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

Mobile Botnet Detection

Prof. (Mrs) Mayuri Khade[1], Aditya Akangire[2], Abhishek Kumar[3], Ujjwal Dewangan[4], Gursimran Singh Mehta[5]
Faculty, Department of computer Science and Engineering[1]
Students, Department of computer Science and Engineering[2,3,4,5]
Sinhgad College of Engineering, Pune, Maharashtra, India

Abstract: *Android, being the most widespread mobile operating systems is increasingly becoming a target for malware. Malicious apps designed to turn mobile devices into bots that may form part of a larger botnet have become quite common, thus posing a serious threat. This calls for more effective methods to detect botnets on the Android platform. Hence, in this paper, we present a deep learning approach for Android botnet detection based on Support vector machine (SVM). Our proposed botnet detection system is implemented as a svm based model that is trained on 342 static app features to distinguish between botnet apps and normal apps.*

Keywords: Mobile botnet detection, SVM

I. INTRODUCTION

A botnet consists of a number of Internet-connected devices under the control of a malicious user or group of users known as botmaster(s). It also consists of a Command and Control (CC) infrastructure that enables the bots to receive commands, get updates and send status information to the malicious actors. Since smartphones and other mobile devices are typically used to connect to online services and are rarely switched off, they provide a rich source of candidates for operating botnets. Thus, the term 'mobile botnet' refers to a group of compromised smartphones and other mobile devices that are remotely controlled by botmasters using CC channels They have a strong ability to detect security threats, to collect malware signatures and to understand the motivation and technique behind the threat .The goal is to set the user up for being unknowingly exposed to a malware infection. You'll commonly see hackers exploit security issues in software or websites or deliver the malware through emails and other online messages.

II. LITERATURE SURVEY

1. Paper Name: Cooperative Network Behaviour Analysis Model for Mobile Botnet Detection Author: Meisam Eslahi, Moslem Yousefi Abstract ::-— Recently, the mobile devices are well integrated with Internet and widely used by normal users and organizations which employ Bring Your Own Device technology. On the other hand, the mobile devices are less protected in comparison to computers. Therefore, the mobile devices and networks have now become attractive targets for attackers. Amongst several types of mobile threats, the mobile HTTP Botnets can be considered as one of the most sophisticated attacks. A HTTP Bots stealthily infect mobile devices and periodically communicate with their controller called Botmaster. Although the Bots hide their activities amongst the normal web flows, their periodic pattern has been used as a measure to detect their activities. In this paper we propose a cooperative network behaviour analysis model to identify the level of periodicity posed by mobile Bots. Finally three metrics is proposed to detect Mobile HTTP Botnets based on similarity and correlation of their group activities. Test results show that the propose model can efficiently classify communication patterns into several periodicity categories and detect mobile Botnets.

2. Paper Name: :- Mobile Botnet Detection: A Deep Learning Approach Using Convolutional Neural Networks Author: Mohammed K. Alzaylaee Abstract : — Android, being the most widespread mobile operating systems is increasingly becoming a target for malware. Malicious apps designed to turn mobile devices into bots that may form part of a larger botnet have become quite common, thus posing a serious threat. This calls for more effective methods to detect botnets on the Android platform. Hence, in this paper, we present a deep learning approach for Android botnet detection based on Convolutional Neural Networks (CNN). Our proposed botnet detection system is implemented as a CNN-based model that is trained on 342 static app features to distinguish between botnet apps and normal apps. The trained botnet detection model was evaluated on a set of 6,802 real applications containing 1,929 botnets from the publicly available ISCX botnet dataset.

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

The results show that our CNN-based approach had the highest overall prediction accuracy compared to other popular machine learning classifiers. Furthermore, the performance results observed from our model were better than those reported in previous studies on machine learning based Android botnet detection

3. Paper Name: Detection of Mobile Botnets using Neural Networks Author: Milan Oulehla, David Malanik abstract : This poster deals with botnets, the most dangerous kind of mobile malware, and their detection using neural networks. Unlike common mobile malware, botnets often have a complicated pattern of behavior because they are not managed by predictable algorithms but they are controlled by humans via command and control servers (CC servers) or via peer-to-peer networks. However, they have certain common features which have been revealed by analysis of contemporary mobile botnets. These features have been used for creation of a neural network training set. Finally, the design of parallel architecture using neural network for useful detection of mobile botnets has been described

4. Paper Name: A Static Approach towards Mobile Botnet Detection Author::- Zakira Inayat,Aws Naser Jabir abstract :The use of mobile devices, including smartphones, tablets, smart watches and notebooks are increasing day by day in our societies. They are usually connected to the Internet and offer nearly the same functionality, same memory and same speed like a PC. To get more benefits from these mobile devices, applications should be installed in advance. These applications are available from third party websites, such as google play store etc. In existing mobile devices operating systems, Android is very easy to attack because of its open source environment. Android OS use of open source facilty attracts malware developers to target mobile devices with their new malicious applications having botnet capabilities. Mobile botnet is one of the crucial threat to mobile devices. In this study we propose a static approach towards mobile botnet detection. This technique combines MD5, permissions, broadcast receivers as well as background services and uses machine learning algorithm to detect those applications that have capabilities for mobile botnets. In this technique, the given features are extracted from android applications in order to build a machine learning classifier for detection of mobile botnet attacks. Initial experiments conducted on a known and recently updated dataset: UNB ISCX Android botnet dataset, having the combination of 14 different malware families, shows the efficiency of our approach. The given research is in progress.

5. Paper Name: Mobile Botnet Detection: A Deep Learning Approach Using Convolutional Neural Networks Author: Suleiman Y. Yerima, Mohammed K. Alzaylaee Abstract: Android, being the most widespread mobile operating systems is increasingly becoming a target for malware. Malicious apps designed to turn mobile devices into bots that may form part of a larger botnet have become quite common, thus posing a serious threat. This calls for more effective methods to detect botnets on the Android platform. Hence, in this paper, we present a deep learning approach for Android botnet detection based on Convolutional Neural Networks (CNN). Our proposed botnet detection system is implemented as a CNN-based model that is trained on 342 static app features to distinguish between botnet apps and normal apps. The trained botnet detection model was evaluated on a set of 6,802 real applications containing 1,929 botnets from the publicly available ISCX botnet dataset. The results show that our CNN-based approach had the highest overall prediction accuracy compared to other popular machine learning classifiers. Furthermore, the performance results observed from our model were better than those reported in previous studies on machine learning based Android botnet detection.

6. Paper Name: Detecting Mobile Botnets Through Machine Learning and System Calls Analysis Author: Sylvio Barbon Junior Abstract: Botnets have been a serious threat to the Internet security. With the constant sophistication and the resilience of them, a new trend has emerged, shifting botnets from the traditional desktop to the mobile environment. As in the desktop domain, detecting mobile botnets is essential to minimize the threat that they impose. Along the diverse set of strategies applied to detect these botnets, the ones that show the best and most generalized results involve discovering patterns in their anomalous behavior. In the mobile botnet field, one way to detect these patterns is by analyzing the operation parameters of this kind of applications. In this paper, we present an anomaly-based and host-based approach to detect mobile botnets. The proposed approach uses machine learning algorithms to identify anomalous behaviors in statistical features extracted from system calls. Using a self-generated dataset containing 13 families of mobile botnets and legitimate applications, we were able to test the performance of our approach in a close-to-reality scenario. The proposed approach achieved great results, including low false positive rates and high true detection rates.

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

III. METHODOLOGY

In This project We Detect Botnet App. Botnet App Means Some malware are installed in the App through the mobile. That Time loss Your Important Mobile Data. So we Avoid All The loss. Our proposed botnet detection system is implemented as a SVM-based model that is trained on app features to distinguish between botnet apps and normal apps.

3.1 Data Flow Diagram

In Data Flow Diagram, we Show that flow of data in our system in DFD0 we show that base DFD in which rectangle present input as well as output and circle show our system, In DFD1 we show actual input and actual output of system input of our system is text or image and output is rumor detected likewise in DFD 2 we present operation of user as well as admin

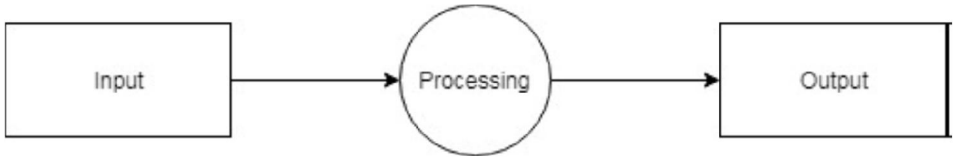

Figure 1: Data Flow(0) diagram

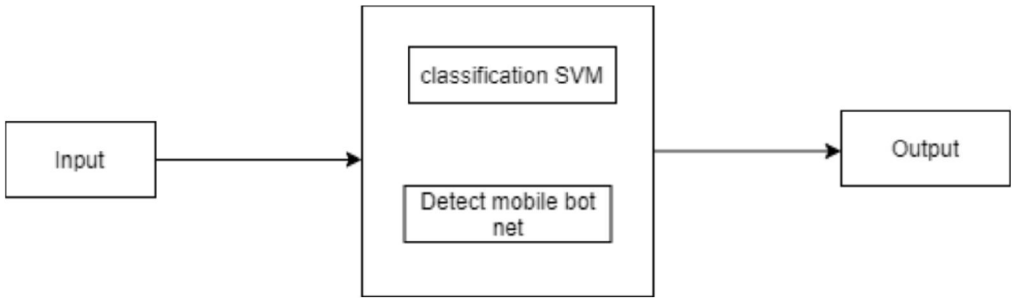

Figure 2: Data Flow(1) diagram

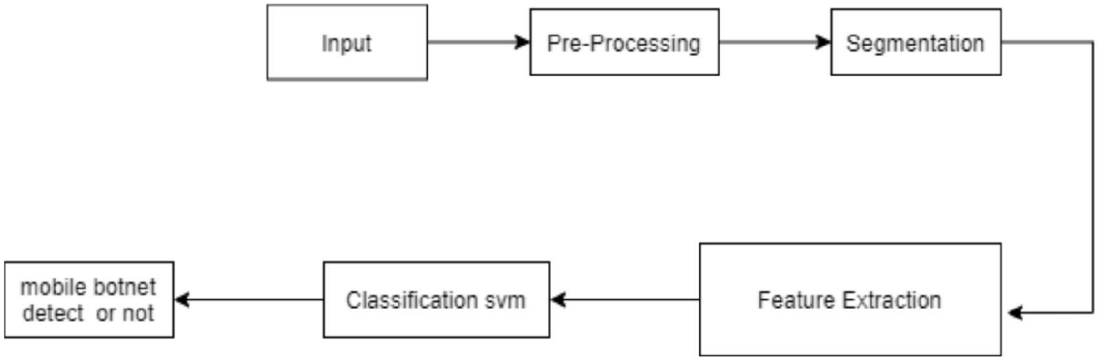

Figure 3: Data Flow(2) diagram

3.2 UML DIAGRAMS

Unified Modeling Language is a standard language for writing software blue prints. The UML may be used to visualize, specify, construct and document the arti facts of a software intensive system. UML is process independent, although optimally it should be used in process that is use case driven, architecture-centric, iterative, and incremental.
The Number of UML Diagram is available.

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

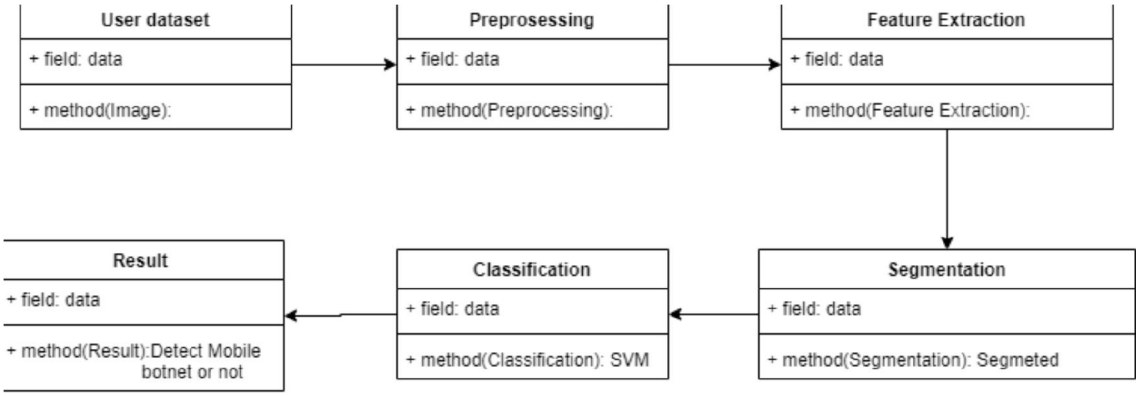

Figure 4: Class Diagram

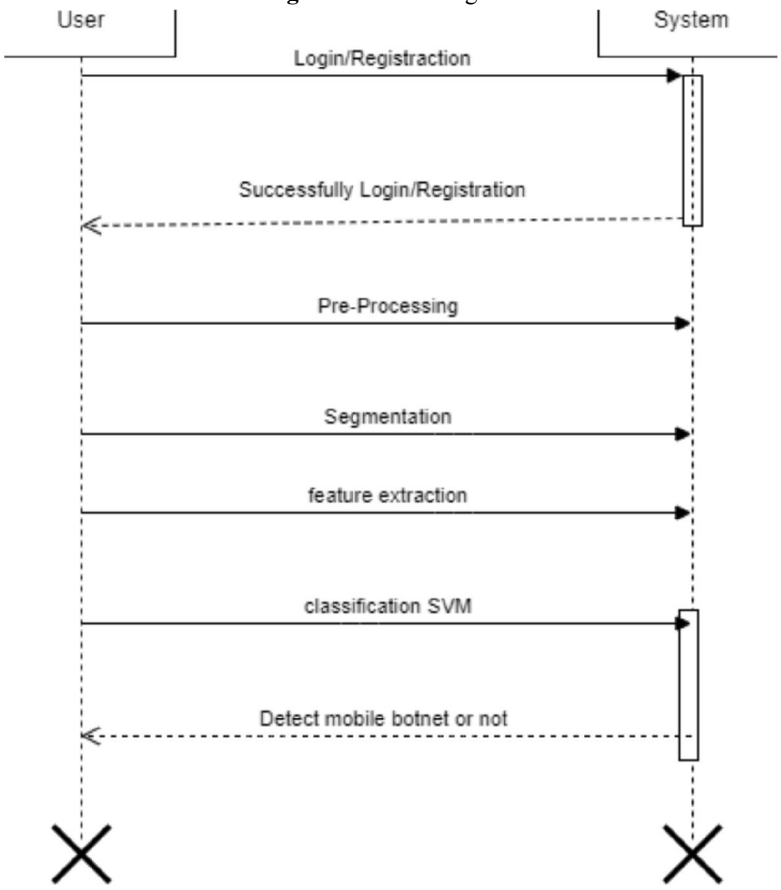

Figure 5: Sequence Diagram

IV. CONCLUSION

Botnets are a Dangerous evolution in the malware world. They are being used to damage systems, steal information and Comprise Systems. They are hard to detect and eliminate. So Our System Is Useful to detect Mobile Botnet

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

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 characteristics," 2012 Information Security for South Africa, Johannesburg, Gauteng, 2012, pp. 1-5. 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.

[3]. 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.

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

[5]. 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

[6]. 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.

[7]. A. J. Alzahrani and A. A. Ghorbani, "SMS mobile botnet detection using a multi-agent system: research in progress," presented at the Proceedings of the 1st International Workshop on Agents and CyberSecurity, Paris, France, 2014

[8]. G. Gu, J. Zhang, and W. Lee, "BotSniffer: Detecting botnet command and control channels in network traffic," in Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08), 2008

[9]. C. Byungha, C. Sung-Kyo, and C. Kyungsan, "Detection of Mobile Botnet Using VPN," in Proceedings of the Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013, pp. 142-148