IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 3, April 2022

Review Paper on 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]

Guide, Department of Computer Engineering[5]

Sinhgad College of Engineering, Pune, Maharashtra, India

Abstract: *A botnet is a network of Internet-connected devices and nodes that transmit malware software, typically installed by Trojan horses, viruses and worms. Many methods for detecting or blocking mobile malware have recently been developed. However, our model differs from ones that have been developed earlier. We are working with a dataset we found on the Kaggle site. Machine learning techniques such as CNN and SVM have been used to derive the results we have achieved. We have a variety of cases that are labelled as attack or not attack, as well as any subtypes that may exist. The suggested system is a web-based tool that provides reliable App/URL botnet prediction.*

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

I. Introduction

The term ‘botnet’ is derived from the terms "roBOT NETwork", referring to a victim being controlled by an attacker. Botnet usage has risen considerably in recent years. Botnets are a collection of computers connected to the internet with a significant amount of bandwidth and computational capacity. The attacker, often known as the botmaster, has the ability to command massive networks of botnets from various locations in order to initiate attacks. Distributed denial of service (DDoS) attacks, email spam, key logging, and password cracking are all hallmarks of a botnet. Botnets are currently one of the most serious threats to the Internet. Botnets have a variety of elements that make them almost unique in terms of structure, capabilities, and technical implementation. A bot herder (or a botmaster), or more than one command and control servers, and multiple, perhaps in millions, controlled nodes are always present to control the bot. A botnet is a type of internet worm that consists of infected nodes that execute commands while attempting to avoid detection by antimalware software. The botmaster is the botnet's supreme commander. The service is currently under threat. In most cases, a client can only handle a portion of the botnet nodes. The client's instruction set is typically a subset of the full instruction set. In truth, the real attacker is whoever controls the botnet (the botmaster) at any particular time.

II. Literature Survey

Sarnsuwan et al. [1] proposed a technique to distinguish the malware by utilizing information mining, where it includes the utilization of information examination method for finding obscure information by substantial connections and examples in enormous informational indexes. These apparatuses can incorporate factual models, numerical calculations and AI strategies. So that, information mining contains more than gathering and overseeing information. Sarnsuwan et al. [22] utilized three information mining calculations that are C4.5 Decision Tree, Random Forest, and Bayesian organization. NBD [2-4] basically realizes the traffic network in the order and control expression of each botnet, taking into account the fact that the social qualities are unique in relation between two expressions. NBD centers generally inspect two kinds of organizational conduct: stream highlights and the pace of disappointment association. The calculations that rely upon utilized stream includes that incorporate the quantity of uplink and downlink of information bundles, the normal length of uplink and downlink of information parcels, the quantity of uplink and downlink, transmission bytes, the term season of information stream, the greatest length of downlink and uplink of information bundles, the all-out length of stacked information parcels in a stream, the pace of the length of information parcels in uplink and downlink, and the normal length

DOI: 10.48175/IJARSCT-3287

of downlink and uplink of information parcels. At present, analysts are adding brain organization and AI to NBD to recognize obscure botnet traffic network. Additionally, this strategy is a hot exploration point in the investigation of botnet traffic and location [5].

Lashkari et al. [6] ran the malicious malwares and innocuous applications on genuine phones, trying not to alter the actual runtime conduct of cutting-edge malware tests that can help identify the climate of the emulator. To get a thorough outline of our malware tests, Lashkari et al. [28] had made a particular situation for each malware classification. The framework approach likewise characterized three conditions of information assortment to beat the covertness of cutting-edge malware. The framework approach comprised of three phases.

In [7], the outcomes showed that the AFSA displayed astounding execution in work improvement, and the capability of applying the AFSA in streamlining issue were uncovered as well. Besides, in [8], the scientists proposed a kind of element selection and backspread network for botnet identification; nonetheless, utilizing an AFSA joined with an SVM classifier could yield prevalent execution. In this review, an arranged model was recommended joining an AFSA calculation and an SVM. The proposed technique was utilized to distinguish the basic highlights deciding the example of a botnet.

III. Problem Statement of System

With the increasing popularity of smartphones and Internet surfing, particularly those based on Android and other Websites, there has been a significant increase in the downloading and sharing of third-party programs and user-generated content, rendering handsets and systems vulnerable to numerous types of malwares. In terms of security and finances, a lot of research is needed in this subject. Malware producers or hackers, have found easier and profitable techniques to attack operating systems that are widely used, are open-source, and the ones that do not prevent or prohibit the installation of software from any harmful third-party source. We are developing a web-based application to overcome some of such problems and detect the bots.

IV. Implementation Details of Module

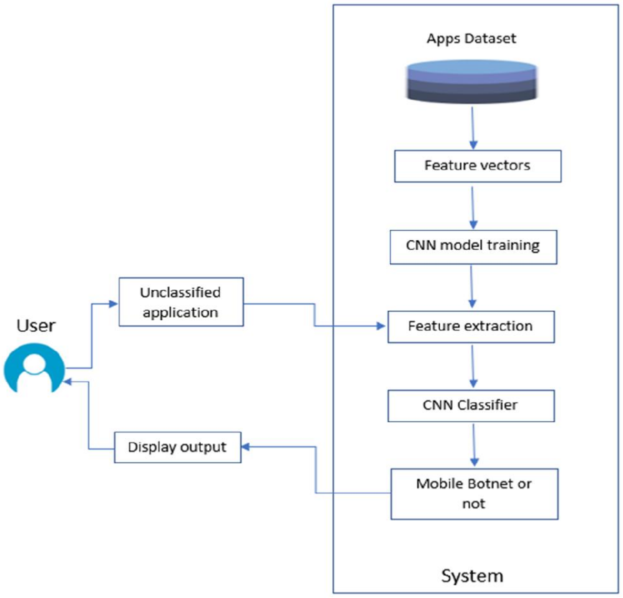

Figure: System Architecture

The proposed system contains following:

4.1 Pre-processing

The system will load the data, check for cleanliness, and then trim and clean given dataset for analysis. There might be instances where the data which has been collected might contain missing values, leading to inconsistency and inaccurate results. Hence, to prevent such inaccuracy, data needs to be pre-processed soas to improve the efficiency of the algorithm and to gain better results. This includes conversion of variables, and removing of any outliers present.

DOI: 10.48175/IJARSCT-3287

4.2 Building the Classification Model

Predicting the sentimental analysis by using supervised machine learning techniques, like SVM algorithm, makes the prediction model highly effective with the major reason being that it provides better results in classification problems.

4.3 Working

The web frontend contains HTML form where user enters the data/URL of apk file details. The web frontend uploads the input provided by the user and is then sent to the backend system. The script running in the backend retrieves the data passed by frontend. The backend process that data with the help of several techniques leading to various features being predicted, such as whether botnet is detected or not. The backend sends the data to frontend after the classification step and depending on the result, the system responds and the output is displayed to the user. Generating a pop-up window to alert the user in case botnet is detected, and sending a mail to the respective developer to inform of such botnets are some new features that have been added to this system

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)

[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)

DOI: 10.48175/IJARSCT-3287