ISSN: 2634 - 8853

Journal of Engineering and Applied Sciences Technology

SCIENTIFIC Research and Community

Review Article

Open Access

# Ransomware Evolution and Defense Strategies

**Anvesh Gunuganti**

USA

## ABSTRACT

Ransomware has become one of the most rampant and financially damaging cyber threats in the modern world, affecting organizations and individuals. This paper aims to give a detailed overview of ransomware, starting with defining and developing the malware type and its main functions. It will culminate by discussing the subject's severe consequences for cybersecurity. Providing background on ransomware starting with its first appearance in the late 1980s, the appraisal goes on to present the different stages of ransomware involving more complex encryption and demanding cryptocurrency as the type of virtual currency for the ransom; the appraisal gives an overview and operation strategies as well as global effects of ransomware incidents. Particular consideration is made to the cost impact, such as monetary losses, negative impact on operations, and society's repercussions when it loses trust in digitally connected procedures. The research also looks at the current defense measures against ransomware and stresses the need to employ proactive security measures, well-developed responses to ransomware attacks, and specific vulnerabilities existing in the sectors. Finally, the study concludes with future recommendations that organizations and individuals can implement about ransomware and its impact from synthesizing thematic analysis findings. Last, this study highlighted the limitations and further research agenda related to ransomware threats in the modern world.

***Corresponding author**
Anvesh Gunuganti, USA.

**Received:** November 06, 2022; **Accepted:** November 11, 2022; **Published:** November 29, 2022

**Keywords:** Ransomware, Cybersecurity, Encryption, Defense Strategies, Incident Response

**Abbreviations**
**RSA:** Rivest-Shamir-Adleman (Encryption Algorithm)
**AES:** Advanced Encryption Standard
**RaaS:** Ransomware-as-a-Service
**MBR:** Master Boot Record

## Introduction

Ransomware has quickly become perhaps the most well- known and hazardous cybercrime in recent years, impacting organizations and people worldwide. Here are some relevant data points:

- **Global Impact:** Cybersecurity Ventures estimates that ransomware attacks will continue to cause more than $265 billion in damages to businesses and organizations worldwide.
- **Frequency of Attacks:** Ransomware attacks always happen at high frequency. For instance, global ransomware attacks amounted to more than 305 million in 2022, considered to have risen from previous years.
- **Targeted Sectors:** The major domains of ransomware attacks are healthcare, finance, government, and SMBs. Healthcare organizations are some of the most at-risk due to the importance of their functions and because they deal with people's personal information.
- **Evolution:** Ransomware has not only graduated from the relatively basic implementation of encryption but has also gone further to incorporate data exhilaration, double extortion, and ransomware as a service, an aspect that sees technologically inexperienced hackers gain access to the software's source. Figure 1 explains the evolution and trends of ransomware.

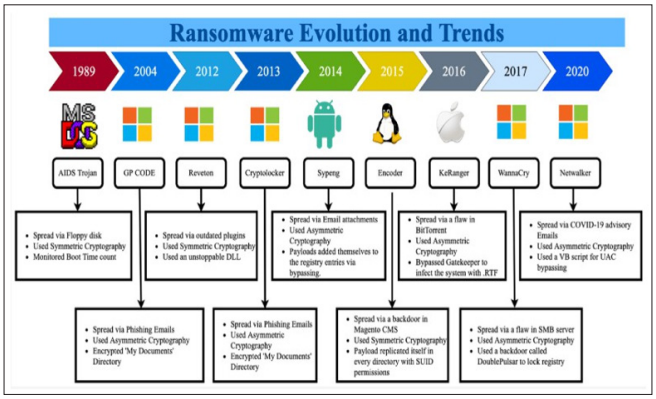


**Figure 1:** Ransomware Evolutions and Trends [1]

## Definition of Ransomware and Its Basic Mechanisms

Ransomware is another kind of malware dedicated to taking control of a computer and its data, encrypting it, and then extorting money from the victim to unblock the control or decrypt the data [1]. This type of cyber threat typically gains access to a system through different channels, such as accessing emails with a dangerous attachment, having kits that take advantage of vulnerability in a program, and false downloads. Ransomware, once triggered, either locks the users out of their systems or encrypts an organization's valuable files using modern forms of cryptography, rendering the files inaccessible without the right decryption key. They will threaten to release sensitive information or encrypt all files owned by the victim, and they always demand money with the assurance that they will return control of the computing system or the data back to the owner once payments have been made in cryptocurrencies, most of the time to ensure that the identity of the buyer is concealed.

- **Infiltration through Various Vectors:** Ransomware becomes part of the operating system through phishing emails with infected attachments and links, exploit kits that seek to find weak points in the software and downloads from compromised Web sites.
- **Swift Encryption or System Lockout:** Ransomware rapidly threatens the confidentiality of important data or denies users access to their computers once criminals set it off.
- **Demand for Ransom Payment:** This involves the attacker's request for a certain amount of money, especially in bitcoins or any other cryptocurrency, to provide decryption keys, release encrypted files, or control the affected system.
- **Use of Advanced Encryption:** Ransomware used today can employ complex encryption algorithms like RSA or AES, meaning that without the correct key, the data cannot be decrypted.
- **Evolution to Double Extortion:** Some add extra layers of pressure by demanding that victims not inform the public of the breach and demanding payments to retrieve the codes to unlock the files.
- **Ransomware-as-a-Service (RaaS) Model:** RaaS models increase the scope of ransomware as a service that provides cybercriminals with access to leasing ransomware tools and infrastructure.
- **Global Impact and Economic Motivation:** Ransomware attacks directly affect the economy and the implementation of countermeasures and are considered an acute problem in cybersecurity.

## History and Evolution of Ransomware

Ransomware has evolved from the era it started in the late 1980s to the modern era [2]. The early ransomware had simple encryption techniques and frequently asked for money through basic communication techniques like post or phone. Ransomware has evolved and become a dangerous GCE threat. Contemporary versions incorporate more elaborate data encryption methods; retrieving lost information without decryption codes is almost impossible. Easy and anonymous payments are made possible by assets such as Bitcoin, which has killed the traditional ransom forms. Some are Crypto Locker, which first appeared in September 2013, using very strong encryption and accepting payment only in Bitcoins; WannaCry in May 2017, in a single day, affected computers in over 150 countries, initially was thought to be an isolated stand-alone ransomware but was later discovered to be symptomatic of a vast worm. Further, ransomware has evolved with business models where perpetrators can buy ransomware as a service (RaaS). Hence, everyone can participate in ransomware attacks. Figure 2 explains the ransomware operations.

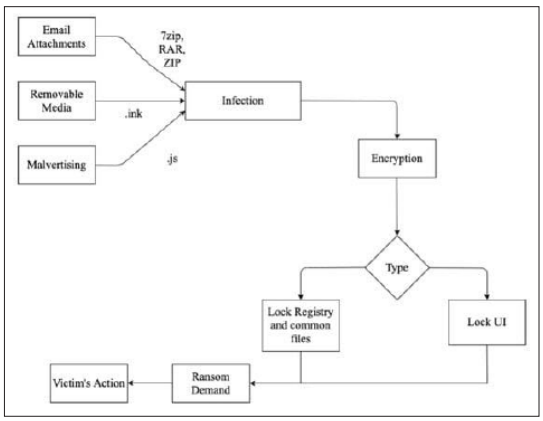


**Figure 2:** Ransomware Sequence of Operations [1]

## Significance of Ransomware in Cybersecurity

Ransomware causes have been established as a severe threat that affects organizations and persons globally. Categorized as the insidious type of malware intent on entering computing systems, encrypting information, and obtaining payments to provide decoding rights, it exemplifies an opposite depth in cybersecurity [3].

- **Impact on Organizations and Individuals:** In its dangerous effect on any organization, ransomware attacks stall or hinder organizational activities, incurring downtime or data loss and may tarnish the organization's image. Ransomware outcomes can be dire to personal data and cause financial loss and immense stress to an individual.
- **Economic and Social Consequences:** Ransomware poses a costly financial threat to its targets, and globally, its damages are in the billions of dollars yearly. These costs comprise the ransom that needs to be paid, recovery expenses, and the time lost in productivity. Criminally, ransomware erodes the public's confidence in technologies and calls attention to flaws in vital industries such as healthcare, finance, and government organizations.
- **Adaptability and Sophistication:** The ransomware threat does not stand still and has established elements of inspired strategies since it uses the modern approach to encrypt data with complex algorithms, using which decryption is only possible with the help of decryption keys. Cybercriminals have resorted to using cryptocurrency, especially when paying ransom, making it difficult to track criminals.
- **Sector-Specific Vulnerabilities:** Different industries are at different risk of ransomware attacks. Most frequently, such information is attacked because the data managed in healthcare organizations is highly valuable; the deterioration of patient care data quality may greatly affect the delivery of medical services. Likewise, financial institutions are exposed due to the nature of offering financial services and handling clients' confidential information.
- **Global Impact and Response:** Ransomware operates worldwide and impacts organizations of every size and location. The more famous cases, such as Wanna Cry or Not Petya, have proven that ransomware attacks are global and universal and can cause substantial losses; therefore, international cooperation and further regulation of cybersecurity measures have been identified.

Lastly, ransomware is one of the most destructive threats in the sphere of cybersecurity, which is why it is necessary to develop reliable protection measures, identify potential threats, and build efficient response plans. Combating this new, more formidable threat demands integrating various sectors' efforts to improve cybersecurity measures and promote awareness to prevent ransomware attacks.

## Impact of Ransomware on Organizations and Individuals

Ransomware attacks are major hazards for organizations and individuals. They are unprecedented and can result in massive operation disruptions, vital data compromise, and enormous organizational financial impacts. Such scenarios cause disruption of business operations, reduce productivity, and negatively impact customers' confidence [4]. Furthermore, it means that ransomware attacks harm reputations, which creates long-term threats to organizations' sustainability. People are also affected by the possible loss of information, blackmailing, and other stress caused by privacy and security breakage.

**Economic and Social Consequences of Ransomware Attacks**
Ransom costs resulting from such attacks are nominal, and damages worldwide amount to billions yearly. Direct costs consist of the money paid to release data to the attacker, which may be hundreds of dollars to millions depending on the organization's value of the ciphered information [5]. These three areas are Defined costs, which refer to the expenditure with a bearing on recovery, cybersecurity, and probable litigation costs. Also, ransomware attacks dangerously interfere with society due to losing confidence in the digital ecosystems and drawbacks of key infrastructural fields like healthcare and financial services. Ransomware disruption emphasizes the efficacy of cybersecurity approaches and preventive methodologies.

**Research Objectives and Scope**
This paper mainly seeks to present a noteworthy analysis of ransomware and its life-changing effects on organizations and people. Moreover, the review intends to ascertain and analyze the most methodologically sound approaches to combating ransomware attacks in modern-day cybersecurity environments. The specific objectives to achieve this aim include: The specific objectives to achieve this aim include:

- **Tracing the Development and Key Milestones of Ransomware:** Exploring the ransomware threat from its development stage, from simple kinds to the most advanced one now.
- **Explaining Operational Mechanisms and Effects:** Explaining how ransomware works in technical processes, how it spreads, and the economic and social consequences of its successful application.
- **Reviewing Current Defense Strategies:** Evaluating the current state of defense approaches and strategies used by the organization and cybersecurity specialists for dealing with ransomware threats. This encompasses assessing prevention, diagnosis, and response measures to crime occurrences.
- **Offering Practical Recommendations for Protection:** Offering practical advice based on findings for organizations and individuals on strengthening the defenses against ransomware attacks. Some advice could be on routines for preventing cyber threat incidences, orientation of employees, and acquisition of innovative security solutions.
- **Identifying Gaps and Future Research Directions:** Find the existing research and knowledge breakdown on ransomware defense. Suggesting directions for future studies to expand knowledge in the field and improve existing and future ransomware defense strategies and counter measures.

In this regard, achieving these objectives will assist the review in providing useful information on the fight against ransomware and help enhance cybersecurity threats' resistance worldwide.

**Research Questions**
How has ransomware evolved, and what are the most effective defense strategies?

**Literature Review**
Ransomware has become one of the most common and monetarily damaging threats and in 2022, confirmed and suspected cases of ransomware attacks reached over 305 million. These cyber-attacks affect almost all spheres of life, including healthcare and small businesses; they explore the weaknesses in the system and people's mistakes to cause significant economic losses. Based on the damages caused, ransomware is expected to cause more than $265 billion by 2031, asserting it is a significant threat to organizations and economies [6]. Basic encryption applications used by ransomware have evolved along with the double extortion scheme, complicating the cybersecurity exercise. To respond adequately to these threats, there is a need to establish the relationship, characteristics, strategy of operation, and consequences of ransomware, which would be the basis for the construction of adequate protection measures.

**Definition and Evolution of Ransomware**
Ransomware has not been present since the very beginning of modern computing in the late 1980s, but it has developed from a simple tool to something more complex [7]. From a basic application that would only encrypt file names and then require payments in the form of money through the post, ransomware has evolved into a very dangerous threat today. Switching to more effective methods of encrypting, such as the RSA-2048 used by Crypto Locker in 2013, was another step. This advancement allowed the attackers to properly lock the users' data and demand payments in digital currencies such as Bitcoin, which improved their anonymity and productivity. On the same note, ransomware strategies have evolved to recognize that it is no longer adequate to simply encrypt an organization's valuable data; rather, attackers are now deploying double extortion tricks to make it clear they will leak the stolen data if their ransom is not paid. Pandemics like WannaCry in 2017 proved that ransomware was a global threat, which used common operating systems' loopholes to install the virus on half a million computers worldwide, thus showing the importance of effective cybersecurity mechanisms [8].

**Challenges in Privacy and Data Protection**
Ransomware is present in numerous types, which can be subdivided into two major types, namely, crypto-ransomware and locker ransomware. Crypto ransomware deals with file encryption, which makes files unavailable unless a set ransom is provided. In contrast, locker ransomware limits users' access to the system or encrypts files like the master boot record (MBR), making the whole operating system nonfunctional. Such threats generally enter systems as phishing emails with the infected files and Web links or as exploit kits that target software and operating system flaws. Once a system is compromised, ransomware follows a distinct attack lifecycle: The malware attack takes the following stages: infiltration, encryption or locking of all files, demand for an amount of money/ ransom (preferably in bitcoins to ensure anonymity), and in some cases, they provide the decryption key after the payment is made. The above lifecycle shows how strategic and methodical cybercriminals pursue their targets to extort money from the victims [5]. Figure 3 explains the Ransomware detection techniques.

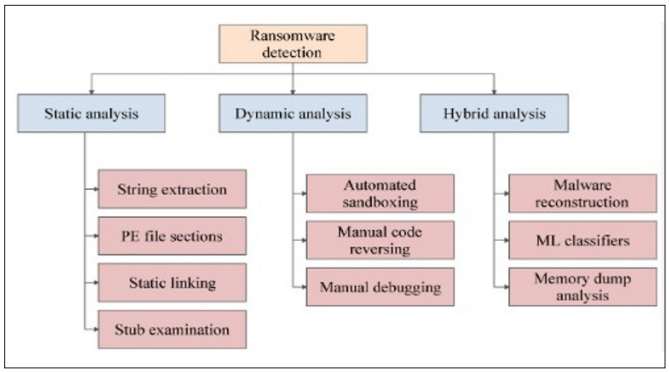


**Figure 3:** Ransomware Detection Techniques [1]

**Applications**
Ransomware is not restricted to specific industries, as each sector has specific vulnerabilities and motives for the attackers. For

instance, in the healthcare sector, organizations are the most targeted in patient care delivery, and the high value is attributed to health records in the black market. Likewise, associated financial risks with financial gains and business reputation are significant in cybersecurity for financial institutions due to ransomware attacks [7]. SMBs are also common targets because hackers assume they have comparatively less developed cybersecurity than bigger companies and are easier targets. Additional trends in ransomware attacks have been seen, such as double extortion attacks, where the attackers will either leak the contents of the targeted organization's data if the ransom established is not paid or continue with the data leak and the attacks that exploit misconfigurations in the cloud services of an organization [2]. Furthermore, ransomware as a service business model has made ransomware attacks accessible to all with even the most basic computer skills, which makes them rather dangerous. Figure 4 also explains the Typical Ransomware mitigation methodologies.

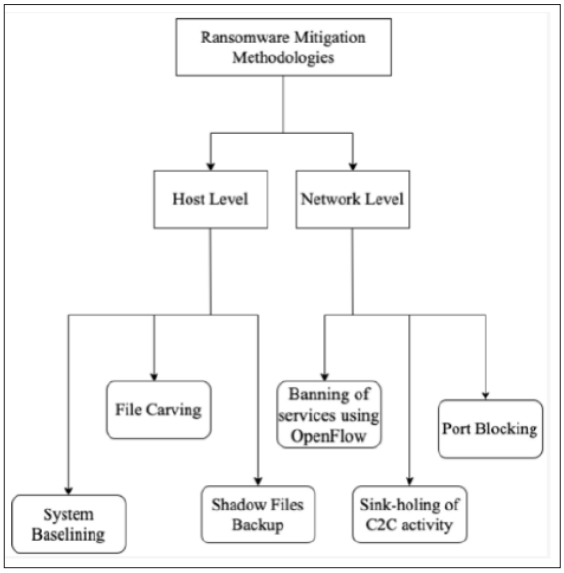


**Figure 4:** Typical Ransomware mitigation methodologies [1]

## Methodology

This paper aims to analyze the defense strategies against ransomware and conclude that ransomware is still a constant threat to cybersecurity due to continuous development. The following section offers a thematic analysis of the paper's findings. It examines and assesses the effectiveness of several defense measures against ransomware with a focus on the case of DJVU Ransomware. Thematic analysis is selected for its logical, methodological method that focuses on making discoveries from decidedly unprofaned data, which is highly relevant when examining the multifaceted approaches to ransomware defense. Thus, by integrating the results of various studies and the peculiarities of specific cases, this review aims to identify recommendations for increasing organizational resistance to ransomware attacks.

## Introduction to Thematic Analysis

Thematic analysis is a type of qualitative research used to analyze data and present certain patterns (themes) included in this data. When it comes to the context of the present review, thematic analysis helps to constitute a solid theoretical background for analyzing the defense from ransomware, mainly based on the results of the case study of the DJVU Ransomware. This methodological approach is chosen as it allows the identification of detailed patterns from different sources and their practical application regarding the use of defense mechanisms against this concrete ransomware type. Thematic analysis is rather clear-sighted because, through superficial and systematic identification of themes, the system offers a clear approach to studying the multifaceted issues concerning ransomware defense and the potential application of such strategies in practice.

## Summary of the Case Study: DJVU Ransomware

The examination of the operational tactics and the consequences of the DJVU Ransomware are described in detail in this study [1]. The recent modifications of DJVU Ransomware are marked by the complex and effective usage of the highly sophisticated types of obfuscation and offline C2 server functions; thus, it affects a wide range of individuals and corporations with considerable consequences for the latter's business continuity and tangible financial losses. Explaining the tactics of DJVU Ransomware in detail, this case study proves the importance of organizations having strong defense measures against this threat, specializing in the methods outlined in the work. Lingering with the details of DJVU Ransomware deepens the practical use of thematic analysis when assessing the defense measures that can successfully respond to such threats.

## Application to Ransomware Defense Strategies

Thematic analysis is a type of qualitative research used for thematic analysis on ransomware protection programs related to the present ransomware variant, and applying the DJVU Ransomware case study, several important themes have been identified as critically important in combating this particular variant. The technological defenses that are present are going to include advanced endpoint protection systems that are used to identify and quarantine ransomware payloads, network segmentation policies that are effectively utilized to control the spread of the ransomware infection in an organization's networks, and secure data backup systems that are used in the event to disinfect the network without capitulating to the attackers demands. Procedural approaches deem it necessary to employ preventive activities that include elaborate incident handling protocols to contain compromised systems and avoid interruption of organizational operations, phishing, and other security awareness campaigns to teach personnel best practices when dealing with the internet and computers, and technical security processes to control for vulnerabilities and prevent new ransomware subtypes from infiltrating organizational systems. This review evaluates the current and future strategies against existing and newly introduced tactics by analyzing these themes related to DJVU Ransomware. This way, the organizations can be fully prepared to protect themselves from new forms of cyber threats, utilizing detailed tactics aligned with the nature of DJVU Ransomware.

## Summary of the Case Study: DJVU Ransomware

Methods used in the thematic analysis must be precedent to guarantee the validity and reliability of the findings. Inter-coder reliability, besides the subjective approach of the primary coders, means that independent coding of the samples by both the researchers and then coming to a consensus improves the reliability of the samples. However, members checking with acquaintances with DJVU Ransomware and peer debriefing corroborate the findings from thematic analysis. Potential sources of bias, including the author's bias, conclusion, and prejudice, are minimized through reflexivity and readable mitigation techniques that enhance the rigor of the findings on the best practices of ransomware defense against DJVU Ransomware. Such methodological approaches help comprehensively analyze the current cybersecurity paradigms and supply practical recommendations for strengthening organizational protection against ransomware attacks.

**Findings and Discussion**

Ransomware is still a huge menace to organizations and persons across the globe, and the attacks remain frequent and elaborate. In 2022, ransomware attacks increased by 151%, affecting healthcare, finance, and government industries. These attacks not only interfere with business but also cause huge losses: by 2031, the losses may exceed $265 billion. Therefore, the further development of ransom tactics – employing more sophisticated encryption algorithms and rendering ransomware as a service – indicates the necessity for effective defense measures. It is important to comprehend ransomware defense tactics' paramount outcomes and related consequences to efficiently cope with these growing cybersecurity threats.

**Synthesis of Key Themes and Insights**

Applying thematic analysis to the identified strategies for ransomware defense and mainly concentrating on the DJVU Ransomware case, it is possible to outline several critical issues for efficient defense against this developing cyber threat.

- **Technological Defenses:** Endpoint protection is used, including the implementation of strong network segmentation and dependable backup systems to minimize the effects of ransomware.
- **Procedural Strategies:** Policies & procedures such as having detailed plans for dealing with incidents, regular training for the staff, and identifying vulnerabilities before they are exploited.
- **Insights into Effective Ransomware Defense Strategies:** The use of ransomware thus needs to be protected by umbrella protection, which combines technical and non-technical countermeasures. Endpoint security, for instance, and other solutions like safe backup of data and files are essential in the fight against ransomware. However, process solutions like proper preparations in dealing with incidents and constant employee education are necessary to contain ransomware's effects and further dissemination in different companies.

**Discussion on the Implications of Findings**

Applying the findings from the analyzed themes of this study implicates crucial meaning in the sphere of cybersecurity measures and strategies, primarily concerning ransomware attacks.

**Implications for Cybersecurity Practices and Policies**

The above-discussed defense strategies show that protection against ransomware requires developing robust cybersecurity solutions capable of repelling and healing from attacks. It is recommended that organizations take preventive measures to tackle cyber security threats and incorporate the usage of contemporary technologies along with information security training for their employees.

**Challenges and Opportunities in Defending Against Ransomware**

Firms face risk and proactively while defending against ransomware. Issues that exist are the growing complexity of ransomware techniques, changing patterns of cyber threats and attacks, and the upsurge of attacks on key industries. Still, there is potential to advance in utilizing new technologies in the cybersecurity field, improving relations between the government and businesses, and increasing the awareness and preparedness of the population in cyberspace.

This discussion focuses on the changes in ransomware threats and stresses the importance of long-term and multi- layered approaches to the corresponding danger problems.

**Conclusion**

Ransomware is still a threat that has not gone away, and it still adapts to attack different organizations and people actively. In recent years, the emergence of ransomware-as-a- service (RaaS) models and advanced encryption has been used in ransomware, accelerating the consequences and increasing the level of ransomware threats. Such events cause not only interruptions of business but also lead to noticeable losses and damage the reputation of the enterprises – members of the chain. Since ransomware threats are continuously developing, mitigation approaches enabling firms to avoid such attacks or lessen their effects are very important.

**Summary of Key Findings**

In this review, the existing critical knowledge regarding ransomware and its countermeasures have been majorly reviewed by focusing on the best studies and research works available in the literature while emphasizing that ransomware is a dynamic threat that has repeatedly affected many organizations and individuals worldwide. Nowadays, ransomware is a highly developed threat, utilizing the modern means of encryption and the ransomware-as-a-service model, threatening various spheres of human life, such as healthcare, finance, and administration. The following findings show that various conception layers, including state-of-the-art technological solutions like endpoint protection and backup security, coordinate with procedural components, including incident response planning and regular cybersecurity training. It is pertinent to comprehend these findings to strengthen immunization against ransomware threats in the contemporary context.

Practical Recommendations for Implementing Defense Strategies
Based on the insights gleaned from the review, the following practical recommendations are proposed for implementing effective ransomware defense strategies:

**For Organizations**

- Ensure the organization implements and deploys better endpoint security technologies to help identify, prevent, and counter ransomware attacks.
- Ensure that network segmentation is well developed to effectively hold specific infections in check and isolate them.
- Ensure that the organization has complete and up-to- date incident response procedures to reduce the effects of ransomware attacks on the organization's operations.
- A newsletter and training sessions should be held to introduce the users to the threats, methods of phishing scams, and how to report a case to the system administration.
- Backup data in secure solutions that allow the original data to remain disconnected from the organization's network in case of ransomware encryption.

**For Individuals**

- It is advisable not to click on links or download attachments from unknown people or companies that appear suspicious.
- Update all the standard applications and operating systems with the latest security measures and releases.
- Always adopt complex, non-reusable passwords for all your accounts and apply MFA, wherever offered, for enhanced security.
- Adhering to these best practices can greatly decrease an organization's susceptibility to ransomware attacks and lower the consequences of a breach if one happens.

## Future Research Directions

Looking forward, future research should focus on addressing the following areas to further enhance ransomware defense strategies:

### Identification of Gaps in Current Research

- Continuation of the existing information on new generations of ransomware threats and their methods to avoid detection by cybersecurity systems.
- Determination of the efficiency of the newer solutions, including artificial intelligence (AI) and machine learning (ML), in identifying and preventing ransomware attacks.
- Isolation of assessing the socio-economic effects of ransomware attacks on different fields of social life and geographic locations to design proper countermeasures.

### Suggestions for Future Studies and Areas of Exploration

- Extension of guidelines for warm-bathing automation and threat intelligence sharing on ransomware across organizations within and between sectors.
- Studying the jurisdiction and adopting policies that could help prevent the activities of ransomware actors and the legislation that might require strengthening to ensure sufficient assistance for the victims.

The study of the human behavior factors in connection with ransomware focuses on the aspects of response and recovery of ransomware incidents for better management and handling of the problem.

## References

1. Kapoor A, Gupta A, Gupta R, Tanwar S, Sharma G, et al. (2021) Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. Sustainability 14: 8.
2. Chen Q, Bridges RA (2017) Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware. 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA) 454-460.
3. Manjezi Z, Botha RA (2019) Preventing and Mitigating Ransomware. Communications in Computer and Information Science 973: 149-162.
4. Lee S, Kim HK, Kim K (2019) Ransomware protection using the moving target defense perspective. Computers & Electrical Engineering 78: 288-299.
5. Reshmi TR (2021) Information security breaches due to ransomware attacks - a systematic literature review. International Journal of Information Management Data Insights 1: 100013.
6. Connolly AY, Borrion H (2022) Reducing Ransomware Crime: Analysis of Victims' Payment Decisions. Computers & Security 119: 102760.
7. Szücs V, Arányi G, Dávid A (2021) Introduction of the ARDS - Anti-Ransomware Defense System Model - Based on the Systematic Review of Worldwide Ransomware Attacks. Applied Sciences 11: 6070.
8. Yaqoob I, Ahmed E, Muhammad Habib ur Rehman, Imran M, Guizani M, et al. (2017) The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks 129: 444-458.