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 14, May 2023

An Advanced Method for the Detection of Botnet Traffic using an Randomized Data Partitioned Learning Model

Akhila S Pillai[1] and Sindhu Daniel[2]
Student, Department of Computer Applications[1]
Assistant Professor, Department of computer Applications[2]
Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India

Abstract: *The proposed system," AN ADVANCED METHOD FOR THE DETECTION OF BOTNET TRAFFIC USING RDPLM," aims to identify botnet attacks and provide users with information about whether or not their system has been hacked by an attacker. Online attacks are on the rise right now. Particularly system attacks have become increasingly common lately. This method helps in locating botnets or malicious websites. The term "botnet" refers to a group of infected computers that can be controlled by an attacker. A botnet's computers are all referred to as zombies. Here, we apply a process to find the connections and decide whether to continue it or not. We are using a process to find the connections and decide whether to continue or not. We are using machine learning in this system to identify each botnet so that we can stop them or know their links. In order to start a botnet, a hacker must first attack a single system or piece of hardware with malware, converting it into a bot. This can be accomplished in a number of ways that are invisible to the user. The hacker's task is then effectively completed. The software is made to automatically attack more and more devices after infecting just one, resulting in the creation of more bots and the formation of a cybercrime. We employed the Random Forest, Naive Byes, SVM, and Decision Tree algorithms in this system. Finding a hyperplane in an N-dimensional space that clearly classifies the data.*

Keywords*:* Random Forest, Naïve Byes, SVM, Decision Tree.

REFERENCES

[1] M. Roesch, "Snort—Lightweight intrusion detection for networks," in Proc. USENIX LISA, Nov. 1999.
[2] J. Zhang and M. Zulkernine, "Network intrusion detection using random forests," in Proc. PST, St. Andrews, NB, Canada, 2005, pp. 53–61.
[3] M. Abu Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "A multifaceted approach to understanding the botnet phenomenon," in Proc. 6th ACM SIGCOMM Conf. Internet Meas., New York, NY, USA, 2006. pp. 41–52.
[4] B. Al-Duwairi and L. Al-Ebbini, "BotDigger: A fuzzy inference system for botnet detection," in Proc. 5th Int. Conf. Internet Monitor. Prot. (ICIMP), Barcelona, Spain, 2010, pp. 16–2.
[5] A support vector machine-based naive Bayes algorithm for spam filtering December 2016 DOI: 10.1109/PCCC.2016.7820655 Conference: 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC).
[6]Koli, Manoj S., and Manik K. Chavan. "An advanced method for detection of botnet traffic using intrusion detection