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: 7.53
Volume 4, Issue 1, May 2024

Detection of Malware Trojans in Software using Machine Learning

Prof. Aravinda Thejas Chandra[1], Ms. Sindhu R[2], Ms. Spoorthi H[3], Ms. Prerana R P[4], Ms. V Bhavana[5]
Associate Professor, Department of Information Science and Engineering[1]
Students, Department of Information Science and Engineering[2,3,4,5]
S J C Institute of Technology, Chikballapur, India
thejaschandra@gmail.com, sindhu.17r@gmail.com, spoorthigowdah007@gmail.com
ppreranarp@gmail.com, bhavnamurthy227@gmail.com

Abstract: *As the prevalence of malicious software, particularly trojans, continues to pose a significant threat to the integrity and security of computer systems, the need for effective detection mechanisms becomes paramount. This research presents a comprehensive approach to the detection of malware trojans in software, leveraging advanced techniques from machine learning, behavior analysis, and signature-based methods. The proposed system employs a hybrid model that combines the strengths of static and dynamic analysis to enhance detection accuracy. Static analysis focuses on examining code structures and identifying potential indicators of trojans presence, while dynamic analysis observes the software's behavior during execution to uncover malicious activities that may evade static analysis. Machine learning algorithms play a crucial role in training the detection system to recognize patterns indicative of trojans behavior. The model is trained on a diverse dataset of both benign and malicious software samples, enabling it to adapt and evolve to emerging threats. Feature extraction techniques are applied to capture the essential characteristics of trojans, contributing to the model's ability to generalize effectively. Furthermore, the system incorporates a signature-based approach, utilizing known patterns and signatures of trojans to quickly identify and mitigate known threats. Regular updates of signature databases ensure the system remains current and capable of detecting the latest trojan variants. To evaluate the effectiveness of the proposed approach, extensive testing is conducted on a variety of software samples, including both well-established trojans and newly emerging threats. The results demonstrate the system's robustness and efficiency in detecting trojan activity, with a low false positive rate. In conclusion, the presented research provides a holistic and adaptive solution for the detection of malware trojans in software. By combining static and dynamic analysis with machine learning and signature-based methods, the proposed system offers a versatile defense against the evolving landscape of trojan threats, contributing to the overall cybersecurity resilience of computer systems..*

Keywords: Trojans, Malware, cybersecurity, static analysis, dynamic analysis , signature based approach, Random forest, machine learning algorithms, efficiency, resilence

REFERENCES

[1] Mohd Faizal, Izham Jaya, Zahian Ismail, Ahmad Firdaus “Trojan Detection System Using Machine Learning Approach”, August 2022,Indonesian Journal of Information Systems.
[2] Yu-Feng Liu, Li-Wei Zhang, Jain Liang, Sheng Qu, Zhi-Qiang Ni “Detecting Trojan Horses Based On System Behaviour Using Machine Learning Method” , July 2021 , Proceedings of the Ninth International Conference on Machine Learning and Cybernetics.
[3] Ma Zhongrui, Huang Yuanyuan, Lu Jiazhong , “Trojan Traffic Detection Based On Machine Learning”, 2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing .
[4]Mohammed Altaiy, Incilay Yildiz,Bahadir Ucan ,“Trojan Traffic Detection Based On Machine Learning”, Aurum Journal Of Engineering Systems And Architecture Volume 7, No 1, 2023 .

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: 7.53
Volume 4, Issue 1, May 2024

[5] Yamjala Supriya, Dammu Sowjanya, Gautam Kumar, Deepali Yadav, Devarakonda lakshmi kameshwari, Malware Detection Techniques: A Survey", sixth international Conference on parallel, distributed and grid computing, 2020.
[6] "A Survey on Malware Detection Using Machine Learning Techniques: Classification, Features and Datasets" by Raja Vikramaditya Singh Chandel and B. B. Gupta (2019).
[7]"Machine Learning Techniques for Android Malware Detection: A Survey" by Arati M. Dixit and Atul S. Auti (2018).
[8]"Machine Learning Based Android MalwareDetection: A Survey" by Z. Jin, W. Wei, and K. W. Hamlen (2018).
[9]"Android Malware Detection Using Machine Learning Techniques" by R. Kharkar, M. Goswami, and M. Bahirat (2017) .
[10]"Android Malware Detection Using Machine Learning Techniques" by S. V. Selvi and G. Hemalatha (2018).
[11]Thimbleby H, Anderson S, Cairns P. A Frameworkfor Modelling Trojans and Computer Virus Infection[M]. Computer Journal, 1998, 41(7): 444-458,1998 .
[12]Wang, R., Wang, W., Gong, X., Que, X., & Ma, J. (2010, April). A Real-Time Video Stream Key FrameIdentification Algorithm for QoS[M]. In Multimedia and Information Technology (MMIT), 2010 Second International Conference on (Vol. 1, pp. 115-118). IEEE, 2010 .
[13]Christodorescu M, Jha S, Seshia S A, et al. Semanticsaware malware detection[M]. In: Security and Privacy, Oakland:IEEE, 2005. 32-46,2005 .
[14] Wu Xianda. Remote control Trojan detection model based on abnormal network behavior [D]. Beijing University of Technology, 2018 .
[15]Yang Weijun, Zhang Shu, Hu Guangjun. Trojan detection method based on attack tree model[J]. Information Network Security, 2011(09): 170-172.
[16]Li Jianbin. Trojan detection technology based on traffic [D]. University of Electronic Science and Technology of China, 2014 .
[17] Wang Zhanhao. Research on Trojan Attackand Prevention Technology [J]. Shanghai Jiaotong University, 2007 .