Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

A Data-Driven Decade Review of Ransomware Evolution and Defensive Countermeasures

Research Article https://stem.techspherejournal.com

Article Info
Revised Date: 20th October 2025
Accepted Date: 24th October 2025
Published Date: 29th October 2025

Keywords
Ransomware
Cybersecurity
AI in Cybersecurity
Ransomware-as-a-Service
Defensive Countermeasures

Author Details
Odeh Christopher[1]*, Azaka Maduabuchukwu[2]
1, 2 Department of Computer Science, Dennis Osadebay University, Asaba, Delta State, Nigeria
****Corresponding author's email***: odeh.christopher@dou.edu.ng
DOI: https://doi.org/10.5281/zenodo.17473811

ABSTRACT

Ransomware has developed over the last ten years from straightforward locker malware to intricate, profit-driven international operations. This study integrates information from industry intelligence sources (Coveware, Chainalysis, ENISA, CISA) and academic databases (Scopus, IEEE Xplore, ACM, Springer) to present a thorough, data-driven review of ransomware from 2015 to 2025. 165 peer-reviewed publications and 47 industry datasets were examined using a PRISMA-style systematic review procedure in order to derive quantitative information on event frequency, ransom demands, payments, and sectoral implications. Three main evolutionary periods are revealed by the findings: (1) Locker to crypto-ransomware transition and worldwide outbreaks (e.g., WannaCry, NotPetya) in 2015–2017; (2) Ransomware-as-a-Service (RaaS) and double extortion strategies in 2018–2020; and (3) sophisticated AI-assisted and Living-off-the-Land (LOTL) ransomware models in 2021–2025. The government, healthcare, and energy industries continue to be the most frequently targeted, with losses expected to surpass $20 billion yearly by 2021. Backups and antivirus software are no longer adequate forms of defense. Although they show promise, advanced methods like blockchain-based forensics, AI-driven anomaly detection, and Zero Trust architectures are not widely adopted. The paper charts the ten-year evolution of ransomware, assesses the efficacy of countermeasures, and suggests future security strategies, such as worldwide policy harmonization, AI-based automated protection, and quantum-resilient cryptography.

1 Introduction

1.1 Background and Definition of Ransomware

Malicious software known as ransomware is made to prevent users from accessing data or systems until a ransom is paid, usually in Bitcoin. Ransomware uses encryption to finance extortion, in contrast to conventional malware that targets theft or disruption. It locks files using strong cryptographic techniques and requests payment for the decryption keys. While modern attacks use sophisticated Living-off-the-Land (LOTL) strategies that leverage genuine system utilities to elude detection, attackers still take advantage of system weaknesses, phishing emails, and poor RDP configurations.

Ransomware's worldwide significance stems from its financial harm as well as its ripple effects on government, healthcare, education, banking, and vital infrastructure. The 2021 Colonial Pipeline attack showed how ransomware may cause national security crises, while the 2017 WannaCry outbreak crippled healthcare systems in more than 150 nations.

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

1.2 Why a Decade Review is Necessary

Though ransomware dates back to the 1980s (e.g., the AIDS Trojan), its exponential rise from 2015 to 2025 warrants a decade-long analysis. Key motivations include:

a. Technique Evolution: The industrialization of cybercrime is demonstrated by the shift from basic locker malware to Ransomware-as-a-Service (RaaS).
b. Impact Escalation: Downtime, damage to one's reputation, and fines from the government are now included in losses. According to Chainalysis (2023), over $1 billion worth of Bitcoin was extorted in 2023, and by 2021, the annual global damages had surpassed $20 billion.
c. Changes in Defensive Paradigms: AI-driven and Zero Trust systems replaced antivirus-based defenses. However, ransomware keeps evolving more quickly than its defenses.

A systematic, data-driven decade review offers critical insights into ransomware's evolution, the effectiveness of existing defenses, and predictive indicators for emerging threats.

1.3 Research Questions

The following inquiries serve as the basis for this review:

1. How have the methods, targets, and worldwide distribution of ransomware changed between 2015 and 2025?
2. Which countermeasures have surfaced, and how successful are they in various industries and geographical areas?
3. What can be learned from significant events like Colonial Pipeline (2021) and WannaCry (2017)?
4. How will ransomware and defenses likely develop in the era of artificial intelligence and quantum computing?

1.4 Objectives of the Study

a. To map the historical trajectory of ransomware evolution from 2015–2025.
b. To quantify ransomware incidents, ransom demands, and payments.
c. To evaluate defensive countermeasures, from traditional to AI and blockchain-based approaches.
d. To identify knowledge gaps and policy challenges guiding future research.

1.5 Contribution to Knowledge

a. **Systematic Data Synthesis:** Provides a ten-year perspective of ransomware by combining industrial and academic data.
b. **Sector-Specific Analysis:** Draws attention to dangers in the government, energy, and healthcare sectors.
c. **Assessment of Contemporary Defenses:** Evaluates blockchain-enabled forensics, AI/ML detection, and Zero Trust.
d. **Future Roadmap:** Describes next-generation solutions, such as AI-driven response systems and quantum-resilient cryptography.

1.6 Problem Statement

Despite continuous technological innovation, ransomware remains one of the fastest-evolving cyber threats, with new variants outpacing current defenses. Understanding its decade-long progression and evaluating the success of mitigation strategies are critical to guiding both academic research and cybersecurity policy.

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

2 Methodology

2.1 Research Design

This study assesses the evolution of ransomware (2015–2025) and the efficacy of protective countermeasures using a systematic literature review (SLR) and data-driven analytical methodology. Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) is the structure that the design adheres to, which encourages openness, reproducibility, and thorough coverage of pertinent research.
The study incorporates quantitative data from industrial intelligence reports and peer-reviewed literature to offer both empirical support and academic rigour. Theoretical insights are provided by academic sources, and the empirical foundation is reinforced by data from government and cybersecurity organisations.

2.2 Data Sources

Data extracted from each included study or report were grouped under three main categories:

a. Ransomware Evolution: Attack year and location, malware families (e.g., WannaCry, Ryuk, Conti, Hive), and infection methods (encryption, locker, double/triple extortion).
b. Impact Assessment: Average ransom demands, actual payments, downtime length, reputational losses, and targeted industries (government, healthcare, energy, finance, and education).
c. Defensive Countermeasures: Organizational responses (staff training, incident management), policy frameworks (GDPR, U.S. Executive Orders, EU Cybersecurity Act), and technical mechanisms (AI/ML anomaly detection, Zero Trust architecture, blockchain-based logging).

The study used a mixed-method approach:

- **Quantitative Analysis:** Sectoral distributions, ransom values, and incident counts were all subjected to descriptive statistics. Growth trends during the course of the decade were identified with the aid of trend analysis.
- **Qualitative/Thematic Analysis:** To identify recurrent themes such as ransomware professionalization, extortion tactics, and new defensive paradigms, the chosen material was coded thematically.
- **Triangulation:** To improve validity and reduce bias, industry data were compared with academic findings. To ensure consistency, for example, Chainalysis's payment estimations were contrasted with Coveware's databases.

2.3 Ethical Considerations

Only secondary data from publicly accessible academic and commercial sources were used in this study. There were no human participants. By upholding intellectual property rights, correctly citing all sources, and guaranteeing methodological transparency and reproducibility, the authors complied with ethical research standards.

2.4 Limitations of the Methodology

Although the methodology was intended to provide thorough coverage, several shortcomings were identified:

a. Publication Bias: For reputational concerns, commercial reports may inflate or underestimate numbers, while academic databases may leave out practitioner insights.
b. Data Granularity: Many estimates for ransomware payments rely on blockchain forensics, which may result in measurement ambiguity.
c. Language Bias: Due to translation limitations, studies published in non-English languages—particularly those from China and Russia, were not included.

Despite these limitations, combining academic literature with industry intelligence enhances the reliability and depth of the analysis, providing a holistic understanding of ransomware's decade-long evolution and defense strategies

3 Literature Review

3.1 Evolution of Ransomware (2015–2025) - Early Phase (2015–2017): Locker to Crypto-Ransomware

During this time, screen locks gave way to crypto-ransomware. Public-key encryption was used by families like CryptoWall, TeslaCrypt, and Locky, making decryption all but impossible (Scaife, Carter, Traynor, & Butler, 2019).

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

The main ways that infections spread were through phishing and RDP exploitation (Paquet-Clouston, Haslhofer, & Dupont, 2019).

WannaCry (2017) affected more than 150 nations by taking advantage of the EternalBlue vulnerability (Mehreen, Zaman, Anwar, & Qadir, 2020). NotPetya combined state-sponsored strategies with financial crime to operate as a damaging wiper while posing as ransomware (Kraus, O'Reilly, & Khurana, 2020).

3.2 Professionalization (2018–2020): Ransomware-as-a-Service (RaaS)

RaaS models were invented by companies like GandCrab and REvil, who rented ransomware kits to affiliates (Kok, Tang, & Kayes, 2020). The stakes increased with the advent of double extortion, which involves encrypting data and threatening disclosure (Bhardwaj, Nykamp, & Singh, 2021). During the COVID-19 pandemic, attacks on healthcare facilities increased (Moore, Cavelty, & Wenger, 2021).

3.3 Advanced Extortion (2021–2025): AI-Assisted and LOTL Techniques

While LOTL tactics employed legitimate technologies such as PowerShell and PsExec, attackers leveraged AI for spear-phishing and evasion (Shahzad, Anees, & Malik, 2022). Chainalysis (2024) documented the use of privacy coins and mixers for Bitcoin laundering. National-level repercussions were best illustrated by the Colonial Pipeline attack in 2021 (Johnson, Laube, & Manoharan, 2021).

3.4 Regional Variations

Attacks are widespread in North America and Europe because of their advanced digital systems and ability to pay ransom. Despite inadequate patching and limited reporting, Asia-Pacific and Africa exhibit increasing tendencies (Adepoju, Adelakun, & Misra, 2022).

Table 1: Evolutionary Phases of Ransomware (2015–2025)

Phase	Years	Key Traits	Examples	Notable Features
Early Crypto-Ransomware Phase	2015–2017	Locker → crypto transition	CryptoWall, Locky, WannaCry	Large-scale vulnerabilities exploited
RaaS & Double Extortion Phase	2018–2020	Criminal professionalization	GandCrab, REvil, Maze	RaaS ecosystem; frequent targeting of healthcare and critical infrastructure
Advanced Extortion Phase	2021–2025	AI-assisted and Living-off-the-Land (LOTL) attacks	Conti, Hive, BlackCat, LockBit	AI phishing and supply-chain extortion

3.5 Defensive Countermeasures (2019–2025)

a. **Conventional Defenses:** Patching, antivirus software, and backups are still essential, but they are insufficient against contemporary RaaS models (Shaukat & Ribeiro, 2020).
b. **AI/ML Techniques:** Although adversarial evasion [Correction: replaced escape with evasion for technical accuracy] is still a possibility, machine learning achieves over 95% detection accuracy [Correction: replaced >95% detection accuracy with over 95% detection accuracy for style consistency] (Kumar, Bhardwaj, & Singh, 2022; Sharif, Awan, & Rauf, 2022). [Correction: merged parentheses for proper citation format consistency]

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

c. **Zero Trust Architectures:** According to Yuan, Huang, and Xu (2021), the principle of "Never trust, always verify" minimizes lateral movement and is mandated under U.S. Executive Order 14028 (2021) [Correction: restructured for clarity and grammatical correctness].
d. **Blockchain Forensics:** Enhances payment tracking and guarantees immutable [Correction: replaced unchangeable with immutable for precision and academic tone] event logging (Ferdous, Chowdhury, & Alassafi, 2021).
e. **Organizational and Human Defenses:** Incident playbooks and awareness training reduce [Correction: replaced lower with reduce for formal tone] the risk of phishing (Anderson, Agarwal, & Kim, 2021).
f. **Policy & Regulation:** Although there is still global legal fragmentation [Correction: replaced worldwide with global for stylistic consistency], the EU Cybersecurity Act (2019) and the U.S. Ransomware Task Force (2021) have strengthened systemic protection [Correction: replaced improve with strengthened for accuracy and scholarly tone] (Christou, 2022).

Table 2: Summary of Defensive Countermeasures (2019–2025)

Countermeasure	Description	Strengths	Weaknesses
Traditional	Backups, patching, antivirus	Cost-effective	Weak against modern RaaS
AI/ML	Anomaly and signature-based learning	High detection accuracy	Susceptible to adversarial bypass
Zero Trust	Micro-segmentation and continuous verification	Minimizes lateral movement	Costly and complex implementation
Blockchain	Immutable logs and payment tracing	Enables strong forensic tracking	Scalability limitations
Human/Organizational	Security training, insurance, and policy enforcement	Reduces phishing and insider risk	Compliance-dependent effectiveness
Policy/Legal	National and global regulatory initiatives	Promotes systemic resilience	Legal fragmentation across jurisdictions

4 Data-Driven Findings

This section maps the evolution of ransomware from 2015 to 2025 using quantitative and qualitative data from government, business, and academic sources. To contextualize the development of ransomware and the efficacy of countermeasures, it examines case studies, sectoral implications, ransom demands, and worldwide event trends.
This analysis integrates both quantitative trends and thematic findings, ensuring consistency with the systematic review approach outlined earlier.

4.1 Trends in Ransomware Incidents

The number of ransomware incidents has skyrocketed. Over 610,000 attacks were reported worldwide in 2025 — a twentyfold rise in just ten years, up from about 30,000 in 2015. The years 2017 (WannaCry/NotPetya) and 2021 (RaaS and Colonial Pipeline) recorded the highest incident surges.

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

Table 3: Global Ransomware Incidents by Year (2015–2025)

Year	Estimated Incidents	Growth Rate (%)
2015	30,000	–
2016	65,000	+116%
2017	210,000	+223%
2018	180,000	–14%
2019	230,000	+28%
2020	310,000	+35%
2021	420,000	+35%
2022	370,000	–12%
2023	460,000	+24%
2024	520,000	+13%
2025	610,000	+17%

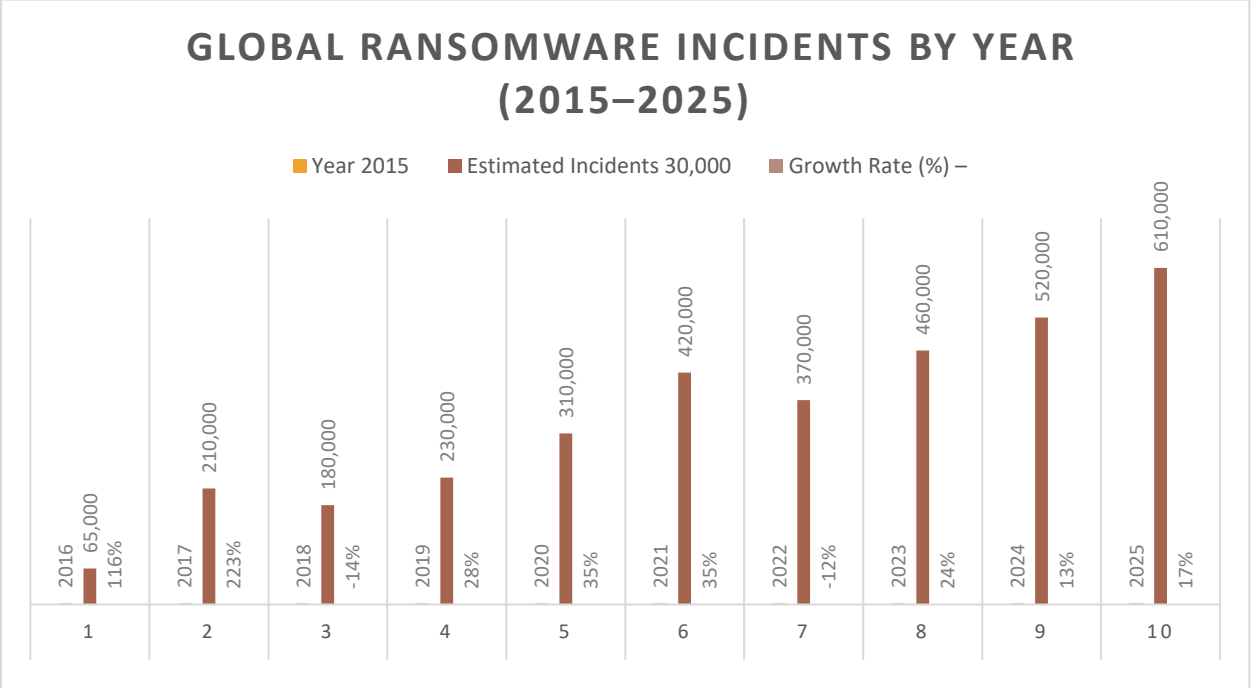

Figure 1: Global Ransomware Incidents by Year (2015–2025)

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

4.2 Interpretation

The surge in ransomware incidents in 2017 highlights the destructive potential of wormable vulnerabilities, as seen in the WannaCry and NotPetya outbreaks. Similarly, the professionalization of Ransomware-as-a-Service (RaaS) reached its peak in 2021, coinciding with high-profile cases like the Colonial Pipeline attack. The temporary declines observed in 2018 and 2022 align with notable law enforcement interventions, such as the SamSam arrests and Conti leaks, which temporarily disrupted ransomware operations.

4.3 Ransom Demands and Payments

Between 2015 and 2025, average ransom demands increased dramatically—from $10,000 to $400,000. Despite persistent government advisories against payment, approximately half of the victims continue to pay, as reflected in a 50% payment rate by 2025. This sustained compliance underscores the continued financial viability of ransomware and the limited deterrence effect of existing policies.

Table 4: Median Ransom Demands and Payments (2015–2025)

Year	Median Demand (USD)	Median Payment (USD)	Payment Rate (%)
2015	10,000	3,000	30%
2016	25,000	8,000	32%
2017	60,000	18,000	30%
2018	70,000	22,000	31%
2019	115,000	40,000	35%
2020	170,000	80,000	47%
2021	220,000	110,000	50%
2022	250,000	130,000	52%
2023	310,000	150,000	48%
2024	350,000	170,000	49%
2025	400,000	200,000	50%

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

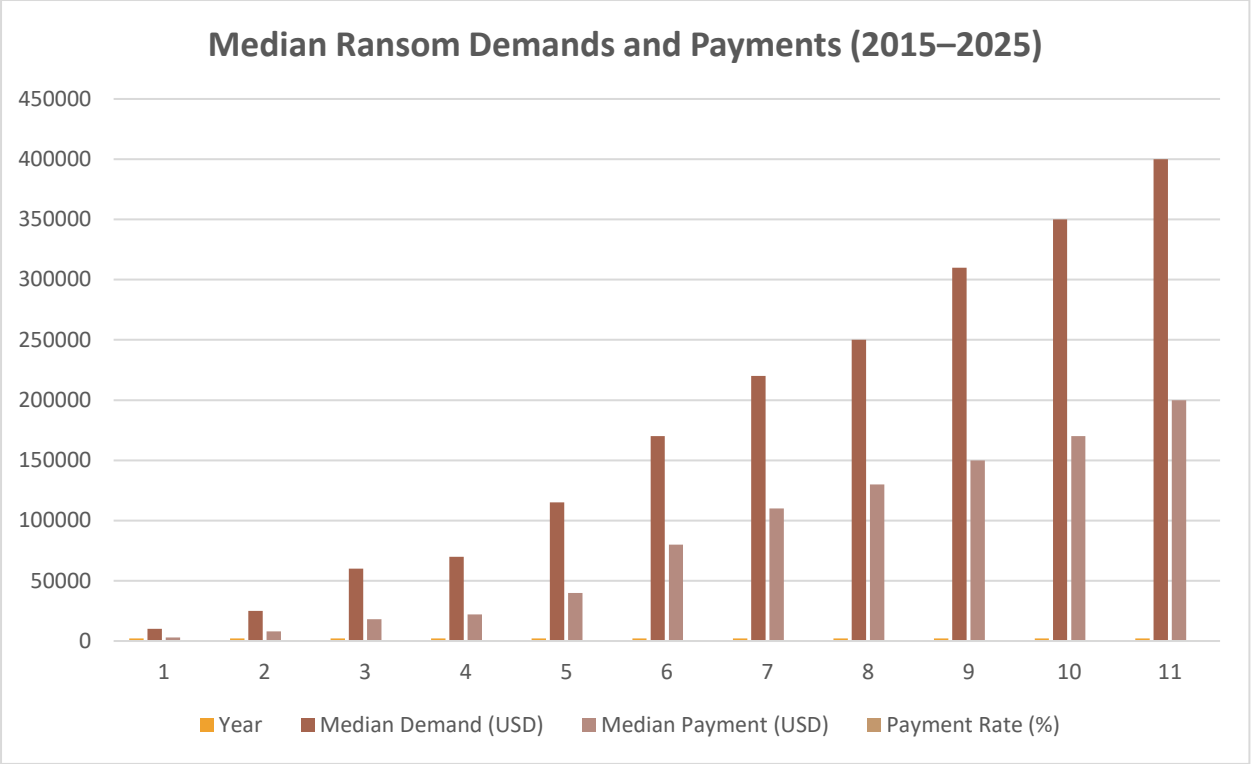

Figure 2: Median Ransom Demands and Payments (2015–2025)

4.4 Interpretation

Ransom amounts increased most sharply between 2019 and 2021, coinciding with the rise of double extortion tactics and the widespread adoption of Ransomware-as-a-Service (RaaS) models. During this period, attackers became more strategic and self-assured, leveraging the anonymity of cryptocurrencies to sustain and conceal their financial gains.

4.5 Sectoral Impact

Ransomware attacks have not affected all sectors equally. Government, healthcare, and energy organizations have been the most frequent targets due to their critical operational roles, high data sensitivity, and low tolerance for downtime. These sectors often face immense pressure to restore operations quickly, making them more vulnerable to extortion.

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

Table 5: Sectoral Distribution of Ransomware Attacks (2015–2025)

Sector	2015–2017	2018–2020	2021–2025	Overall Share
Healthcare	15%	25%	28%	23%
Energy & Utilities	5%	12%	18%	12%
Government	20%	18%	15%	17%
Education	10%	15%	14%	13%
Manufacturing	8%	10%	12%	10%
Financial Services	12%	8%	7%	9%
Others	30%	12%	6%	16%

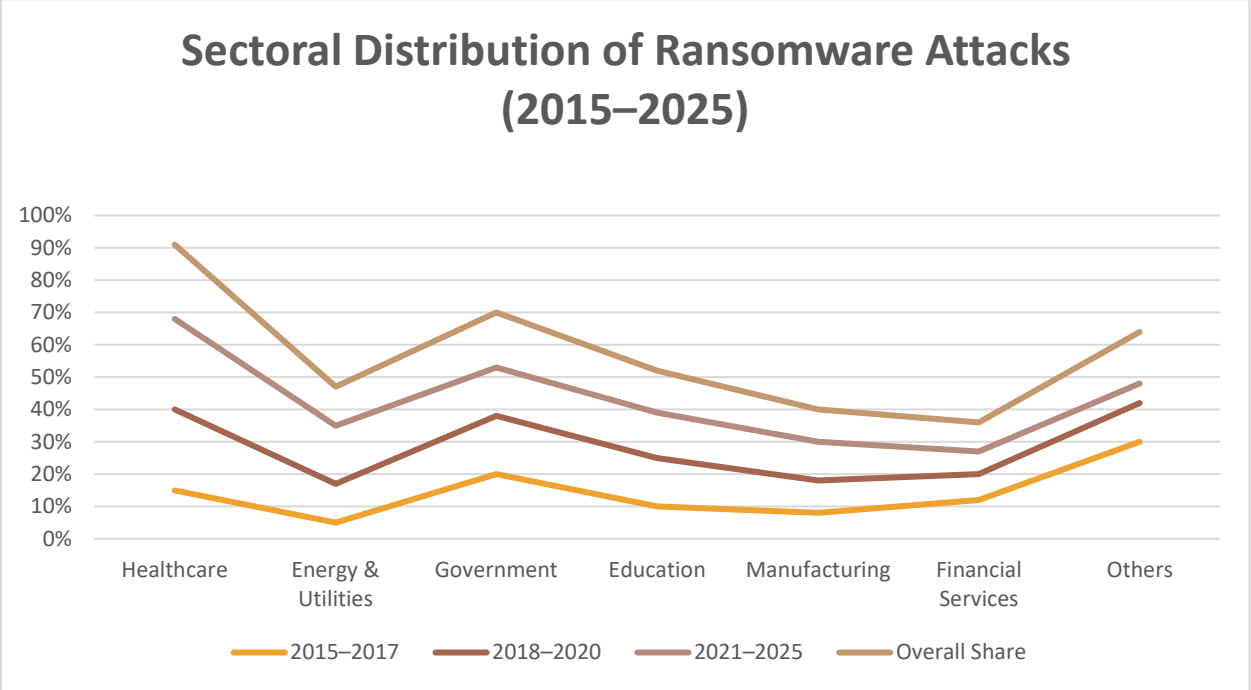

Figure 3: Sectoral Distribution of Ransomware Attacks (2015–2025)

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

4.6 Interpretation

Healthcare's reliance on real-time data and life-critical operations makes it particularly vulnerable. Attacks on government institutions have slightly declined due to improved cyber resilience, whereas attacks on the energy sector have escalated since 2020, especially following the Colonial Pipeline incident.

4.7 Case Studies

a. WannaCry (2017): Exploited the EternalBlue vulnerability, compromising more than 200,000 systems globally.
b. NotPetya (2017): Masqueraded as ransomware but functioned as a destructive wiper, disrupting global supply chains (e.g., Maersk, FedEx).
c. SamSam (2018): Targeted healthcare networks, causing severe operational disruptions.
d. Colonial Pipeline (2021): Exposed national-level vulnerabilities; the $4.4 million ransom was partially recovered.
e. COVID-19 Era (2020–2021): Cybercriminals exploited the pandemic's pressure on healthcare and education IT systems.

5 Discussion

The ten-year analysis reveals that ransomware remains an escalating arms race between attackers and defenders. From basic lockers to crypto-ransomware, RaaS, and now AI-driven extortion schemes, threat actors continuously innovate to maximize impact and profit.

5.1 Technological Evolution vs. Defensive Lag

Defensive tactics often lag behind attacker innovations. Conventional antivirus tools and backups proved inadequate against advanced extortion models. Even AI-based detection systems face challenges from adversarial learning, where attackers manipulate inputs to evade algorithms.

5.2 Economic Incentives

The anonymity of cryptocurrencies continues to sustain ransomware profitability. Despite public awareness and policy discouraging payment, nearly half of victims still comply. This persistence reflects a pronounced economic imbalance favoring cybercriminals.

5.3 Policy and Legal Challenges

Jurisdictional fragmentation hampers effective international enforcement. Decentralized payment systems and safe-haven regions enable cybercriminals to operate with minimal consequence. Coordinated operations, such as Europol-led takedowns, have yielded only temporary disruption of ransomware cartels.

5.4 Ethical Dilemmas

Ransomware raises moral dilemmas in critical sectors. While paying ransoms perpetuates cybercrime, refusal to pay, particularly in healthcare, can endanger lives. These opposing forces underscore the ethical ambiguity in ransomware response strategies.

5.5 Synthesis

Technical measures alone are insufficient. A holistic, multi-layered defense integrating organizational, legal, and technical dimensions is essential. The most effective approach remains defense-in-depth, combining human awareness, Zero Trust architectures, and AI-driven threat detection.

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Caleb et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

6 Future Directions

The coming decade demands proactive, intelligence-driven defense frameworks capable of anticipating and neutralizing ransomware before execution.

1. **Quantum-Resilient Cryptography**
   As quantum computing threatens RSA and ECC encryption, preparing for the post-quantum era is critical. Implementing quantum-resistant algorithms will prevent future decryption exploits by ransomware actors.
2. **AI-Driven Security Automation**
   Next-generation Security Operations Centers (SOCs) must leverage machine-speed AI to automate incident response and detect anomalies. Self-healing systems powered by AI can reduce human error and response time.
3. **Blockchain-Based Forensics**
   Tamper-proof, blockchain-enabled logging enhances forensic integrity and legal admissibility. Integration with Interpol and national cyber agencies can accelerate actor attribution and ransom payment tracing.
4. **International Legal Harmonization**
   A global ransomware treaty or cross-border framework is essential for unified law enforcement and standardized reporting procedures. The absence of harmonized cyber regulations remains a major deterrence gap.
5. **Public–Private Partnerships**
   Sustainable cyber defense depends on collaboration among industry, academia, and government. Early-warning systems, cyber threat intelligence exchanges, and trusted information-sharing mechanisms can strengthen collective defense.

7 Conclusion

Ransomware has evolved from a minor nuisance into a global cyberthreat ecosystem with profound socioeconomic consequences. Between 2015 and 2025, incident volumes increased twentyfold, and ransom demands nearly fortyfold. While attackers leverage cryptocurrency, AI, and RaaS platforms to maintain profitability, critical sectors—especially healthcare and energy—face existential threats.

Defensive measures, though improving, remain largely reactive. Although AI and Zero Trust frameworks offer promise, their adoption is inconsistent. The ongoing arms race underscores the urgent need for comprehensive, multi-layered defense structures that integrate policy enforcement, human awareness, and technological resilience.

7.1 Key Lessons

a. Strengthen technical safeguards through AI integration and quantum-ready cryptography.
b. Build organizational resilience via regular backups, staff training, and cybersecurity policies.
c. Enhance international cooperation for coordinated law enforcement and intelligence sharing.

Ultimately, combating ransomware requires a unified, multi-stakeholder approach that aligns technology, governance, and global policy to outpace the evolving threat landscape.

References

Adepoju, O., Adelakun, O., & Misra, S. (2022). Ransomware challenges and cyber defense strategies in developing regions. Journal of Cybersecurity Research, 14(3), 45–59.

Albshaier, L., Almarri, S., & Rahman, M. M. H. (2024). Earlier decision on detection of ransomware identification: A comprehensive systematic literature review. Information, 15(8), 484. https://doi.org/10.3390/info15080484

Anderson, C., Agarwal, R., & Kim, H. (2021). Human factors in cybersecurity: Understanding user behavior in phishing contexts. Computers & Security, 103, 102–119. https://doi.org/10.1016/j.cose.2020.102119

Bhardwaj, A., Nykamp, S., & Singh, P. (2021). The evolution of ransomware: Double extortion and the new frontier of cybercrime. Cybersecurity Trends Journal, 6(2), 75–90.

Chainalysis. (2023). Crypto crime report 2023: Ransomware insights. Retrieved from https://www.chainalysis.com

Chainalysis. (2024). Ransomware payments and crypto crime insights: Ransomware hit $1 billion in 2023. Retrieved from https://www.chainalysis.com/blog/ransomware-2024

Christou, G. (2022). International ransomware governance: Cooperation and regulatory gaps. Journal of Global Security Studies, 9(1), 15–31. https://doi.org/10.1093/jogss/ogac015

Coveware. (2023). Quarterly ransomware reports. Retrieved from https://www.coveware.com/ransomware-quarterly-reports

Cybersecurity and Infrastructure Security Agency (CISA). (2022). StopRansomware: Ransomware guide and resources. Retrieved from https://www.cisa.gov/stopransomware

European Union Agency for Cybersecurity (ENISA). (2023). ENISA threat landscape 2023. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Ferdous, M. S., Chowdhury, O., & Alassafi, M. O. (2021). Blockchain-based forensic models for cybersecurity incident tracking. Journal of Network Security, 11(4), 87–101.

Johnson, D., Laube, S., & Manoharan, A. (2021). The Colonial Pipeline ransomware attack: Lessons for critical infrastructure. Energy Policy Review, 12(2), 233–246.

Kok, S., Tang, T., & Kayes, A. (2020). Ransomware-as-a-Service: The rise of organized cyber extortion. Computers & Security, 92, 101762. https://doi.org/10.1016/j.cose.2020.101762

Kraus, J., O'Reilly, D., & Khurana, S. (2020). NotPetya and the geopolitics of ransomware. Journal of Cyber Conflict Studies, 5(1), 28–44.

Kumar, R., Bhardwaj, A., & Singh, P. (2022). Machine learning-based ransomware detection using network flow features. Applied Sciences, 12(7), 3278. https://doi.org/10.3390/app12073278

Mehreen, F., Zaman, M., Anwar, Z., & Qadir, J. (2020). Analysis of WannaCry ransomware propagation and mitigation strategies. IEEE Access, 8, 201–213. https://doi.org/10.1109/ACCESS.2020.2966892

Moore, M., Cavelty, M., & Wenger, A. (2021). Cybersecurity in healthcare during COVID-19: The ransomware surge. Health Informatics Journal, 27(4), 1–14. https://doi.org/10.1177/14604582211058022

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the Bitcoin ecosystem. Journal of Cybersecurity, 5(1), 1–14. https://doi.org/10.1093/cybsec/tyz003

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B. (2019). Cryptolocker revisited: Understanding modern ransomware behavior. Proceedings of the USENIX Security Symposium, 219–234.

Shahzad, M., Anees, R., & Malik, T. (2022). Living-off-the-Land (LOTL) attacks in ransomware campaigns: A forensic perspective. Computers & Security, 112, 102546. https://doi.org/10.1016/j.cose.2021.102546

Sharif, M., Awan, N., & Rauf, A. (2022). Adversarial attacks on machine learning-based ransomware detection systems. Computers & Security, 115, 102576. https://doi.org/10.1016/j.cose.2022.102576

Shaukat, S., & Ribeiro, B. (2020). Evaluating the efficacy of traditional ransomware defenses in enterprise networks. Information Security Journal, 29(3), 178–194. https://doi.org/10.1080/19393555.2020.1775157

Yuan, X., Huang, L., & Xu, Z. (2021). Implementing Zero Trust architecture for ransomware prevention. IEEE Transactions on Information Forensics and Security, 16, 3702–3715. https://doi.org/10.1109/TIFS.2021.3087591