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

Mobile Botnet Detection A Machine Learning Approach using SVM

Pratik Dattatray Ambawale, Varun Vijay Wagh and Prof. Tejaswini Mali
Department of Artificial Intelligence & Data Science
ISBM College of Engineering, Nande, Pune, India
ambawalepratik@gmail.com,varunpatil0066@gmail.com
varunpatil0066@gmail.com , teju314@gmail.com

Abstract: *The security and privacy of smartphone users are seriously threatened by mobile botnets, which allow malevolent actors to carry out a variety of illegal actions, such as DDoS attacks, data theft, and resource exploitation. These mobile botnets are becoming more and more sophisticated, making it difficult to detect them with conventional signature-based and heuristic methods. This study proposes a machine learning-based method for mobile botnet detection that makes use of Support Vector Machines (SVM).The study focuses on behavioural feature extraction from mobile device system-level data and network traffic. The SVM model is used for classification once feature selection techniques have been used to select the most pertinent and discriminative attributes. The SVM model, making use of its capacity to manage nonlinear classification and high-dimensional data.Tests carried out on a variety of network traffic and system behaviour datasets gathered from mobile devices show encouraging outcomes for the detection of botnets. Compared to conventional detection techniques, the SVM classifier outperforms them in identifying mobile botnet activities with a high degree of accuracy, precision, and recall.The suggested SVM-based method improves mobile device security by offering a flexible and successful mobile botnet detection solution. The results of this study open the door to the development of strong and durable mobile security systems by providing insights into the proactive identification and mitigation of mobile botnet threats through the use of machine learning techniques.*

Keywords: Mobile Botnets, Machine Learning, Support Vector Machines (SVM), Botnet Detection, Smartphone Security, Behavioural Analysis, Network Traffic Analysis.

REFERENCES

[1]. M. Eslahi, M. Yousefi, M. V. Naseri, Y. M. Yussof, N. M. Tahir and H. Hashim, "Cooperative network behaviour analysis model for mobile Botnet detection," *2016 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, Penang, Malaysia, 2016, pp. 107-112, doi: 10.1109/ISCAIE.2016.7575046.

[2]. Suleiman Y. Yerima, Mohammed K. Alzaylaee"Mobile Botnet Detection: A Deep Learning Approach Using Convolutional Neural Networks". https://arxiv.org/abs/2007.00263, https://doi.org/10.48550/arXiv.2007.00263

[3]. Milan Oulehla, Zuzana KomínkováOplatková,DavidMalanik(2016). "Detection of Mobile Botnets using Neural-Networks". FTC 2016 - Future Technologies Conference 2016 6-7 December 2016 | San Francisco, United States

[4]. S. Anwar, J. M. Zain, Z. Inayat, R. U. Haq, A. Karim and A. N. Jabir, "A static approach towards mobile botnet detection," 2016 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, 2016, pp. 563-567, doi: 10.1109/ICED.2016.7804708.

[5]. Wadi' Hijawi, Ja'farAlqatawna, Hossam Faris. "Toward a Detection Framework for Android Botnet",2017 International Conference on New Trends in Computing Sciences, http://dx.doi.org/10.1109/ICTCS.2017.48

[6]. V. G. T. da Costa, S. Barbon, R. S. Miani, J. J. P. C. Rodrigues and B. B. Zarpelão, "Detecting mobile botnets through machine learning and system calls analysis," 2017 IEEE International Conference on Communications (ICC), Paris, France, 2017, pp. 1-6, doi: 10.1109/ICC.2017.7997390.

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