Original Article
ISSN (Online): 2350-0530
ISSN (Print): 2394-3629

International Journal of Research - GRANTHAALAYAH
September 2025 13(9), 124–141

THE EVOLUTION AND MITIGATION OF RANSOMWARE: TECHNIQUES, TACTICS AND RESPONSE STRATEGIE

Ehigiator Egho-Promise [1], George Asante [2], Hewa Balisane [3], Adeyinka Oluwabusayo Abiodun [4], Abdulrahman Salih [5], Folayo Aina [6], Halima Kure [7]

[1] Department of Computing, University College Birmingham, United Kingdom
[2] Department of Information Technology Education, Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development, Kumasi, Ghana
[3] Business School, The University of Law, United Kingdom
[4] Africa Centre of Excellence on Technology Enhanced Learning, National Open University of Nigeria Abuja
[5] Northumbria University London, Department of Computer and Information Science
[6] Department of Computing, School of Engineering and Computing, University of Central Lancashire, United Kingdom
[7] Department of Engineering & Computing, University of East London

Received 07 August 2025
Accepted 10 September 2025
Published 13 October 2025

Corresponding Author

Ehigiator Egho-Promise, eegho-promise@ucb.ac.uk

DOI
10.29121/granthaalayah.v13.i9.2025.6361

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Ransomware is still one of the most current and dangerous types of malware on the internet. Ransomware is detrimental in its impact towards both personal and corporate entities, while its consequences are often financially and operationally disastrous. This paper focuses on analysing the ransomware threat capabilities and trends during the last ten years and how cybercriminals have updated their approaches to the threat. The research explores the evolution of ransomware, such as the ransomware-as-a-service (raas), second-stage extortion schemes, sophisticated encryption, and obfuscation techniques. Further, the study measures present-day mitigation measures like endpoint protection, employee training, and incident response systems and defines unmet needs in the present defensive measures. While the paper evaluates cases where organisations have successfully enacted response strategies, organization must ensure proactivity, backed-up presence and effective cybersecurity policies. In addition, the study expects future developments in ransomware attacks to involve artificial intelligence tools to enhance the strategies and attacks towards the key areas of interest, such as the healthcare and energy sectors. The study highlights the necessity for effective legal measures to counter the work of ransomware actors who operate internationally and offers improvements to the policy and defence measures.

Keywords: Ransomware, Malware, Mitigation, Response Strategies, Tactics, Evolution

1. INTRODUCTION

Ransomware is one of the most dangerous cyber threats affecting organisations and people worldwide. Ransomware is a computer virus that steals a victim's data and extorts money from the victim, preferably in crypto currencies Alshaikh et al. (2020). Unlike everyday cyber threats that only interrupt services or simply steal users' data, ransomware demands money by locking users out of their data. Ransomware has risen in prominence over recent years, costing billions of dollars and affecting various sectors, including healthcare, education, and critical infrastructure.

The changes to the ransomware approach have been fast and complex. At the start of the evolution of malware, ransom ships became very basic. These ransomwares were delivered through emails containing links to infected attachments. The approach of the present time is much more sophisticated than that described above Chen and Bridges. (2017). Modern attacks include 'double extortion,' where cybercriminals first steal data from their targets and then demand a ransom for not making it public. Ransomware as a Service (RaaS) has also exposed cybercrime to anyone without fathomable IT knowledge, enabling them to pull off devastating attacks using rented ransomware tools. New attack scenarios are now the Remote Desktop Protocol (RDP) exploits and supply chains, which put pressure on traditionally defined methods Chidukwani et al. (2022).

The application experience of ransomware demonstrates its relevance on both corporate and individual levels. It is ruthless; corporations suffer financial loss and untold harm to their reputation Conti et al. (2018). Ransomware also poses risks to personal identity because hackers can focus on files like financial data, photos, and messages. Data is now an asset that an organisation cannot afford to lose due to the severity of the ransomware attack. Education, risk mitigation, and preparedness for cyberattacks have become increasingly important since ransomware attacks are now inevitable; hence, prevention is imperative in the various sectors Duraibi et al. (2023).

Today, ransomware threats are described as dynamic. Cybercriminals have become more creative and complex in their methodologies and strategies. State Fiscal Year (SFY) 2012 is growing faster than conventional security measures, and solutions are inadequate. This makes ransomware attacks a serious threat – the activities of hackers change as they learn that their previous tactics are not effective anymore Duraibi et al. (2023). This has led not to a stalemate between attackers and defenders but to an endless cycle of development and counter-development, with many modern threats employing artificial intelligence and automation to create bespoke attacks that are hard to stop.

Over time, ransomware strategies have become more complex and thus added new angles to the problem. Gymnastics such as double extortion has complicated the confrontation. The effect is not just money extortion but damage of the organisation's reputation and legal standing Farion-Melnyk et al. (2021). The presence and activity of cybercriminals are on the rise, and the multi-phase approach is now common: the first stage is social engineering or targeting exposed remote access; the second is the uncontrollable spread of the threat in the network area. This web of tactics makes identifying and mitigating ransomware threats even more challenging, even in organisations that consider themselves well protected from such cyber threats Jenkinson (2022).

The constant growth and diversification of ransomware render conventional security measures ineffective. This escalating threat demands an integrated approach that incorporates Threat Intelligence, continuous monitoring, and prompt responses to ransomware attacks and their countermeasures Mos and Chowdhury (2020).

The purpose of this study is to analyse the evolution of ransomware techniques and tactics, examine mitigation strategies and response tactics, identify gaps in current response strategies and propose improvements.

2. LITERATURE REVIEW

2.1. HISTORICAL PERSPECTIVE ON RANSOMWARE

Ransomware, a type of malware that encrypts its victim's files and demands a certain amount of money to decrypt them, has undergone a major development process. Ransomware history dates back to the late 1980s with the AIDS Trojan, also known as the PC Cyborg Virus O et al. (2018). This example came through floppy disks and only encrypted the file names, but it created the premise for the advanced ransomware seen today Berrueta et al. (2019). Ransomware has experienced several important stages in its evolution into the threat it is today Alenezi et al. (2020). Initially, ransomware could be considered very simple, affecting a single user. However, as more and more internet users came to the fore, hackers shifted towards exploiting online threats, leading to many ransomware attacks. The first among these is the GpCode Trojan, which, in the mid-2000s, connected RSA encryption to lock files more securely Ryan (2020).

Bitcoins and other cryptocurrencies are considered as the most secure method for collecting ransom money Conti et al. (2018). As a result of this development, ransomware became a popular criminal business model. Others indicated specific virus attacks like WannaCry and NotPetya witnessed in 2017, which were marked by enormous destruction when ransomware was combined with network weakness Ucci et al. (2019). In recent years, a new trend has emerged: Ransomware-as-a-Service, wherein ransomware authors lease out their malware for a percentage of sales Hacquebord et al. (2022). This business model has also made the ransomware business even more professionalised, to the extent that anyone with no IT background could engage in malicious activity, thus amplifying the rate and sophistication, among other things. New attack methods, for instance, applying machine learning to penetration, are gradually improving the threat environment, making ransomware resistant Lee et al. (2019).

2.2. MODERN RANSOMWARE TECHNIQUES AND TACTICS

The latest ransomware attack techniques employ highly evolved methods of penetrating a company's systems and utilise sophisticated forms of data encryption. An active form of threat is phishing, in which cybercriminals send out emails that look like legitimate ones Nagar (2024). These are normally sent with attachments or links that install ransomware. For example, an ordinary invoice may contain a link that, once clicked, will launch an attack on the system. This technique, highly based on social engineering, still holds good due to its reliance on human mistakes Yaqoob et al. (2017). Another well-known technique by which ransomware penetrates an organisation's system is through Remote Desktop Protocol (RDP) attacks Wang et al. (2018). RDP has become one of the most used tools for administrators to work with systems remotely and simultaneously. The attackers use common cracking practices to weaken passwords or inappropriately access the

RDP settings' vulnerabilities. Once an attacker is inside the system, the ransomware is delivered directly and compromises the organisation's network without being detected Szücs et al. (2021).

Modern ransomware variants employ asymmetric encryption McIntosh et al. (2021). This prevents victims from decrypting their files without paying the ransom. An example of this is seen in the Crysis ransomware family: the program encrypts data securely and effectively Chittooparambil et al. (2019). Ransomware, particularly through Ransomware-as-a-Service (RaaS), is one of the emerging, innovative, and perilous cybercrime trends Ganguli (2024). Although hacking tools are difficult to master, RaaS simplifies the process so that even inexperienced hackers can launch ransomware attacks, as other experts handle the technical details. Such services are marketed on the black market with customer support, updates, news, and user manuals, similar to software products. The availability of the RaaS model has broadened access to ransomware for a wider range of attackers, resulting in a rise in ransomware incidents worldwide Kang and Gu (2023).

A more recent form of attack is double extortion, where attackers not only encrypt data but also demand that victims pay the ransom and keep their personal information from being leaked Meurs et al. (2024). This method forces victims to pay by threatening both data encryption and potential data disclosure. For instance, the Maze ransomware group pioneered this approach by leaking data from non-compliant victims to blackmail them, thereby increasing the pressure on their targets O'Meara and Parisi (2020).

Furthermore, some ransomware groups have discovered new tactics, such as disabling backups and recovery systems to hinder recovery, using anti-analysis techniques to avoid detection, and targeting specific sectors or businesses to maximise damage Kapoor et al. (2021). These strategies show that ransomware is a constantly evolving field due to advancing cybersecurity measures. As cybercriminals continue this highly inventive and persistent effort, cybersecurity professionals must rise to the challenge and do everything possible to protect valuable information and maintain the integrity of information systems.

2.3. RANSOMWARE MITIGATION AND RESPONSE STRATEGIES

Effective mitigation and response strategies are crucial in defending against ransomware attacks and managing their consequences. The primary line of defence involves robust endpoint detection solutions, comprehensive backup strategies, and stringent network segmentation.

Endpoint Detection and Response (EDR) systems are vital, providing real-time monitoring and analysis of events happening on endpoints Cappello (2024). These systems utilize behavioural analysis to detect unusual activity that could indicate a ransomware attack, such as unauthorized data encryption. Once detected, EDR systems can automatically isolate affected endpoints to prevent ransomware spread within the network Kaur and Tiwari (2021).

Backup Strategies are equally critical in ransomware mitigation. Organizations should maintain regular, encrypted, isolated backups of all essential data [29]. These backups should be stored in multiple locations, including off-site and cloud environments, to ensure redundancy. The 3-2-1 backup rule is often advocated, involving three copies of data on two different media with one off-site. This strategy ensures that data can be restored even during a ransomware attack with minimal disruption Silverman (2016).

Network Segmentation is also pivotal in limiting the spread of ransomware once it penetrates the network. Organizations can contain the spread of the infection by organising networks into smaller, controlled zones. This limits access to sensitive information and critical infrastructure, which is only accessible through secure and monitored channels, thus reducing the overall impact of an attack Rudd et al. (2016).

An Incident Response (IR) Plan is essential when an attack occurs Ahmad et al. (2021). This plan should include immediately isolating infected systems, identifying the ransomware variant using available cyber threat intelligence, and consulting legal counsel to understand the implications of potential data breaches. Best practices recommend forming a response team that includes IT, security, legal, and public relations members to handle various aspects of the incident efficiently Skopik et al. (2016).

Legal, Ethical, and Policy Considerations in ransomware response also require careful attention Mierzwa et al. (2022). Organizations must report ransomware incidents to regulatory bodies depending on the nature of the data compromised and its jurisdiction. Ethically, the decision to pay a ransom is controversial. While paying the ransom may be pragmatically necessary to recover data, it also funds and incentivizes future activities. Policies at both organizational and national levels should aim to establish clear guidelines on handling ransom payments, reporting incidents, and cooperating with law enforcement Lubin (2022). Internationally, collaboration and adherence to cybersecurity policies and standards, such as those set by the National Institute of Standards and Technology (NIST), can help unify response efforts and strengthen defences Al-Hawamleh (2024). These guidelines assist organizations in preparing for, responding to, and recovering from ransomware attacks, ensuring a standardization of cybersecurity practices.

2.4. GAPS IN CURRENT RESEARCH AND PRACTICES

Even though there has been a lot of research and solutions to ransomware, major loopholes still exist in existing research and anti-ransomware measures. The former lacks the development of preventive models that can detect and neutralise an attack before it becomes active. Current endpoint detection systems only work well against known threats but tend to miss unknown threats. Another area that needs to be researched is the role of artificial intelligence (AI) and machine learning (ML) in ransomware detection and response systems Jakka et al. (2022). Sustainable use of AI and ML is still open in cybersecurity, to enhance these technologies to meet the potential sophistication levels of ransomware Jakka et al. (2022).

Even though some organisations use effective measures to prevent ransomware, most organizations fail to introduce strict, proven, and constantly updated backup procedures Szücs et al. (2021). This makes them insecure since even a single backup that is not encrypted can be a big letdown through data loss or an extortion attempt. There is a recurring problem concerning training and awareness programs. This leads to phishing and social engineering attacks. But it should be noted that training improves the first line of defence Nguyen et al. (2023). These gaps indicate continued research and improvement of practical approaches to strengthening the ransomware threat response. Thus, the topic: The Evolution and Mitigation of Ransomware: Techniques, Tactics and Response Strategies

3. EVOLUTION OF RANSOMWARE: TECHNIQUES AND TACTICS

3.1. TECHNICAL EVOLUTION OF RANSOMWARE ATTACKS

The Technical Evolution of Ransomware Attacks can be explored through advancements in encryption, changes in attack strategy, and increasingly sophisticated obfuscation and anti-detection techniques.

Ransomware relies heavily on encryption to lock files and extort payments from victims. Over time, the sophistication of encryption techniques has progressed, making it more challenging for victims and cybersecurity experts to recover data. The usage of encryption algorithms began with simple plain symmetric methods through to DES, AES, RSA, and SHA Alraizza and Algarni (2023). Among these encryption techniques, AES and RSA are mostly used, with 35.1% and 33.0% respectively Begovic et al. (2023).

Recent developments in ransomware also reflect a trend toward hybrid encryption schemes and ever-stronger key sizes. Ransomware developers now implement secure key management, often generating unique keys per victim or device, further complicating decryption efforts. Compared to the earlier days of ransomware attacks, the situation has evolved from an unfocused mass attack to widespread, sophisticated attacks on particular organizations and industries.

Another level of ransomware evolution is code obfuscation. Attackers now use polymorphic and metamorphic coding style to make the ransomware binaries difficult to identify by known mechanisms. This is because, every instance becomes different and therefore using same signature to detect it becomes ineffective. The rationale for this transformation is to add obscurity to the code, which will make reverse engineering of the code more difficult Md Sultan et al. (2020).

Also, some ransomware attacks use fileless malware that do not leave a detectable file on the computer. With this, Traditional antivirus programs do not detect the malware because, instead of leaving a detectable file on the system, the malware occupies the system memory Kara (2022).

Lastly, ransomware is delivered now as a service. In Ransomware-as-a-Service (RaaS), developers provide ransomware tools and platform to the affiliates where they get an opportunity to execute the attack with ease of convenience. Just like the other affiliate marketing techniques, RaaS platforms offer the affiliates with enhanced concealment features and avoid discovery Kibet et al. (2022).

3.2. BEHAVIORAL PATTERNS AND TRENDS

Ransomware attacks have evolved in predictable ways over time, and there are certain commonalities in the attack patterns that can be identified. These trends are based on delivery methods. These methods include Phishing and Social Engineering Alkhalil et al. (2021), Exploit Kits Hopkins and Dehghantanha (2017), and Remote Desktop Protocol (RDP) Attacks Vitla (2024).

3.3. KEY CASE STUDIES IN RANSOMWARE ATTACKS

High-profile ransomware attacks have shaped how organizations and cybersecurity professionals understand and respond to ransomware threats. Each case provides unique insights into attacker strategies, common vulnerabilities, and response challenges.

1) WannaCry Ransomware

WannaCry ransomware (also known as Wana Decrypt0r, W Cry, WannaCry, WannaCrypt, and WanaCrypt0r) was observed during a massive attack across multiple countries on 12 May 2017. According to multiple reports from security vendors, the total of 300,000 systems in over 150 countries had been severely damaged. The attack affected a wide range of sectors, including healthcare, government, telecommunications and gas/oil production Trautman and Ormerod (2018).

The spread of WannaCry was fast due to exploiting a known Windows Server Message Block (SMB) vulnerability using the EternalBlue exploit, created by the US National Security Agency (NSA) and later released by the hacking group Shadow Brokers. This permitted it to travel horizontally through networks without needing input from users Trautman and Ormerod (2018).

WannaCry utilized symmetric encryption for file locking and ransom requests. A security researcher stumbled upon a "kill switch" domain by accident, and once registered, it halted the malware from spreading.

2) Ryuk (2018-Present)

Ryuk ransomware succeeded in attacking big organizations such as the healthcare and public services. It is frequently associated with “big game hunting”, or attacks designed on large targets, individuals who are willing to pay large amounts of ransoms. The attackers with advanced planning and reconnaissance [48] usually perpetrate the Ryuk ransomware. Ryuk strikes normally start with an infection means (TrickBot or Emotet malware) to help the cyber attackers to understand the environment and take control of the system resources to disable all counter measures before unleashing Ryuk Warikoo (2023). Ryuk uses three stages: infectious phase, espionage phase, and execution phase. This shows that there is a necessity of multiple layers of protection most importantly of email gateways, endpoint protection, and intrusion detection. Also, Ryuk’s attack on critical services shows why a good response strategy should involve isolation of the affected systems, notifying the law enforcement, and developing a ransom decision policy.

4. MITIGATION AND RESPONSE STRATEGIES FOR RANSOMWARE ATTACKS

4.1. PREVENTION TECHNIQUES

4.1.1. EMPLOYEE TRAINING AND AWARENESS PROGRAMS

Employees should be trained to recognize phishing attempts and avoid clicking on suspicious links or attachments. Employees should be trained to question unsolicited requests for sensitive information or changes to account settings, as ransomware often exploits social engineering tactics Hillman, D., Harel, Y., & Toch, E. (2023). Regular simulated phishing tests can help reinforce training and identify employees who may be more susceptible to such attacks Hillman et al. (2023). Furthermore, these proactive measures aim to prevent threat from exploiting vulnerability to cause Disclosure, Alteration or Denial of service Balisane et al. (2024).

4.1.2. SECURITY PRACTICES

1) **Network Segmentation:** Breaking down the network into smaller, separate segments can restrict the spread of ransomware within the network after an

initial attack. It is important to segregate critical systems, particularly those with sensitive data, to avoid unauthorized access by attackers in different areas of the network Almulla and Rahman (2025).

2) **Regular Patching and Updates:** regularly update of operating systems, software, and firmware can improve security. Ransomware often targets vulnerabilities, but by fixing known flaws, you can reduce these risks. This involves fixing security holes in SMB that were exploited in WannaCry Connolly and Wall (2019).

3) **System Hardening:** Unnecessary services, ports, and protocols should be turned off in order to decrease the potential areas for attack. System hardening requires strict access controls and the use of multi-factor authentication (MFA) for sensitive system access.

4.2. DETECTION AND CONTAINMENT

4.2.1. TECHNIQUES FOR RAPID RANSOMWARE DETECTION

1) **Intrusion Detection Systems (IDS):** IDS have the capability to identify unusual activity that may signal a ransomware attack, like abrupt spikes in encryption activity or the quick generation of encrypted files. These systems keep an eye on network traffic to detect any malicious behavior Samonte et al. (2024).

2) **Behavioral Analysis:** Typically, ransomware displays distinct behaviors like encrypting many files, leaving ransom notes, or trying to shut down antivirus programs. Behavioral analysis tools have the ability to detect these patterns in an early stage, even without a recognized signature Albshaier et al. (2024).

3) **File Integrity Monitoring:** File Integrity Monitoring can assist in identifying ransomware in its early stages by observing critical files and directories for any unauthorized modifications. Alerts may be triggered by sudden changes or numerous file edits.

4.2.2. APPROACHES FOR CONTAINMENT TO LIMIT SPREAD

1) **Isolate Infected Systems:** Isolating infected systems upon detection helps prevent the spread of ransomware. Disconnecting from the network or shutting down compromised systems can create a delay for response efforts.

2) **Blocking Unnecessary Network Traffic:** By limiting outbound connections to identified malicious IP addresses or domains, ransomware can be prevented from communicating with its command-and-control server, halting data exfiltration or ransom payment endeavors Pour et al. (2023).

3) **Application Whitelisting:** Application whitelisting is utilized to block unauthorized programs (such as ransomware) from launching; allowing only approved software to operate on the network.

4.3. INCIDENT RESPONSE AND RECOVERY

4.3.1. STRUCTURED RESPONSE STRATEGIES (POST-ATTACK)

1) **Incident Response Plan:** Organizations need a well-established and practiced plan for addressing ransomware attacks with defined roles, duties, and communication procedures. The plan must focus on

controlling the attack, maintaining evidence for forensic examination, and collaborating with external organizations like law enforcement and cybersecurity companies.

2) **Forensic Analysis:** Following containment, performing a forensic analysis is essential in comprehending the attack vector, extent of harm, and any vulnerabilities that were exposed. This data aids in warding off future attacks and bolstering defenses Egho-Promise et al. (2024).

4.3.2. IMPORTANCE OF DATA BACKUPS AND DISASTER RECOVERY PLANNING

1) **Regular Backups:** It is essential to back up data, both locally and remotely, regularly. To avoid ransomware from encrypting backup files, it is important to keep backups separate from the network, such as by using air-gapped or cloud-based storage options.
2) **Disaster Recovery Testing:** Regular testing of disaster recovery plans is essential to ensure that systems and data can be quickly restored in the event of a ransomware attack. Optimizing recovery times is essential in order to reduce downtime and restore critical services without having to pay the ransom Thomas and Galligher (2018).

4.3.3. LEGAL CONSIDERATIONS (REPORTING, REGULATORY REQUIREMENTS)

1) **Reporting Obligations:** Several nations enforce rules mandating the reporting of cyberattacks, particularly those concerning sensitive information. Not reporting a ransomware attack can result in legal repercussions such as fines and penalties.
2) **Data Privacy Regulations:** Non-compliance with data privacy regulations like GDPR or HIPAA can occur when ransomware attacks lead to data breaches. Legal teams must guarantee adherence to applicable laws and collaborate closely with regulatory agencies to handle the breach's repercussions.
3) **Law Enforcement Involvement:** Reporting ransomware incidents to authorities can assist in investigations and offer advice on handling ransom demands. Collaboration with authorities could also aid in averting upcoming attacks.

4.4. EMERGING MITIGATION TECHNOLOGIES

4.4.1. ROLE OF AI AND MACHINE LEARNING IN RANSOMWARE DETECTION

1) **AI-Powered Threat Detection:** By analyzing extensive sets of data, machine learning algorithms are able to recognize new ransomware types by spotting patterns that are not easily seen by conventional signature-focused systems. AI technologies can examine behaviours, network traffic, and system activities to detect possible threats Egho-Gavua et al. (2025), Ferdous et al. (2024).
2) **Predictive Analytics:** AI in Predictive Analytics can forecast and identify threats by examining past attack information, enabling entities

to apply proactive defense strategies rooted in predictive attack patterns Egho-Promise et al. (2024).

4.4.2. EXPLORATION OF ADVANCED ENCRYPTION-BREAKING METHODS AND FORENSICS

1) **Decryption Tools:** Decryption tools are sometimes created by cybersecurity researchers and law enforcement to help victims of certain ransomware without having to pay the ransom. Projects such as NoMoreRansom have played a crucial role in decrypting specific types of ransomware Connolly and Borrion (2022).
2) **Advanced Forensics for Ransomware:** New methods in forensics for ransomware are being developed that concentrate on examining encrypted files in order to determine vulnerabilities that could aid in decryption or tracing the source of the attack. This involves examining encryption keys, ransomware payloads, and interactions with Command and Control (C and C) servers Connolly and Borrion (2022).

5. FUTURE TRENDS IN RANSOMWARE TECHNIQUES AND MITIGATION

5.1. ANTICIPATED EVOLUTION OF RANSOMWARE TECHNIQUES

Ransomware of the future will have AI and ML as some of the driving forces behind its future development, thus making the attacks smart. Organized ransomware actors are adducing AI tools across the progress, from collecting data on potential targets to learning from their interactions with those targets in real-time while launching and executing assaults. Machine learning algorithms can pattern users' activity, traffic, and configuration and find vulnerabilities that usual security practices cannot detect. As ransomware actors continue to leverage these technologies, it will become even easier for them to launch and avoid detection, hence the difficulty in arresting them Bajwa et al. (2021). AI plays a great role in ransomware's technicality and the overall aspects of the attacks. AI-powered bots may also be employed for social engineering by ransomware groups, making precision about phishing and impersonation of formal channels. These bots can also evaluate the target's openness through the kind of posts on social networking sites, email interaction, and connections, making it easier for attackers to plan better and more convincing attacks. In addition, there are even more worrying trends within the expected changes in ransomware in that critical infrastructure is being targeted. In the past, ransomware attacks were aimed at individual enterprises and their data; however, critical infrastructure sectors, including energy grids, water production, and healthcare systems, were attacked. An incident in these sectors could lead to dire consequences as it will not only paralyses services to most companies and households but also present critical threats to public and national security. The future ransomware attacks may also have new techniques, such as exploiting the zero-day vulnerability. In combination with the application of high-level encryption, the specified method can be almost invulnerable to traditional anti-malware tools to eliminate the attacks in real time Wang et al. (2023). In conclusion, ransomware attacks in the future will be smarter, more personal, and more destructive. The use of artificial intelligence and machine learning will enhance the ransomware groups' capabilities to navigate past the traditional security measures more efficiently; at

the same time, the adaptation of targeting essential infrastructures will take the attacks to a completely different and dangerous level. This is an ever-changing frontier, and organisations and cybersecurity specialists need to be ready to address this by deepening their security apparatus and adopting a proactive, adaptive approach to their security measures.

5.2. FUTURE RANSOMWARE MITIGATION AND RESPONSE

Looking at the tendencies of ransomware attacks in modern society, its counteraction and remediation in the future will depend on the improvements of technologies based on artificial intelligence, international cooperation, and legal regulation. Presumably, one of the most important developments in countering ransomware will be the increasing use of artificial intelligence in identifying threats Thomas and Galligher (2018). These systems will be crucial in detecting real-time threats and allowing organisations to spot and act on anomalies, understand what malware is doing and tackle new threats faster. AI and machine learning algorithms will play a major role in threat analysis as the applications help to parse through the application's traffic, users' behaviour, and known attack patterns. It will decrease the time needed to identify and stop ransomware before it could inflict huge harm Sharma et al. (2024).

Besides the AI-based detection model, much is expected from elaborated threat intelligence sharing and international cooperation in ransomware mitigation. These cross-border cyber criminal groups pose a big threat to national and corporate security. Now that ransomware attacks are becoming more geographically dispersed, whenever possible, there will be an increasing measure of international cooperation between governments and organizations to share a range of threat indicators, tactics, and techniques. Cooperation in identifying attackers and creating adequate defence strategies can occur faster. Presumably, similar international standards of cybersecurity, like the GDPR of the European Union or the CISA of the United States of America, will be further developed and adopted to enhance this cooperation. Combination work will remain paramount when tracing and apprehending ransomware sources and their sponsors, even if they are located in parts of the world with scant regard for cybersecurity. As the size and scope of ransomware attacks increase, intelligence and enforcement will require legal and regulatory updates to address the global nature of the threat. Today, legal countermeasures against ransomware are limited and differ from nation to nation in terms of preparedness and legal strategy Pour et al. (2023). The future will probably witness the evolution of international conventions and agreements that will permit more coordination of efforts to address ransomware at the structural level. Some of these legal structures will have to deal with questions like how to govern the flow of information across borders, how to control the uses of virtual currencies – often used in ransom demands – and how to hold organizations that do not adequately protect their networks responsible. Legal enactments will also demand codifying ethical ransom-related issues. Furthermore, organisations will be required to take a more aggressive stance in protecting against ransomware through the so-called 'zero trust' architecture, which entails the idea that both internal and external users and devices may be breached. This approach will entail the constant validation of all the access requests and will eliminate the possibility of the malware to spread in a network Hicks (2023).

6. DISCUSSION AND IMPLICATIONS

6.1. SUMMARY OF FINDINGS

Preliminary observation: the cycle of ransomware development and the ways to combat it shows that the dynamics in the sphere have also increased the level of attacks and the level of attack prevention. Ransomware strategies have shifted from the simple hack-and-scare models to more advanced and highly planned encrypted phishing and ransomware business models. New approaches are also more malicious than before, because they use double extortion. First, they take data and then encrypt it; they threaten to make the information public if the ransom is not paid. In response, mitigation measures are frequently taken, such as training the employees and segmenting the network. AI-based technologies and behaviour-based detection mechanisms are also increasingly useful in the early identification of ransomware attacks. Nevertheless, organisations are plagued with issues about how effectively they can mitigate ransomware risks due to weaknesses in human nature and technology.

6.2. IMPLICATIONS FOR CYBERSECURITY POLICIES

The implications of the current study are quite important in understanding cybersecurity policies within organizations. Although ransomware attacks are constantly rising in complexity and scale, organisations must beef up their cybersecurity approaches as much as possible. Cyber security policies should therefore include Awareness, Segregation, Firewall, and Patching. Furthermore, policies must focus on incident response and backup strategies to ensure rapid restoration in case of an attack. Another important area that will require attention is legislative amendments. Policymakers must focus on multi-stakeholder cyberspace cooperation, to have a common threat intelligence and refer to international cooperation as creating common norms for protecting organisations and reporting cyber incidents.

6.3. LIMITATIONS AND CHALLENGES

This study faced three main limitations and challenges: Limited data on ransomware, limited quantitative data, and lack of consensus on ransomware definition. Because of the nature of the incidents, there is often no reported information about the detailed occurrence of actual attacks or the efficacy of security measures. Also, since it is a rapidly growing and evolving field, certain approaches may give no longer relevant results after a relatively short period. One of the difficulties was the issue of the effectiveness of some of the mitigation measures, as many organizations do not disclose the complete data in the course of recovery operations and, therefore, assess the effectiveness of their strategies. In addition, the emphasis on real-world examples may not cover the variety of attack types, particularly those aimed at less-covered small-scale organizations.

7. CONCLUSIONS

7.1. SUMMARY OF CONTRIBUTIONS

This research has delivered a detailed exploration of ransomware and its prevention measures and written down useful information about cyber attackers' mapper-forming methods and businesses' protective measures. It elaborated on the

changing modus operandi of ransomware attacks, such as double extortion and ransomware as a service, RaaS, and, more specifically, the trend that ransomware has become a highly targeted problem. Additionally, it measures major risk prevention measures: frequent backups, employee awareness, and sophisticated detection tools, which show their efficiency in addressing and minimizing ransomware attacks. The analysis of cases added more knowledge on how organizations can strengthen their cyber security policies to include proactive measures and incident response strategies. In conclusion, it can be stated that the current study makes a positive research contribution to the field of cybersecurity by emphasising that static and single-point approaches are no longer sufficient because ransomware is launching various attacks that have not been previously seen.

7.2. FINAL REMARKS

Preventing ransomware is especially important because it lies in the sociology of a proactive approach to cybersecurity threats and risks. Due to the further development of ransomware attacks and their effects, corresponding technical and personnel measures, the development of concepts for reacting to such attacks, and cooperation between companies and sectors are required. Ransomware threats are persistent, meaning that organizations must be reliable and proactive in their mitigation strategies by implementing new technologies, including the use of artificial intelligence, for threat detection and ensuring everyone in an organization is aware of the threats. The extent of international cooperation that needs to be made and the creation of cybersecurity policies cannot be overemphasized because ransomware attacks are now invading even the most sensitive structures worldwide. Finally, this research restates that despite some progress in addressing ransomware risk, organisations must adopt more robust strategies to improve their mitigation systems against this threat. In conclusion, the pre-emptive holistic approach remains the best way of addressing the increasing menace of ransomware.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Alshaikh, H., Ramadan, N., & Hefny, H. A. (2020). Ransomware Prevention and Mitigation Techniques. International Journal of Computer Applications, 177(40), 31–39. https://doi.org/10.5120/ijca2020919899

Chen, Q., & Bridges, R. A. (2017, December). Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware. In 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA) (454–460). IEEE. https://doi.org/10.1109/ICMLA.2017.0-119

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cybersecurity of Small-To-Medium Businesses: Challenges, Research Focus and Recommendations. IEEE Access, 10, 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899

Conti, M., Gangwal, A., & Ruj, S. (2018). On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective. Computers & Security, 79, 162–189. https://doi.org/10.1016/j.cose.2018.08.008

Duraibi, S., Kaur, C., & Pawar, A. B. (2023, December). Cyber Extortion Unveiled: The Evolution, Tactics, Challenges, and Future of Ransomware. In 2023 International Conference on Computational Science and Computational Intelligence (CSCI) (861–867). IEEE. https://doi.org/10.1109/CSCI62032.2023.00144

Farion-Melnyk, A., Rozheliuk, V., Slipchenko, T., Banakh, S., Farion, M., & Bilan, O. (2021). Ransomware Attacks: Risks, Protection, and Prevention Measures. In 2021 11th International Conference on Advanced Computer Information Technologies (ACIT) (473–478). IEEE. https://doi.org/10.1109/ACIT52158.2021.9548507

Jenkinson, A. (2022). Ransomware and Cybercrime. CRC Press. https://doi.org/10.1201/9781003278214

Mos, M. A., & Chowdhury, M. M. (2020). The Growing Influence of Ransomware. In 2020 IEEE International Conference on Electro Information Technology (EIT) (643–647). IEEE. https://doi.org/10.1109/EIT48999.2020.9208254

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of Ransomware. IET Networks, 7(5), 321–327. https://doi.org/10.1049/iet-net.2017.0207

Berrueta, E., Morato, D., Magana, E., & Izal, M. (2019). A Survey on Detection Techniques for Cryptographic Ransomware. IEEE Access, 7, 144925–144944. https://doi.org/10.1109/ACCESS.2019.2945839

Alenezi, M. N., Alabdulrazzaq, H., Alshaher, A. A., & Alkharang, M. M. (2020). Evolution of Malware Threats and Techniques : A Review. International Journal of Communication Networks and Information Security, 12(3), 326–337. https://doi.org/10.17762/ijcnis.v12i3.4723

Ryan, M. (2020). The Ransomware Revolution : How Emerging Encryption Technologies Created a Prodigious Cyber Threat (Doctoral dissertation, UNSW Sydney).

Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey of Machine Learning Techniques for Malware Analysis. Computers & Security, 81, 123–147. https://doi.org/10.1016/j.cose.2018.11.001

Hacquebord, F., Hilt, S., & Sancho, D. (2022). The Near and Far Future of Ransomware Business Models. Trend Micro Research.

Lee, K., Lee, S.-Y., & Yim, K. (2019). Machine Learning-Based File Entropy Analysis for Ransomware Detection in Backup Systems. IEEE Access, 7, 110205–110215. https://doi.org/10.1109/ACCESS.2019.2931136

Nagar, G. (2024). The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies. Valley International Journal Digital Library, 1282–1298. https://doi.org/10.18535/ijsrm/v12i06.ec09

Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-Garadi, M. A., Imran, M., & Guizani, M. (2017). The Rise of Ransomware and Emerging Security Challenges in the Internet of Things. Computer Networks, 129, 444–458. https://doi.org/10.1016/j.comnet.2017.09.003

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), 7943586. https://doi.org/10.1155/2018/7943586

Szücs, V., Arányi, G., & Dávid, Á. (2021). Introduction of the ARDS-Anti-Ransomware Defense System Model Based on The Systematic Review of Worldwide Ransomware Attacks. Applied Sciences, 11(13), 6070. https://doi.org/10.3390/app11136070

McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P. (2021). Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions. ACM Computing Surveys (CSUR), 54(9), 1–36. https://doi.org/10.1145/3479393

Chittooparambil, H. J., Shanmugam, B., Azam, S., Kannoorpatti, K., Jonkman, M., & Samy, G. N. (2019). A Review of Ransomware Families and Detection Methods. In Recent Trends in Data Science and Soft Computing: Proceedings of the 3rd International Conference of Reliable Information and Communication Technology (IRICT 2018) (pp. 588–597). Springer International Publishing. https://doi.org/10.1007/978-3-319-99007-1_55

Ganguli, P. (2024). The Rise of Cybercrime-as-a-Service : Implications and Countermeasures. SSRN. https://doi.org/10.2139/ssrn.4959188

Kang, Q., & Gu, Y. (2023). A Survey on Ransomware Threats: Contrasting Static and Dynamic Analysis Methods. Preprints. https://doi.org/10.20944/preprints202311.0798.v1

Meurs, T., Cartwright, E., Cartwright, A., Junger, M., & Abhishta, A. (2024). Deception in Double Extortion Ransomware Attacks: An Analysis of Profitability and Credibility. Computers & Security, 138, 103670. https://doi.org/10.1016/j.cose.2023.103670

O'Meara, M. M. K., & Parisi, A. (2020). Current Ransomware Threats. https://apps.dtic.mil/sti/trecms/pdf/AD1110335.pdf

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. Sustainability, 14(1), 8. https://doi.org/10.3390/su14010008

Cappello, M. (2024). A Comprehensive Analysis of EDR (Endpoint Detection and Response), EPP (Endpoint Protection Platform), and Antivirus Security Technologies (Master's Thesis, Πανεπιστήμιο Πειραιώς).

Kaur, H., & Tiwari, R. (2021, November). Endpoint Detection and Response Using Machine Learning. In Journal of Physics: Conference Series (2062, 1, 012013). IOP Publishing. https://doi.org/10.1088/1742-6596/2062/1/012013

Prince, N. U., Al Mamun, M. A., Basfar, R., Wadho, S. A., Asim, M. M., Rabby, S. M. A. H., & Ali, S. (2024). Strengthening Enterprise Cybersecurity: A Survey on Ransomware Mitigation and Recovery Strategies. Nanotechnology Perceptions, 446–462.

Silverman, R. (2016). Surely, we'll Need Backups. Preservation, Digital Technology & Culture, 45(3), 102–121. https://doi.org/10.1515/pdtc-2016-0013

Rudd, E. M., Rozsa, A., Günther, M., & Boult, T. E. (2016). A Survey of Stealth Malware Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions. IEEE Communications Surveys & Tutorials, 19(2), 1145–1172. https://doi.org/10.1109/COMST.2016.2636078

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How Can Organizations Develop Situation Awareness for Incident Response: A Case Study of Management Practice. Computers & Security, 101, 102122. https://doi.org/10.1016/j.cose.2020.102122

Skopik, F., Settanni, G., & Fiedler, R. (2016). A Problem Shared is a Problem Halved: A Survey on the Dimensions of Collective Cyber Defense Through Security Information Sharing. Computers & Security, 60, 154–176. https://doi.org/10.1016/j.cose.2016.04.003

Mierzwa, S., Drylie, J., & Bogdan, D. (2022). Ransomware Incident Preparations With Ethical Considerations and Command System Framework Proposal. Journal

of Leadership, Accountability and Ethics, 19(2), 110. https://doi.org/10.33423/jlae.v19i2.5112

Lubin, A. (2022). The Law and Politics of Ransomware. Vanderbilt Journal of Transnational Law, 55, 1177.

Al-Hawamleh, A. (2024). Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security. International Journal of Computing and Digital Systems, 15(1), 1315–1331. https://doi.org/10.12785/ijcds/150193

Jakka, G., Yathiraju, N., & Ansari, M. F. (2022). Artificial Intelligence in Terms of Spotting Malware and Delivering Cyber Risk Management. Journal of Positive School Psychology, 6(3), 6156–6165.

Nguyen, C., Jensen, M., & Day, E. (2023). Learning Not to Take The Bait: A Longitudinal Examination of Digital Training Methods and Overlearning on Phishing Susceptibility. European Journal of Information Systems, 32(2), 238–262. https://doi.org/10.1080/0960085X.2021.1931494

Alraizza, A., & Algarni, A. (2023). Ransomware Detection Using Machine Learning: A Survey. Big Data and Cognitive Computing, 7(3), 143. https://doi.org/10.3390/bdcc7030143

Begovic, K., Al-Ali, A., & Malluhi, Q. (2023). Cryptographic Ransomware Encryption Detection: Survey. Computers & Security, 132, 103349. https://doi.org/10.1016/j.cose.2023.103349

Md Sultan, A., Bakar, A., Abdul Ghani, A. A., Mohd Ali, N., & Admodisastro, N. (2020). Hybrid Obfuscation Technique to Protect Source Code from Prohibited Software Reverse Engineering. IEEE Access, 8, 187326–187342. https://doi.org/10.1109/ACCESS.2020.3028428

Kara, I. (2022). Fileless malware threats: Recent Advances, Analysis Approach Through Memory Forensics, and Research Challenges. Expert Systems with Applications, 214, 119133. https://doi.org/10.1016/j.eswa.2022.119133

Kibet, A., Esquivel, R., & Esquivel, J. (2022). Ransomware : Ransomware as a Service (RaaS), Methods to Detect, Prevent, Mitigate and Future Direction. Journal of Emerging Technologies and Innovative Research, 9(11), b264–b278.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science, 3. https://doi.org/10.3389/fcomp.2021.563060

Hopkins, M., & Dehghantanha, A. (2017). Exploit kits: The Production Line of the Cybercrime Economy. arXiv preprint. https://doi.org/10.1109/InfoSec.2015.7435501

Vitla, S. (2024). Unsecured Remote Desktop Protocol (RDP) access: A Gateway for Ransomware Attacks and Corporate Extortion. Journal of Computer Science and Technology Studies, 6(2), 150–165. https://doi.org/10.32996/jcsts.2024.6.2.17

Trautman, L., & Ormerod, P. (2018). WannaCry, Ransomware, and the Emerging Threat to Corporations. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3238293

Warikoo, A. (2023). Perspective Chapter: Ransomware. In IntechOpen. https://doi.org/10.5772/intechopen.108433

Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating Organizational Phishing Awareness Training on an Enterprise Scale. Computers & Security, 132, 103364. https://doi.org/10.1016/j.cose.2023.103364

Balisane, H., Egho-Promise, E., Lyada, E., Aina, F., Sangodoyin, A., & Kure, H. (2024). The Effectiveness of a Comprehensive Threat Mitigation Framework in Networking: A Multi-Layered Approach to Cybersecurity. International

Research Journal of Computer Science, 11(6), 529–538. https://doi.org/10.26562/irjcs.2024.v1106.03

Almulla, Z., & Rahman, H. (2025). The Role of Network Segmentation and Micro-Segmentation in Operational Technology Security. In Proceedings of the ICAIIC 2025 (pp. 342–347). IEEE. https://doi.org/10.1109/ICAIIC64266.2025.10920695

Connolly, Y. A., & Wall, D. (2019). The Rise of Crypto-Ransomware in a Changing Cybercrime Landscape: Taxonomising Countermeasures. Computers & Security, 87, 101568. https://doi.org/10.1016/j.cose.2019.101568

Samonte, M. J., Jose, M. Z., Sandoval, M., & De Luna, J. M. (2024). Exploring Data Breach Prevention Strategies in Real-Time Systems Integration and Architecture in the Healthcare Industry. In Proceedings of the 2024 12th International Conference on Computer and Communications Management (ICCCM '24) (pp. 155–163). Association for Computing Machinery. https://doi.org/10.1145/3688268.3688291

Albshaier, L., Budokhi, A., & Aljughaiman, A. (2024). A Review of Security Issues when Integrating IoT with Cloud Computing and Blockchain. IEEE Access, 12, 109560–109595. https://doi.org/10.1109/ACCESS.2024.3435845

Pour, M. S., Nader, C., Friday, K., & Bou-Harb, E. (2023). A Comprehensive Survey of Recent Internet Measurement Techniques for Cybersecurity. Computers & Security, 128, 103123. https://doi.org/10.1016/j.cose.2023.103123

Egho-Promise, E., Idahosa, S., Asante, G., & Okungbowa, A. (2024). Digital Forensic Investigation Standards in Cloud Computing. Universal Journal of Computer Sciences and Communications, 3(1), 23–45. https://doi.org/10.31586/ujcsc.2024.923

Thomas, J. E., & Galligher, G. C. (2018). Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware. Computer and Information Science, 11(1), 14–25. https://doi.org/10.5539/cis.v11n1p1

Egho-Promise, E. I., Asante, G., Balisane, H., Salih, A., Aina, F., Kure, H., & Gavua, E. K. (2025). Leveraging Artificial Intelligence For Predictive Cybersecurity: Enhancing Threat Forecasting and Vulnerability Management. International Journal of Innovative Research in Advanced Engineering, 12(2), 68–79. https://doi.org/10.26562/ijirae.2025.v1202.01

Ferdous, J., Islam, M. R., Mahboubi, A., & Islam, M. (2024). AI-Based Ransomware Detection: A Comprehensive Review. IEEE Access, 12, 136666–136695. https://doi.org/10.1109/ACCESS.2024.3461965

Egho-Promise, E., Lyada, E., Asante, G., & Aina, F. (2024). Towards Improved Vulnerability Management in Digital Environments: A Comprehensive Framework for Cybersecurity Enhancement.

Connolly, A. Y., & Borrion, H. (2022). Reducing Ransomware Crime: Analysis of Victims' Payment Decisions. Computers & Security, 119, 102760. https://doi.org/10.1016/j.cose.2022.102760

Bajwa, J., Munir, U., Nori, A., & Williams, B. (2021). Artificial Intelligence in Healthcare: Transforming the Practice of Medicine. Future Healthcare Journal, 8(2), e188–e194. https://doi.org/10.7861/fhj.2021-0095

Wang, L., Wei, X., Zhang, Y., Gao, Y., & Niu, Q. (2023). A Double Encryption Protection Algorithm for Stem Cell Bank Privacy Data Based on Improved Aes and Chaotic Encryption Technology. PLoS ONE, 18(10), e0293418. https://doi.org/10.1371/journal.pone.0293418

Sharma, A., Babbar, H., & Vats, A. K. (2024). Enhanced Ransomware Detection Using Gradient Boosting Algorithms: A Cybersecurity Dataset Approach. In 2024

5th IEEE Global Conference for Advancement in Technology (GCAT) (pp. 1–5). IEEE. https://doi.org/10.1109/GCAT62922.2024.10923841

Hicks, A. (2023). SoK : Log-Based Transparency Enhancing Technologies. arXiv preprint arXiv :2305.01378.