International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 10 | Oct - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Ransomware Evolution and Defence Strategies

Nikita Srinivas Kasabed

Post Graduate Student

Computer Science Department

Dr. D. Y. Patil Arts, Commerce, and Science, Pimpri. City – Pune, Country – India

Abstract

Ransomware has become one of the most severe cybersecurity challenges of the 21st century, affecting organizations across industries, from healthcare to energy infrastructure. Initially dismissed as a nuisance in the late 1980s and early 2000s, ransomware has evolved into a mature cybercriminal enterprise, generating billions of dollars in illicit revenue. Its sophistication is reflected in the adoption of strong cryptographic techniques, the emergence of ransomware-as-a-service (RaaS), and the adoption of double and triple extortion tactics.

The problem is exacerbated by the increasing use of encrypted internet traffic, which limits visibility for traditional security tools. Encryption, while essential for protecting privacy, has created blind spots that ransomware actors exploit to deliver payloads, communicate with command-and-control (C2) servers, and exfiltrate sensitive data. As recent research indicates, more than 85% of cyberattacks are now conducted over encrypted channels, complicating detection and defense.

This paper traces the historical evolution of ransomware, analyzes its attack lifecycle, and highlights the technical, legal, and organizational challenges in defending against it. It also explores defense strategies, including preventive measures, advanced detection approaches such as Encrypted Traffic Analytics (ETA), and emerging solutions like AI-driven detection and federated learning. The paper concludes by stressing the need for a layered, adaptive defense model that balances visibility, privacy, and performance in an encrypted-first digital ecosystem.

1. Introduction

The digital age has introduced unprecedented opportunities for communication, commerce, and innovation. However, it has also created fertile ground for cybercrime. Among the most prominent and disruptive forms of cybercrime is **ransomware**, a malicious software that encrypts data or locks access to systems until victims pay a ransom.

The impact of ransomware is far-reaching:

- **Financial Losses:** According to IBM's 2024 *Cost of a Data Breach Report*, ransomware incidents cost organizations an average of USD 5.13 million per breach, excluding ransom payments.
- **Operational Disruption:** The 2021 Colonial Pipeline attack disrupted fuel distribution across the eastern United States.
- **Reputational Damage:** Companies suffer not only monetary losses but also long-term erosion of customer trust.

Meanwhile, a fundamental shift in internet communication — the rise of encryption protocols such as TLS 1.3 and QUIC — has made it increasingly difficult for defenders to detect malicious traffic. As the uploaded reference paper points out, encryption has created a "perfect hiding place" for attackers.

This paradox — the same encryption that protects legitimate users also conceals cybercriminal activity — underscores the complexity of ransomware defense in today's world.

2. Evolution of Ransomware

Ransomware's development can be understood through distinct stages:

2.1 Early Ransomware (1989–2005)

- The **AIDS Trojan** (1989) is considered the first ransomware. Distributed on floppy disks, it demanded $189 via postal mail.
- These early attempts were technically unsophisticated and could be bypassed with basic recovery tools.

2.2 Crypto-Ransomware (2005–2013)

- Attackers began incorporating **RSA and AES encryption**, ensuring that only they held the decryption keys.
- Variants like CryptoLocker (2013) marked the turning point, combining strong encryption with Bitcoin payments for anonymity.

2.3 Ransomware-as-a-Service (2016–Present)

- Groups began renting ransomware kits on underground forums.
- Platforms like **Cerber and GandCrab** allowed affiliates to deploy ransomware in exchange for a share of profits.
- This democratized ransomware, enabling even low-skilled actors to conduct devastating attacks.

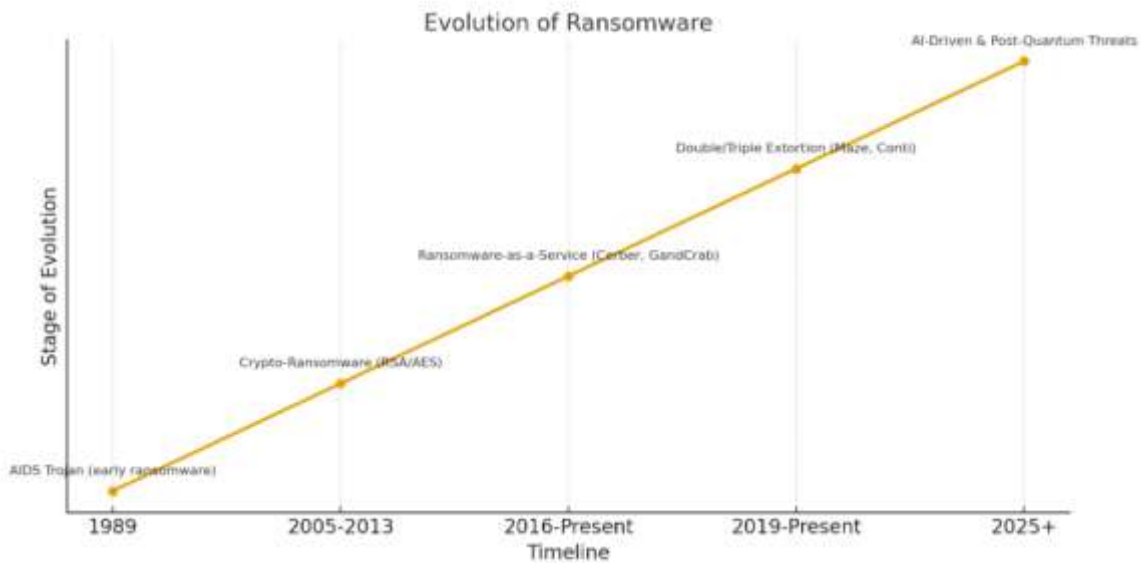
2.4 Double and Triple Extortion (2019–Present)

- Groups such as **Maze and REvil** pioneered *double extortion*, threatening to leak stolen data if victims refused to pay.
- **Triple extortion** added pressure tactics such as DDoS attacks or contacting customers of the victimized organization.

2.5 AI and Automation (Emerging, 2025)

- Reports suggest adversaries are now experimenting with **AI-driven phishing** and **automated vulnerability scanning** to improve success rates.
- Future ransomware may incorporate **post-quantum cryptography**, posing new challenges.

Figure 1: Evolution of Ransomware Timeline



3. Ransomware Attack Lifecycle

A typical ransomware attack follows these steps:

1. **Initial Access:** Phishing emails, malicious attachments, or exploiting unpatched vulnerabilities (e.g., EternalBlue in WannaCry).

2. **Execution and Payload Delivery:** Malware is downloaded, often hidden within encrypted HTTPS traffic, bypassing signature-based IDS.

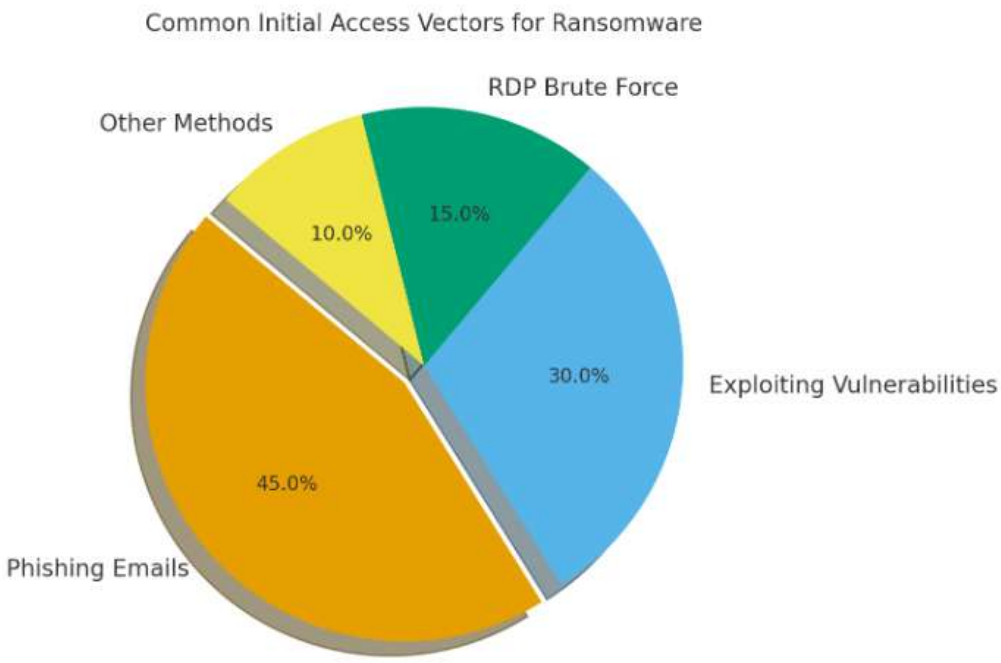
3. **Lateral Movement:** Attackers use tools such as Mimikatz or RDP brute force.

4. **Privilege Escalation:** Admin credentials are stolen.

5. **Data Encryption and Exfiltration:** Files are encrypted with strong algorithms, and data is exfiltrated over encrypted channels.

6. **Ransom Demand and Monetization:** Victims are presented with ransom notes demanding cryptocurrency payments.

Figure 2: Common Initial Access Vectors for Ransomware



4. Challenges in Detection and Defense

4.1 Encrypted Traffic as a Blind Spot

The rise of TLS 1.3 and QUIC has made over 75% of internet traffic encrypted. While this protects user privacy, it blinds traditional IDS and firewalls that rely on Deep Packet Inspection (DPI). As highlighted in the reference study, signature-based detection is now largely ineffective since encrypted packets cannot be inspected for known malware signatures.

4.2 Signature vs. Anomaly Detection

- **Signature-based IDS:** Accurate for known attacks, but fails against novel ransomware variants hidden in encrypted traffic.
- **Anomaly-based IDS:** Can detect unusual behavior but often generate false positives.

4.3 Legal and Ethical Challenges

Decrypting traffic for inspection may violate privacy laws like GDPR and HIPAA. Attackers exploit this by using trusted cloud services (Google Drive, Dropbox) that organizations exempt from decryption.

Table 1: Comparison of Detection Strategies

Detection Method	Strengths	Weaknesses
Signature-Based IDS	Accurate for known threats; low false positives	Ineffective against novel/encrypted threats; cannot see hidden payloads
Anomaly-Based IDS	Detects zero-day and unknown threats	High false positive rate; resource-intensive to tune and maintain
TLS Inspection	Provides full visibility into traffic; strong detection	Performance overhead; legal/privacy concerns (GDPR/HIPAA); costly infrastructure
Encrypted Traffic Analytics	Preserves privacy; scalable with AI/ML; detects without decryption	Relies on metadata patterns; less precise than decryption; evolving attacker evasion

5. Défense Strategies

5.1 Preventive Measures

- **Zero Trust Architecture (ZTA):** Implements the principle of "never trust, always verify."
- **Multi-Factor Authentication (MFA):** Essential for reducing credential theft risks.
- **Patch Management:** Timely updates prevent exploitation of known vulnerabilities.

5.2 Detection Approaches

- **TLS Inspection:** Offers deep visibility but impacts performance and privacy.
- **Encrypted Traffic Analytics (ETA):** Uses packet metadata and TLS fingerprints (JA3) to detect anomalies without full decryption.

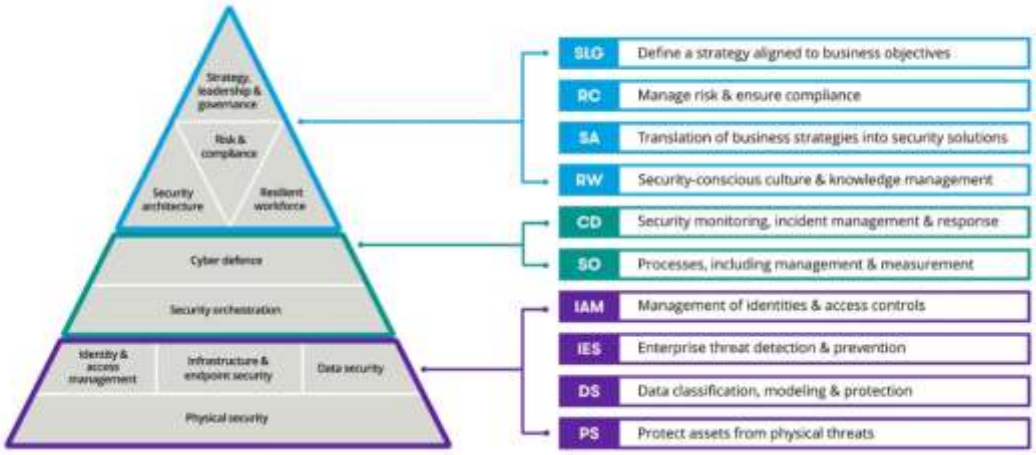
5.3 Response and Recovery

- **Immutable Backups:** Critical for recovery without paying ransom.
- **Incident Response Playbooks:** Enable rapid isolation and recovery.
- **Threat Hunting:** Identifies early signs of compromise.

5.4 Emerging Solutions

- **AI-Driven Detection:** Machine learning trained on encrypted traffic metadata has shown >95% detection accuracy.

- **Federated Learning:** Allows organizations to collaborate on training models without sharing sensitive data.



6. Case Studies

6.1 WannaCry (2017)

- **Background:** WannaCry was one of the first ransomware campaigns to achieve global notoriety. It spread in May 2017, affecting more than **200,000 computers across 150 countries** within days.
- **Attack Method:** Exploited the **EternalBlue vulnerability (MS17-010)** in Microsoft Windows, a flaw originally developed as a cyberweapon by the NSA and later leaked by the hacking group Shadow Brokers.
- **Impact:**
  - Crippled healthcare systems in the UK's National Health Service (NHS), causing canceled surgeries and delayed treatments.
  - Disrupted transportation, telecom, and manufacturing worldwide.
  - Estimated financial damage exceeded **$4 billion globally**.
- **Key Lessons:**
  - Highlighted the importance of **timely patch management**.
  - Demonstrated how ransomware can evolve from a criminal tool to a **nation-state-level cyber threat**.

6.2 Ryuk and Conti (2018–2021)

- **Background:** Ryuk and Conti were linked to the Russian-speaking cybercrime group "Wizard Spider." They targeted **large enterprises, hospitals, and government organizations**.
- **Attack Method:**
  - Initial access typically gained through **phishing emails or TrickBot/Emotet malware infections**.
  - Once inside, attackers performed **manual lateral movement**, disabling antivirus tools and stealing admin credentials.
- **Impact:**
  - Ryuk was behind dozens of attacks on **U.S. hospitals during the COVID-19 pandemic**, forcing emergency procedures to revert to paper-based processes.

- Ransoms often ranged from **$100,000 to $10 million**, paid in Bitcoin.
- Conti introduced **double extortion**, threatening to leak stolen sensitive data if ransom was not paid.

- **Key Lessons:**
- Healthcare and critical services are prime ransomware targets due to their reliance on uptime.
- The **double extortion model** reshaped the ransomware landscape, making backups alone insufficient for defense.

6.3 Colonial Pipeline Attack (2021)

- **Background:** The Colonial Pipeline ransomware attack in May 2021 was carried out by the **DarkSide group**, crippling one of the largest U.S. fuel pipelines.

- **Attack Method:**
- Initial access gained through a compromised VPN account.
- Attackers encrypted systems controlling pipeline operations and exfiltrated sensitive data.

- **Impact:**
- Forced a **five-day shutdown** of pipeline operations, leading to **fuel shortages across the U.S. East Coast**.
- Colonial Pipeline paid a ransom of **$4.4 million in Bitcoin** (later partially recovered by the U.S. DOJ).
- Sparked **government-level discussions** on ransomware as a national security issue.

- **Key Lessons:**
- Showed that ransomware is not just an IT issue but a **critical infrastructure threat**.
- Led to U.S. government executive orders mandating **Zero Trust adoption** and improved cyber hygiene across critical sectors.

6.4 LockBit 3.0 (2022–2025)

- **Background:** LockBit is one of the most active RaaS (Ransomware-as-a-Service) operations globally. Its **3.0 version**, also known as “LockBit Black,” emerged in 2022.

- **Attack Method:**
- Affiliates purchase or rent the ransomware kit and deploy it against victims.
- LockBit introduced **customizable ransom notes** and **data leak sites** on the dark web.

- **Impact:**
- By 2025, LockBit has been responsible for thousands of attacks worldwide, targeting both small businesses and multinational corporations.
- Innovated by offering a **“bug bounty program” for criminals**, incentivizing affiliates to improve the malware.

- **Key Lessons:**
- LockBit demonstrates the professionalization of ransomware groups, operating much like legitimate tech companies.
- Highlights the difficulty of combating RaaS, as hundreds of independent affiliates distribute the malware.

7. Future Directions

The fight against ransomware is not static; it evolves in tandem with technological advances, regulatory frameworks, and attacker innovation. Several emerging trends will define the future of ransomware threats and the defences required to combat them:

7.1 Quantum Threats

- **Impact on Cryptography:** Current ransomware relies on algorithms like **AES (symmetric)** and **RSA/ECC (asymmetric)**. While these are secure against classical computers, advances in **quantum computing** could render them vulnerable. Algorithms such as **Shor's algorithm** can theoretically break RSA/ECC within feasible time once large-scale quantum computers emerge.
- **Post-Quantum Cryptography (PQC):** Governments and research institutions are racing to standardize **quantum-resistant algorithms**. NIST is leading efforts to adopt lattice-based cryptography, which is resistant to quantum attacks.
- **Ransomware Implications:** Attackers may use quantum capabilities to develop **unbreakable ransomware encryption** or to crack corporate defenses reliant on outdated cryptography. Organizations will need to adopt PQC to remain resilient in a post-quantum world.

7.2 AI-Powered Ransomware

- **Adaptive Malware:** Machine Learning (ML) and Artificial Intelligence (AI) are being weaponized by attackers. Future ransomware could automatically adapt its **attack path** by analysing network defences in real time.
- **Deepfake-Driven Phishing:** AI tools can generate convincing **phishing emails, voice messages, and even video deepfakes**, dramatically increasing infection success rates.
- **Defender's AI vs. Attacker's AI:** This creates an **AI arms race**, where defenders deploy AI-driven anomaly detection (e.g., Encrypted Traffic Analytics) while attackers counter with AI capable of mimicking normal network traffic to evade detection.
- **Potential Scenario:** Imagine ransomware that can **dynamically choose** between encryption, exfiltration, or DDoS depending on the victim's defense posture.

7.3 Global Cooperation

- **Ransomware-as-a-Service (RaaS) Ecosystems:** Groups like **LockBit and Conti** function as decentralized criminal enterprises, making them hard to dismantle. Affiliates operate globally, often outside the jurisdiction of victimized nations.
- **Law Enforcement Challenges:** Cross-border legal hurdles, lack of extradition treaties, and political complexities often shield ransomware groups. For example, many operate from regions where prosecution is unlikely.
- **Examples of Progress:**
  - The **REvil takedown (2021)** demonstrated successful international cooperation when law enforcement across multiple countries arrested affiliates.
  - The **No More Ransom initiative**, launched in 2016, has provided free decryption tools to thousands of victims.
- **Future Needs:** Stronger **international frameworks, intelligence sharing, and cyber diplomacy** are required to dismantle RaaS supply chains.

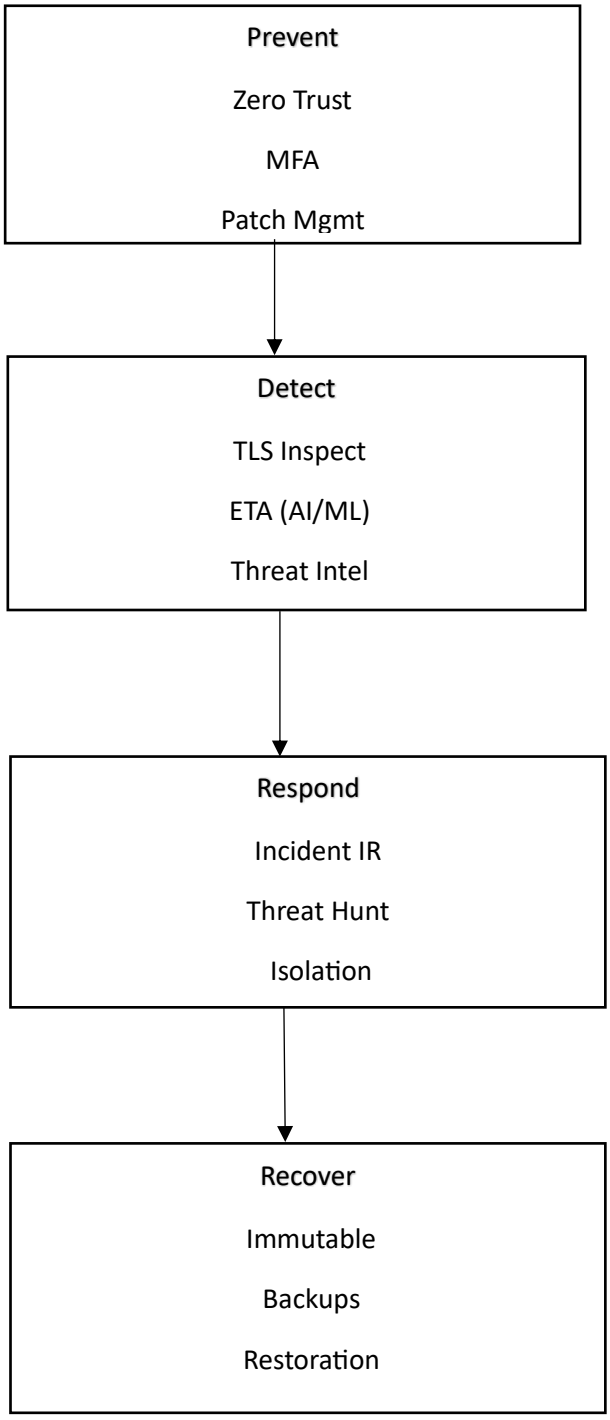
7.4 Policy and Regulation

- Governments are increasingly considering policies that:
  - Prohibit or restrict ransom payments.

- Mandate **Zero Trust adoption** in critical infrastructure.
- Require **cyber incident reporting** within strict timeframes.

- The policy direction of 2025 and beyond will influence whether ransomware remains a profitable enterprise or becomes too risky for attackers.

Figure: Layered Ransomware Defense Model



8. Conclusion

Ransomware has undergone a dramatic transformation over the past three decades — from simple **screen lockers** demanding modest payments to highly organized criminal enterprises leveraging **state-of-the-art cryptography, double/triple extortion, and RaaS business models**. This evolution highlights a fundamental truth: ransomware is not

just malware, but an **ecosystem of tools, actors, and incentives** that thrives in the gaps of current security and legal frameworks.

The rise of **encrypted traffic** as the default on the internet has further shifted the balance in favor of attackers, limiting the effectiveness of traditional Intrusion Detection Systems (IDS). At the same time, defenders are confronted with the challenge of balancing **security, privacy, and performance** in a world where decryption may be both impractical and unlawful.

8.1 The Path Forward: Layered Défense

Defending against ransomware requires a **multi-layered, adaptive strategy**, not reliance on any single tool:

1. **Preventive Measures**

o Adoption of **Zero Trust Architecture (ZTA)** ensures that trust is never assumed, and every access request is continuously verified.

o **Multi-Factor Authentication (MFA)** significantly reduces the risk of credential theft, one of the most common initial attack vectors.

o **Patch management** must be prioritized to close known vulnerabilities that ransomware routinely exploits.

2. **Detection Approaches**

o **TLS Inspection** provides visibility but must be applied selectively due to performance and privacy concerns.

o **Encrypted Traffic Analytics (ETA)** offers a scalable, privacy-preserving alternative by analyzing metadata patterns with AI.

3. **Recovery and Resilience**

o **Immutable, offline backups** remain one of the most effective defenses, ensuring recovery even when ransomware encrypts production systems.

o **Well-rehearsed incident response playbooks** minimize downtime and financial damage.

o **Threat hunting** ensures early detection before ransomware executes fully.

4. **Emerging Solutions**

o **AI and Machine Learning** provide the ability to detect subtle anomalies invisible to traditional methods.

o **Federated Learning** allows collaborative defense across industries without violating data privacy laws.

8.2 Final Reflection

The future of ransomware defense will be shaped by a combination of **technological innovation, regulatory evolution, and international cooperation**. While no single solution can fully neutralize the threat, organizations that adopt **layered, adaptive defenses** will be positioned to not only survive but also thrive in the face of the ransomware challenge.

Ultimately, the ransomware battle is an **endless arms race** — one that defenders can only win by staying proactive, collaborative, and innovative.

References

- Kharraz, A., & Kirda, E. (2017). *Ransomware: A survey on recent advances*. Security and Communication Networks. https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1730

- Europol (2023). *Internet Organised Crime Threat Assessment (IOCTA) 2023*. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023

- CERT-EU (2022). *Ransomware Threat Landscape*. https://cert.europa.eu/static/whitepapers/CERT-EU-Security-Whitepaper-Ransomware.pdf

- IBM Security (2024). *Cost of a Data Breach Report 2024*. https://www.ibm.com/reports/data-breach

- National Institute of Standards and Technology (NIST). (2022). *Zero Trust Architecture (SP 800-207)*. https://csrc.nist.gov/publications/detail/sp/800-207/final

- Cybersecurity & Infrastructure Security Agency (CISA). (2023). *Stop Ransomware: Ransomware Guide*. https://www.cisa.gov/stopransomware/ransomware-guide

- Coveware (2024). *Quarterly Ransomware Report Q1 2024*. https://www.coveware.com/blog/q1-2024-ransomware-marketplace-report

- Palo Alto Networks Unit 42 (2023). *Ransomware Threat Report*. https://unit42.paloaltonetworks.com/ransomware-threat-report-2023

- McAfee Enterprise & FireEye (2022). *Cybercrime in a Pandemic World: The Impact of COVID-19*. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-cybercrime-pandemic.pdf