IBIMA Publishing
Journal of Information Assurance & Cyber security
https://ibimapublishing.com/articles/JIACS/2026/387036/
Vol. 2026 (2026), Article ID 387036, 12 pages, ISSN: 2165-9923
https://doi.org/10.5171/2026.387036

Research Article

Ransomware Threats and Defensive Strategies: Insights from Literature and Practice

Mariusz ŁAZARSKI

Doctoral Seminar Participant, WSB University, Dąbrowa Górnicza, Poland
contact@mlazarski.org

Received date:15 October 2025; Accepted date:15 December 2025; Published date: 13 January 2026

Academic Editor: JERZY STANIK

Abstract

Ransomware attacks represent one of the most critical and rapidly evolving threats in the contemporary cybersecurity landscape. The growing sophistication of ransomware campaigns has led to severe financial, operational, and reputational losses, particularly for organizations that lack adequate preparedness and response capabilities. This paper examines ransomware threats by reviewing current detection techniques and analyzing key defensive strategies reported in academic literature and practical case studies. The study emphasizes the importance of multilayered security architectures that integrate technical safeguards, organizational measures, and regulatory compliance. Particular attention is given to the role of digital forensics in incident response, including evidence preservation, attack attribution, and post-incident analysis supporting the development of effective prevention frameworks. The paper also highlights the relevance of legal regulations and compliance requirements as essential components in reducing legal exposure and reputational damage following ransomware incidents. The analysis indicates that effective ransomware mitigation requires an integrated and proactive approach combining advanced security technologies, well-defined organizational procedures, and emerging solutions based on artificial intelligence and automation. These elements collectively enhance detection accuracy, response efficiency, and organizational resilience. The paper concludes by underlining the need for continuous adaptation of defensive strategies in response to the evolving ransomware threat landscape.

Keywords: ransomware; digital forensics; countermeasures; cybersecurity.

Cite this Article as: Mariusz ŁAZARSKI (2026), “Ransomware Threats and Defensive Strategies: Insights from Literature and Practice", Journal of Information Assurance & Cyber security, Vol. 2026 (2026), Article ID 387036, https://doi.org/10.5171/2026.387036

Introduction

Ransomware attacks represent one of the most critical threats in the modern digital environment, affecting both private entities and public institutions. As a form of malicious software, ransomware targets computer systems by encrypting data or blocking access to operational resources, subsequently demanding a ransom payment in exchange for restoring control. The scale of this problem has shown a steady increase each year, as confirmed by data published by cybersecurity organizations such as CERT Poland (CERT Poland, 2024).

A particularly concerning development is the growing popularity of the Ransomware-as-a-Service (RaaS) model (Broadhurst et al., 2014; Bada and Nurse, 2019), which significantly increases the accessibility of such criminal activities. This business model not only enhances the effectiveness of attacks but also makes prevention and mitigation efforts considerably more challenging.

The consequences of ransomware incidents extend far beyond financial loss. They also include a deterioration of customer trust, serious disruptions to critical (Huang et al., 2018) infrastructure, and, in certain cases, violations of legal regulations such as the provisions of the General Data Protection Regulation (GDPR, 2016).

Therefore, the issue of ransomware requires a comprehensive, interdisciplinary approach that integrates the technical aspects of cybersecurity with forensic analysis and the implementation of appropriate regulatory frameworks.

This paper discusses strategies for detecting, analyzing, and preventing ransomware attacks. Particular emphasis is placed on the role of digital forensics in the investigative process, as well as on the importance of preventive measures and legal compliance as key components in building organizational resilience against such threats.

The main objective of this study is to present a holistic perspective on ransomware, encompassing its technical, forensic, and regulatory dimensions.

Research Questions and Hypotheses

Research Questions:

What detection and response methods are currently the most effective in mitigating ransomware attacks within the context of organizational cybersecurity?

How do digital forensics tools and procedures support the analysis of ransomware incidents and the identification of perpetrators?

What data protection strategies and crisis management procedures minimize the risk of information loss resulting from ransomware attacks?

Which regulatory and legal aspects of combating ransomware are most critical for ensuring digital security and organizational compliance?

Hypotheses:

The implementation of multilayered security mechanisms combined with regular data backups significantly reduces the impact of ransomware attacks, lowering organizational losses by more than 50%.

The adoption of digital forensics tools and procedures increases the likelihood of successful data recovery without the need to pay ransom.

The automation of threat detection processes and integration with threat intelligence platforms contributes to a reduction of at least 30% in the average response time to ransomware incidents.

Topology of Ransomware Attacks

Ransomware attacks vary in terms of their execution methods and the objectives pursued by cybercriminals. In the scientific literature, several fundamental types of ransomware are distinguished, depending on their mode of operation and intended impact.

Encrypting ransomware – this type of malware encrypts files or entire data storage systems on infected devices, rendering them inaccessible until a ransom is paid. Victims are typically instructed to transfer payment most often in cryptocurrency in exchange for a decryption key. This is the most common and destructive form of ransomware, targeting both individuals and large organizations.

Locker ransomware – this variant prevents users from accessing the operating system or key applications by blocking the interface and displaying a ransom demand. In this case, the data themselves are usually not encrypted, but access to the system environment is restricted. The main goal of this type of ransomware is to create psychological pressure and force victims to comply with the attackers' demands.

Ransomware-as-a-Service (RaaS) (Gazet, 2010; Kharraz et al., 2015; Scaife et al., 2016; Paquet-Clouston et al., 2019) – this business model represents a major transformation in the cybercrime ecosystem. In the RaaS framework, ransomware developers offer ready-made malicious software to other cybercriminals in exchange for a share of the ransom profits. This service-based approach lowers the entry barrier to cybercrime and contributes to the rapid proliferation and diversification of ransomware attacks.

The growing sophistication of these attack types illustrates the dynamic nature of the ransomware threat landscape. The commercialization of ransomware through the RaaS model has transformed it into a scalable, profit-driven criminal enterprise, comparable in structure and efficiency to legitimate software industries.

Active and Passive Attacks

Ransomware can also be classified based on the nature of its operation into active and passive attacks.

Active attacks involve direct and intentional actions by cybercriminals, such as phishing campaigns, exploitation of security vulnerabilities, or manual compromise of the victim's infrastructure. These attacks are characterized by high dynamics, rapid propagation within the IT environment, and the need for immediate response and threat isolation (Broadhurst et al., 2014; Gazet, 2010). Active ransomware incidents often rely on social engineering techniques and privilege escalation, allowing attackers to quickly gain administrative control over targeted systems.

Passive attacks, on the other hand, are based on hidden and long-term activity. They may involve system monitoring, theft of authentication data, or preparation of the environment for a later encryption attack. In many cases, the malicious software is introduced into the system well in advance, with activation triggered only when specific conditions are met (for example, reaching a predefined number of encrypted files). For such attacks, behavioral analysis and continuous anomaly monitoring play a crucial role in detection and early mitigation (Broadhurst et al., 2014; Gazet, 2010).

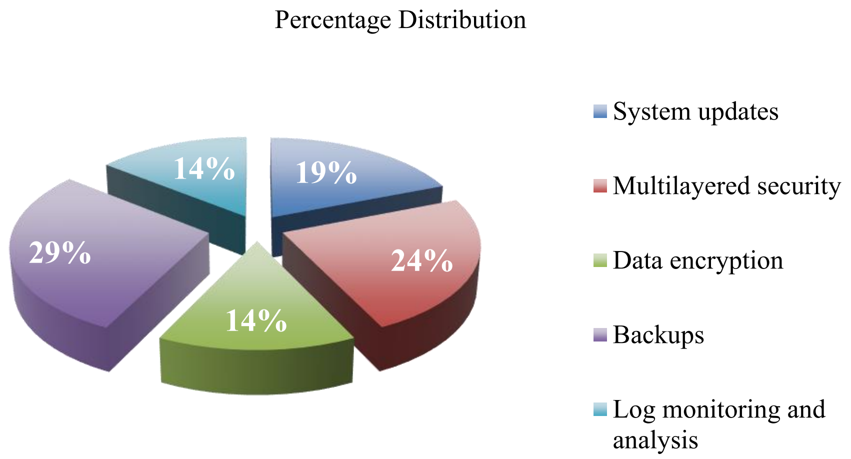

Fig 1. Percentage Distribution of Security Measures

Source: Author's own work based on an aggregated literature review and synthesized secondary data; the figure does not reproduce any previously published visual material (Glet, 2023; Ministry of Digital Affairs, 2023).

Figure 1 presents the percentage distribution of key cybersecurity measures implemented to mitigate ransomware risks. The largest share (30%) is attributed to regular data backups, highlighting their critical role in ensuring data recovery and business continuity. Multilayered security mechanisms (25%) and system updates (20%) are also recognized as essential components of an effective defense strategy, significantly reducing the probability of successful attacks. Data encryption (15%) and log monitoring with analysis (10%) contribute to strengthening both proactive and reactive aspects of organizational cybersecurity.

Mechanisms for Detecting Ransomware Attacks

Early detection of ransomware attacks is crucial to prevent their further spread and minimize potential losses. There are several methods commonly used to detect ransomware activity:

Network traffic monitoring – ransomware often generates abnormal network activity when encrypting data or attempting to communicate with command-and-control (C2) servers. Analyzing network traffic patterns makes it possible to identify unauthorized activities and potential indicators of compromise (Symons and Prasanna, 2020; Moore et al., 2009).

Tracking abnormal processes – many ransomware variants initiate unusual processes within the operating system, attempting to modify a large number of files or gain access to critical system resources. Monitoring active processes and applications enables early detection of such anomalies before the attack reaches full execution (Scaife et al., 2016; Paquet-Clouston et al., 2019).

System log analysis – system logs contain detailed information about all activities occurring within the operating system. Careful examination of logs can reveal irregular actions, such as sudden changes in file structures or access permissions, which may indicate the presence of ransomware (Kharraz et al., 2015; Symons and Prasanna, 2020).

Effective detection relies on combining these methods into a multilayered monitoring strategy that integrates network analysis, behavioral detection, and real-time system auditing.

Countermeasures against Ransomware Attacks

Effective counteraction against ransomware attacks requires a multilayered protection strategy that combines both technical and procedural security measures. The following practices are considered essential components of an effective defense framework:

Regular system and application updates – ransomware frequently exploits known software vulnerabilities. Regularly updating operating systems and applications provides protection against newly discovered threats and minimizes the risk of infection through outdated components (Accenture, 2021; Government Centre for Security, 2023).

Multilayered security mechanisms – implementing multiple layers of protection, such as firewalls, intrusion detection systems (IDS), and antivirus software, enhances an organization’s ability to detect and block ransomware activity at different stages of attack execution (Ars Technica, 2022; Malwarebytes, 2022).

Data encryption – encrypting sensitive data before an attack occurs prevents unauthorized access, even if the system becomes compromised. Properly implemented encryption can significantly reduce the risk of data exposure or permanent loss (Gazet, 2010; Kharraz et al., 2015).

Regular data backups – maintaining consistent and secure backup copies of critical data remains one of the most effective defenses against ransomware. In the event of file encryption, data can be restored from backups, thereby minimizing operational and financial losses (Sophos, 2022; Trusted Third Party, 2019).

The integration of these preventive measures, combined with employee awareness training and incident response planning, forms the foundation of a resilient cybersecurity strategy capable of mitigating ransomware threats.

The Role of Digital Forensics in the Analysis of Ransomware Attacks

Digital forensics plays a key role in the analysis of ransomware-related incidents. Experts in this field examine the traces left by malicious software (Broadhurst et al., 2014; Connolly and Wall, 2019; Kharraz et al., 2015; Paquet-Clouston et al., 2019), including system logs, executable files, and other forms of digital evidence that can help identify the perpetrators of an attack. Digital forensics enables the following critical functions:

- Data recovery – specialists in digital forensics can attempt to recover data encrypted by ransomware using specialized recovery tools and decryption techniques. Although full restoration is not always possible, forensic analysis often allows for partial data retrieval or reconstruction of critical system elements (Scaife et al., 2016; Symons and Prasanna, 2020).
- Identification of the attack source – through detailed examination of digital traces, forensic investigators can determine the origin of an infection, identify the exploited vulnerabilities, and map out the methods used by attackers to infiltrate the system (Moore et al., 2009; Ministry of Digital Affairs, 2023)
- Prevention of future attacks – forensic investigations contribute to the development of improved protection strategies by identifying systemic weaknesses and attack vectors. Lessons learned from forensic analyses are essential for designing stronger cybersecurity frameworks and preventing the recurrence of similar incidents in the future.

Examples of Ransomware Attacks

Table 1. Comparison of Organizational Responses to Ransomware Incidents

Response Method	% of Organizations	Average Response Time
Backup and data restoration	65%	1-3 days
Ransom payment	18%	1 day
System reset	12%	2–5 days
No effective response	5%	More than 5 days

Source: Author's own work based on comparative analysis and synthesis of secondary sources; estimated values derived from reports and case studies. The table does not reproduce any previously published tables or datasets (CERT Poland, 2024; Trusted Third Party, 2019).

The percentages represent approximate proportions of organizations employing specific response methods (backup and restoration, ransom payment, system reset, or no response). These figures do not originate from direct surveys or empirical studies but are estimated averages derived from the analysis of reports and case studies.

Table 1 presents the most common organizational responses to ransomware incidents and their corresponding recovery times. The majority of organizations choose to restore data from backups, which results in a moderate recovery period. Some companies decide to pay the ransom, which shortens response time but significantly increases the risk of repeated attacks. A lack of effective response, on the other hand, may lead to prolonged operational disruptions and substantial financial losses.

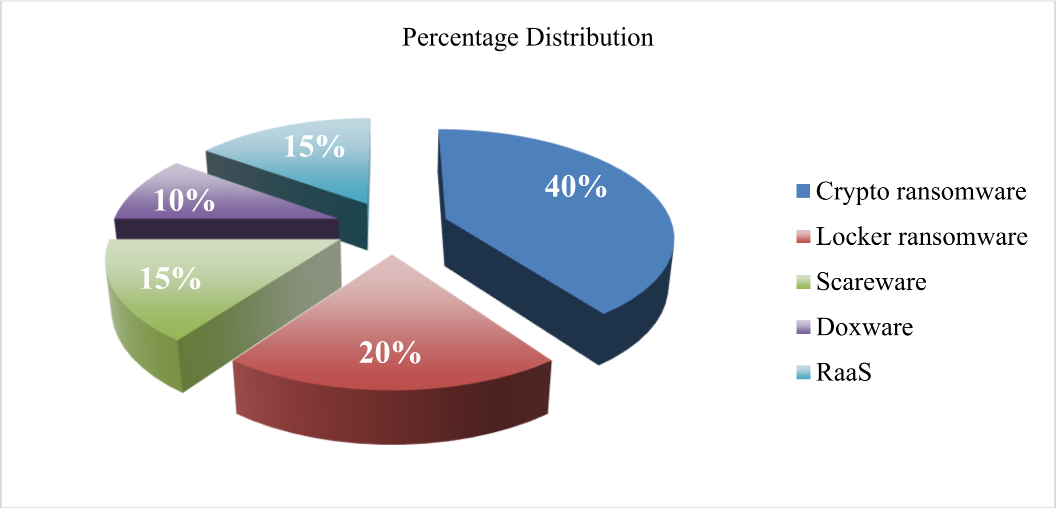

Fig 2. The Most Common Types of Ransomware

Source: Author's own work based on an aggregated literature review and synthesized secondary data; original visualization created by the author. The figure does not reproduce any previously published visual material (e.g., Glet, 2023; CERT Poland Reports, 2024).

It is worth noting that the percentages are approximate and represent the relative share of ransomware types in reported incidents rather than precise empirical values

Table 2. Characteristics of Selected Ransomware Types

Ransomware Type	Description
Locker Ransomware	Blocks access to the operating system, preventing the user from using the computer or device. It does not encrypt data but completely restricts interaction with the system, often displaying a ransom demand.
Scareware	A form of malicious software that frightens users with false alerts - for example, fake notifications about system infections - and persuades them to pay for a supposed "solution" (such as fake antivirus programs).
Doxware (Leakware)	This type of ransomware threatens to publicly release sensitive or private user data if the ransom is not paid. In addition to encryption, it uses reputational blackmail as an additional form of coercion.
Ransomware-as-a-Service (RaaS)	A cybercriminal business model in which ransomware developers offer their software to other criminals in exchange for a share of the profits. This enables even individuals without technical expertise to launch ransomware attacks.

Source: Author's own work based on literature review; original descriptive table structure created by the author. The table does not reproduce any previously published tables or datasets (e.g., Glet, 2023; CERT Poland, 2024).

The percentages presented indicate the approximate share of ransomware types within the overall population of attacks. The table illustrates both the mechanisms of operation and the prevalence of individual ransomware categories. This combined classification and statistical approach provides a more informative perspective for the reader.

Ransomware attacks have become a major threat to both public and private sector organizations. Examples of such incidents include:

WannaCry Virus (Government Centre for Security, 2020)

In 2017, WannaCry infected over 200,000 computers across 150 countries by exploiting a vulnerability in the Windows operating system. The attack caused severe disruptions, including within the UK's National Health Service (NHS), where access to patient data was blocked (Ministry of Digital Affairs, 2023).

Colonial Pipeline Attack (CERT Poland, 2024)

In 2021, the DarkSide cybercriminal group targeted the U.S. fuel supply system, demanding a ransom to restore access to critical infrastructure. The incident led to significant fuel distribution disruptions across the United States (Accenture, 2021).

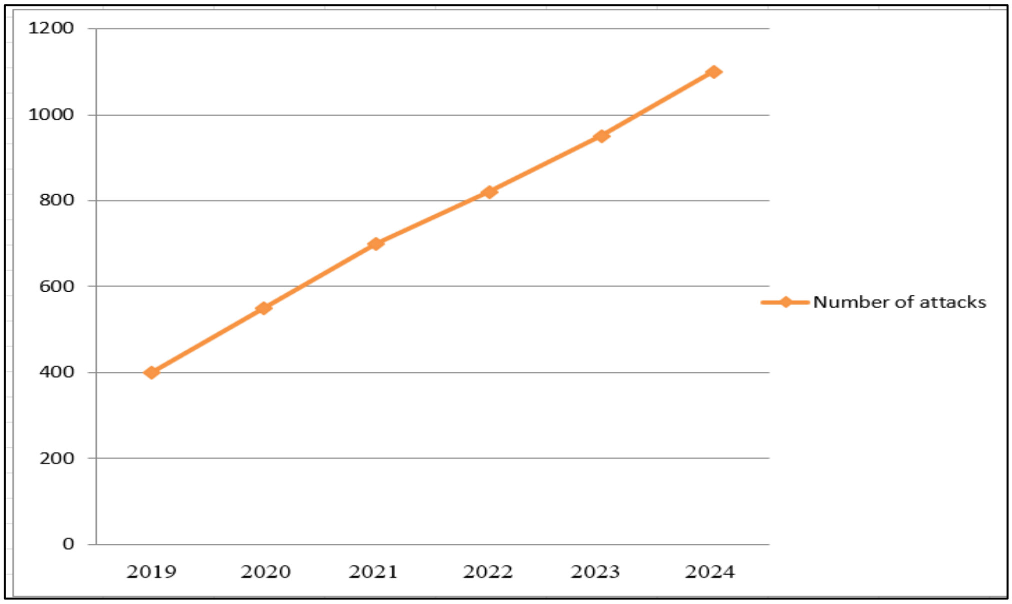

Fig 3. Estimated Number of Ransomware Attacks in Europe (2019–2024)

Source: Author's own work based on aggregated trend analysis and synthesized secondary data; original visualization created by the author. The figure does not reproduce any previously published visual material (e.g., Accenture, 2021; CERT Poland, 2024).

The data presented are estimates based on reports from cybersecurity institutions (e.g., CERT Poland, Government Centre for Security) and on the analysis of market trends.

Legal and Regulatory Framework

Legal regulations such as the GDPR (General Data Protection Regulation) and national cybersecurity laws impose obligations on organizations to ensure an adequate level of personal data protection and to respond promptly to incidents involving data breaches. According to Article 32 of the GDPR (GDPR, 2016), data security measures include, among others, encryption systems, regular data backups, and continuous security monitoring.

The integration of technical safeguards such as firewalls, Endpoint Detection and Response (EDR) systems, Security Information and Event Management (SIEM) solutions (Ars Technica, 2022; Dark Reading, 2022; Google, 2022), and automated backup mechanisms with compliance procedures, including internal security policies, business continuity plans, and employee training programs, not only reduces the likelihood of incidents but also mitigates potential legal consequences. In practice, this approach minimizes the risk of financial penalties imposed by supervisory authorities and helps protect the organization's reputation among clients and business partners.

As a result, the regulatory framework is no longer perceived merely as an administrative obligation but as a crucial element of organization security.

Security Checklists and Response Scenarios

Effective defense against ransomware attacks requires the implementation of a set of proven procedures and tools that together create a multilayered protection system for the organization. The following checklist of best practices can serve as a reference point for companies and institutions:

Regular system and application updates – operating systems, servers, and business applications should be regularly updated to eliminate vulnerabilities that could be exploited by cybercriminals.

Offline backups and regular testing – performing data backups disconnected from the main network (e.g., offline media or isolated cloud environments) reduces the risk of backup encryption. Equally important is regular testing of data restoration processes.

Zero Trust policy and network segmentation – applying the principle of least privilege, limiting user permissions, and segmenting IT infrastructure reduce the potential scope of an attack's spread (Ars Technica, 2022; Avast, 2021).

Monitoring and anomaly detection systems (SIEM, EDR, NDR) – centralized logging and the use of incident detection and response tools enable rapid identification of unusual activities within the system (Google, 2022; Eset, 2021).

Employee training and awareness building – the human factor remains the weakest link in security. Regular training on phishing awareness, safe email use, and basic cyber hygiene significantly reduces the risk of successful attacks.

Business Continuity Plan (BCP) – developing and testing contingency scenarios allows an organization to quickly resume critical operations after an attack.

Cyber insurance – an increasing number of organizations choose cyber insurance policies covering the consequences of cybersecurity incidents, including ransomware. Although they do not replace preventive measures, they can significantly reduce the financial impact of incidents (OECD, 2022).

This checklist should be adapted to the specific characteristics of each institution, including its size and the type of data it processes.

Even the most advanced protections cannot guarantee complete immunity against ransomware. Therefore, every organization should maintain an Incident Response Plan (IRP) (Accenture, 2021; Government Centre for Security, 2023), defining the procedures to be followed in the event of a security incident. The following presents an example of a typical ransomware response scenario:

Incident identification and detection – the first step involves recognizing that an attack has occurred. Monitoring systems (e.g., SIEM, IDS/IPS) and user reports of unusual messages, inaccessible files, or sudden system slowdowns are commonly used for detection.

Isolation of infected assets – promptly disconnecting infected devices from internal and external networks can prevent further spread. Temporary suspension of compromised user accounts is often applied as well.

Incident analysis and assessment – the security team (SOC or CSIRT) analyzes system logs, executable files, and other evidence to determine the attack vector, the number of affected systems, and the extent of data loss. Digital forensics plays a crucial role in this stage.

System and data recovery – if verified backup copies are available, the environment can be restored to its pre-attack state. However, it is essential to ensure that the threat has been fully neutralized before restoration.

Internal and external communication – following technical containment, management, employees, and when necessary clients and business partners should be informed. In the case of personal data breaches, organizations are also obligated to report incidents to supervisory authorities such as the Data Protection Office or CERT.

Decision on ransom negotiations – although some companies choose to pay the ransom, security experts and law enforcement strongly advise against it. Paying does not guarantee data recovery and may encourage future attacks.

Post-incident preventive actions – after resolving the crisis, it is essential to conduct a post-mortem analysis, identify infrastructure and procedural weaknesses, and reinforce them. Updating the business continuity plan and retraining staff based on lessons learned is equally important.

Implementing security checklists and ransomware incident response scenarios helps minimize confusion during a crisis and supports decision-making under time pressure. In practice, this not only reduces material losses but also strengthens long-term organizational resilience in an environment where cyber threats are becoming increasingly sophisticated and widespread.

Research Methodology

The study was conducted using a multi-stage, interdisciplinary methodology combining literature review, statistical data analysis, and case studies. This approach made it possible to obtain a comprehensive picture of ransomware threats and effective counteraction strategies.

A systematic review of academic literature and industry reports was carried out, including publications from CERT Poland, the Government Security Centre (RCB), the Ministry of Digital Affairs, and peer-reviewed studies in the fields of cybersecurity and digital forensics (Accenture, 2021). The review identified current trends in ransomware evolution, available detection and prevention methods, as well as relevant legal and regulatory frameworks.

Quantitative data were used to illustrate the effectiveness of different protection strategies and response methods to ransomware incidents. The data sources included reports from (CERT Poland, 2024; Trusted Third Party, 2019), and other industry analyses. The analysis covered, among others, the proportion of organizations using backup recovery, ransom payment, system reset, or no response to incidents, as well as the dynamics of ransomware type occurrences. These data were used to produce visualizations such as percentage charts and comparative tables (Accenture, 2021).

Selected case studies were used to demonstrate the practical effects of ransomware attacks. The analysis focused on major national and international incidents, including the WannaCry virus attack in 2017 and the Colonial Pipeline incident in 2021. The studies examined the attack mechanisms, mitigation measures applied, financial and operational impacts, organizational response strategies, and the role of digital forensics (Accenture, 2021).

The combination of literature review, statistical analysis, case studies, and expert insights allowed for data triangulation, enhancing the reliability and validity of the research. This approach enabled the identification of relationships between ransomware types and the effectiveness of protection mechanisms, leading to the development of practical recommendations for organizations.

Conclusions

Ransomware remains one of the key threats in the field of cybersecurity, requiring coordinated efforts in detection, response, and digital forensics. Effective protection against such attacks necessitates the implementation of multilayered security measures, regular data backups, and continuous monitoring of system anomalies. In the future, an important direction of development will be the automation of detection and response processes (Symons and Prasanna, 2020; Ars Technica, 2022; Google, 2022), supported by the use of artificial intelligence and the integration of threat intelligence platforms (Dark Reading, 2022; Eset, 2021).

The analysis conducted in this study allows for the formulation of the following conclusions:

The complexity and widespread nature of ransomware attacks affect both the public and private sectors, causing significant financial, operational, and reputational losses.

The necessity of multilayered protection demonstrates that effective defense requires combining technical measures (firewalls, EDR, and SIEM systems), organizational measures (security procedures and employee training), and legal compliance (adherence to regulations such as GDPR).

The importance of data backups and business continuity - regular creation and testing of backup copies remain the most reliable method of minimizing the impact of ransomware incidents.

The significance of monitoring and anomaly analysis early detection of unusual processes, network traffic patterns, or system log changes significantly increases the likelihood of reducing losses.

Future directions in cybersecurity development, the automation of detection and response processes, the application of artificial intelligence, and the integration with threat intelligence platforms enabling real-time information sharing will play a key role in enhancing ransomware defense capabilities.

Future research will focus on empirical validation of the proposed framework using real-world organizational data.

References

- Accenture (2021) *Cyber threat intelligence report*. [Online]. Available at: https://www.accenture.com/us-en/insights/security/cyber-threat-intelligence [Retrieved 10 September 2025].
- Ars Technica (2022) *Colonial Pipeline ransomware analysis*. Ars Technica.
- Avast (2021) *History of ransomware*. Avast Blog.
- Bada, A. and Nurse, J.R.C. (2019) 'The human factor in cybersecurity: A research agenda,' *Computers & Security*, 87.
- Bitdefender (2021) *Mid-year threat landscape report*. [Online]. Available at:
- https://www.bitdefender.com/files/News/CaseStudies/study/404/BD-Security-Behavior-Report-Final-at.pdf [Retrieved 10 September 2025].
- BleepingComputer (2021) *Ransomware news and updates*. BleepingComputer.
- Broadhurst, R., Grabosky, P., Alazab, M. and Chon, S. (2014) 'An analysis of ransomware and strategies to combat it,' *Asian Criminology*, 9(2), pp. 135–150.
- CERT Poland (2024) *Annual Report on the State of Cybersecurity in Poland.* [Online]. Available at: https://cert.pl/en/uploads/docs/Report_CP_2024.pdf [Retrieved 10 September 2025].
- Check Point (2023) *Cyber attack trends: Ransomware report*. [Online]. Available at: https://www.checkpoint.com/resources/report-3854/report--cyber-security-report-2024-3a0a [Retrieved 10 September 2025].
- Cisco Talos (2022) *Annual cybersecurity report*. [Online]. Available at: https://www.cisco.com/c/en/us/products/security/security-reports.html [Retrieved 10 September 2025].
- CISA (2022) *Ransomware guidance and resources*. [Online].Available at: https://www.cisa.gov/sites/default/files/2023-01/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf [Retrieved 10 September 2025].
- Connolly, L.Y. and Wall, D.S. (2019) 'The rise of crypto-ransomware in a changing cybercrime landscape,' *Computers & Security*, 87, pp. 101–111.
- CrowdStrike (2023) *Adversary profiling / Adversary universe insights.* [Online]. Available at: https://www.crowdstrike.com/en-us/platform/threat-intelligence/adversary-profiling/ [Retrieved 10 September 2025].
- CrowdStrike (2022) *Global threat report 2022*. [Online]. Available at: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2022GTR.pdf [Retrieved 10 September 2025].
- CSO Online (2021) *Best practices against ransomware*. CSO Online.
- Dark Reading (2022) *Trends in ransomware and cybercrime*. Dark Reading.
- ENISA (2023) *Threat landscape 2023*. [Online]. Available at: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf [Retrieved 10 September 2025].
- ESET WeLiveSecurity (2021) *Modern ransomware techniques*. ESET.
- European Union (2016) *General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679.* [Online]. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng [Retrieved 10 September 2025].
- Europol (2023) *Internet organised crime threat assessment (IOCTA).* [Online]. Available at:
- https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN.pdf [Retrieved 10 September 2025].

- FBI IC3 (2021) *Internet crime report*. [Online]. Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf [Retrieved 10 September 2025].
- Fortinet (2022) *FortiGuard Labs threat report*. [Online]. Available at: www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-1h-2022.pdf [Retrieved 10 September 2025].
- Gazet, A. (2010) 'Comparative analysis of various ransomware virii,' *Journal in Computer Virology*, 6(1), pp. 77–90.
- Government Centre for Security (RCB) (2023) *Analysis of ransomware threats in the public sector*. [Online]. Available at: https://www.gov.pl/web/rcb/akademia-bezpieczenstwa-rcb2 [Retrieved 10 September 2025].
- Google TAG (2022) *Tracking ransomware gangs*. Google.
- Huang, D., Aliapoulios, M., Li, V. et al. (2018) 'Tracking ransomware end-to-end,' *IEEE Security & Privacy*, 16(4), pp. 55–64.
- IBM Security (2021) *Cost of a data breach report*. [Online]. Available at: https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91 [Retrieved 10 September 2025].
- Interpol (2021) *Cybercrime annual report*. [Online]. Available at: https://www.interpol.int/content/download/17965/file/INTERPOL%20Annual%20Report%202021_AR.pdf [Retrieved 10 September 2025].
- Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L. and Kirda, E. (2015) 'Cutting the Gordian knot: A look under the hood of ransomware attacks,' *DIMVA Conference Proceedings*. Springer.
- Krebs on Security (2022) *Ransomware attack investigations*. Krebs on Security.
- Mandiant (FireEye) (2021) *Ransomware activity report*. [Online]. Available at: https://services.google.com/fh/files/misc/rpt-mtrends-2021-en.pdf [Retrieved 10 September 2025].
- Malwarebytes Labs (2022) *Ransomware incident reports*. Malwarebytes.
- CSIS & McAfee (2020) *The Hidden Costs of Cybercrime*. [Online]. Available at: https://www.csis.org/analysis/hidden-costs-cybercrime [Retrieved 10 September 2025].
- Microsoft Security (2022) *Microsoft defense against ransomware, extortion, and intrusion.* [Online]. Available at: https://learn.microsoft.com/en-us/security/ransomware/ [Retrieved 10 September 2025].
- Ministry of Digital Affairs (Poland) (2023) *Report on the state of cybersecurity*. [Online]. Warsaw. Available at: https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf [Retrieved 10 September 2025].
- Moore, T., Clayton, R. and Anderson, R. (2009) 'The economics of online crime,' *Journal of Economic Perspectives*, 23(3), pp. 3–20.
- OECD (2022) *Policy Framework on Digital Security: Cybersecurity for Prosperity.* [Online]. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c/a69df866-en.pdf [Retrieved 10 September 2025].
- Paquet-Clouston, M., Haslhofer, B. and Dupont, B. (2019) 'Ransomware payments in the Bitcoin ecosystem,' *Journal of Cybersecurity*, 5(1).
- Palo Alto Networks (2022) Unit 42 ransomware threat report. [Online]. Available at: https://fqm.ca/wp-content/uploads/2023/07/paloalto-2023-unit42-ransomware-extortion-report.pdf [Retrieved 10 September 2025].
- Rapid7 (2021) *Ransomware defense strategies*. Rapid7.
- Scaife, N., Carter, H., Traynor, P. and Butler, K. (2016) 'Cryptolock (and drop it): Stopping ransomware attacks on user data,' *USENIX Security Symposium Proceedings*.

- SecurityWeek (2022) *Global ransomware trends*. SecurityWeek.
- Sophos (2022) *State of ransomware 2022*. [Online]. Available at: https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/ [Retrieved 10 September 2025].
- Symons, C. and Prasanna, R. (2020) 'Adapting cybersecurity frameworks for ransomware resilience,' *Journal of Information Security and Applications*, 54.
- Symantec (Broadcom) (2021) *Ransomware protection and mitigation strategies*. [Online]. Available at: https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf [Retrieved 10 September 2025].
- The Hacker News (2022) *Ransomware attack stories*. The Hacker News.
- The Register (2021) *Ransomware evolution timeline*. The Register.
- Trend Micro (2022) *Ransomware in the modern enterprise*. [Online]. Available at: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/rethinking-tactics-annual-cybersecurity-roundup-2022 [Retrieved 10 September 2025].
- Verizon (2022) *Data breach investigations report (DBIR)*. [Online]. Available at: https://www.verizon.com/business/resources/reports/dbir/ [Retrieved 10 September 2025].
- Wired (2021) *Inside a ransomware attack*. WIRED.