Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The Evolution of Ransomware: A Technical Analysis of Attack Vectors and Propagation Mechanisms (2015-2025)

Vipul Gupta
Jain Deemed To Be Universiry
Bangalore, India

Vishwas Gowda R
Jain Deemed To Be Universiry
Bangalore, India

Thatte Pavan Kumar
Jain Deemed To Be Universiry
Bangalore, India

Abstract—Over the past decade, ransomware has grown into one of the most serious threats in the field of cybersecurity. This paper provides a technical analysis of how ransomware has evolved between 2015 and 2025. By reviewing information from research papers, security reports, and threat intelligence sources, the study traces the shift from simple, automated attacks to more advanced, targeted operations often known as "Big Game Hunting."

The findings show a clear change in how attacks are carried out. Earlier ransomware mainly relied on mass phishing and self-spreading techniques, whereas modern attacks focus on exploiting weak points such as Remote Desktop Protocol (RDP), Virtual Private Networks (VPNs), and newly discovered software vulnerabilities. The study also highlights how attackers have moved from automated spreading methods to controlled, manual approaches that allow deeper access into systems.

In addition, the paper examines how encryption and evasion techniques have improved over time. Modern ransomware often uses partial or intermittent encryption to avoid detection. At the same time, extortion methods have become more aggressive, evolving from simple file encryption to double and even triple extortion strategies involving data theft and external pressure.

Overall, the study suggests that traditional security methods are no longer sufficient. Organizations need to adopt more advanced approaches such as Zero Trust models and behavior-based detection to effectively defend against modern ransomware attacks.

I. INTRODUCTION

Over the past decade, ransomware has grown into one of the most serious challenges in cybersecurity, impacting individuals, businesses, and even critical national infrastructure. What initially began as simple malware that locked user files in exchange for small payments has now developed into well-organized and profit-driven cybercrime operations. Recent studies and industry reports [1]–[3] show a clear increase not only in the number of ransomware attacks but also in their level of sophistication.

In the early years, ransomware attacks mainly depended on basic encryption techniques and were widely distributed through phishing emails. However, as research indicates [2], attackers gradually started using stronger encryption algorithms such as AES and RSA, making it extremely difficult to recover encrypted data without paying a ransom. At the same time, the approach of attackers has changed significantly—from targeting random users to focusing on specific high-value organizations, a strategy commonly known as "Big Game Hunting."

Today's ransomware attacks exploit multiple entry points, including weak credentials in Remote Desktop Protocol (RDP), vulnerabilities in Virtual Private Network (VPN) systems, and unpatched software flaws [4], [6]. Attackers also use advanced techniques such as lateral movement, privilege escalation, and legitimate administrative tools to move within networks without being easily detected [10]. Reports from cybersecurity organizations [7], [11] suggest that ransomware operations have become more structured, often following a Ransomware-as-a-Service (RaaS) model, which allows attackers with limited technical skills to participate in complex attacks.

Another important shift can be seen in extortion methods. Earlier ransomware attacks focused only on encrypting files, but modern variants now include double and triple extortion strategies. In these cases, attackers not only encrypt data but also steal sensitive information and threaten to release it publicly if their demands are not met [5], [6]. In addition, new evasion techniques such as intermittent encryption have been introduced to avoid detection by traditional security tools [12].

Major incidents like WannaCry demonstrated how quickly ransomware can spread across systems using automated techniques [9], [13]. In contrast, more recent ransomware families such as Ryuk and LockBit rely on targeted attacks and careful planning to maximize impact [10], [11]. These developments highlight that ransomware is no longer just a technical problem but also a serious economic and organizational threat.

Considering these changes, it is important to study how ransomware has evolved in terms of attack methods, propagation techniques, and defense mechanisms. This paper presents a technical analysis of ransomware evolution from 2015 to 2025, with a focus on key trends in attack strategies,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

encryption methods, and extortion models. The goal is to provide insights that can help organizations strengthen their defenses against modern ransomware threats.

II. LITERATURE REVIEW

Over the past decade, ransomware has rapidly evolved, becoming one of the most serious threats in cybersecurity. This growth has led to extensive research focusing on how ransomware operates, how it spreads, and how it can be detected and prevented. Researchers and industry experts have studied both its technical development and the changing strategies used to defend against it.

The study "The Evolution and Mitigation of Ransomware" [1] gives a clear overview of how ransomware has changed over time. It explains how early attacks, which mainly relied on simple encryption, have now become more advanced and involve multiple stages of intrusion. The authors also highlight the importance of taking preventive measures such as regular software updates, network segmentation, and improving user awareness.

In another study, "Crypto-Ransomware: A Revision of the State of the Art, Advances and Challenges" [2], the focus is on the cryptographic side of ransomware. It explains how attackers use strong encryption methods like AES and RSA, which make it extremely difficult to recover data without paying the ransom. The study also points out that newer hybrid encryption techniques make detection even more challenging.

The paper "Earlier Decision on Detection of Ransomware Identification" [3] looks at different detection methods, especially those based on machine learning and behavioral analysis. It concludes that detecting ransomware at an early stage is still very difficult because modern ransomware is designed to remain hidden and avoid traditional detection systems.

Real-world reports provide additional insights into how ransomware operates in practice. For example, the HHS report on REvil ransomware [4] shows how attackers target important sectors like healthcare by exploiting weaknesses in remote access systems. Similarly, the Maze ransomware report [5] introduces the concept of double extortion, where attackers not only encrypt data but also threaten to release it publicly if the ransom is not paid.

The Cl0p ransomware attack using the MOVEit vulnerability [6] highlights a newer trend where attackers exploit zero-day vulnerabilities and supply chain weaknesses. This shows a shift from random attacks to more targeted and large-scale operations. The CISA report on ALPHV/BlackCat [7] further shows how modern ransomware uses advanced programming languages like Rust and can run across multiple platforms.

Threat intelligence reports, such as those from Palo Alto Networks Unit 42 [8], give a broader view of ransomware trends. They discuss the rise of Ransomware-as-a-Service (RaaS), which allows even less-skilled attackers to launch ransomware attacks, making the threat more widespread.

Detailed technical studies of specific ransomware families also help in understanding their behavior. Research on WannaCry [9], [13] explains how it spread rapidly using the EternalBlue exploit, infecting systems without user interaction. Similarly, studies on TrickBot and Ryuk [10] show how attackers now focus on targeted attacks, using techniques like lateral movement and privilege escalation to maximize damage.

The CISA report on LockBit [11] highlights how modern ransomware groups have become highly organized and efficient, using faster encryption methods and automated tools for data theft. In addition, research on ransomware detection [12] explores advanced techniques like adaptive file system analysis to detect newer evasion methods such as intermittent encryption.

Overall, existing literature clearly shows that ransomware has evolved from simple attacks into highly organized and complex operations. Although detection and prevention techniques have improved, the increasing sophistication of ransomware continues to create major challenges for cybersecurity professionals.

III. METHODOLOGY

This research adopts a systematic literature review approach to analyze and synthesize technical knowledge related to the evolution of ransomware. The objective of this methodology is to collect, evaluate, and organize information from multiple credible sources in order to understand how ransomware techniques, strategies, and impacts have changed over time.

• Sources: The study is based on a wide range of reliable sources, including technical reports published by cybersecurity organizations such as CISA, HHS, Mandiant, and Palo Alto Networks Unit 42. In addition, academic journals such as IEEE Access and ACM Computing Surveys were used to gain theoretical insights. Industry whitepapers and forensic analyses from cybersecurity vendors like Trend Micro, Fortinet, and SentinelOne were also included to provide real-world perspectives on ransomware behavior and attack patterns.

• Timeframe: The analysis focuses on the period from 2015 to 2025. This timeframe was selected because it captures the major transformation in ransomware—from early-stage attacks before the WannaCry outbreak to modern, highly advanced campaigns involving artificial intelligence techniques and zero-day vulnerabilities.

• Selection Criteria: Only relevant literature was selected for this study based on specific technical parameters. Priority was given to sources that discuss Tactics, Techniques, and Procedures (TTPs), cryptographic mechanisms used in ransomware, and detailed forensic investigations of major ransomware families. General or non-technical discussions were excluded to maintain the depth and quality of analysis.

• Analysis Framework: To ensure a structured approach, the collected data was categorized into four key dimensions: Attack

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Vectors, Propagation Mechanisms, Encryption Techniques, and Extortion Models. Each category was analyzed separately to identify trends, similarities, and changes over time. The combined findings from these categories provide a comprehensive understanding of the evolution of ransomware.

This methodology enables a clear and organized examination of ransomware development, supported by both academic research and practical industry insights.

TIMELINE OF MAJOR RANSOMWARE FAMILIES

The following timeline illustrates the distinct eras of ransomware evolution, marking key technical innovations.

TABLE 1
EVOLUTION OF RANSOMWARE ERAS

Era	Notable Families	Year	Key Innovations & Technical Characteristics
Early Era	CryptoLocker, TeslaCrypt	2013–2015	Introduction of asymmetric encryption for files; use of Bitcoin payment infrastructure
Worm Era	WannaCry, NotPetya	2017	Automated propagation using SMB exploits (EternalBlue) for lateral movement without human interaction
Targeted Era	Ryuk, SamSam, GandCrab	2018–2019	Manual hacking ("Big Game Hunting"); enterprise targeting via RDP/Phishing; post-exploitation deployment
RaaS Era	REvil, LockBit 2.0, Maze	2020–2021	Double extortion; data exfiltration before encryption; industrialized affiliate models
Hybrid Era	BlackCat (ALPHV), Cl0p, Royal	2022–2025	Intermittent encryption; cross-platform languages (Rust/Go); supply chain zero-day exploits (MOVEit)

IV. T CHNICAL EVOLUTION ANALYSIS

A. Attack Vectors Evolution

A. Between 2015 and 2017, ransomware attacks mainly relied on large-scale phishing campaigns. Attackers would send emails with malicious attachments such as Word macros or JavaScript files, or use exploit kits like Angler and Rig to take advantage of browser vulnerabilities [8].

B. From 2018 to 2020, the approach became more targeted. Instead of attacking randomly, hackers focused on gaining access to systems through weak credentials. Remote Desktop Protocol (RDP) became one of the most commonly used entry points. At the same time, cybercriminals began selling access to compromised systems on dark web forums. Vulnerabilities in VPN services like Pulse Secure, Fortinet, and Citrix were also heavily exploited during this period, especially by groups such as REvil [4].

C. From 2021 onwards, ransomware attacks have become even more advanced, focusing on exploiting zero-day vulnerabilities in widely used software. A key example is the Cl0p group exploiting a vulnerability in MOVEit Transfer (CVE-2023-34362), which allowed them to compromise hundreds of organizations through a single weakness [6].

B. P pagation Mechanisms

A. A major turning point came in 2017 with WannaCry, which introduced self-spreading (worm-like) ransomware. It used the EternalBlue exploit to scan networks for vulnerable systems and spread automatically without any user action [1].

B. In contrast, modern ransomware attacks are more controlled and strategic. Groups like Ryuk and BlackMatter no longer rely on automatic spreading. Instead, they move through networks manually using legitimate tools such as PsExec, Windows Management Instrumentation (WMI), and Cobalt Strike. Attackers often steal credentials directly from system memory using tools like Mimikatz, gain administrator-level access, and then spread the ransomware across the network using centralized management tools like Group Policy Objects (GPO) [10].

C. Encryption Techniques and Evasion

1) I ermittent Encryption

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

D. To avoid detection, modern ransomware does not always encrypt entire files. Instead, it uses a technique called intermittent encryption, where only parts of a file are encrypted. This makes the attack faster and harder to detect by security systems that look for fully encrypted files [17].

E. Different methods are used in this approach:

- Encrypting only the beginning portion of a file
- Encrypting small chunks at regular intervals
- Encrypting a certain percentage of the file
- Automatically adjusting the method based on file size

2) Cross-Platform Languages (Rust and Go)

A. Ransomware developers are now using modern programming languages like Rust and Go, which make their malware more flexible and harder to analyze.

B. For example, BlackCat (ALPHV) uses Rust, allowing it to run on multiple platforms such as Windows, Linux, and VMware ESXi. This is especially useful in enterprise environments where virtual machines are widely used, as attackers can directly encrypt virtual disk files.

C. Similarly, ransomware written in Go, such as Hive, is harder to reverse engineer and can run on different operating systems without much modification [18].

D. Extortion Models

A. Ransomware attacks have also evolved in how they demand payment. Earlier attacks (2015–2018) used a simple method: encrypt the victim's files and demand money to unlock them.

B. Later, attackers introduced double extortion, where they not only encrypt files but also steal sensitive data. If the victim refuses to pay, the data is leaked publicly [5].

C. More recently, triple extortion has emerged. In this case, attackers go a step further by targeting the victim's customers or partners, sometimes using DDoS attacks or direct threats to increase pressure.

D. Some groups, like Cl0p, have even stopped encrypting files altogether. Instead, they rely only on stealing data and threatening to expose it. This helps them avoid detection by traditional anti-ransomware tools.

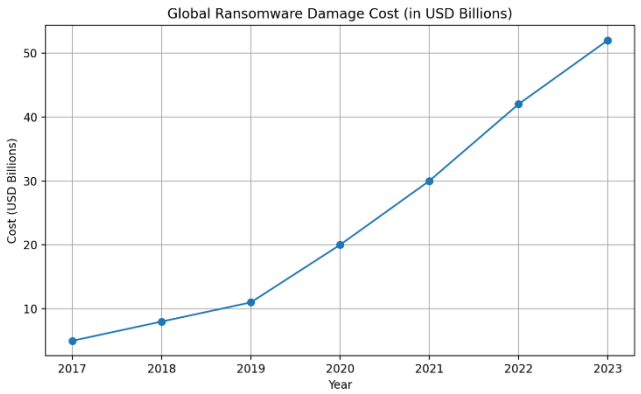
Defence Evolution Analysis

Defensive strategies have been forced to evolve in lockstep with attacker TTPs, moving from signature based models to holistic architectures.

TABLE 2
Mapping of attacker TTPs to defensive evolution strategies

Attacker TTP	Defensive Evolution
Mass Phishing / Attachments	**Email Filtering and Sandboxing:** Transition from signature-based detection to advanced techniques such as executing suspicious attachments in cloud-based sandboxes to identify malicious behavior.
Worm Propagation (SMB)	**Vulnerability Management:** Implementation of strict patching policies (e.g., MS17-010) and disabling outdated protocols like SMBv1 to prevent exploitation.
Credential Abuse (RDP)	**MFA and Access Control:** Enforcing Multi-Factor Authentication (MFA) for remote access and restricting RDP behind secure VPNs or access gateways.
Lateral Movement	**Zero Trust Architecture (ZTA):** Adopting a "never trust, always verify" approach with continuous authentication and micro-segmentation, assuming the network may already be compromised.
Intermittent Encryption	**Behavioral Heuristics:** Use of Endpoint Detection and Response (EDR) systems that monitor suspicious API call patterns (e.g., vssadmin delete shadows) instead of relying solely on file entropy detection [3].
Shadow Copy Deletion	**Immutable Backups:** Use of Write Once, Read Many (WORM) storage and offline or air-gapped backups that remain secure even if administrative credentials are compromised.

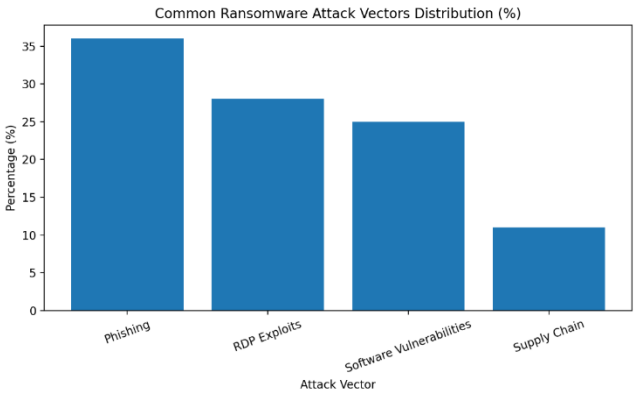
V. CASE STUDIES



As shown in Fig. 1, the global cost of ransomware has increased

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

significantly from 2017 to 2023, reflecting the growing sophistication and impact of modern ransomware attacks.



As illustrated in Fig. 2, phishing remains the most common attack vector, followed by RDP-based attacks and software vulnerabilities, highlighting the continued reliance on both human and technical weaknesses.

A. WannaCry (2017): The Worm

WannaCry is widely considered one of the most impactful ransomware incidents, mainly because of how quickly it spread across the world. By taking advantage of the EternalBlue vulnerability (MS17-010), it was able to infect more than 200,000 systems in over 150 countries within a very short time frame [9].

A notable technical feature of WannaCry was its built-in "kill switch" mechanism. The malware attempted to connect to a specific domain, and if the connection was successful, it would stop executing. This behavior was likely intended to detect sandbox environments. However, it unintentionally helped security researchers contain the attack by registering the domain, which effectively slowed and eventually halted its spread [1].

B. Ryuk (2018–2020): Targeted "Big Game Hunting"

Ryuk represents a clear shift from large-scale automated attacks to more focused and strategic targeting. Often described as "big game hunting," this approach involves going after high-value organizations rather than random victims. Ryuk was usually deployed after initial access was gained through malware like TrickBot or Emotet, followed by careful observation of the victim's network [10].

From a technical standpoint, Ryuk operators used techniques such as Wake-on-LAN to activate systems that were turned off, ensuring maximum impact during encryption. They also removed backup options by deleting Windows shadow copies using commands like vssadmin delete shadows. This made recovery much more difficult and increased the pressure on victims to pay the ransom [10].

C. LockBit 3.0 (2022–2023): The RaaS Standard

LockBit 3.0, also referred to as LockBit Black, reflects how ransomware has evolved into a well-organized service-based model. It operates under the Ransomware-as-a-Service (RaaS) concept, where developers provide the tools and affiliates carry out the attacks, making it highly scalable and widespread [11].

Technically, LockBit includes several advanced features. It introduced a bug bounty program to improve its own system, showing how professionalized these operations have become. The ransomware also uses password-protected execution, requiring a specific key to run, which makes automated analysis more difficult. In addition, it uses a tool called "StealBit" to quickly extract sensitive data before encrypting files [12].

D. Cl0p (2023): The Zero-Day Exploiter

Cl0p demonstrates a modern trend where attackers focus on exploiting newly discovered vulnerabilities rather than relying on traditional methods. It specifically targeted enterprise file transfer solutions such as MOVEit and GoAnywhere. In the MOVEit incident, Cl0p exploited a SQL injection vulnerability (CVE-2023-34362) to gain unauthorized access to sensitive information across multiple organizations [6].

In terms of technique, the attackers installed a web shell (human2.aspx), which allowed them to maintain access and directly extract data from databases and file systems. Interestingly, in many cases, Cl0p did not encrypt the victim's files at all. Instead, it relied entirely on stolen data as leverage, highlighting a shift toward data-focused extortion methods [6].

E. BlackCat (ALPHV) (2021–2024): The Cross-Platform Innovator

BlackCat, also known as ALPHV, is notable for being one of the first major ransomware families written in Rust. This marks a move toward using modern programming languages that offer better performance and flexibility [7].

Because of Rust, BlackCat can run on multiple platforms, including Windows and Linux, making it highly adaptable in different environments. It also provides flexible configuration options, allowing attackers to choose how encryption is carried out, whether fully or partially, depending on their needs [7].

In addition to its technical capabilities, BlackCat has pushed extortion strategies further. In one instance, the group filed a complaint with the U.S. Securities and Exchange Commission (SEC) against a victim organization for not disclosing a breach. This shows how attackers are increasingly using legal and regulatory pressure as part of their overall strategy [7].

CONCLUSION

Over the years, ransomware has changed a lot in the way it works and spreads. Earlier, attackers used simple methods like sending bulk phishing emails and targeting random users. But now, the attacks have become more planned and focused, targeting specific organizations using advanced techniques like zero-day vulnerabilities and supply chain attacks.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

At the same time, attackers are also improving their tools. They are using faster and smarter encryption methods, and even creating ransomware that can work on multiple platforms like Windows and Linux. In some cases, they don't even encrypt files anymore—they just steal data and use it to threaten the victim.

Because of this, traditional security methods are no longer enough. Companies cannot depend only on firewalls or basic protection. Instead, they need stronger security practices like Zero Trust, where every user and system is continuously verified. They should also use secure backup systems, strong authentication, and tools that can detect unusual behavior early.

In the end, ransomware is constantly evolving, and so should our defences. Organizations must stay updated, proactive, and prepared to handle these modern threats effectively.

REFERENCES

[1] "The evolution and mitigation of ransomware," *Granthaalayah*. [Online]. Available: https://www.granthaalayahpublication.org/journals/granthaalayah/article/download/6361/6310/35967 (accessed Feb. 5, 2026).

[2] "Crypto-ransomware: A revision of the state of the art, advances and challenges," *MDPI Electronics*. [Online]. Available: https://www.mdpi.com/2079-9292/12/21/4494 (accessed Feb. 5, 2026).

[3] Earlier decision on detection of ransomware identification: A comprehensive systematic literature review," *MDPI Information*. [Online]. Available: https://www.mdpi.com/2078-2489/15/8/4844 (accessed Feb. 5, 2026).

[4] "REvil/Sodinokibi ransomware vs. the health sector," *HHS.gov*. [Online]. Available: https://www.hhs.gov/sites/default/files/revil-update-tlpwhite.pdf (accessed Feb. 5, 2026).

[5] Maze ransomware," *HHS.gov*. [Online]. Available: https://www.hhs.gov/sites/default/files/maze-ransomware.pdf (accessed Feb. 5, 2026).

[6] "Clop ransomware likely sitting on MOVEit transfer vulnerability (CVE-2023-34362)," *Kroll*. [Online]. Available: https://www.kroll.com/en/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362 (accessed Feb. 5, 2026).

[7] "#StopRansomware: ALPHV BlackCat," *CISA*. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a (accessed Feb. 5, 2026).

[8] "Ransomware threat assessments," *Palo Alto Networks Unit 42*. [Online]. Available: https://unit42.paloaltonetworks.com/ransomware-threat-assessments/7/ (accessed Feb. 5, 2026).

[9] Static and dynamic analysis of WannaCry ransomware," *IEICE*. [Online]. Available: https://www.ieice.org/publications/proceedings/bin/pdf_link.php (accessed Feb. 5, 2026).

[10] "TrickBot, Ryuk, and the HPH sector," *HHS.gov*. [Online]. Available: https://www.hhs.gov/sites/default/files/trickbot-ryuk-and-the-hph-sector.pdf (accessed Feb. 5, 2026).

[11] "Understanding ransomware threat actors: LockBit," *CISA*. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a (accessed Feb. 5, 2026).

[12] "Ransomware encryption detection: Adaptive file system analysis against evasive encryption tactics," *CSU Research Output*. [Online]. Available: https://researchoutput.csu.edu.au/en/publications/ransomware-encryption-detection-adaptive-file-system-analysis-aga/ (accessed Feb. 5, 2026).

[13] "WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms," *ResearchGate*. [Online]. Available: https://www.researchgate.net/publication/332088162 (accessed Feb. 5, 2026).