© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1719628

Ransomware Attack Patterns: Detection, Prevention, And Recovery Strategies

DUROJAYE EMMANUEL OLATUNJI[1], ADENEYE JOHN[2], ABASS SAMUEL RAMID[3], MBAH DEMIAN CHIDI[4], AJIBAYE PATRICK MAYOWA[5]
[1, 2, 3, 4, 5] *Ogun State Institute of Technology*

Abstract- ***Ransomware has emerged as one of the most devastating forms of cybercrime in the modern digital era. This research examines ransomware attack patterns, analyzing the distinct phases through which these attacks are executed, the detection techniques employed to identify them, and the prevention and recovery strategies organizations can adopt to minimize damage. [1,4] By synthesizing current research and real-world case studies, this research provides a comprehensive overview of how ransomware operates and how individuals and organizations can defend against it. Findings indicate that a multi-layered security approach — combining behavioral detection, network segmentation, employee training, and immutable backups — offers the most robust defense against ransomware threats. [5,7]***

I. INTRODUCTION

Ransomware is a type of malicious software (malware) that encrypts a victim's files or locks them out of their systems entirely, after which attackers demand a ransom payment — typically in cryptocurrency — in exchange for restoring access. [5] Since its earliest recorded form in 1989 (the AIDS Trojan), ransomware has evolved dramatically, growing from simple screen-locking tools into sophisticated, multi-stage cyberattacks capable of crippling global organizations. [4]

The scale and impact of ransomware attacks have grown alarmingly. According to Allianz Commercial, ransomware activity increased by 50% year-on-year during the first half of 2023, driven largely by the emergence of Ransomware-as-a-Service (RaaS) platforms that allow even low-skilled cybercriminals to launch attacks at scale.

[1] In 2024, attacks surged even further, with 63 publicly disclosed incidents recorded in August 2024 alone — the highest monthly figure on record. [6] Ransom demands escalated alongside attack frequency, with the average extortion demand exceeding USD 5.2 million in the first half of 2024, and a record single ransom payment of USD 75 million recorded in March 2024. [6]

The consequences of ransomware extend far beyond financial loss. Attacks on healthcare institutions, government agencies, and critical infrastructure threaten human safety and disrupt essential services. [6] The February 2024 attack on Change Healthcare disrupted pharmacy operations across the United States and exposed the health data of an estimated one-third of all Americans, illustrating the far-reaching societal impact of a single ransomware incident. [8]

This research is structured as follows: Section 2 reviews related literature. Section 3 describes the methodology. Section 4 presents results and discussion. Section 5 concludes with key recommendations.

II. RELATED STUDIES / LITERATURE REVIEW

A growing body of research has examined ransomware from multiple perspectives, including its technical evolution, organizational impact, and countermeasures. This section reviews key studies that inform this research.

2.1 Evolution and Taxonomy of Ransomware

Early ransomware research focused on classifying malware types and understanding encryption mechanisms. Researchers identified two primary

classes: crypto ransomware, which encrypts victim files using asymmetric cryptographic algorithms such as AES and RSA, and locker ransomware, which locks users out of their systems without encrypting the underlying data. [5] Subsequent studies documented the emergence of Ransomware-as-a-Service (RaaS) as a business model enabling non-technical actors to deploy sophisticated attacks, fundamentally lowering the entry barrier for cybercriminals. [1]

2.2 Attack Vectors and Lifecycle Analysis

Flashpoint (2023) conducted a detailed analysis of the ransomware attack lifecycle, identifying seven distinct phases from initial reconnaissance through extortion. [2] Similarly, Picus Security (2024) examined the attack chain from the defender's perspective, emphasizing the critical importance of detecting lateral movement and privilege escalation before payload deployment. [9] Both studies converge on the finding that organizations with mature detection capabilities at the lateral movement phase significantly reduce ransomware impact.

2.3 Detection Approaches

The Journal of Knowledge Learning and Science Technology (2023) reviewed machine learning and AI-based approaches to ransomware detection, finding that behavioral models outperform traditional signature-based methods against novel ransomware variants. [4] Static and dynamic analysis methods were also found to be effective in controlled environments, though their real-time applicability in enterprise settings remains limited. [5]

2.4 Prevention and Organizational Factors

Cyber Management Alliance (2024) identified a multi-layered defense-in-depth approach as the most effective prevention posture, incorporating technical controls, security awareness training, and network segmentation. [7] The study further noted that organizations enforcing Multi-Factor Authentication (MFA) and the Principle of Least Privilege (PoLP) experienced significantly fewer successful intrusions. [7] The widely cited Change Healthcare breach of February 2024 — attributed to the absence of MFA on a critical account — reinforces these findings. [8]

2.5 Recovery and Resilience

Infrascale (2025) and IJRASET (2025) both highlighted backup integrity and incident response preparedness as the most critical factors in ransomware recovery. [3,5] Their research found that 76% of ransomware attacks in 2024 successfully compromised backup data, and that organizations with tested, offline backup systems recovered in a fraction of the time compared to those without. [3] TRM Labs (2024) further documented the increasing use of double extortion tactics and their psychological impact on victim organizations' ransom payment decisions. [6]

III. METHODOLOGY

This research adopts a qualitative, systematic literature review methodology to examine ransomware attack patterns, detection mechanisms, prevention strategies, and recovery approaches. The study synthesizes findings from peer-reviewed journals, technical security reports, and industry publications published between 2023 and 2026.

3.1 Research Design

A descriptive and analytical research design was employed. Rather than conducting live experiments or penetration testing, this research examines and synthesizes existing knowledge to build a comprehensive, structured understanding of the ransomware threat landscape. [10] This approach is appropriate for the scope of this study, as it allows for broad coverage of attack patterns, detection techniques, and mitigation strategies across diverse organizational contexts.

3.2 Data Collection

Primary data sources include peer-reviewed articles from the IRE Journal, the Journal of Knowledge Learning and Science Technology, and IJRASET. Secondary sources include technical reports from Allianz Commercial, TRM Labs, Cyber Management Alliance, Infrascale, Picus Security, Flashpoint, Fortinet, and IBIMA Publishing. [1,2,3,4,5,6,7,8,9,10] Sources were selected based on their relevance to ransomware attack patterns, recency (2023–2026), and credibility of the publishing organization.

3.3 Analytical Framework

The analysis is organized around four thematic areas: (1) ransomware types and taxonomy, (2) attack lifecycle phases, (3) detection techniques, and (4) prevention and recovery strategies. Each theme was examined across multiple sources to identify convergent findings, emerging trends, and gaps in current defenses. [4,9]

3.4 Threat Model

The research adopts the MITRE ATT&CK framework as a reference model for categorizing ransomware tactics, techniques, and procedures (TTPs). This framework provides a structured vocabulary for describing attacker behaviors across the kill chain — from initial access through impact — enabling consistent analysis across different ransomware families and incidents. [9]

IV. RESULTS AND DISCUSSION

4.1 Ransomware Attack Patterns and Lifecycle

The review of literature confirms that modern ransomware attacks follow a consistent multi-phase lifecycle. [2,9] The key phases identified across sources are as follows:

- Reconnaissance and Target Selection: Attackers conduct passive and active reconnaissance to identify high-value targets, increasingly focusing on 'Big Game Hunting' — targeting organizations most likely to pay large ransoms such as healthcare providers and government agencies. [1,2]
- Initial Access: Phishing emails, exploitation of unpatched vulnerabilities, and brute-forcing of weak RDP credentials remain the dominant initial access vectors. The absence of MFA was a critical enabler in the Change Healthcare breach of 2024. [8,9]
- Lateral Movement and Privilege Escalation: Attackers move laterally across networks, escalating privileges and establishing persistence. Dwell time has historically exceeded 200 days in sophisticated campaigns, though modern ransomware is deployed within 24 hours in over half of cases. [3]
- Deployment and Encryption: The ransomware payload is deployed across the network, encrypting files using strong algorithms (AES/RSA). Shadow copies and backup files are frequently deleted to prevent recovery. [5]
- Extortion: Attackers demand payment in cryptocurrency. In double extortion schemes, stolen data is threatened for public release on leak sites, with average demands exceeding USD 5.2 million in H1 2024. [6]

4.2 Detection Findings

The literature consistently identifies behavioral detection and machine learning as the most effective detection approaches for modern ransomware. [4] Traditional signature-based antivirus tools are insufficient against novel and polymorphic ransomware variants, which are designed to evade static signatures. [4,5] Key detection mechanisms identified include:

- Network Traffic Monitoring: Anomalous C2 communications and unusual file access patterns detected via SIEM platforms provide early warning indicators. [4,10]
- Behavioral Detection via EDR: Monitoring for mass file renaming, rapid encryption activity, shadow copy deletion, and unusual privilege escalation enables real-time response and endpoint isolation. [5,9]
- Machine Learning Models: AI and deep learning models trained on file activity, system calls, and network behavior outperform signature-based tools, particularly against zero-day ransomware variants. [4]
- Honeypots and Deception Technology: Decoy files and systems that no legitimate user would access provide early, high-fidelity alerts upon interaction by ransomware or attackers. [7]

4.3 Prevention Findings

The research findings strongly support a defense-in-depth approach to ransomware prevention, with no single control providing adequate protection on its own. [5,7] The most critical prevention measures identified across all reviewed sources are:

- Multi-Factor Authentication (MFA): Enforcing MFA on all accounts — especially privileged and remote access accounts — was identified as one of the highest-impact controls. Its absence was

directly linked to major breaches including Change Healthcare (2024). [7,8]

- Patch Management: Regular, automated patching of operating systems and applications eliminates exploitable vulnerabilities. Organizations that delay patching remain disproportionately vulnerable. [7]
- Network Segmentation and Zero Trust: Segmenting the network and adopting Zero Trust principles limits lateral movement and reduces the blast radius of successful intrusions. [7]
- Security Awareness Training: Human error remains a primary attack enabler. Regular phishing simulations and training programs were found to significantly reduce susceptibility to social engineering. [5,7]
- The 3-2-1 Backup Rule: Maintaining three copies of data on two media types with one offline copy — and testing restoration regularly — was identified as the most critical recovery enabler. 76% of 2024 ransomware attacks compromised backup data, making offline and immutable backups essential. [3,5]

4.4 Recovery Findings

Recovery from ransomware requires a structured, pre-planned incident response approach. [3,10] Key findings from the literature on recovery include:

- Isolation and Containment: Immediate disconnection of infected systems from the network is the first and most critical step, limiting encryption spread. Organizations with rehearsed incident response plans complete isolation significantly faster. [7,10]
- Forensic Analysis: Post-containment forensics to identify the attack vector, ransomware strain, and scope of compromise is essential for targeted remediation and future hardening. [9,10]
- Backup Restoration: Recovery from verified, uncompromised offline backups remain the safest restoration path. In 2024, the average recovery time was 24 days, emphasizing the value of preparation and tested backups. [3]
- Ransom Payment Decision: Paying the ransom does not guarantee data recovery and funds further criminal activity. Organizations are advised to engage law enforcement (FBI IC3) and incident response professionals before making payment decisions. [6,8]
- Post-Incident Hardening: A thorough post-incident review to address root causes, update incident response plans, and conduct tabletop exercises is essential to prevent recurrence. [7,10]

4.5 Discussion

The findings of this research reveal that ransomware is no longer a purely technical threat — it is an organizational and human challenge requiring a holistic response. [1,7] The convergence of RaaS platforms, double extortion tactics, and AI-enhanced attack tools has fundamentally shifted the threat landscape, making attacks faster, more targeted, and more damaging than ever before. [1,6]

A consistent theme across all reviewed sources is the gap between the sophistication of attackers and the preparedness of most organizations. Despite well-documented best practices, basic controls such as MFA and offline backups remain inconsistently implemented. [7,8] The Change Healthcare incident demonstrates that even large, well-resourced organizations can suffer catastrophic breaches due to a single missing control. [8]

The research also highlights an important tension in the ransom payment debate. While paying a ransom may appear to offer the fastest path to recovery, it reinforces the ransomware ecosystem and provides no guarantee of data restoration. [6] Organizations that invest in preventive controls and recovery capabilities are both less likely to be successfully attacked and better positioned to recover without payment when attacks do occur. [3,5]

V. CONCLUSION

Ransomware represents one of the most serious and rapidly evolving cybersecurity threats of the modern era. [1,6] This research has examined ransomware attack patterns, detection techniques, prevention strategies, and recovery approaches, drawing on a systematic review of current literature and industry reports.

The findings demonstrate that no single security control is sufficient; effective defense requires a

comprehensive, multi-layered approach that integrates proactive prevention, early detection, and robust recovery capabilities. [4,5,7]

Key recommendations arising from this research include: enforcing Multi-Factor Authentication across all accounts [7,8]; implementing automated patch management to eliminate exploitable vulnerabilities [7]; adopting network segmentation and Zero Trust architecture to limit lateral movement [7]; conducting regular security awareness training and phishing simulations [5,7]; maintaining tested, offline, immutable backups following the 3-2-1 rule [3,5]; deploying behavioral and AI-powered endpoint detection tools [4]; and developing, rehearsing, and continuously updating an incident response plan. [10]

The cost of prevention is far smaller than the cost of recovery. [3] As ransomware continues to evolve in sophistication and scale, organizations that invest in a security-first culture, continuous monitoring, and resilient architectures will be best positioned to withstand attacks, minimize disruption, and maintain the trust of their stakeholders. [7,8]

REFERENCES

[1] Allianz Commercial. (2024). Ransomware attacks were up 50% year-on-year in 2023: 3 trends to be vigilant for in 2024. World Economic Forum Annual Meeting. Retrieved from https://www.weforum.org/stories/2024/02/3-trends-ransomware-2024/

[2] Flashpoint. (2023). The Seven Phases of a Ransomware Attack: A Step-by-Step Breakdown of the Attack Lifecycle. Security Boulevard. Retrieved from https://flashpoint.io/blog/the-anatomy-of-a-ransomware-attack/

[3] Infrascale. (2025). Ransomware Recovery Guide, Strategies and Tactics. Retrieved from https://www.infrascale.com/ransomware-recovery-guide/

[4] Journal of Knowledge Learning and Science Technology. (2023). Understanding Ransomware Attacks: Trends and Prevention Strategies. ISSN: 2959-6386 (Online), Vol. 2, Issue 1. Retrieved from https://jklst.org/index.php/home/article/view/183

[5] IJRASET. (2025). A Survey of Ransomware Resilience: Strategies for Prevention and Recovery. Retrieved from https://www.ijraset.com/research-paper/a-survey-of-ransomware-resilience-strategies-for-prevention-and-recovery

[6] TRM Labs. (2024). Ransomware in 2024: Latest Trends, Mounting Threats, and the Government Response. Retrieved from https://www.trmlabs.com/resources/blog/ransomware-in-2024-latest-trends-mounting-threats-and-the-government-response

[7] Cyber Management Alliance. (2024). Ransomware Resilience: Prevention and Recovery in 2024. Retrieved from https://www.cm-alliance.com/cybersecurity-blog/ransomware-resilience-prevention-and-recovery-in-2024

[8] National Cooperative Bank. (2024). Ransomware Has Evolved: Updated 2024 Trends & Best Practices. Retrieved from https://www.ncb.coop/blog/ransomware-has-evolved-updated-2024-trends-best-practices

[9] Picus Security. (2024). The Ransomware Attack Lifecycle from the Defender's Perspective. Retrieved from https://www.picussecurity.com/resource/the-ransomware-attack-lifecycle-from-the-defenders-perspective

[10] IBIMA Publishing. (2026). Ransomware Threats and Defensive Strategies: Insights from Literature and Practice. Retrieved from https://ibimapublishing.com/articles/JIACS/2026/387036