MOBILE BOTNET DETECTION

Vishal Prabhakar Patare
Computer Engineering
Dy Patil College of Engineering
Ambi, Pune, India
vpatare22@gmail.com

Rajeshri Milind Bhole
Computer Engineering
Dy Patil College of Engineering
Ambi, Pune, India
rajeshrimbhole@gmail.com

Vishant Sharad Tambe
Computer Engineering
Dy Patil College of Engineering
Ambi, Pune, India
vishanttambe2001@gmail.com

Hitesh Gohad
Computer Engineering
Dy Patil College of Engineering
Ambi, Pune, India
hiteshgohad983441@gmail.com

Abstract— Now a days mobile has become tbe important aspect of persons life. Highly pervasive mobile operating systems are increasingly targeted for malware and botnet applications designed to turn mobile devices into bots that can be part of a larger botnet, they have become very common and therefore pose a serious threat that this botnet -Calls for more effective methods for detection on the android platform hence in this paper we present a deep learning approach for android botnet detection based on support vector machine. Botnets are fully integrated and optimized for mobile devices. The security of mobile devices is not designed to detect botnets and other threats. This allows botnets to infect machines and go unnoticed. In this paper, we propose an enhanced botnet detection technique called "Logdog" for mobile devices using log analysis. The effectiveness of this method has been demonstrated by experimentation on Android devices.

Keywords—, Botnet, video archives, Support Vector machine and Convolutional neural network, Python, etc.

I. INTRODUCTION

A botnet is a large number of devices on the Internet that are under the control of a malicious user or group of people called botmaster(s). It also has a Command and Control (CC) system that allows bots to take commands, receive updates, and send status updates to malicious humans while often using smartphones and other mobile devices to access online services on it is rarely extinguished, they provide a rich source of would-be bot-nets The term 'mobile botnet' therefore refers to a group of compromised smartphones and other mobile devices remotely controlled by botmasters using the CC method.Users are downloading an increasing number of mobile phone applications in response to advancements in smartphones. Botnet is actually the network of devices that are under control of botmaster. Since the Android operating system provides an open source environment, these applications are available from third parties on the Google Play Store and various other application stores. The Google Play Store is a collection of services that allow users to discover, install, and purchase applications from their Android devices or the web. Developers can easily reach Android application users through the Google Play Store. The Android mobile platform is becoming increasingly popular with an estimated 1.8 million applications in the official Google's Android Market, with over 25 billion downloads as of December 2015.

II. RELATED WORK

In a study by Qadir et al., the aim was to address the gap in the understanding of mobile botnets and their communication characteristics. Thus, they provided an in-depth analysis of Command and Control (C&C) and created the URL of the Android botnet. Combining static and dynamic analytics with visualization uncovered relationships between the analyzed botnet families, providing insight into each malicious infrastructure In the same study, a dataset of 1929 samples from 14 Android botnet families was compiled and released to the research community. This dataset is known as the ISCX Android botnet dataset and is available from. This paper and several previous works on Android botnets have used the full data set or a subset thereof to evaluate the proposed Android botnet detection techniques Anwar et al. proposed a static approach towards mobile botnet detection where they used MD5 hashes, permissions, broadcast clients and back.

Unlike most existing studies, our paper proposes a deep learning based Android botnet detection system, using convolutional neural networks. Also, unlike previous studies that only use app permissions, our system is based on 342 features that represent permissions, API calls, commands, additional files, and intents. Furthermore, different from the study in [9] that only used permutations, we do not transform the feature vectors into images before model training. Instead our feature vectors are used directly to train 1D SVM models. This makes our approach computationally less demanding

III. PROPOSED WORK

A. *Problem Defination*

In this project We Detect Botnet App. Botnet App means that some malware is installed through mobile in the App. That time you lose important mobile data. So we avoid All The loss. Our proposed botnet detection system is implemented as a SVM-based model, which is trained on app features to distinguish botnet apps from normal apps.

B. *Proposed System*

In this system an algorithm is devised for content based retrieval of video to give effective search results to E-learners. The methodology used is more efficient than the existing one. The main ingredients of this process are detected audio from video using NB algorithm within some time interval and accuracy of character set given as input to NLP algorithm for text extraction. Both of these algorithms give highly accurate results within less computation time. In future we plan to make use of more efficient and usable algorithms to separate audio from video, to extract text from audio and video segments and to divide video in multiple segments to choose key-frames among them. We can increase the number of nodes and analyse the performance.

IV. PROPOSED METHODOLOGY

A. Dataset Description

Several datasets are to be had for this paintings consisting of the Bot-IoT and the united states-NB15 datasets. The Bot-IoT dataset consists of over 72 million facts with forty two functions (27 Integer, 13 Float, and a pair of String kinds) and become created by means of putting in a botnet community in a controlled environment and tracking the community visitors to seize any packets that have been being despatched. The dataset carries categorised ordinary and malicious site visitors which incorporates assaults which include DDoS, DoS, OS Scan, and so on. The other dataset, UNSW-NB15 consists of 43 capabilities (14 Float, 6 Strings and 23 Integer types) and a pair of. Five million statistics that are classified as either assault visitors or ordinary site visitors and further multiplied to the class of attack and the subcategory. In addition to DDoS and DoS attacks, the dataset incorporates information for Fuzzers, Backdoor, Reconnaissance and Worm attacks. These statistics have been accumulated in pcap files and then transformed to CSV to create the dataset. Both datasets had been compiled and made publicly available via UNSW Canberra for research functions. Furthermore, it is found that the USA-NB15 dataset is a greater polished dataset, in which has similar attributes to then Bot-IoT dataset but is greater diverse in the sort of malicious information it has.

B. Classification Algorithm

Several classifiers have been used and evaluated in this paintings. Scikit-analyze library in Python changed into used in this work. For the evaluation, the confusion matrix became computed to calculate precision, bear in mind, and F-Measure using the actual and predicted labels from the model. The classifiers used in this paper are:

B1. Support Vector Machine

Support Vector Machine or SVM is one of the most popular Supervised Learning algorithms, which is used for Classification as well as Regression problems. However, primarily, it is used for Classification problems in Machine Learning.

The goal of the SVM algorithm is to create the best line or decision boundary that can segregate n-dimensional space into classes so that we can easily put the new data point in the correct category in the future. This best decision boundary is called a hyperplane.

SVM chooses the extreme points/vectors that help in creating the hyperplane. These extreme cases are called as support vectors, and hence algorithm is termed as Support Vector Machine. Consider the below diagram in which there are two different categories that are classified using a decision boundary or hyperplane:

CONCLUSION AND FUTURE WORK

IN THIS PAPER, WE PROPOSED A DEEP LEARNING MODEL BASED ON 1D SVM FOR ANDROID BOTNET DETECTION. WE EVALUATED THE MODEL THROUGH EXTENSIVE EXPERIMENTS WITH 1,929 BOTNET APPS AND 4,387 CLEAN APPS. THE MODEL OUTPERFORMS SEVERAL POPULAR MACHINE LEARNING CLASSIFIERS EVALUATED ON THE SAME DATA SET. THE RESULTS (ACCURACY: 98.9%; PRECISION: 0.983; RECALL: 0.978; F1- SCORE: 0.981) INDICATE THAT OUR PROPOSED SVM BASED MODEL CAN BE USED TO IDENTIFY NEW, PREVIOUSLY UNSEEN ANDROID BOTNETS MORE ACCURATELY THAN OTHER MODELS. FOR FUTURE WORK, WE WILL AIM TO IMPROVE THE MODEL TRAINING PROCESS BY AUTOMATING THE DETECTION AND SELECTION OF KEY INFLUENCING PARAMETERS (I.E. NUMBER OF FILTERS, FILTER LENGTH, AND NUMBER OF FULLY CONNECTED (DENSE) LAYERS) THAT JOINTLY RESULT IN OPTIMAL PERFORMANCE SVM MODEL

ACKNOWLEDGMENT

We would prefer to give thanks the researchers likewise publishers for creating their resources available. We are grateful to guide, reviewer for their valuable suggestions and also thank the college authorities for providing the required infrastructure and support.

REFERENCES

[1] S. Y. Yerima and S. Khan “Longitudinal Perfomance Anlaysis of Machine Learning based Android Malware Detectors” 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), IEEE

[2] H. Pieterse and M. S. Olivier, ”Android botnets on the rise: Trends and charac- teristics,” 2012 Information Security for South Africa, Johannesburg, Gauteng, 2012, pp. 1-5.

[3] Letteri, I., Del Rosso, M., Caianiello, P., Cassioli, D., 2018. Performance of botnet detection by neural networks in software-dened networks, in: CEUR WORKSHOP PROCEEDINGS, CEUR-WS.

[4] Hauptmann, Alexander G., Rong Jin, and Tobun D. Ng. "Video retrieval using speech and image information." Electronic Imaging 2003. International Society for Optics and Photonics, 2003.

[5] Kadir, A.F.A., Stakhanova, N., Ghorbani, A.A., 2015. Android botnets: What urls are telling us, in: International Conference on Network and System Secu- rity, Springer. pp. 78–91.

[6] ISCX Android botnet dataset. Available from https://www.unb.ca/cic/datasets/android- botnet.html. [Accessed 03/03/2020]

[7] M. Eslahi, M. V. Naseri, H. Hashim, N. M. Tahir, and E. H. M. Saad, ”BYOD: Current State and Security Challenges,” presented at the IEEE Symposium on Computer Applications Industrial Electronics, Peneng, Malaysia, 2014

[8] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, ”Botnets: A survey,” Computer Networks, vol. 57, pp. 378-403, 2013.

[9] A. J. Alzahrani and A. A. Ghorbani, ”SMS mobile botnet detection using a multi-agent system: research in progress,” presented at the Proceedings