IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Special Issue 2, March 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

| International Conference on Recent Innovations in Engineering and Technology (ICRIET'23)|

| Sharadchandra Pawar College of Engineering, Pune, India |

|| Volume 11, Special Issue 2, March 2023 ||

Android Mobile Botnet and Fake Advertisement Detection Using SVM Algorithm

Dube Pratiksha[1], Gaykar Shital[2], Sabale Apeksha[3], Prof. Mandlik S. Y.[4] , Prof. Pawar S. H.[5]

Students, Department of Computer Engineering, Jaihind College of Engineering, Kuran Pune, India [1,2,3]

Assistant Professor, Department of Computer Engineering, Jaihind College of Engineering, Kuran Pune, India [4,5]

ABSTRACT: Today, many applications such as government applications, commercial applications, and other most applications rely on the internet. Android, being the most widespread mobile operating system, is increasingly becoming a target for different types of viruses such as botnet, DOS, threat, and Phishing attacks. The research area of detecting smartphone-based botnets is really a challenging issue and only a few ideas exist to solve it. 70% of applications on Android have various advertisements, so some of them are fake and some are real. Hence, in this paper, we present a machine learning approach for android mobile botnet and fake advertisement detection based on SVM (Support Vector Machine).

KEYWORDS: Botnet Detection, SVM, Machine Learning, Fake advertisement, attacks

I. INTRODUCTION

The term "bot" comes from a robot that automatically works according to a computer program or scripts were written by the bot master. Currently, mobile Bonet attacks have shifted from computers to smartphones due to their functionality, ease of exploit, and financial intentions. A botnet is nothing more than a collection of bots (also called zombies) that are controlled by a bot master on a command-and-control server. The owner of a botnet is known as a "bot master" or "bot herder," and it can be a single person or group of people who can infect several computers without the owners' knowledge. It creates botnets mostly for financial gain by using other people's identities. The bot master can control large networks of botnets from different locations to launch attacks. The main motive behind the creation of a botnet is to perform various malicious activities like identity theft, launching Denial of Service (DDoS) attacks, phishing attacks, click fraud, sending spam emails, and stealing the personal information of Android users. The botnet master can control many bot computers from a remote location. Malicious attackers perform various operations and create a botnet. In that system, we detect the botnet in that application and check whether the advertisement is fake or real. The focus is to reduce dimensions during feature selection as part of a machine-learning solution. In this system, we present a machine-learning approach that leverages support vector machines (SVM) for Android botnet detection and fake advertisement detection. The SVM model employs 342 static features to classify new or previously unseen apps as either "botnets" or "normal." As a result, SVMs have better generalization capabilities and hence can be used in situations where the number of training samples is low, and the data has many features. SVMs have been widely used in text and image classification problems and in voice recognition and anomaly detection (e.g., in security, fraud detection, and healthcare).

Most of the existing detection techniques can only detect malware on Android applications; however, Android botnet applications cannot be detected so the article focused on the detection of the botnet and fake advertisements in Android applications. The remainder of this paper is organized as follows: Section 2 provides a related work Section 3 deals with the System architecture of android botnet and fake advertisement detection using machine learning; Section 4 shows the objectives of the system.

II. BACKGROUND

The term "botnet" first appeared in 1993 with the introduction of the first botnet, "Eggdrop" (Wang, 2003). Following that, more advanced botnets are created, with new features and functions until 2002. During these years,

most of the attackers started using botnets, which rapidly increased cyberattacks. The oldest internet botnet can be traced to 1988, with the emergence of Internet Relay Chat, abbreviated IRC and these IRC bots provided automated services to users The first bots used on IRC were Jyrki Alakuijala's Puppe, Greg Lindahl's Game Manager (for the Hunt the Wumpus game), and Bill Wisner's Bartender. WebCrawler was the first bot used to index web pages, and it was created in 1994. First AOL used WebCrawler in 1995, then procured by Excite in 1997. In 1996 the most famous internet crawler, Googlebot, originally called BackRub when was created. In 1999 the IRC network was released. The widely used botnet protocol is IRC which is extremely popular, and it can be easily found for use by a botmaster. A novel and superior version of the SW- based bot network was released in 2008. There are several publications on the botnet from 2005 to 2013, as shown in Figure1.

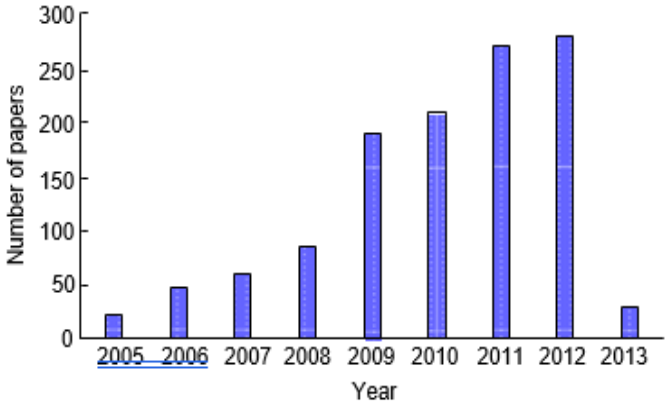

Figure 1. Number of publications on the botnet from 2005 to April 2013

III. RELATED WORK

In this paper [1] analysis the existence of the botnet and its management. The world has not got sufficient data and a convincing procedure for detecting a botnet. The hazard of Botnet is not strange to anyone as they have existed for a long time, there is a lot of research that needs to be done to put a check on them. Nowadays things are added on to check the botnet in the server. A study also gave network topologies in botnets and discussed some techniques through which the botnets can be detected and monitored, and the network topologies used by the botnets in attacking a server.

In this paper [2] Focus on inferring suitable Smartphone-based botnet detection techniques from the study of network and device-level information. A study also gave botnet work detection both in a wired and wireless network with their detection approaches. As bots within a bot network behave uniquely at the device level, it is necessary to consider the information at both the device level and network level to design an effective Smartphone based bot network detection development. However, the approach should consider additional problems such as data encryption and communication behaviors. Additionally, it is necessary to consider effective time-consuming intelligent association algorithms to improve the efficiency of the device-level behavior of a bot.

In this paper [3] Discusses Botnet, Botnet history, and the life cycle of botnet apart from classifying various Botnet detection techniques. Researchers have been mainly focused on botnet detection and trying to trace the Command-and-Control server. As Feily, et. al. summarized Botnet and its detection techniques in their proposed work, they classified detection techniques as Honeynet. It is useful to find the existing botnet, based on an intrusion detection system. Lei Zhan and Paul Watters proposed the botnet attack using the principles of fast flux and domain flux. They also compared fluxing detection methods. The second approach is intrusion detection based, which

is further divided into four parts signature-based, Anomaly-based, DNS-based, and Mining Based. A botnet can be categorized according to the architecture used to build communication channels.

In this paper [4] the transformation of the advertising market under the influence of platform companies, using the US example, to show the mechanism of digital disruption in the print media business model. The development of digital infrastructure has allowed platform companies to collect and monetize data, a deliver

personalized ads to users throughout the internet. A structural shift has occurred - traditional media have ceased to be the main channels for transmitting advertising messages to certain social groups, and advertising platforms are able to find them and deliver their ads on their own. In the framework of "platform capitalism", many print media to survive try to transform themselves in accordance with the logic of the economic platform model (developing their website, data collection, monetization, and integration into the logic of social networks).

In this paper [5] 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 has the highest overall prediction accuracy compared to other popular machine learning classifiers and it is a popularly used approach. Furthermore, the performance results observed from our model were better than those reported in previous studies on machine learning-based Android botnet detection.

IV. SYSTEM ARCHITECTURE

Smartphone users still blindly trust applications and the default settings of smart devices and are using them without knowledge of the risks associated with them. Although mobile botnets are a relatively new concept for users, cyber researchers are also unfamiliar with them. Our system uses the SVM machine learning algorithm to detect botnets and fake advertisements. We also use an app to try to prevent botnets. The system focuses on reducing dimensions during feature selection as part of the machine-learning solution. This work proposes a machine-learning approach to botnet detection and mitigation by analyzing network traffic-derived datasets.

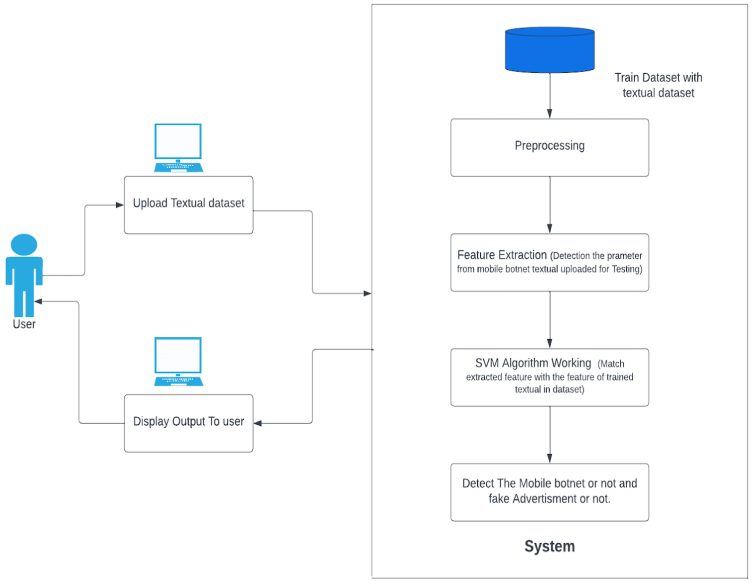

Figure 2. System Architecture

V. OBJECTIVE

- To find mobile application features botnet or normal.
- To prevent virus-like Botnet.
- To detect fake advertisements.
- Classify whether the output is botnet or normal with the help of a machine learning algorithm.

VI. CONCLUSION AND FUTURE WORK

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 app Botnet. Fake advertisement detection has many open issues that require the attention of researchers. For instance, in order to reduce the spread of fake advertisements, identifying key elements involved in the spread of advertisements is an important step. Machine learning techniques can be employed to identify the key sources involved in the spread of fake advertisements. So in future , we have to develop a software that detect botnet in android applications as well as fake advertisements using SVM algorithm

REFERENCES

[1] Rimsha Malik and Bhavya Alankar, "Botnet and Botnet Detection Techniques," International Journal of Computer Applications (0975 – 8887)., School of Engineering Science and Technology (SEST) Jamia Humdard, New Delhi, India M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science., Volume 178 – No.17, (June 2019).

[2] Dr. K. Muthumanickam, Dr. T. Sengolrajan, Mr. R. Palanikumar, Dr. R. Shankar,"Smartphone-Based Botnet Detection using Behavioral Analysis," Second International Conference on Power, Energy, Control and Transmission system from IEEE., Department of Information Technology Kongunadu College of Engineering and Technology., (May 26, 2021).

[3] Navdeep Kaur and Maninder Singh, "Botnet and Botnet Detection Techniques in Cyber Realm," CSED, Thapar University Patiyala (Panjab), India.

[4] Alexander A. Balayan and Leonid V. Tomin, "The Transformation of the Advertising Industry in the Age of Platform Capitalism," IEEE Xplore., Department of Political Science HSE Campus in St. Petersburg, Russia(June 29, 2020).

[5] Suleiman Y. Yerima and Mohammed k. Alzaylaee, "Mobile Botnet Detection: Deep learning Approach using Convolutional Neural Networks," IEEE Xplore., the University of Birmingham., (July 21, 2020).

[6] MahantSesh Borgi, Viraj Malik, Breznew Colaco, Pratik Dessai, Harsha Chari, Shailendra Aswale, "Advertisement Click Fraud Detection System: A survey., International journal of Engineering Research & Technology (IJERT)., vol. 10., (May-2021).

[7] Suleiman Y. yerima and Abul Bashar, "A Novel Android Botnet Detection System Using Image Based and Manifest File Features., Cyber Technology Institute, Faculty of Computing, Engineering and Media, De Montfort University, Leicester LE1 9BH, UK., (2022).

[8] Abdullah M. Almuhaideb and Dalal Y. Alynanbaawi, "Application of Artificial Intelligence to Detect Android Botnets: A survey., IEEE Xplore., Saudi Aramco Cybersecurity Chair, Department of Networks and Communications, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia., (29 June 2022).

[9] Muhammad Yusof and Madihah Mohd Saudi and Farida Ridzuan, "A New Mobile Botnet Classification based on Permission and API Calls"., Seventh International Conference on Emerging Security Technologies (EST)., (2017).

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details