International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

A Review of the Conceptual Evolution of Ransomware-as-a-Service in Cybercrime Ecosystems

Vinayak Badure[1], Hariom Yannawar[2], Vaishnavi Godbole[3] ,Harsha Boghe[4] Sakshi Kubade[5],Sanika Dhongade[6],Dr.Pravin Kulurkar[7]

[1]Dept. of Computer Science and Engineering (Cyber Security)
G H Raisoni College of Engineering and Management ,Nagpur
[2] Dept. of Computer Science and Engineering (Cyber Security)
G H Raisoni College of Engineering and Management,Nagpur
[3] Dept. of Computer Science and Engineering (Cyber Security)
G H Raisoni College of Engineering and Management,Nagpur
[4]Dept. of Computer Science and Engineering (Cyber Security)
G H Raisoni College of Engineering and Management,Nagpur
[5]Dept. of Computer Science and Engineering (Cyber Security)
G H Raisoni College of Engineering and Management,Nagpur
[6]Dept. of Computer Science and Engineering(Cyber Security)
G H Raisoni College of Engineering and Management,Nagpur

[7]Dr. Pravin Kulurkar, Asstt.Professor, Dept. of Computer Science and Engineering(Cyber Security),
G H Raisoni College of Engineering and Management, Nagpur, India

---

Abstract -

Ransomware has emerged as one of the most disruptive forms of cybercrime in the modern digital era. With the rapid evolution of cybercriminal operations, the emergence of the Ransomware-as-a-Service (RaaS) model has significantly increased the scale and accessibility of ransomware attacks. This paper reviews the study "Cybercrime Business Evolved: A Concept Analysis of Ransomware-as-a-Service" and evaluates its contribution to cybersecurity research. The reviewed work focuses on clarifying the conceptual structure of the RaaS model and identifying the key actors, characteristics, and operational mechanisms within ransomware ecosystems. Using a structured concept analysis approach, the study identifies defining attributes such as service-based cybercrime operations, distributed roles among actors, and revenue-sharing mechanisms. This review summarizes the research objectives, methodology, and key findings of the study, followed by a critical analysis of its strengths and limitations. The discussion further highlights the implications of the RaaS model for cybersecurity policy, digital infrastructure protection, and organizational risk management. Although the research offers valuable conceptual insights into the evolving cybercrime economy, future studies should integrate empirical data and case-based analyses to strengthen the understanding of ransomware ecosystems.

***Key Words*:**
Cybercrime, cybersecurity, ransomware, ransomware-as-a-service, digital crime economy.

1.INTRODUCTION

The increasing reliance on digital technologies across industries has significantly transformed modern society. Organizations now depend heavily on information systems, cloud infrastructures, and network-based services for their operations. While this technological transformation has enhanced efficiency and connectivity, it has also increased exposure to cyber threats. Among these threats, ransomware has emerged as one of the most damaging forms of cybercrime.

Ransomware refers to malicious software designed to encrypt or block access to computer systems and data until a ransom is paid. In recent years, ransomware attacks have evolved from isolated incidents into highly

organized cybercriminal activities. A particularly significant development in this evolution is the emergence of the Ransomware-as-a-Service (RaaS) model.

The RaaS model functions similarly to legitimate Software-as-a-Service platforms, where developers create ransomware tools and distribute them to affiliates who conduct the attacks. This model enables individuals with limited technical expertise to participate in cybercrime, significantly expanding the reach of ransomware attacks. As a result, ransomware operations have become more scalable, coordinated, and financially profitable.

The purpose of this review paper is to critically examine the research conducted on the concept of Ransomware-as-a-Service and evaluate its contribution to understanding modern cybercrime ecosystems.

2. SUMMARY OF THE RESEARCH PAPER

The primary research problem addressed in the reviewed study is the lack of a clear conceptual definition of Ransomware-as-a-Service within cybersecurity literature.
Although the term is widely used in threat intelligence reports and cybersecurity Discussions, its defining characteristics and operational structure are often inconsistently described.
The study aims to clarify the concept by identifying the essential attributes that distinguish RaaS from traditional ransomware operations. It also seeks to explain the
roles played by different actors within the ransomware ecosystem.

OBJECTIVES

The study focuses on several key objectives:
1. To identify the defining attributes of Ransomware-as-a-Service.
2.To analyze the organizational structure of ransomware ecosystems.
3. To examine the roles and interactions between actors involved in ransomwareoperations.
4. To conceptualize RaaS as a structured cybercriminal business model.
These objectives emphasize conceptual clarification rather than empirical measurement of ransomware incidents.

METHODOLOGY

The research employs an eight-step concept analysis framework to analyze the RaaS phenomenon. Concept analysis is a qualitative research method designed to clarify the meaning, attributes, and boundaries of complex concepts.
The framework includes the following steps:
1. Selecting the concept
2. Determining the purpose of analysis
3. Identifying all possible uses of the concept
4. Determining defining attributes
5. Identifying model cases
6. Identifying borderline and contrary cases
7. Identifying antecedents and consequences
8. Identifying empirical referents

Through this structured approach, the study systematically examines how RaaS is described across cybersecurity literature and identifies its fundamental characteristics.

DATA SOURCES

The study relies primarily on secondary sources, including:
• Academic cybersecurity publications
• Cyber threat intelligence reports
• Existing ransomware research
• Documented descriptions of ransomware operations
Rather than collecting new data, the research synthesizes existing knowledge to
construct a conceptual framework.

KEY RESULTS

The study identifies several defining features of the Ransomware-as-a-Service model.
First, RaaS functions as a service-based cybercrime model, where ransomware developers provide tools and infrastructure to affiliates who conduct attacks.
Second,the ecosystem involves multiple actors, including developers, affiliates, infrastructure
providers, negotiators, and money-laundering facilitators. Third, RaaS operations are typically decentralized and transnational, making law-enforcement interventions more difficult.
Another key finding is the existence of profit-sharing mechanisms, where affiliates share a percentage of ransom payments with developers. This financial

structure incentivizes collaboration and expands the ransomware ecosystem.

CRITICAL ANALYSIS

Strengths of the StudyOne of the major strengths of the study is its strong conceptual focus. By clarifying the structure of the RaaS model, the research provides a useful framework for understanding the evolution of ransomware operations.

Another strength lies in the systematic methodology used in the study. The eight-step concept analysis framework ensures a comprehensive examination of the concept and reduces ambiguity in defining its characteristics.

Additionally, the study highlights the ecosystem nature of cybercrime, emphasizing that ransomware attacks involve coordinated efforts from multiple actors rather than individual attackers.

Weaknesses and Limitations

Despite its contributions, the study also has several limitations. The most significant limitation is the reliance on secondary data sources rather than empirical evidence.

The research does not include quantitative data or case studies that demonstrate how the RaaS model operates in real-world scenarios.

Furthermore, the study provides limited discussion of defensive strategies or policy responses that organizations can implement to mitigate ransomware threats.

Finally, because cybercrime evolves rapidly, the conceptual framework may require continuous updates as new ransomware models emerge.

DISCUSSION

The findings of the study highlight the increasing professionalization and commercialization of cybercrime. The RaaS model demonstrates how cybercriminal groups adopt business strategies similar to those used by legitimate technology companies.

This evolution has significant implications for cybersecurity. The service-based nature of ransomware operations lowers the barrier to entry for cybercriminals and allows attacks to scale rapidly. As a result, organizations across multiple sectors—including healthcare, finance, and government—are increasingly vulnerable to ransomware attacks.

From a theoretical perspective, the research contributes to cybersecurity literature by framing ransomware operations as complex socio-technical ecosystems rather than isolated criminal activities.

FUTURE RESEARCH DIRECTIONS

Future research should focus on expanding the conceptual framework developed in the study by incorporating empirical evidence. Researchers could analyze real ransomware campaigns to validate the roles and relationships identified in the conceptual model.

Comparative studies examining different ransomware groups could also reveal variations in operational structures and financial models. Additionally, interdisciplinary research integrating cybersecurity, criminology, and economics may provide deeper insights into the motivations and strategies of cybercriminal organizations.

Another important direction involves studying effective cybersecurity defense mechanisms that can disrupt the RaaS ecosystem.

CONCLUSION

The reviewed study provides a comprehensive conceptual analysis of the Ransomware-as-a-Service model and its role within modern cybercrime ecosystems. By applying a structured concept analysis framework, the research identifies the defining attributes,actors, and operational mechanisms associated with RaaS.

The study demonstrates that ransomware has evolved into a sophisticated service-based cybercrime model characterized by distributed roles, profit-sharing structures,and global collaboration among attackers. These developments significantly increase the complexity of cybersecurity threats.

Although the research offers valuable theoretical insights, future studies should incorporate empirical data and case-based analyses to strengthen understanding of ransomware ecosystems and support the development of effective cybersecurity strategies.

REFERENCES

[1] D. S. Wall, *Crime, Security and Information Communication Technologies*. London, U.K.: Routledge, 2017.
[2] M. Yar and K. F. Steinmetz, *Cybercrime and Society*, 3rd ed. London, U.K.: Sage, 2019.
[3] A. Hutchings and R. Clayton, "Exploring the provision of online booter services," *Deviant Behavior*, vol. 37, no. 10, pp. 1163–1178, 2016.
[4] Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, 2023.
[5] ENISA, *ENISA Threat Landscape Report*, 2023.
[6] CrowdStrike, *Global Threat Report*, 2024.
[7] Sophos, *The State of Ransomware Report*, 2024.
[8] IBM Security, *Cost of a Data Breach Report*, 2024.
[9] Check Point Research, *Ransomware Report*, 2023.
[10] Kaspersky, *Ransomware Evolution Report*, 2024.
[11] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, 2023.
[12] CISA, *Ransomware Guide*, 2023.
[13] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544–546, 2018.
[14] S. Mansfield-Devine, "Ransomware: Taking businesses hostage," *Network Security*, vol. 2016, no. 10, pp. 8–17, 2016.
[15] J. O'Kane, S. Sezer, and K. McLaughlin, "Obfuscation: The hidden malware," *IEEE Security & Privacy*, vol. 9, no. 5, pp. 41–47, 2011.
[16] R. Richardson and M. North, "Ransomware: Evolution, mitigation and prevention," *International Management Review*, vol. 13, no. 1, pp. 10–21, 2017.
[17] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the Gordian knot: A look under the hood of ransomware attacks," in *Proc. Int. Conf. Detection of Intrusions and Malware*, 2015, pp. 3–24.
[18] K. Savage, P. Coogan, and H. Lau, "The evolution of ransomware," Symantec Security Response, 2015.
[19] N. Perlroth, *This Is How They Tell Me the World Ends*. New York, NY, USA: Bloomsbury, 2021.
[20] Verizon, *Data Breach Investigations Report (DBIR)*, 2024.
[21] Palo Alto Networks, *Unit 42 Ransomware Threat Report*, 2023.
[22] FireEye (Mandiant), *M-Trends Report*, 2024.
[23] S. Romanosky, "Examining the costs and causes of cyber incidents," *Journal of Cybersecurity*, vol. 2, no. 2, pp. 121–135, 2016.
[24] OECD, *Cybersecurity Policy Framework*, 2021.
[25] World Economic Forum, *Global Cybersecurity Outlook*, 2024.