IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 1, November 2023

Malicious Application Detection in Windows Using Machine Learning

Sanskar Patil[1], Mrs. Swati Jakkan[2], Sumit Pawar[3], Prerana Gholve[4], Aditi Kunkekar[5]

Faculty, Department of Computer Engineering [2]

Student, Department of Computer Engineering [1,3,4,5]

RMD Sinhgad School of Engineering, SPPU, Pune, India

Abstract: *As the proliferation of digital technology continues, the threat landscape for Windows operating systems has become increasingly complex. Malicious applications, including viruses, ransomware, and spyware, pose a significant risk to both individuals and organizations. To combat this growing threat, there is a pressing need for effective and efficient methods for detecting and mitigating malicious applications. This research paper presents an innovative approach to Malicious Application Detection in Windows using Support Vector Machine (SVM) algorithms. SVM is a powerful machine learning technique that has been successfully applied in various classification tasks, including malware detection. The primary objective of this study is to develop a robust and reliable system that can differentiate between benign and malicious applications in a Windows environment. We start by collecting a comprehensive dataset of Windows applications, comprising both legitimate and malicious software samples. Feature extraction techniques are employed to convert the application data into a suitable format for SVM analysis. These features may include file attributes, system call sequences, and behaviour analysis metrics.*

Keywords: Malicious Application Detection, Machine Learning Based Detecting, Windows Malware Detection, Windows Security.

REFERENCES

[1]. Mahmoud Alfadel, Diego Elias Costa, and Emad Shihab. 2021. Empirical Analysis of Security Vulnerabilities in Python Packages. In 2021 IEEE International Conference on Software Analysis, Evolutionand Reengineering(SANER).446–457. https://doi.org/10.1109/SANER50967.2021.00048

[2]. Vitalii Avdiienko, Konstantin Kuznetsov, Alessandra Gorla, Andreas Zeller, Steven Arzt, Siegfried Rasthofer, and Eric Bodden. 2015. Mining Apps for Abnormal Usage of Sensitive Data. In 2015 IEEE/ACM 37th IEEE International Conference on Software Engineering, Vol. 1. 426–436. https://doi.org/10.1109/ICSE.2015.61

[3]. Aadesh Bagmar, Josiah Wedgwood, Dave Levin, and Jim Purtilo. 2021. I Know What You Imported Last Summer: A study of security threats in the Python ecosystem. CoRR abs/2102.06301 (2021). arXiv:2102.06301 https://arxiv.org/abs/ 2102.06301

[4]. Adam Baldwin. 2019. Plot to steal cryptocurrency foiled by the npm security team. https://blog.npmjs.org/post/185397814280/plotto-steal-cryptocurrencyfoiled-by-the-npm.

[5]. Alex Birsan. 2021. Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies. https://medium.com/@alex.birsan/ dependency-confusion-4a5d60fec610

[6]. Mengdi Huai, Di Wang, Chenglin Miao, and Aidong Zhang. 2020. TowardsInterpretationofPairwiseLearning. In Thirty-fourth AAAI Conference on Artificial Intelligence.

[7]. Sandy Huang, Nicolas Papernot, Ian Goodfellow, Yan Duan, and PieterAbbeel. 2017. Adversarial attacks on neural network policies. arXiv preprint arXiv:1702.02284 (2017).

[8]. L´eonardHussenot, Matthieu Geist, and Olivier Pietquin. 2019. Targeted Attacks on Deep Reinforcement Learning Agents through Adversarial Observations. arXiv preprint arXiv:1905.12282 (2019).

IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 1, November 2023

[9]. Rahul Iyer, Yuezhang Li, Huao Li, Michael Lewis, Ramitha Sundar, and Katia Sycara. 2018. Transparency and explanation in deep reinforcementlearningneuralnetworks. InProc. OftheAAAI/ACM Conference on AI, Ethics, and Society.

[10]. Michael Kearns and Satinder Singh. 2002. Near-Optimal Reinforcement Learning in Polynomial Time. Mach. Learn. (2002).