IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

A Solution to Detecting Botnets using Convolutional Neural Networks and Support Vector Machine Algorithms

Vipul Jha[1], Omkar Katule[2], Tanvi Bajad[3], Shreyas Agadi[4], Priyanka Bendale[5]
Students, Department of Computer Engineering[1,2,3,4]
Faculty, Department of Computer Engineering[5]
Sinhgad College of Engineering, Pune, Maharashtra, India

Abstract: *A botnet is an Internet-connected network of devices and nodes that spread malware software, such as Trojan horses, viruses, and worms. Recently, numerous approaches for detecting and combating mobile malware have been developed. Our model, on the other hand, is distinct from previous models. We're using a dataset that we found on the Kaggle website. The findings we obtained were obtained using machine learning techniques such as CNN and SVM. We have a range of attack or non-attack scenarios, as well as any subtypes that may occur. The proposed system is a web-based tool that predicts App/URL botnets with high accuracy.*

Keywords: Convolutional Neural Network, Support Vector Machine, Botnet, Attacks, Web application

REFERENCES

[1]. Sarnsuwan, N. Charnsripinyo, C., Wattanapongsakorn, N., "A new approach for internet worm detection and classification", In 6th International Conference on Networked Computing, 2012.
[2]. Shanthi, K., Seenivasan, D., "Detection of botnet by analyzing network traffic flow characteristics using open-source tools". In Proceedings of the 9th IEEE International Conference on Intelligent Systems and Control (ISCO '15), India, 2015
[3]. Kirubavathi, G., Anitha, R., "Botnet detection via mining of traffic flow characteristics", Computers and Electrical Engineering, 2016
[4]. Zhang, J., Perdisci, R., Lee, W., Luo, X., Sarfraz, U., "Building a scalable system for stealthy P2Pbotnet detection", IEEE Transactions on Information Forensics and Security, 2015
[5]. Chen, R., Niu, W., Zhang, X., Zhuo, Z., Lv, F., "An Effective conversation-based botnet detection method. Mathematical Problems in Engineering", 2017
[6]. Lashkari, A., Draper-Gil, G., Mamun, M., Ghorbani, "Characterization of traffic using time-based features". In the proceeding of the 3rd International Conference on Information System Security and Privacy, 2017
[7]. H. Chen, S. Wang, J. Li, and Y. Li, "A hybrid of artificial fish swarm algorithm and particle swarm optimization for feedforward neural network training", in Proceedings of the International Conference on Intelligent Systems and Knowledge Engineering, 2007.
[8]. J. L. Liao and K. C. Lin, "A Study of Feature Selection Integrated with Back- Propagation Network for Botnet Detection", National Chung Hsing University, Taichung, Taiwan, 2013.
[9]. Ahmad Karim, Rosli Salleh and Syed Adeel Ali Shah "DeDroid: A Mobile Botnet Detection Approach Based on Static Analysis", IEEE
[10]. Vikramajeet Khatri, "Mobile Guard Demo", IEEE Zubaile Abdullah and Madihah Mohd Saudi "Mobile Botnet Detection: Proof of Concept", IEEE
[11]. AV-Comparatives Security Survey, 2019, Security Survey2019en.pdf
[12]. Amro, B.: "Personal Mobile Malware Guard PMMG: a mobile malware detection technique based on user's preferences". IJCSNS International Journal of Computer Science and Network Security, Vol. 18, No. 1, pp. 18–24 (2018)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, May 2022
Impact Factor: 6.252

[13]. Idrees, F., Rajarajan, M., Conti, M., Chen, T., Rahulamathavan, Y.: "Pindroid: a novel android malware detection system using ensemble learning methods". Computers Security, Vol. 68, pp. 36–46 (2017)

[14]. Chaba, S., Kumar, R., Pant, R., Dave, M.: "Malware Detection Approach for Android systems Using System Call Logs", arXiv preprint arXiv:1709.0880 (2017)

[15]. McLaughlin, N., Martinez del Rincon, J., Kang, B, et al.: "Deep android malware detection". In Proc. of the Seventh ACM on Conference on Data and Application Security and Privacy, pp. 301–308 (2017)