware,” Journal of Information Security and Applications, vol. 71, 2022, doi: 10.1016/j.jisa.2022.103387.

[26] M. Nicho, R. Yadav, and D. Singh, “Analyzing WhisperGate and BlackCat Malware: Methodology and Threat Perspective,” International Journal of Advanced Computer Science and Applications, vol. 14, no. 4, 2023, doi: 10.14569/IJACSA.2023.0140456.

[27] McAfee Blogs, “Ransomware Maze,” https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/.

[28] Q. Kerns, B. Payne, and T. Abegaz, “Double-Extortion Ransomware: A Technical Analysis of Maze Ransomware,” in Lecture Notes in Networks and Systems, 2022. doi: 10.1007/978-3-030-89912-7_7.