A Study of Ransomware Detection and Encryption Blocking Performance Verification: Focusing on Global Antivirus

Kangsik Shin *
KAIST Cyber Security Research Center
Daejeon, South Korea
ksshin90@kaist.ac.kr

GyuHyeon Choi
KAIST Cyber Security Research Center
Daejeon, South Korea
gyuhyeon@kaist.ac.kr

KyeongSeok Lee
KAIST Cyber Security Research Center
Daejeon, South Korea
harvist@kaist.ac.kr

Jeongho Lee
KAIST Cyber Security Research Center
Daejeon, South Korea
ddanzit@kaist.ac.kr

Ho-Mook Cho‡
KAIST Cyber Security Research Center
Daejeon, South Korea
chmook79@kaist.ac.kr

***Abstract*—This study evaluates the ransomware defense capabilities of leading antivirus (AV) products in Endpoint environments. Through controlled experiments with nine AV solutions and 157 recent ransomware samples from six families: Clop, Conti, Akira, Maze, Play, and Chaos, we measured detection performance and encryption-blocking effectiveness. Findings reveal that while certain products achieve high detection accuracy, most fail to provide adequate protection against file encryption. Notably, Play ransomware encryption was blocked only by one product, underscoring substantial limitations in conventional AV. Our results highlight the need for multi-layered defenses and resilient backup strategies, along with more effective behavioral approaches, to better protect against evolving ransomware threats.**

Keywords—Ransomware, Antivirus, Detection, Encryption Blocking, Malware Defense, Cybersecurity

I. Introduction

Ransomware has rapidly become one of the most critical threats confronting the global cybersecurity ecosystem [1]. Rather than merely corrupting files or disrupting system availability, this type of attack encrypts users' critical data and system resources and then demands financial compensation, inflicting severe harm not only on individual users but also on businesses, public institutions, and national infrastructure [2]. In particular, the proliferation of Ransomware-as-a-Service (RaaS), combined with increasingly sophisticated attack techniques, has lowered the barrier of entry for attackers and intensified the defensive challenges faced by security practitioners [3].

To mitigate these threats, most PC users have traditionally relied on antivirus (AV) software. Conventional AV systems primarily utilize signature-based and heuristic detection methods to identify and block known malware and their variants. In recent years, these solutions have evolved to integrate machine learning–driven detection and behavioral analysis, thereby enhancing their overall effectiveness [5,6]. Nonetheless, concerns remain regarding whether current AV products provide sufficient protection in practice—particularly in terms of early ransomware detection and the capability to halt malicious file encryption, both of which are defining characteristics of ransomware attacks [7,8].

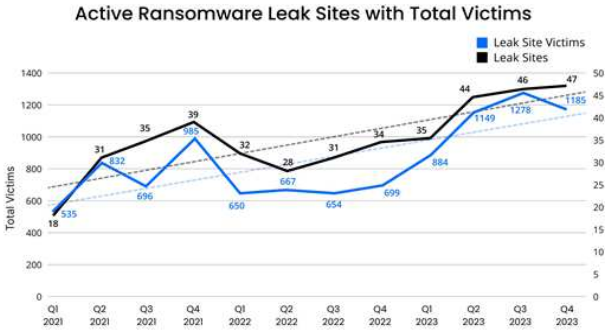

Fig. 1. Statistics on dark web platforms used by ransomware groups to negotiate ransom demands with victim organizations.

However, in many cases, the sample collection environments and testing conditions were not disclosed, and evaluations were limited to whether detection occurred, without measuring the extent of encryption prevention. As a result, there is a notable gap in quantitative validation concerning how rapidly antivirus products can intervene during ongoing encryption and mitigate the extent of data loss [9,10].

Accordingly, this study aims to systematically evaluate the ransomware detection and encryption-blocking capabilities of leading antivirus solutions in PC environments. By simulating real-world user conditions with diverse infection vectors and contemporary ransomware samples, we conduct a quantitative evaluation of each product's detection rate and encryption-blocking rate. The outcomes of this research are expected to validate the practical constraints of existing antivirus technologies while offering actionable guidance for user security strategies and informing future improvements in the security industry.

II. Related Work

A. Antivirus

Antivirus software is a fundamental security tool for detecting, preventing, and eliminating malicious software (malware) within computer and network environments. It continuously monitors systems in real time, identifying suspicious files or behaviors, and applying countermeasures such as quarantine or removal. Modern antivirus solutions also sustain current malware databases through automated updates and extend their protection with additional features—

including email filtering, integrated firewalls, sandbox execution, and cloud-based analytics—that collectively enhance the security posture of Endpoint(personal computing) devices [11].

Conventional antivirus detection techniques are generally grouped into three categories. The first is signature-based detection, which matches known malware signatures against a database. While this approach offers speed and precision, it is less effective against newly modified variants. The second is heuristic detection, which examines unusual code structures or suspicious patterns to identify previously unseen threats. The third is behavior-based detection which continuously monitors runtime activities—such as large-scale file encryption or system configuration changes—to detect and halt attacks in real time [12].

Beyond traditional techniques, ransomware detection employs a range of specialized methods. Signature-based detection leverages known ransomware patterns but remains limited against emerging variants. In contrast, behavioral analysis targets distinctive runtime activities—such as file encryption attempts, renaming operations, or the disabling of security safeguards—allowing defenses to extend to previously unidentified threats. Encryption detection methods identify ransomware activity by measuring entropy changes during file modifications or by flagging abnormal file extensions. Moreover, machine learning–driven detection utilizes large-scale data training to differentiate subtle distinctions between benign and malicious behaviors, offering adaptive protection against ransomware variants [13].

B. Ransomware Behavior and Characteristics

Ransomware is a type of malicious software that encrypts files on an infected system or denies access to the system, forcing victims into paying a ransom. Unlike attacks aimed at simple destruction, its primary objective is financial extortion by holding data hostage. Typically, ransomware takes advantage of a combination of robust symmetric and asymmetric cryptography—so strong that even experts struggle to break it—effectively rendering files inaccessible. Once infection occurs, users are often made immediately aware through actions such as screen locks or the alteration of critical file extensions. Attackers typically leave a "ransom note" that enumerates encrypted files and outlines recovery instructions, demanding payment—often in difficult-to-trace cryptocurrencies such as Bitcoin—in exchange for the decryption key [14,15]. Yet, payment offers no certainty of data recovery; reports exist of victims receiving no decryption key or suffering partial and permanent data loss even after paying.

Ransomware typically gains entry through a range of infection vectors, which have grown increasingly sophisticated. Predominant attack avenues include phishing emails carrying malicious attachments or links, drive-by downloads, and exploitation of unpatched software vulnerabilities. Upon successful compromise, adversaries typically employ privilege-escalation techniques to secure administrative access and conduct network scanning to enable lateral movement across the LAN. In many campaigns, ransomware operators also exfiltrate internal information—such as sensitive data and credentials—to threaten disclosure or extortion, and they may delete or corrupt backups to frustrate recovery and drive ransom demands up [16]. As illustrated in Figure 2, ransomware typically operates in sequential stages. The process begins with evasion of antivirus defenses, followed by communication with a command-and-control (C&C) server to obtain the necessary encryption keys or supplementary instructions. Attackers then prioritize the encryption of designated targets, especially recently created files, to maximize damage, while simultaneously deleting system restore points to inhibit recovery options. Certain ransomware groups orchestrate tailored intrusions against enterprises and institutions, embedding themselves within internal systems for extended dwell times before triggering coordinated, large-scale encryption events. Consequently, ransomware has evolved into a compound threat that goes beyond encryption, combining data exfiltration, service disruption, and psychological pressure. Effective mitigation therefore requires a coordinated strategy of prevention, detection, rapid response, and secure backup [17,18].

III. Experimental Evaluation of Ransomware Detection and Encryption Blocking

This experiment was designed to evaluate how effectively antivirus solutions can respond to ransomware in realistic environments. With ransomware evolving rapidly, reliance on signature-based detection alone has proven inadequate, highlighting the growing need for behavior-based approaches and multi-layered defense architectures. This study therefore quantitatively evaluates detection accuracy and encryption-blocking rate using a representative set of ransomware samples in simulated real-world environments. To ensure consistency, equivalent testbeds were deployed with individual antivirus products installed. Following system reboots and an approximately five-minute stabilization period, ransomware samples were introduced and executed via custom software. Detection performance was evaluated by examining antivirus notifications, logs, and quarantine results, while encryption-defense success rates were manually documented by verifying whether document files on the host systems had been encrypted.

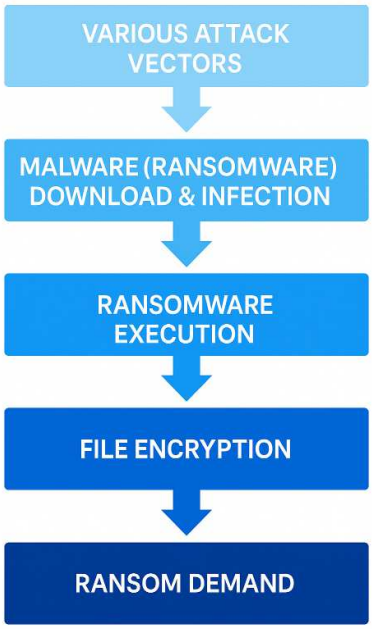

Fig. 2. Operation Mechanism of Ransomware

TABLE I

DEVICE SPECIFICATION\

Test PC	
CPU	i5-12400
GPU	On-board Intel UHD Graphics 730
Memory	16GB
Storage	SSD 500GB
1OS	Windows 10 Pro 64bit

A. Construction of Experimental Environment and Definition of Test Scenarios

To validate ransomware detection and encryption-blocking capabilities, we established a controlled test environment comprising nine PCs with antivirus solutions installed and a dedicated server hosting a database for command orchestration and system control. All test PCs were configured with identical hardware specifications and operating systems (Table 1). Three testers conducted the evaluation, each overseeing three PCs, with one designated administrator responsible for coordinating the deployment and execution of ransomware samples. Custom-built orchestration software was deployed on each PC, while the administrator system issued download and execution commands concurrently, with real-time logs collected and stored in the database (DB). This configuration ensured a standardized environment that enabled reproducible performance evaluations without manual intervention.

Two experimental scenarios were defined: (1) detection capability at the point of execution and (2) quantitative measurement of encryption-blocking effectiveness. All antivirus products were tested using their default configurations, with no additional tuning. To facilitate testing, specific folders and the custom control software were added to exclusion lists to prevent premature blocking. Scenario 1 employed six recently collected ransomware families—Clop, Conti, Akira, Maze, Play, and Chaos—as representative samples. Scenario 2 aimed to evaluate the practical effectiveness of antivirus solutions in defending against encryption.

TABLE II

OVERVIEW OF SELECTED ANTIVIRUS

Antivirus	Version
AhnLab V3 365 Clinic	4.15.0.1
Alyac 5.1	5.1.29.15139
ESET NOD32	18.2.17.0
Bitdefender Antivirus Plus	27.0.54.270
Avast Premium Security	25.8.10387a
Norton	25.8.10387
Windows Defender	4.18.25080.5
Avira Internet Security	1.1.110.2513
AVG Internet Security	25.8.10387a

B. Selection of Evaluation Targets and Ransomware Samples

The antivirus products evaluated in this study were personal-use versions compatible with the Windows operating system. Product selection adhered to two principal criteria: (1) certification from a globally recognized testing authority such as AV-Comparatives or AV-TEST at least once, and (2) significant market penetration in both domestic and international contexts. Applying these criteria yielded approximately 20 candidate solutions, from which nine were randomly selected for experimentation, as detailed in Table 2.

The ransomware dataset was curated to emphasize families that had recently demonstrated both high prevalence and severe impact. Samples were acquired through a proprietary crawling framework and malware database repositories, subject to three filtering criteria: (1) classification of samples from six ransomware families active among roughly 1.3 million collected specimens, (2) verification of sample authenticity via VirusTotal to ensure dataset reliability, and (3) confirmation of operational behavior through Anyrun analysis and manual execution. In total, nine antivirus solutions and 157 ransomware samples from six families were designated as the evaluation corpus. This dataset

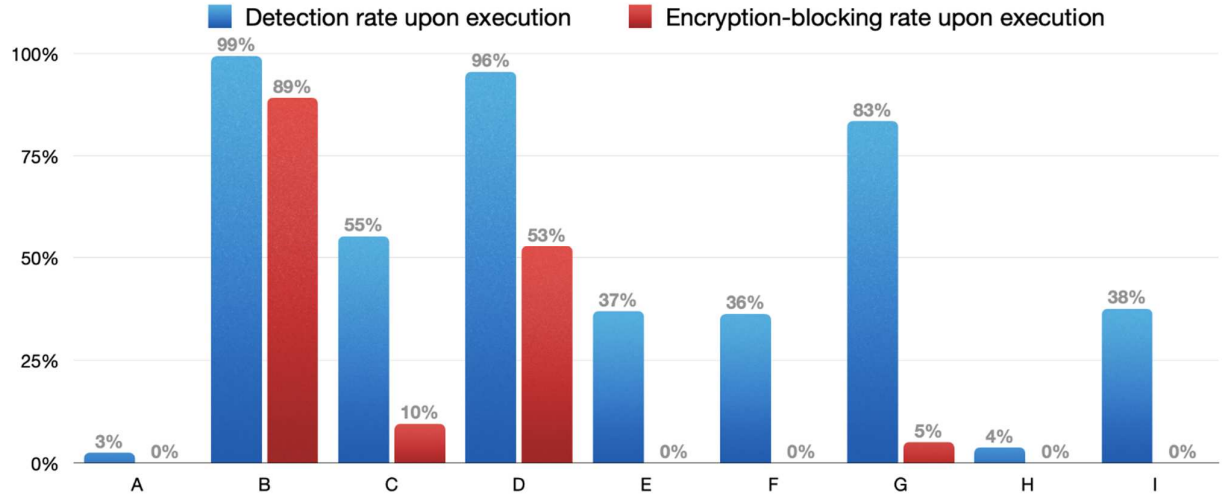

Fig. 3. Comparison of Execution Detection and Encryption-Blocking Rates of Nine Antivirus Products

enabled a comprehensive assessment of each product's detection performance and its effectiveness in preventing or mitigating ransomware-driven file encryption.

IV. Results and Analysis

With the ransomware dataset and experimental environment established, we carried out testing over the course of June 2025. The evaluation examined nine antivirus solutions (labeled A through I) against six ransomware families, quantifying both detection accuracy and encryptionblocking effectiveness.

Results highlighted marked disparities between the ability to detect ransomware and the capacity to halt encryption. Product B exhibited the strongest and most balanced performance, achieving a 99% detection rate and an 89% blocking rate. Product D achieved a high detection rate of 96% but only a 53% blocking rate, indicating limitations in real defensive strength. By contrast, Products C and G yielded detection rates of 55% and 83%, respectively, yet their blocking rates were as low as 10% and 5%, demonstrating insufficient resilience against file encryption. The remaining solutions—A, E, F, H, and I—recorded detection rates ranging from 3% to 38%, with blocking rates uniformly at 0%, reflecting minimal security value. We further analyzed performance at the ransomware-family level.

A. Evaluation of Detection-Rate

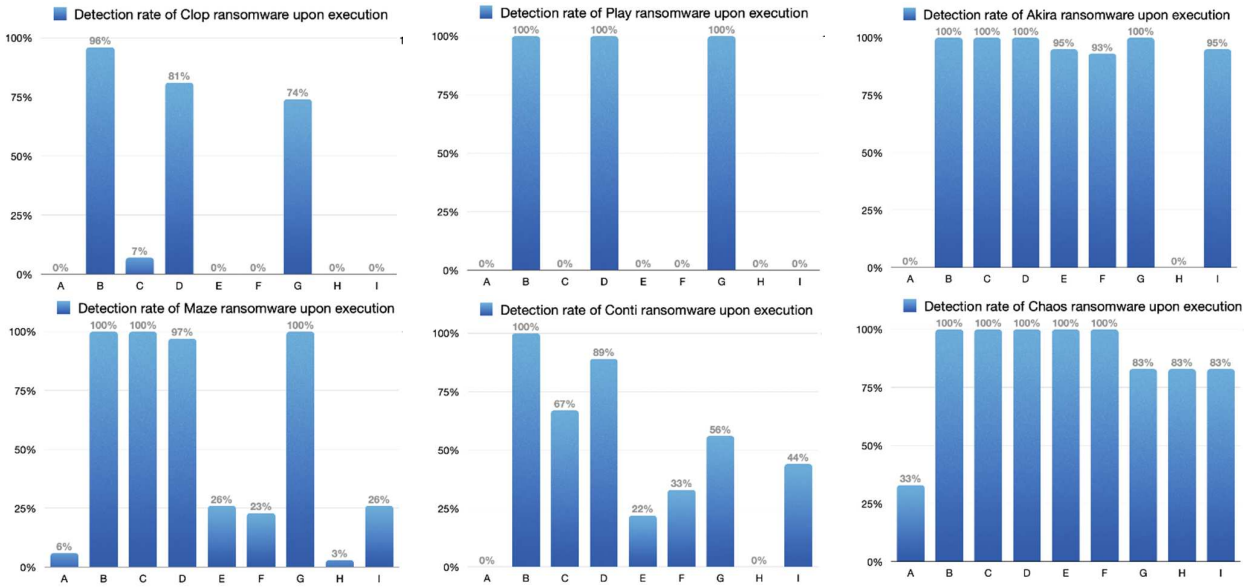

Fig. 9. Detection rates by ransomware type

B. Evaluation of Encryption-Blocking Rate

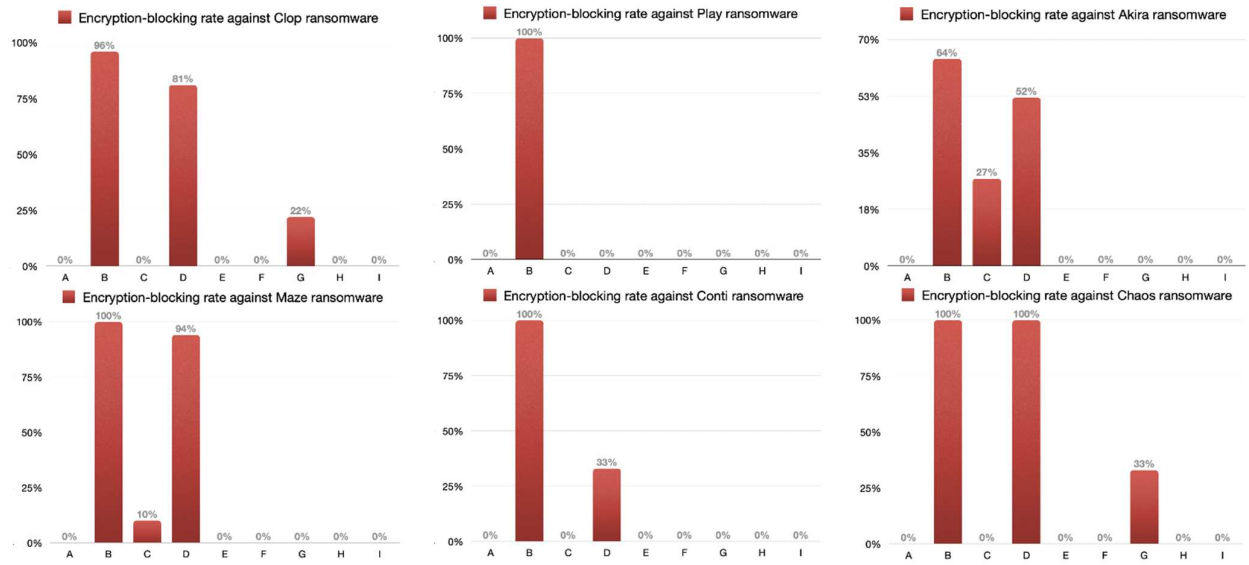

Fig. 10. Encryption blocking rates by ransomware type

The detection-rate evaluation reflects the extent to which antivirus solutions accurately identify ransomware at execution. Performance was assessed by ransomware family, and average detection rates were derived accordingly. Product B demonstrated the highest consistency, detecting over 98% of all ransomware types. Products D and G also performed relatively well, each exceeding 70%. By contrast, Products A and I produced poor results, failing to detect four of the six ransomware families, with successful detection limited to Maze and Chaos. A family level analysis further indicated that Akira and Chaos samples were generally well recognized across products, while Clop and Play ransomware exhibited low detection rates for most solutions.

The encryption-blocking metric assesses the ability of antivirus solutions to halt file encryption following ransomware execution. Consistent with the detection-rate methodology, evaluations were conducted per ransomware family with blocking rates first calculated for each family and then averaged across families. Product B exhibited the most robust performance: for all families except Akira, its detection aligned with a 100% encryption-blocking outcome, while for Akira its effectiveness decreased to 64%. Product G, despite high detection scores, performed poorly in preventing subsequent file encryption. A family-level analysis confirmed that, aside from Product B, nearly all antivirus products displayed low blocking effectiveness, with Play ransomware proving especially resilient—Only Product B successfully blocked Play ransomware; all other products failed to prevent encryption.

V. Conclusion and Future Work

This study evaluated the detection and encryption-blocking capabilities of leading antivirus (AV) products for Endpoint(personal PCs) device, employing 157 recent ransomware samples. The results demonstrated that although certain products achieved balanced performance across detection and blocking metrics, a substantial number showed high detection rates yet failed to halt encryption, thereby exposing critical limitations in protecting end-user data. Clear differences also emerged across ransomware families: some were effectively detected, whereas others evaded both detection and blocking. These outcomes underscore the persistent reliance of commercial antivirus products on signature-based mechanisms and the inherent structural shortcomings of such approaches in countering the rapidly evolving tactics of modern ransomware. Thus, antivirus solutions alone cannot constitute a comprehensive defense. Effective mitigation requires secure backup management, multi-layered defense strategies, and the integration of complementary technologies such as behavior-based detection. Future work should expand the evaluation to include a broader range of products and ransomware variants, while conducting in-depth investigations into the root causes of post-detection blocking failures to better understand and address the structural limitations of antivirus solutions. Beyond simple detection and blocking tests, incorporating complex attack scenarios—such as data exfiltration and backup tampering—will enable more realistic evaluations and provide practical and actionable security guidance for individuals and enterprises facing ransomware threats.

Acknowledgment

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) funded by the Korea government (00235509, Development of security monitoring technology based network behavior against encrypted cyber threats in ICT convergence environment)

References

[1] ENISA, “Threat Landscape 2024,” European Union Agency for Cybersecurity, 2024.

[2] Fortinet, “2025 Global Threat Landscape Report,” Fortinet, 2025.

[3] MELAND, Per Håkon; BAYOUMY, Yara Fareed Fahmy; SINDRE, Guttorm. The Ransomware-as-a-Service economy within the darknet. Computers & Security, 2020, 92: 101762.

[4] Alkhateeb, Ehab M., and Mark Stamp. "A dynamic heuristic method for detecting packed malware using naive bayes." 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA). IEEE, 2019.

[5] Zahoora, U., Khan, A., Rajarajan, M., Khan, S. H., Asam, M., & Jamal, T. (2022). Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto Ensemble classifier. Scientific reports, 12(1), 15647.

[6] Berrueta, E., Morato, D., Magaña, E., & Izal, M. (2019). A survey on detection techniques for cryptographic ransomware. IEEE Access, 7, 144925-144944..

[7] Kok, S., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019). Ransomware, threat and detection techniques: A review. Int. J. Comput. Sci. Netw. Secur, 19(2), 136.

[8] Rohith, Cheerala, and Gagandeep Kaur. "A comprehensive study on malware detection and prevention techniques used by anti-virus." 2021 2nd international conference on intelligent engineering and management (iciem). IEEE, 2021.

[9] Chatzoglou, E., Karopoulos, G., Kambourakis, G., & Tsiatsikas, Z. (2023, August). Bypassing antivirus detection: old-school malware, new tricks. In Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1-10).

[10] Lin, Yung-She, and Chin-Feng Lee. "Ransomware detection and prevention through strategically hidden decoy file." International Journal of Network Security 25.2 (2023): 212-220.

[11] https://www.sophos.com/en-us/cybersecurity-explained/antivirus

[12] WANJALA, Muchelule Yusuf; JACOB, Neyole Misiko. Review of Viruses and Antivirus patterns. Glob. J. Comput. Sci. Technol, 2017, 17: 1-3.

[13] Kunku, Kavitha, A. N. K. Zaman, and Kaushik Roy. "Ransomware detection and classification using machine learning." 2023 IEEE Symposium Series on Computational Intelligence (SSCI). IEEE, 2023.

[14] Mohurle, Savita, and Manisha Patil. "A brief study of wannacry threat: Ransomware attack 2017." International journal of advanced research in computer science 8.5 (2017).

[15] Alqahtani, Abdullah, and Frederick T. Sheldon. "A survey of crypto ransomware attack detection methodologies: An evolving outlook." Sensors 22.5 (2022): 1837.

[16] Lang, M., Connolly, L., Taylor, P., & Corner, P. J. (2023). “The evolving menace of ransomware: A comparative analysis of pre-pandemic and mid-pandemic attacks.” Digital Threats: Research and Practice, 4(4), 1- 22.

[17] Oz, H., Aris, A., Levi, A., & Uluagac, A. S. “A survey on ransomware: Evolution, taxonomy, and defense solutions.” ACM Computing Surveys (CSUR), 54(11s), 1-37.