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 11, May 2023

Botnet Detection using SVM Algorithm

Yash Birdavade[1], Ram Todkar[2], Aashish Walke[3] ,Sambhaji Shinde[4], Dr. Neelam A Kumar[5]
Students, Department of Computer Engineering[1,2,3,4]
Professor, Department of Computer Engineering[5]
Shree Ramchandra College of Engineering Pune, Maharashtra, India

Abstract: *The proliferation of mobile devices and their increasing connectivity have led to the emergence of mobile botnets, posing a significant threat to the security and privacy of users. Mobile botnets are networks of compromised mobile devices controlled by malicious actors for various illicit activities, including spamming, distributed denial of service (DDoS) attacks, and information theft. Traditional security measures are often insufficient to detect and mitigate mobile botnet attacks due to their dynamic and stealthy nature. This project proposes a novel approach for mobile botnet detection using machine learning techniques. The objective is to develop a robust and accurate system that can identify and classify mobile devices participating in botnets based on their behavioural patterns and network activities.*

Keywords: Machine Learning, SVM Algorithm, Mobile Botnet

REFERENCES

[1]. M. EslahiC.Kang-yu et al.in To Study different algorithms of Machine Learning to Detect Mobile Botnets.
[2]. Falguni Ghatkar, Sakshi kharche, Priyanka Doifode, Jagruti Khairnar, Prof. Neelam Kumar," To Study Different
[3]. Types of Supervised Learning Algorithm" May 2023, International Journal of Advanced Research in Science, Communication and Technology.
[4]. Zubail Abdullah, Madihah Mohd Saudi et al.in ABC: Android botnet classification Using feature selection and classification algorithms.
[5]. Dr. K. Muthu Manickam Dr. T. Sengolrajan Smartphone Based Botnet Detection using Behavioral Analysis.
[6]. Suleiman Y. Yerima and Mohammed K. Alzaylaee Mobile Botnet Detection: A Deep Learning Approach Using Convolutional Neural Networks.
[7]. ArashMahboubi, SeyitCamtepe Stochastic Modeling of IoT Botnet Spread: A Short Survey on Mobile Malware.
[8]. S. Y. Yerima and S. Khan "Longitudinal PerfomanceAnlaysis of Machine Learning based Android Malware Detectors" 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), IEEE.
[9]. Kadir, A.F.A., Stakhanova, N., Ghorbani, A.A., 2015. Android botnets: What urls are telling us, in: International Conference on Network and System Security, Springer. pp. 78–91.
[10]. ISCX Android botnet dataset. Available from https://www.unb.ca/cic/ datasets/androidbotnet.html. [Accessed 03/03/2020]
[11]. M. Eslahi, R. Salleh, and N. B. Anuar, "Bots and botnets: An overview of characteristics, detection and challenges," in Proceedings of the IEEE International Conference on Control System, Computing and Engineering (ICCSCE), 2012, pp. 349-354.
[12]. J. Dae-il, C. Kang-yu, K. Minsoo, J. Hyun-chul, and N. Bong-Nam, "Evasion technique and detection of malicious botnet," in Proceedings of the Internet Technology and Secured Transactions (ICITST), 2010 International Conference for, 2010, pp. 1-5.
[13]. Z. Yajin and J. Xuxian, "Dissecting Android Malware: Characterization and Evolution," in Proceedings of the Symposium on Security and Privacy (SP), 2012, pp. 95-109.
[14]. M. Eslahi, M. Rohmad, H. Nilsaz, M. Var Naseri, N. Tahir, and H.Hashim, "Periodicity classification of

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 11, May 2023

[15]. HTTP traffic to detect HTTP Botnets," in Proceedings of the Computer Applications Industrial Electronics (ISCAIE), 2015

[16]. T. Strazzere and T. Wyatt, "Geinimi trojan technical teardown," Lookout Mobile Security, 2011.

[17]. Gu, R. Perdisci, J. Zhang, and W. Lee, "BotMiner: clustering analysis of network traffic for protocol- and structure-independent botnet detection,"in Proceedings of the 17th conference on Security symposium, San Jose, CA, 2008, pp. 139-154.

[18]. M. Eslahi, R. Salleh, and N. B. Anuar, "MoBots: A new generation of botnets on mobile devices and networks," in Proceedings of the IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE), 2012, pp. 262- 266.