

Decoding Ransomware: A Thematic Analysis of Trends and Countermeasures

Joseph Ohene Buabeng, Dr. Richard Essah

Takoradi Technical University, Ghana

DOI: <https://doi.org/10.51583/IJLTEMAS.2025.1408000051>

Received: 06 Aug 2025; Accepted: 14 Aug 2025; Published: 04 September

Abstract: This study investigates the evolving landscape of ransomware attacks and critically evaluates the effectiveness of current countermeasures. Drawing on a thematic analysis of secondary data from global case studies, cybersecurity reports, and academic literature, the research highlights the commodification of ransomware through Ransomware-as-a-Service (RaaS). It identifies key attack vectors, including phishing, Remote Desktop Protocol (RDP) exploitation, and unpatched vulnerabilities, while examining the increasing sophistication of extortion tactics such as double and triple extortion. Organisational responses are assessed, distinguishing proactive defenders with layered security infrastructures from reactive institutions hampered by limited preparedness, particularly in under-resourced regions. Findings indicate that resilience depends on comprehensive strategies that integrate technological safeguards, user education, and policy-level interventions. This study concludes that ransomware is no longer merely a technical threat but a systemic challenge requiring coordinated action across sectors and jurisdictions. Practical recommendations are offered to support scalable, context-aware defences and foster cybersecurity maturity.

Keywords: Ransomware, Thematic Analysis, Cybersecurity, Countermeasures, Digital Resilience

I. Introduction

The accelerating pace of digital transformation has revolutionised communication, data storage, and operations across industries. However, this progress has also increased exposure to cyber threats, none more disruptive than ransomware. Designed to encrypt sensitive data and demand payment, ransomware has evolved from scattered incidents into a global criminal enterprise. Projections from Cybersecurity Ventures estimate annual damages will reach \$57 billion by 2025, with an attack occurring every two seconds (Cybersecurity Ventures, 2025). The average ransom demand now exceeds \$1.2 million, while recovery costs can escalate to \$2.7 million or more for organisations without robust defences.

One of the most concerning developments is the rise of Ransomware-as-a-Service (RaaS), which enables even low-skilled threat actors to launch advanced attacks using off-the-shelf malware kits (MITRE ATT&CK, 2024). This commodification has expanded the threat landscape, placing critical sectors such as healthcare, finance, education, and infrastructure at heightened risk. Despite significant investments in cybersecurity, ransomware incidents continue to rise in scope and sophistication. Notable attacks, including WannaCry in 2017 and the Colonial Pipeline breach in 2021, illustrate that even well-resourced organisations remain vulnerable. Emerging tactics like double extortion, where attackers encrypt and exfiltrate data for leverage, have rendered traditional defences insufficient.

This study interrogates the evolution of ransomware and evaluates whether current mitigation strategies are adequate. Through qualitative thematic analysis of global case studies and expert literature, it identifies patterns in attack vectors, sector-specific vulnerabilities, and offers practical measures to build resilience.

Problem Statement

Despite increased investment and awareness, ransomware attacks continue to escalate in frequency and sophistication. Incidents such as the Colonial Pipeline (2021) and WannaCry (2017) highlight persistent vulnerabilities, even among well-protected organisations. Attackers exploit unpatched systems, human error, and poor cyber hygiene. Emerging tactics such as double extortion have rendered conventional defences insufficient. This study investigates the evolution of ransomware threats and assesses the effectiveness of existing mitigation strategies.

Objectives of the Study

1. Trace the evolution of ransomware tactics and platforms.
2. Examine common attack vectors and exploited vulnerabilities.
3. Analyse prevention, detection, and response strategies.
4. Recommend actionable measures for enhancing resilience.

Research Questions

1. How have ransomware threats evolved over the past decade?
2. What are the most commonly exploited vulnerabilities and delivery mechanisms?

3. How effective are existing defence and response practices?
4. What improvements can strengthen organisational preparedness?

Significance of the Study

This research provides timely insights for cybersecurity professionals, policymakers, business leaders, and academics. By dissecting ransomware tactics and evaluating countermeasures, the study supports informed strategies for prevention and incident response. It also emphasises the importance of a multi-layered defence model combining technology, education, and planning. For institutions in developing regions, the findings offer guidance to strengthen infrastructure and resilience.

Scope and Limitations of the Study

This study focuses on ransomware incidents and countermeasures documented between 2015 and 2025. While adopting a global perspective, the analysis emphasises regions with developing cybersecurity frameworks, particularly in sub-Saharan Africa. The research relies exclusively on secondary sources such as academic literature, government reports, and cybersecurity white papers. Key limitations include the exclusion of classified data, interviews, and real-time organisational assessments. Broader political and legal dimensions (such as cyber warfare and state-sponsored actors) fall outside the scope.

II. Literature Review

Historical Development of Ransomware

The earliest known ransomware, the AIDS Trojan of 1989, was rudimentary, delivered via floppy disks and demanding payment to a post office box (KnowBe4, 2021). By 2013, CryptoLocker introduced public-key encryption and anonymous Bitcoin payments, significantly intensifying the threat (CryptoLocker, 2023). The WannaCry outbreak of 2017 exploited the EternalBlue vulnerability, infecting over 300,000 systems and causing damages estimated at \$4 billion (Cloudflare, 2025).

The introduction of Ransomware-as-a-Service (RaaS) has transformed ransomware into a commercial model. Groups such as REvil, Conti, and LockBit lease malware kits to affiliates, expanding the scale of attacks (MITRE ATT&CK, 2024).

Common Attack Vectors and Delivery Mechanisms

Ransomware is commonly deployed through phishing emails, malicious attachments, and Remote Desktop Protocol (RDP) exploits. Fortinet (2025) reports phishing accounts for over 41% of infections. Software vulnerabilities also serve as major entry points, as seen in the WannaCry incident. Supply chain compromises such as the Kaseya VSA breach highlight the growing sophistication of infiltration techniques.

Impacts of Ransomware

The consequences of ransomware extend beyond ransom payments, including downtime, data restoration costs, regulatory penalties, and reputational damage. The Colonial Pipeline attack disrupted fuel supplies in 17 U.S. states, while WannaCry forced hospital cancellations across the UK's NHS, costing approximately £92 million (Kaspersky, 2025).

Mitigation Strategies

Organisations employ multi-layered defences: endpoint detection and response (EDR), firewalls, secure backups, and AI-driven behavioural analytics (SentinelOne, 2024). Non-technical measures include employee awareness training, cyber drills, and compliance with standards such as NIST and ISO 27001. According to Sophos (2024), organisations relying on backup recovery incurred median costs of \$750,000, significantly less than the \$3 million for those who paid ransoms.

Challenges in Countering Ransomware

Despite technological advances, several challenges persist. Human error remains a major vulnerability, manifesting as weak passwords, poor access controls, and phishing susceptibility. Incident underreporting undermines public understanding and law enforcement response efforts. Jurisdictional boundaries further complicate prosecution, especially when attackers operate from countries with inadequate cybercrime enforcement.

Additionally, ethical dilemmas emerge when organisations must choose between ransom payment and prolonged disruption. While ransom payment may restore operations, it often fuels continued criminal activity and poses reputational risks.

Thematic Analysis Table

Table 1: Ransomware Attack Vectors and Corresponding Countermeasures

Attack Vector	Example Incident	Countermeasures	Effectiveness
Phishing Emails	WannaCry (2017)	User awareness training, email filters	Moderate
Remote Desktop Exploits	Colonial Pipeline (2021)	Multi-factor authentication, system patching	High

Software Vulnerabilities	WannaCry (2017)	Timely updates, vulnerability scanning	High
Supply Chain Attacks	Kaseya VSA Breach (2021)	Vendor risk management, zero trust architecture	Moderate

III. Methodology

Research Design

A qualitative, descriptive research design was employed to examine ransomware attacks and countermeasures. This approach facilitated thematic interpretation and contextual depth, enabling exploration of attacker tactics, organisational responses, and emerging trends.

Population and Scope

The study analysed ransomware incidents affecting organisations worldwide between 2015 and 2025, with particular attention to under-resourced regions such as sub-Saharan Africa.

Data Collection

Data were drawn exclusively from secondary sources, including peer-reviewed articles, cybersecurity agency reports (e.g., CISA, ENISA), security firm bulletins (e.g., Kaspersky, Sophos, Trend Micro), and case studies.

Data Analysis

Thematic content analysis was adopted. Information was coded under themes such as *Attack Vectors*, *Mitigation Strategies*, and *Policy Response*. Cross-case comparison enabled the identification of recurring patterns. Triangulation improved reliability.

Ethical Considerations

All sources were properly referenced using APA 7th edition guidelines. Sensitive information regarding breached organisations was reported objectively. The study adhered to institutional protocols for ethical use of public data.

Limitations of Methodology

Constraints included the absence of primary data, reliance on reported incidents, and lack of real-time forensic evidence. Quantitative metrics and user surveys were excluded due to scope limitations.

Interpretation and Implications

The insights derived through thematic analysis highlight the complex interplay between technological evolution, institutional preparedness, and socio-political structures influencing regional responses to ransomware threats.

Three dominant themes emerged regarding the current cybersecurity landscape: the evolution of ransomware attack vectors, adaptive countermeasures employed in resource-constrained environments, and the socio-political dynamics affecting cybersecurity governance. These thematic categories reveal not only the characteristics of the threat landscape but also how vulnerabilities are shaped and mitigated in context-specific ways. The convergence of these themes suggests a pressing need for multi-dimensional approaches to cybersecurity that integrate technical solutions with behavioural awareness and policy coherence. For instance, the persistence of phishing and social engineering exploits underscores the importance of user-oriented interventions, such as cybersecurity literacy and culturally grounded awareness campaigns.

Policy fragmentation further compounds vulnerability. Inconsistent legislation and weak enforcement mechanisms limit coordination and accountability, especially at the regional levels. A harmonised regulatory environment is therefore essential for enhancing operational readiness and fostering interjurisdictional collaboration.

Institutional capacity, encompassing both technological and human elements, is crucial for resilience, highlighting the need for sustained investment in cybersecurity infrastructure and professional development, especially in under-resourced regions that require targeted support through strategic partnerships, international funding, and locally tailored capacity-building initiatives. Methodologically, thematic analysis has offered interpretive depth and flexibility, enabling the identification of contextually rich patterns and relationships, and its compatibility with both deductive and inductive reasoning has facilitated a robust exploration of qualitative data. However, limitations regarding subjectivity and the generalizability of findings remain, suggesting that future research could benefit from methodological triangulation by integrating thematic analysis with longitudinal or quantitative approaches to enhance generalizability and policy relevance.

Strategic Recommendations

Infrastructure Investment - Strengthen endpoint detection, patch management, and backup systems through sustained funding.

Tailored User Education - Implement culturally relevant awareness programs to address phishing and social engineering.

Policy Harmonisation - Develop enforceable cybercrime legislation and harmonise regional policies for cross-border collaboration.

Capacity Building - Provide targeted support in under-resourced regions through partnerships and international funding.

Integration with Development - Position cybersecurity not as a niche, but as a foundation for governance and economic growth.

Contribution to Knowledge

This study contributes by:

- Applying thematic analysis to ransomware research.
- Highlighting socio-technical factors shaping institutional resilience.
- Providing a framework for policy and practice interventions in resource-constrained environments.

Limitations and Future Research

Findings are context-specific and shaped by qualitative interpretation. Future research should explore mixed methods designs, longitudinal studies, or comparative analyses across regions to enhance generalizability and policy relevance.

Final Reflections

Ransomware remains a fluid, formidable challenge. This study emphasises the need for context-sensitive resilience strategies combining technology, education, and governance. Only through coordinated, cross-sectoral efforts can societies mitigate current threats and foster long-term cybersecurity resilience.

References

1. Cloudflare. (2025). WannaCry ransomware: What it was and how it spread. Cloudflare. <https://www.cloudflare.com>
2. Cloudwards. (2025). The latest ransomware statistics & trends. Cloudwards. <https://www.cloudwards.net/ransomware-statistics/>
3. Colonial Pipeline ransomware attack. (2023). In Wikipedia. https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack
4. Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications.
5. CryptoLocker. (2023). In Wikipedia. <https://en.wikipedia.org/wiki/CryptoLocker>
6. Cybersecurity Ventures. (2025). Ransomware damage is expected to cost the world \$57B in 2025. <https://cybersecurityventures.com>
7. Fortinet. (2025). Ransomware statistics 2025: Latest trends & must-know insights. Fortinet. <https://www.fortinet.com>
8. Kaspersky. (2025). WannaCry ransomware: All you need to know. Kaspersky. <https://www.kaspersky.com>
9. KnowBe4. (2021). AIDS Trojan ransomware. <https://www.knowbe4.com/ransomware-knowledgebase/aids-trojan>
10. MITRE ATT&CK. (2024). REvil ransomware. <https://attack.mitre.org/software/S0496/>
11. SentinelOne. (2024). REvil ransomware: Analysis, detection, and mitigation. SentinelOne. <https://www.sentinelone.com/anthology/revil/>
12. Sophos. (2024). The state of ransomware 2024. Sophos. <https://www.sophos.com/en-us/content/state-of-ransomware>
13. Trend Micro. (2023). Ransomware spotlight report: Conti and LockBit. Trend Micro. <https://www.trendmicro.com>
14. WannaCry ransomware attack. (2023). In Wikipedia. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack