Bulletin of Nexus
Multidisciplinary International Research Journal, Double-Blind Peer Reviewed, Open Access Journal
ISSN : 3065-7865 / Volume-2, Issue-4 / April - 2025

Original Article

Ransomware and Emerging Cyber Threats in 2025

Nida Ibrahim Khedekar
Second Year, IT, College of Science (Computer Science & Information Technology), Mahad

Manuscript ID:
BN-2025-020405

ISSN: 3065-7865

Volume 2

Issue 4

April 2025

Pp. 22-27

Submitted: 30 Jan 2025

Revised: 05 Feb 2025

Accepted: 10 Mar 2025

Published: 30 Apr 2025

DOI: 10.5281/zenodo.15962178

DOI link:
https://doi.org/10.5281/zenodo.15962178

Abstract

By 2025, ransomware will become one of the most complex and harmful cybersecurity threats worldwide. Ransomware is no longer limited to simple cryptographic attacks and contains polymorphic variants driven by artificial intelligence that develop in real time, allowing people to avoid traditional anti-virus defenses and aim for intersector vulnerability. In this article, we examine the surprising rise in ransomware as a service (RAAS). This reduced the barriers to entry for cybercriminals and increased the frequency and scope of attacks from health, education, government, and financial perspectives. Data such as Symantec (2024), ENISA (2024), and IBM X-Force (2023) show how phishing, AI-controlled malware, uncertain clouds, and IoT infrastructure are used in invasive systems. The patient's condition was severe. They are unprepared organizations that face increased downtime, financial losses, ethical dilemmas associated with ransom payments, and system-wide paralysis. Case statistics show that 68% of the organizations involved did not have a sustainable security plan. Furthermore, the imminent threat of quantum computers casts further uncertainty on current encryption standards. Despite efforts by agencies such as the CISA and Miter to improve their defense, global responses still lack cohesion. This study highlights the important need for proactive and respectable defense strategies, a unified international legal framework, and stronger public-private cooperation to mitigate these developing threats. The results showed that ransomware is no longer a digital nuisance. It poses a threat to national security and weapons that can disrupt the wells of the people if not addressed by urgency and collective resistance.

Keywords: *ransomware, cybersecurity, RAAS, malware AI, cybercrime, data, artificial intelligence*

Introduction

The digital revolution has changed the operations of individuals, organizations and governments. However, due to the large connectivity and dependency on digital systems, there is a corresponding increase in cyberwar spots. Ransomware is a kind of malicious software that encrypts files and requires payment for decryption, and has proven to be one of the most urgent cybersecurity challenges of a decade. In contrast to previous versions of ransomware, modern variants offer extensibility such as data stripping, double or triple forced or triple forced, and polymorphic properties that can escape traditional antivirus solutions. As businesses switch to the cloud and number of IoT devices (the Internet of Things), cybercriminals discover more opportunities for penetration. Today's threat players use social engineering, zero-day weaknesses and AI-controlled malware to carry out faster, more hidden and harmful attacks than ever before. The rise of cybercrime as a service, particularly Services as Ransomware (RAAS), has significantly reduced the technical requirements for carrying out largescale attacks. The research paper will examine the development of ransomware and cyber threats by 2025, the tactics used by attackers, their impact on various sectors, and defensive measures adopted around the world.

Objective:

1. Ransomware development and effectiveness assessment from 2015 to 2025.
2. Understand the operational and technical nature of modern ransomware attacks.
3. Evaluation of the effectiveness of current cybersecurity strategies.

Provides implementationable recommendations for cyber resistance.

Address for correspondence:

Nida Ibrahim Khedekar,Second Year, IT, College of Science (Computer Science & Information Technology), Mahad

Email: *khedekarnidai@gmail.com*

How to cite this article:

Khedekar, N. I. (2025). Ransomware and Emerging Cyber Threats in 2025. Bulletin of Nexus, 2(4), 22–27. https://doi.org/10.5281/zenodo.15962178

Quick Response Code:

Website: https://bnir.us

Review of Literature

Over the years, many studies and industry reports have provided critical insights into ransomware and other cyber threats, as they impact society. These include:

1. Symantec (2024) indicates that ransomware attacks have increased 350% in the last decade and have increased socio-economic impacts across the board. The 2024 ENISA Threat Landscape Report identified ransomware as the highest risk threat in online environments and noted that the techniques of data exfiltration and extortion have been developing alongside ransomware.
2. In 2023, IBM X-Force noted that ransomware groups now operate a double or triple extortion model in which victims receive additional pressure, while thieves take steps to avoid detection by utilizing stealth approaches.
3. The MITRE ATT&CK Framework (2023) disclosed the behaviors of threat actors and attack vectors in space. The ATT&CK Framework is a method by which managers develop a thought process for criminal operations.
4. CISA (2024) advised national cyber strategies focused on critical infrastructure with the element of public-private cooperation in order to mitigate cyber risk.
5. Kaspersky Labs (2023) discussed the rise of AI-operating malware tools and predicted that ransomware variants will increase specifically targeting mobile and IoT.
6. Gartner (2024) emphasized the importance of predictive analytics and AI-based detection as central components of the response to next-generation cyber threats and the growth of cloud computing environments.
7. When viewed together as sources, their meaning indicates that strategic security planning and technology should be integrated as solutions, but collaboration among all parties is required at the local, national, and international levels.

Research Methodology

In this study, a qualitative approach was adopted using secondary data. Such data are obtained from reliable sources, including official publications, research on cybersecurity, research in educational journals, and threat intelligence websites. This study will use both thematic analysis and comparative case studies to help understand the activity of ransomware in 2025.

Scope of Work:

- It will explore the years from 2015 to 2025 by examining both current and emerging cybersecurity threats.
- It considers the community and service sectors of healthcare, financial services, the government, and education.

Limitations:

- This study will use open sources that anyone can access in public.
- It did not include any real-time incident data nor classified intelligence.
- The real-time reporting of attacks and classified intelligence sources is not accessible to this study.
- A detailed quantitative analysis was not possible, partly due to inconsistent reporting on cyber threat activity and partly due to the opaque nature of many organizations affected by cyber activity, which limited our transparency when reporting out their statistics.
- While cyber threat activity is considered in a global context, this research focuses on the trends and developments occurring in the United States, the European Union, and selected areas of Asia.

Data Analysis

Ransomware and other cyber threats have made tremendous advances over the past decade. This section analyses various data sources around threat information, including global cybersecurity reports, sector-specific incident protocols, CISA (2024), Cyfirma (2025), and IBM X-Trals 3 (2024). In addition, we analyze financial damages as well as behavioral trends related to attack vectors, organizations, and threat actors.

Increase in Attacks

In the case of ransomware attacks, the level of change between 2022 and 2025 showed a staggering trend, with attacks on health systems rising by just 93%. Analysts have identified two reasons for this change. One was the case in which the Internet became more digitalized, and the second was budget woes in cybersecurity in the public-sector domain. We noted February 2025 as the record number for attacks across nearly every sector.

Table 1: Ransomware Incidents by Sector (Feb 2025)

Sector	No. of Attacks
Manufacture	159
FMCG	116
Transportation	77
Real Estate & Construction	76
IT	71

Services	67
Hospitality	60
Banking & Finance	50
Healthcare	46
Government & Law	44
Education	37
Energy	17
E-Commerce	15
Media & Internet	14
Metals & Mining	2

This rise has typically been unexpected, not so with explicit digital sectors such as real estate, hospitality, and mining, which points to the opportunistic and far-reaching nature of ransomware.

Financial Damages Estimates

The damage caused by the ransomware is staggering. Dials, ransom payments, recovery costs, and loss of reputation affect all parties in each equation. The healthcare sector and funding estimated losses in billions.

Table 2: Estimated Damage by Sector (2024–2025)

Sector	No. of Attacks	Estimated Damage (in USD)
Healthcare	145	1.5 billion
Finance	120	2.2 billion
Education	90	500 million
Government Services	75	1.1 billion

Statistics indicate that ransomware is more than a digital threat; it is a systemic risk to national security and public health. Hospitals had to defer patient transfers, financial networks slowed down to process various transactions, and educational platforms experienced prolonged outages.

Attack Vectors and Techniques

The following list of attack vectors articulates the most probable entry points for ransomware in 2025, as defined by Symantec (2024) and Miter at and CK (2023): 1. Phishing E (45% of attacks) 2. Remote-Desk Top Protocol (RDP) 3. Malvertising 4. Supply Chain Attack. Phishing remains the best vector because it affects human error. Cybercriminals have implemented AI to avoid traditional spam filters and create plausible phishing messages, even for sophisticated, technically diverse users.

Duration and Preparedness

The average downtime for companies that had been struck by ransomware in 2025 was 21 days. Moreover, 32% of the organizations involved had a ransomware-specific remediation plan. This gap represents preparation for operational paralysis, and these organizations are now susceptible to
in addition, to the ransomware attacks. Additionally, 68% of the companies had no effective backup plans. Many people have backups on the same network, and are thus equally susceptible to malware encryption or data deletion.

Sector-Specific Observations

1. Healthcare: Attackers target healthcare because the necessity of the services presents two things: urgency for recovery and a large ransom payoff. The precarious nature of patient information also makes double compression tactics more effective.
2. Finance: Financial institutions have sophisticated and multi-stage ransomware campaigns.
3. Education: Schools and universities have small goals for underfunded IT environments, particularly for supporting online learning.
4. Government Services: These attacks are exceedingly strategic, politically motivated, and can also aim to cripple bourgeois infrastructure.

Ransomware-as-a-service (RaaS) impact

Ransomware-as-a-Service Platforms (Raas) have emerged, and with platform vendors such as Revil, Darkide, and Lockbit, cybercriminal operations have become much more streamlined. Ransomware-as-a-Service Operatives include raw malware, dashboards, and a menu of software services (i.e., customer support).

1. Raas accounted for greater than 70% of ransomware campaigns in 2025.
2. RaaS operations and businesses include revenue-sharing agreements in exchange for a split in the ransom tense, as developers actually take a cut of payments.

AI-Driven and Polymorphic Malware

Ransomware used in 2025 is polymorphic, which means that the ransomware mutates to evade detection. AI is being used to:

1. People that exploit vulnerabilities in real time

2. Auto-escalate privileges
3. Change code signatures to evade antivirus detection

Cybercriminals vary AI usage in deep learning to map out the weakest systems in a network before deploying ransomware, making nefarious acts more organized and targeted.

Cloud and IoT vulnerabilities

The variety of cloud services and IoT integration offers new avenues for changing their methods.

IoT Risk: SMART-Because devices such as TVs, medical devices, wearables, and various other devices often do not align with the organization's established security policies, which are agents of access to secure networks, they just wait for attackers to exploit them.

Many organizations have no visibility in cloud/IAAS; therefore, ransomware can move laterally after it gains an access point.

Quantum Threats: Future risks

Quantum computing is not an active threat in ransomware campaigns; however, it remains a potential future risk. Quantum algorithms may eventually make all of our current encryption standards useless and allow adversaries to decrypt secure data and leverage financial or critical information.

Some Cyber security companies are working on post-quantum encryption algorithms; however, reliable post-quantum encryption is still years away from mainstream acceptance.

Summary and Insights

In 2025, ransomware does not simply encrypt data. This is a surveillance, extortion, and disruption system. Their methods included the following:

1. Double or triple extortion (Encryption/Stealing/leaking)
2. Using AI and automation capabilities to speed up the attack
3. Manipulating the supply chain, organization is being stealthy while gaining reach
4. Polymorphic malware is becoming too smart for antivirus tools.

   Organizations that do not have a mindset toward proactive defense now face being compromised, having their data taken, and experiencing reputational destruction and complete financial ruins.

Results or Findings

The assessment of incoming call reports offers some important indications that highlight the overall scale and seriousness of ransomware in 2025 and the overall scale and seriousness of cyber threats.

1. The health sector was the primary target of this study. 145 confirmed incidents and estimated damages of US$1.5 billion, being that health systems are the leading cyberattack targets. Owing to the significant and critical nature of health information and the urgency of health services, health sector entities have become the principal targets for cybercriminals eager to collect fast ransom payments.
2. Ransomware-as-a-service (RaaS) is the most successful, as it makes up over 70% of ransomware attacks, meaning that even individuals with basic technical skills can lead an attack. AI-Reinforced attacks are smarter, more difficult to identify, and avoid detection. Shaders that comprise artificial intelligence operate in real time, consider user behaviors, and ensure that doing so looks realistic. This movement indicates a meaningful shift from present malware to rapidly evolving adaptive learning threats.
3. Phishing is the primary entry point. Even though progressive malware has increased in volume, basic phishing-email is still the primary entry point of 45% of ransomware incidents. Attackers use AI to produce realistic emails and increase their overall success rates.
4. Cloud and Internet of Things platforms are problematic. Ransomware attacks are increasingly targeting IoT devices (misunderstandings and unstable APIs), specifically intelligent medical devices and industrial sensors, which are increasing the associated threat.
5. Critical Infrastructure Is Affected by Continuous Assaults: Government trading and energy and transport systems are under constant assault. These sectors are targeted
6. because attackers seek the most catastrophic failure, and by definition, they are meaningless and redundant.
7. Significant economic consequences were associated with downtime. All at an average 21-day downtime period Operational and reputational losses are far greater than serious and damaging ones. The recovery process often exceeds the ransom, particularly for SMEs and medium-sized enterprises (SMEs).
8. Typically, the backup efforts are futile. 68% of the organizations studied lacked air or constant backup, significantly hindering recovery, or in some cases, made recovery impossible. In fact, many organizations had to agree to pay ransom to recover and resume activities.
9. Unethical and legal disruptions around ransom payments: The lack of a consistent global legal framework for ransom payments made what was already difficult even more complex. Some countries remain prohibited from ransom payments, while others allow anything, but the

decision leads to ambiguity and ethical dilemmas.

10. Quantum computing is a potential threat. Although it is not currently used in ransomware attacks, it is warned that quantum computing could soon undermine encryption methods and create highly possible barriers in obtaining ransom.

Discussion

The outcomes prove that ransomware, as of 2025, is no longer a simple tor scheme but an actual cyber weapon and has the potential to create systemic disorders. The growing frequency of attacks and the diversity of hospital victims for mining companies show that the sector is unprotected. Raas has also professionalized cybercrime and created it into organized service companies.

The direct integration of AI and its development into malware have become game changers. Unlike earlier malware, current ransomware can learn, change, and rest for the best time. It is not surprising that wear attacks show qualities similar to military procedures and precision.

The organization is still behind the curve in defense. By a fair number, there is no plausible defense structure. Not training employees to detect phishing attacks or patching known vulnerabilities quickly enough. The defense gap between the pace of technological advances in both aspects of cybersecurity is a key challenge.

Another consideration is the issue of whether to pay ransom. Payments can return operations almost straight away, but could also encourage attackers or financial criminals to receive payment, and it may not even result in full recovery of data. This great divide requires unified legal breeding and an international cybercrime policy directive. It is critical to discuss national and public security.

Conclusion

Ransomware has grown from a digital nuisance to one of the most important cybersecurity issues today. In 2025, landscapes will be defined by automation, refinement, and scale. The spread of RAAS and AI reinforcement malware allows attackers to start demanding campaigns and targets both public and private organizations.

Analyses show that this technology has evolved further, but defenses have not been held, particularly in health agencies, education authorities, or small businesses. Human mistakes, a lack of planning, and outdated infrastructure continue to function as the weakest compounds in cybersecurity.

In the future, cybersecurity should not be treated as a responsibility but as an organization's priorities. From executive decision-makers to frontline employees, everyone must be trained, effective, and equipped to recognize and respond to cyber threats. It is not a battle in which you can fight just a single organization.

Recommendations

Based on the results and trends identified in this study, the following ten recommendations have been proposed to enhance cyber resistance to ransomware and emerging cyber threats, enabling employees to identify social engineering tactics that make important contributions to ransomware infections (Symantec, 2024).

- By taking over the security framework with Zero Trust, users or devices cannot be trusted within the network. This reduces the chances of internal spread in response to violations (NIST 2024).
- The backup solution should be unchangeable (not modified by malware), similar to the air from the primary system. This ensures that even after the ransomware encrypts them, important data can be restored (Kaspersky Labs, 2023).
- More stringent cybersecurity regulations require companies to report attacks. A global framework must be created for consistency and co-response (CISA 2024).
- Promotion of cooperation between technology companies, law enforcement, and state businesses can improve the detection and reduction of early threats in various areas (ENISA, 2024).
- Implement legal restrictions or insurance contracts that prevent ransom payments. This reduces the motivation of attackers and blocks the financial support for ransomware groups (Gartner, 2024).
- Promote ethical initiatives for hacking and bug bounties to identify weaknesses before malicious actors do so. Bug bounty platforms have proven successful in identifying critical system weaknesses (IBM X-Force, 2023).
- Use AI and machine learning technologies to monitor network activity, identify anomalies, and prevent attacks in real-time. This can significantly improve response times (Microsoft Security Intelligence, 2025).
- The company should perform regular patch management and quarterly penetration testing. Obsolete software is the main entry point for ransomware (Miter At and CK, 2023).
- Create a committed incident response team along with a crisis management plan. Precisely defined protocols allow for rapid action against violations, including legal, technical, and communication strategies (NIST 2024).

Acknowledgement

I would like to expand the reports and knowledge that have formed the basis for cybersecurity researchers

and organizations, as well as the paper. Their sustained commitment to the persecution, analysis, and communication of the ever-changing landscape of cyber threats was invaluable. Contributions from Symantec, Enisa, IBM X-Force, Kaspersky, CISA, and others not only enrich this research but also serve as an important resource for experts and political decision makers around the world. We also recognized the tireless efforts of cybersecurity experts on the frontline. This defends their work from threats that are often invisible to the public. Ultimately, I am grateful for the guidance and encouragement of mentors and colleagues who influenced this research, as well as the opportunity to share this knowledge with hope, awareness, dialogue, and measures regarding ransomware and emerging cyber risks.

Financial support and sponsorship
Nil.

Conflicts of interest
The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. CISA. (2024). *National Cybersecurity Strategy. Cybersecurity and Infrastructure Security Agency*. https://www.cisa.gov
2. ENISA. (2024). *Threat Landscape Report. European Union Agency for Cybersecurity.* https://www.enisa.europa.eu
3. Gartner. (2024). *Cybersecurity Trends and Predictions. Gartner Research*.
4. IBM X-Force. (2023). *Security Intelligence. IBM Corporation*. https://securityintelligence.com
5. Kaspersky Labs. (2023). *The State of Ransomware. Kaspersky Global Research*.
6. Microsoft Security Intelligence. (2025). *Trends in Ransomware. Microsoft Inc.* https://www.microsoft.com/security
7. MITRE ATT&CK Framework. (2023). *Tactics and Techniques*. https://attack.mitre.org/
8. NIST. (2024). *Cybersecurity Framework. National Institute of Standards and Technology.* https://www.nist.gov/cyberframework
9. Symantec. (2024). *Annual Cybersecurity Threat Report. NortonLifeLock Inc.*
10. CYFIRMA. (2025). *Tracking Ransomware – February 2025.* https://www.cyfirma.com/research/tracking-ransomware-february-2025/