

Leveraging Behavioral Analysis and Machine Learning for Effective Ransomware Mitigation

Dorina-Mariana DAMIAN

Faculty of Electronics, Telecommunications, and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest,
Romania
dorina.damian@stud.etti.upb.ro

Abstract

Ransomware attacks pose significant threats to individuals and organizations, causing data loss, financial damage, and operational disruptions. Traditional antivirus solutions often fail to detect new ransomware variants. This article proposes a proactive approach to ransomware mitigation by integrating behavioral analysis and machine learning algorithms into software solutions. By analyzing the behavior of files and processes, our solution aims to detect and prevent ransomware attacks before they can cause significant harm, thus protecting critical data and systems. By continuously monitoring process behaviors and employing anomaly detection techniques, this approach dynamically identifies and terminates malicious processes without relying on predefined signatures or process names. This paper details the implementation, working principles, and effectiveness of this solution through comprehensive analysis.

Index terms: anomaly detection techniques, behavioral analysis, critical data, Machine Learning, ransomware

References

- [1]. R. Naydenov, S. Garcia, A. Gomaa, V. Valeros, A. Malatras, E. Tsekmezoglou, "ENISA threat landscape for ransomware attacks", ENISA, 2022.
- [2]. M. Aggarwal, "Ransomware Attack: An Evolving Targeted Threat", 2023.
- [3]. B.T. Magar, "Cactus Ransomware: How it works and how to respond? Emerging Threats Protection Report," Emerging Threats Protection Report, Available: <https://www.logpoint.com/wp-content/uploads/2023/12/et-cactus-4-12.pdf>.
- [4]. F.T. Liu, K.M. Ting, Z.-H. Zhou, "Isolation Forest", IEEE International Conference on Data Mining, 2009.
- [5]. S. Hariri, M. Carrasco, R. J. Brunner, "Extended Isolation Forest", IEEE Transactions on Knowledge and Data Engineering, vol. 33, no. 4, April 2021.

- [6]. D. Mohamed, A. El-Kilany, H. M. O. Mokhtar, "A Hybrid Model for Documents Representation," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 3, pp. 317-324, 2021.