iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 13 **Issue:** III **Month of publication:** March 2025

**DOI:** https://doi.org/10.22214/ijraset.2025.67557

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue III Mar 2025- Available at www.ijraset.com*

# A Survey of Ransomware Resilience: Strategies for Prevention and Recovery

Atharva Abhijit Kelkar[1], Palavi Manohar Adhav[2], Yogesh Madhukar Upare[3], Pratiksha Sawant[4]
*Department of computer science, PVG's College of Science & Commerce*

***Abstract: Ransomware and mobile malware have rapidly evolved into critical cybersecurity challenges, leveraging encryption, obfuscation, and self-updating techniques to evade detection[1]. Detection methods, such as static and dynamic analysis[2] and machine-learning-based anomaly detection [3], show promise in mitigating threats. Proactive approaches, including behavior-based detection and hybrid cryptography like PayBreak [4], are essential for early threat identification and recovery. AI-driven defenses and situational awareness models [5] can improve detection rates, while socio-technical solutions and NIST recommendations offer enhanced recovery strategies [6]. Future research should focus on automated detection systems and mitigating zero-day threats***

***Keywords: Ransomware, Malware,Ransomware Detection, Phishing and Social Engineering, Honeypot.***

## I. INTRODUCTION

*1) What is Cybersecurity?*

Cybersecurity is the practice of protecting computers, servers, cell phones, and networks from malicious attack. Cybersecurity encompasses a wide range of techniques, including firewalls, virus programs, intrusion detection systems, and encryption. Cybersecurity is important for safeguarding individual information, corporate data, and financial data. With increasing digital gadgets and internet use worldwide, cyber attacks have become more sophisticated and frequent, making cybersecurity more necessary than ever [7]. Industries like healthcare, finance, and government are particularly vulnerable, highlighting the necessity of continuous advancements in cybersecurity technologies.

*2) What is Ransomware?*

Ransomware is malicious software that has been designed to lock a computer system or encrypt files until money is paid in the form of a ransom. Ransomware typically enters devices through phishing emails, compromised websites, or application vulnerabilities. Ransomware either encrypts information or blocks individuals from accessing their systems when triggered. Victims are then presented with a ransom fee, which in most cases is paid in cryptocurrencies for anonymity reasons [8].

One of the most infamous ransomware attacks was the WannaCry attack of 2017, which spread rapidly and caused massive disruption. The attack affected organizations around the world, from hospitals, shipping companies, and government agencies. The rapid spread and impact of WannaCry was indicative of the increasing demand for improved cybersecurity to combat such attacks.

*3) Types of Ransomware:*

Ransomware is available in different forms, all with different ways of attacking:

*a)* *Crypto Ransomware:* Crypto ransomware encrypts files such that they are useless until a payment is made to them. Without the decryption key, the files are useless, and the attackers provide the option to deliver this after payment [4].

*b)* *Locker Ransomware:* This ransomware type locks users out of their devices entirely without encrypting files. Victims are denied access to their operating system, and a ransom is demanded to access it [9]

*c)* *Ransomware-as-a-Service (RaaS):* Ransomware products are sold by cybercriminals to other hackers for a payment or share of the ransom. This approach allows inexperienced hackers to carry out complex attacks with minimal effort [10].

*4) Examples of Ransomware:*

*a)* A crypto ransomware attack that encrypted files and demanded payment in Bitcoin. It affected organizations from various industries globally.

©IJRASET: All Rights are Reserved 

*b)* Petya: A form of ransomware that replaces a computer's boot process, locking out users completely and demanding payment to unlock it [9].

*c)* CryptoLocker: A ransomware that encrypts critical files and demands a ransom to decrypt them. It primarily attacked individual consumers and small businesses [2]

Fig.1 Types of Ransomwares

Mobile operating systems and web-connected systems have expanded the attack surface for ransomware writers. Sectors like healthcare, finance, and critical infrastructure have been regular targets because they depend on sensitive information and business continuity [11]. The COVID-19 pandemic further exacerbated vulnerabilities as remote work increased, leading to heightened ransomware activity [12]. This study aims to explore detection and mitigation strategies to help users and organizations safeguard against the evolving ransomware threat.

*5) How Ransomware Spreads:*

a) Attackers employ different ways to spread ransomware:

- Phishing Emails: Phishing emails are the most common method. They trick users into opening attachments or clicking on links that download ransomware onto their systems [13].
- Malicious Websites: Infected websites or pop-up ads can automatically download ransomware when users visit them
- Remote Desktop Protocol (RDP) Attacks: Attackers exploit weak or default RDP passwords to infiltrate systems and disseminate ransomware [14].

*6) Challenges in Combating Ransomware:*

One of the biggest challenges is early detection of ransomware since it can be hidden in systems. Traditional antivirus software is generally ineffective against new or modified ransomware variants, which can bypass signature-based detection methods [2].
Sophisticated evasion techniques, such as code obfuscation and self-propagation malware, further complicate detection [15]. Additionally, some ransomware waits until it recognizes critical files to encrypt, making detection further complicated. Organizations hence have to introduce more sophisticated technologies, such as anomaly detection via AI and behavior-based monitoring, to counteract these new-fangled threats.

*7) Applications of Ransomware Research:*

Research into ransomware has a number of applied applications:

*a)* Improved Detection Tools: Behavioral monitoring tools can detect suspicious behavior, such as file encryption or unauthorized access, and prevent ransomware attacks before harm is caused [3]

*b)* User Education: Training users on phishing attacks and social engineering methods can reduce the threat of being attacked by ransomware. Awareness campaigns can help users identify and avoid potential threats [16].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

*c)* More Secure Security Policies: Government organizations and nongovernmental organizations may develop security policies based on research findings to protect critical infrastructure and key services from ransomware attacks [17].

*d)* Enhanced Mobile Security: Mobile app developers can implement stronger security measures to prevent malicious apps from spreading ransomware or other malware [2]. These include the implementation of sandboxing, permission boundaries, and anomaly detection on mobile operating systems.

Ransomware is an effective cybersecurity attack that continuously evolves its attack strategies along with evasion methods. The traditional antivirus methods are no longer potent enough to counter such evolving threats [2]. Advances in AI-driven detection models, behavior tracking, and predictive threat detection hold potential for reducing ransomware attacks [3].

User training, international collaboration, and security measures with an integrated approach are the solution to the global phenomenon of ransomware [11]. Companies can better protect themselves against the ever-evolving threat of ransomware through multi-layered security solutions.

## II. METHODOLOGY

This research amalgamates the results of various research papers to create a broad, multi-level defense system to fight ransomware and mobile malware. Machine learning algorithms were used heavily for anomaly detection based on behavior to find suspicious network activities and possible malware infections [11]

Static and dynamic analysis techniques were used to identify pattern signatures of malicious code by scanning executable files and runtime patterns [2] Hybrid encryption-based analysis was the nucleus of the PayBreak model, which offered recovery after infection by decrypting ransomware-encrypted files [4]

Behavior analysis methods were utilized through AI-driven Windows process monitoring for identifying ransomware at the pre-encryption phase [18]. Anomaly detection systems also tracked network behavior deviations for identifying stealthy malware infections [7]. Memory forensics was utilized for tracking ransomware activity in real time, such as recognizing API manipulation patterns and memory access anomalies [19]

Honeypot-based approaches were experimented with to mislead attackers and secure valuable assets through the imitation of vulnerabilities and study of ransomware interactions [20]. Further, a three-tier security measure through virtual machines was used to quarantine and scan malicious files before they infected the host system [13].

The live-forensic hypervisor approach, suggested by Hirano et al., traced and examined memory access patterns to identify ransomware and flag anomalies at runtime [21]. Situational awareness models were used to observe device and network activity in real-time, triggering early warnings for impending ransomware attacks [5]

Public and private malware datasets were used to inform the taxonomy of countermeasures and train machine learning algorithms [16]. Comparative studies were performed to ascertain the effectiveness of current ransomware countermeasures, emphasizing minimizing false positives and maximizing detection rates [16]

Socio-technical solutions focused on user training and simulation drills to enhance awareness and response capacity. Simulation-driven awareness training enabled the education of users on phishing, social engineering strategies, and ransomware infection situations [6]. The effectiveness of each technique was validated in controlled settings using actual ransomware samples to analyze detection accuracy and response times [12].

Generative AI's potential for crafting phishing emails was analyzed experimentally, revealing how AI-driven social engineering could increase ransomware's reach and effectiveness [22]. By integrating behavior-based monitoring, encryption analysis, anomaly detection, and user education, this comprehensive defense framework provides a multi-faceted approach for mitigating ransomware threats.

## III. GAPS AND CHALLENGES

Detection prior to encryption is one of the biggest challenges when it comes to fighting ransomware [14]. Zero-day variants are not detectable by signature-based methods, thus rendering detection challenging for new forms of ransomware[23],[17].

Adversaries rely on vulnerabilities within Windows API calls to gain persistence on affected systems [18]. In addition, they also use sophisticated obfuscation methods to stay hidden from their traditional antivirus detection [6],[2]

Organizations often face aging cybersecurity infrastructure, thus increasing their exposure to current ransomware attacks [13]. The speedy evolution of ransomware families and attack vectors has also surpassed the creation of good detection systems [9],[24].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Social engineering techniques, including phishing messages and ill-intentioned links, are still the most effective means of distributing ransomware[25]. Most users are not trained or aware enough to detect such threats, making them more vulnerable [26]. The application of generative AI has further increased the authenticity of phishing attacks, making them harder to detect [22].

Small enterprises are most exposed because of financial and operational limitations that discourage the adoption of thorough cybersecurity protocols [5],[27],[15]. Most of these enterprises do not have effective incident response plans to deal with ransomware attacks [19].

Ransomware has also widened its target surface to encompass mobile devices and cloud infrastructure, increasing the challenge of protecting contemporary IT environments [8]; [12]. Ransomware attacks on mobile malware on IoT devices add to the complexity of cybersecurity efforts, given that many IoT devices are not equipped with defenses that can keep malware out [12].

False-positive rates are still a critical concern in most detection solutions, which causes inefficiency in mitigation and response [1]. Endpoint security solutions are normally applied but are usually lacking when challenged by complex attacks utilizing encryption and dynamic code loading mechanisms [28],[4].

Lastly, the lack of global cybersecurity standards and legal frameworks enables ransomware attackers to escape prosecution [11], [10]. The international nature of ransomware attacks places higher demands on industries, governments, and global regulatory agencies to work together more closely. Resolving these issues is accomplished with a multi-pronged strategy of sophisticated detection tools, user awareness, enhanced incident response plans, and cooperation on an international level.

### A. *Advantages:*

1) Comprehensive Coverage of Ransomware Types: Many papers provided detailed explanations of various ransomware types (e.g., Crypto Ransomware, Locker Ransomware, RaaS). This helps in understanding their characteristics and attack methods.
2) Analysis of Detection Techniques: The research papers extensively discussed different detection techniques, including static, dynamic, and hybrid analysis. Advanced methods like behavior-based monitoring, machine learning, and AI-driven detection were also covered[3].
3) Use of Real-World Case Studies: Several documents provided real-world case studies like WannaCry and Petya attacks to demonstrate the impact and mitigation strategies for ransomware.
4) Identification of Evasion Techniques: Many papers discussed evasion techniques like obfuscation, encryption, and API exploitation, providing insights into how attackers bypass traditional detection tools.
5) Recommendations for Future Research: Papers proposed future research directions, including developing automated incident response systems and improving zero-day detection techniques. This guidance is valuable for cybersecurity experts and researchers.

### B. *Limitations:*

1) Limited Focus on Mobile Ransomware: Although mobile malware was mentioned, there was limited in-depth analysis of mobile ransomware and IoT-targeted attacks in some documents. Considering the growing use of mobile devices, this is a gap.
2) Generalized Defense Strategies: Some papers offered broad recommendations without providing specific, implementable steps for different industries or organization sizes. More tailored strategies could enhance practical application.
3) Outdated Data in Some Papers: Some references and data points (e.g., older statistics or case studies from early 2010s) may no longer reflect the current cybersecurity landscape. Given the rapid evolution of ransomware, continuous updates are essential.
4) High-Level Discussions Without Technical Depth: Several papers lacked in-depth technical discussions of newer detection methods like AI-driven anomaly detection or memory forensics. More technical details on model architectures and algorithms would benefit developers and researchers.
5) Limited Discussion of International Regulations: While some papers mentioned international collaboration and legal frameworks, most did not delve deeply into existing regulations, cross-border challenges, or policy recommendations.

## IV. CONCLUSION

Ransomware and mobile malware are still constantly evolving, proving to be formidable challenges to cybersecurity. Although advancements in behavior-based detection, pre-encryption algorithms, and memory forensics have enhanced the detection rate, zero-day ransomware is still hard to tackle [14],[29]. AI-powered models and response automation systems bring promise for enhanced mitigation and threat detection in the future [3],[18].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The proactive measures of tools such as PayBreak reflect encouraging defense measures for file recovery after an attack [4]. Further, extending the application of honeypot technologies can assist in misleading attackers and safeguarding important assets [20]. In order to boost cybersecurity defenses, combining sophisticated detection mechanisms with socio-technical solutions is crucial in mitigating the effects of ransomware [12].

User training and awareness are vital in building resilience against ransomware attacks [5]. User training on phishing, social engineering techniques, and safe behavior can minimize vulnerabilities. Additionally, the necessity for international cooperation and regulation has become more urgent than ever to counter the globalized nature of ransomware attacks[10],[11].

There needs to be more cooperation among private organizations and government organizations for building strong countermeasures[8] The regulatory guidelines need to address enhancing cross-border cooperation and streamlining responses to ransomware attacks [30].

Subsequent research should focus on augmenting AI-based anomaly detection, incident response systems, and lowering false positive rates for ransomware detection [2],[21]. Organizations can better shield themselves against the continually evolving world of ransomware attacks by using a multi-layered method that encompasses technical and non-technical safeguards[22],[25],[31].

Through ongoing improvement, user training, and international coordination, cybersecurity practitioners can build better defenses against the ongoing threat of ransomware.

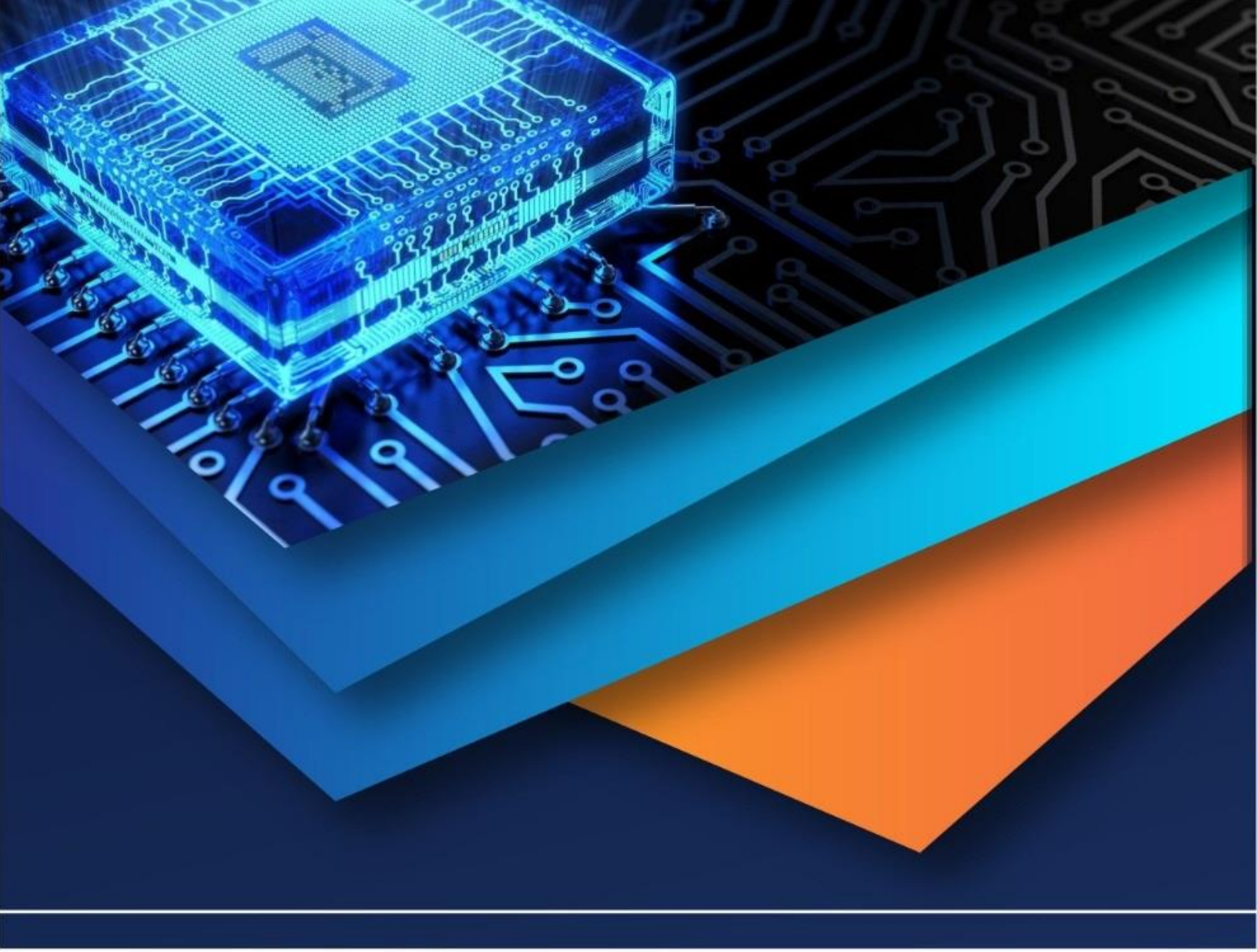
## REFERENCES

[1] Zheng, N. Dellarocca, N. Andronio, S. Zanero, and F. Maggi, “GreatEatlon: Fast, Static Detection of Mobile Ransomware.”
[2] S. Sen, E. Aydogan, and A. I. Aysan, “Coevolution of Mobile Malware and Anti-Malware.”
[3] A. Shabtai, L. Tenenboim-Chekina, D. Mimran, L. Rokach, B. Shapira, and Y. Elovici, “Mobile malware detection through analysis of deviations in application network behavior,” Comput Secur, vol. 43, pp. 1–18, 2014, doi: 10.1016/j.cose.2014.02.009.
[4] E. Kolodenker, W. Koch, G. Stringhini, and M. Egele, “PayBreak : Defense against cryptographic ransomware,” in ASIA CCS 2017 - Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security, Association for Computing Machinery, Inc, Apr. 2017, pp. 599–611. doi: 10.1145/3052973.3053035.
[5] J. A. H. Silva, L. I. B. López, Á. L. V. Caraguay, and M. Hernández-álvarez, “A survey on situational awareness of ransomware attacks-detection and prevention parameters,” Remote Sens (Basel), vol. 11, no. 10, May 2019, doi: 10.3390/rs11101168.
[6] D. F. Sittig and H. Singh, “A socio-technical approach to preventing, Mitigating, and recovering from Ransomware attacks,” Appl Clin Inform, vol. 7, no. 2, pp. 624–632, Jun. 2016, doi: 10.4338/ACI-2016-04-SOA-0064.
[7] A. Qamar, A. Karim, and V. Chang, “MOBILE MALWARE ATTACKS: REVIEW, TAXONOMY & FUTURE DIRECTIONS.”
[8] [8] N. Sharma and R. Shanker, “Analysis of Ransomware Attack and Their Countermeasures: A Review,” in Proceedings of the International Conference on Electronics and Renewable Systems, ICEARS 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1877–1883. doi: 10.1109/ICEARS53579.2022.9751949.
[9] A. K. Muslim, D. Z. Mohd Dzulkifli, M. H. Nadhim, and R. H. Abdellah, “A Study of Ransomware Attacks: Evolution and Prevention,” Journal of Social Transformation and Regional Development, vol. 1, no. 1, Jun. 2019, doi: 10.30880/jstard.2019.01.01.003.
[10] H. Alshaikh, N. Ramadan, and H. A. Hefny, “Ransomware Prevention and Mitigation Techniques General Terms,” 2020.
[11] A. Alqahtani and F. T. Sheldon, “A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook,” Mar. 01, 2022, MDPI. doi: 10.3390/s22051837.
[12] M. Ashawa and S. Morris, “Analysis of Mobile Malware: A Systematic Review of Evolution and Infection Strategies,” Journal of Information Security and Cybercrimes Research, vol. 4, no. 2, pp. 103–131, Dec. 2021, doi: 10.26735/krvi8434.
[13] A. L. Y. Ren, C. T. Liang, I. J. Hyug, S. N. Brohi, and N. Z. Jhanjhi, “A three-level ransomware detection and prevention mechanism,” EAI Endorsed Transactions on Energy Web, vol. 7, no. 26, 2020, doi: 10.4108/eai.13-7-2018.162691.
[14] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, “Prevention of crypto-ransomware using a pre-encryption detection algorithm,” Computers, vol. 8, no. 4, Dec. 2019, doi: 10.3390/computers8040079.
[15] V. Kouliaridis, K. Barmpatsalou, G. Kambourakis, and S. Chen, “A survey on mobile malware detection techniques,” IEICE Trans Inf Syst, vol. E103D, no. 2, pp. 204–211, 2020, doi: 10.1587/transinf.2019INI0003.
[16] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, “Evaluation of machine learning classifiers for mobile malware detection,” Soft comput, vol. 20, no. 1, pp. 343–357, Jan. 2016, doi: 10.1007/s00500-014-1511-6.
[17] N. Shah and M. Farik, “Ransomware-Threats, Vulnerabilities And Recommendations,” INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, vol. 6, no. 06, 2017, [Online]. Available: www.ijstr.org
[18] W. Z. A. Zakaria, M. F. Abdollah, O. Abdollah, and S. M. W. M. S.M.M, “Ransomware Behavior on Windows Endpoint: An Analysis,” Journal of Social Science and Humanities, vol. 6, no. 5, pp. 25–31, Oct. 2023, doi: 10.26666/rmp.jssh.2023.5.4.
[19] D. Paul Joseph and J. Norman, “A Review and Analysis of Ransomware Using Memory Forensics and Its Tools,” in Smart Innovation, Systems and Technologies, Springer, 2020, pp. 505–514. doi: 10.1007/978-981-13-9282-5_48.
[20] R. Moussaileb, R. Navas, and N. Cuppens, “Watch Out! Doxware on The Way,” 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212620308206
[21] M. Hirano and R. Kobayashi, “Machine Learning-based Ransomware Detection Using Low-level Memory Access Patterns Obtained From Live-forensic Hypervisor,” May 2022, doi: 10.1109/CSR54599.2022.9850340.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[22] F. Teichmann, "Ransomware attacks in the context of generative artificial intelligence—an experimental study," International Cybersecurity Law Review, vol. 4, no. 4, pp. 399–414, Dec. 2023, doi: 10.1365/s43439-023-00094-x.
[23] T. Yan Lin and M. Fadli, "Study on Prevention and Solution of Ransomware Attack."
[24] John Oluwafemi Ogun, "Advancements in automated malware analysis: evaluating the efficacy of open-source tools in detecting and mitigating emerging malware threats to US businesses," International Journal of Science and Research Archive, vol. 12, no. 2, pp. 1958–1964, Aug. 2024, doi: 10.30574/ijsra.2024.12.2.1488.
[25] L. Y. Connolly and D. S. Wall, "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures," Comput Secur, vol. 87, Nov. 2019, doi: 10.1016/j.cose.2019.101568.
[26] X. Luo and Q. Liao, "Awareness education as the key to ransomware prevention," Information Systems Security, vol. 16, no. 4, pp. 195–202, 2007, doi: 10.1080/10658980701576412.
[27] V. Ramteke and N. Gupta, "A study on Defacing Ransomware: Are we aware and ready?," 2021. [Online]. Available: https://www.researchgate.net/publication/353878947
[28] D. Hinderaker, M. Olsvik, D. Sarjomaa, S. Skylstad, and L. E. Pedersen, "Exploring Destructive Malware: A Practical Approach to Wiper Malware Developing wiper malware to identify weaknesses and improve security in Windows systems Bachelor's thesis in Digital Infrastructure and Cybersecurity Supervisor: Eigil Obrestad and," 2024.
[29] A. Arabo, R. Dijoux, T. Poulain, and G. Chevalier, "Detecting ransomware using process behavior analysis," in Procedia Computer Science, Elsevier B.V., 2020, pp. 289–296. doi: 10.1016/j.procs.2020.02.249.
[30] J. A. Gómez Hernández, P. García Teodoro, R. Magán Carrión, and R. Rodríguez Gómez, "Crypto-Ransomware: A Revision of the State of the Art, Advances and Challenges," Nov. 01, 2023, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/electronics12214494.
[31] U. Tariq, I. Ullah, M. Yousuf Uddin, and S. J. Kwon, "An Effective Self-Configurable Ransomware Prevention Technique for IoMT," Sensors, vol. 22, no. 21, Nov. 2022, doi: 10.3390/s22218516.
[32] M. Alam, S. Sinha, S. Bhattacharya, S. Dutta, D. Mukhopadhyay, and A. Chattopadhyay, "RAPPER: Ransomware Prevention via Performance Counters," Apr. 2020, [Online]. Available: http://arxiv.org/abs/2004.01712
[33] S. Haque, Z. Eberhart, A. Bansal, and C. McMillan, "Semantic Similarity Metrics for Evaluating Source Code Summarization," in IEEE International Conference on Program Comprehension, IEEE Computer Society, 2022, pp. 36–47. doi: 10.1145/nnnnnnn.nnnnnnn.
[34] H. Hangaard, H. M. Rånes, M. Staveland, and L. E. Pedersen, "Recovery Solutions for Ransomware and Wiper Attacks in Large, Heterogeneous IT Infrastructures Bachelor's thesis in Digital Infrastructure and Cyber Security Supervisor: Eigil Obrestad Co-supervisor," 2024.
[35] M. Conti, A. Gangwal, and S. Ruj, "On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective," Apr. 2018, doi: 10.1016/j.cose.2018.08.008.
[36] Kumari, M. Z. A. Bhuiyan, J. Namdeo, S. Kanaujia, R. Amin, and S. Vollala, "Ransomware Attack Protection: A Cryptographic Approach," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer Verlag, 2019, pp. 15–25. doi: 10.1007/978-3-030-24907-6_2.
[37] C. Seifert, J. W. Stokes, C. Colcernian, J. C. Platt, and L. Lu, "ROBUST SCAREWARE IMAGE DETECTION."
[38] A. Tandon and A. Nayyar, "A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat," in Advances in Intelligent Systems and Computing, vol. 839, Springer Verlag, 2019, pp. 403–420. doi: 10.1007/978-981-13-1274-8_31.
[39] M. Anghel and A. Racautanu, "A note on different types of ransomware attacks."
[40] P. O'Kane, S. Sezer, and D. Carlin, "Evolution of ransomware," IET Networks, vol. 7, no. 5, pp. 321–327, Sep. 2018, doi: 10.1049/iet-net.2017.0207.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)