A Survey on Detecting Activity of Fake User in Social Media by Intelligent Bot Using Artificial Intelligent

[1]Jatin Vagheshwari, [2]Hinal Somani
[1, 2] Department of Computer Engineering
[1]PG Scholar, LJ Institute of Engineering & Technology, Ahmedabad,India
[2]Ass.prof, LJ Institute of Engineering & Technology, Ahmedabad,India

Abstract- *with the growing development of mobile networks and powerful smartphones, botnets have invaded the mobile domain. Social media, like Twitter, Facebook, and YouTube have created a new communication channel for spammers. Bot started to exploit social media for different fakeactivity, such as sending spam, recruitment of new bots, and botnet command and control.This is survey on a detection technique for social media based mobile botnets using Twitter. The botnet has many bot army that is use to send spam massages to the social media and distributes the denial of service attacks. The bot master handle the all the activity of bots.OSNs provide ideal channels for bot masters. The main attacks by the command and control channel.*

Keywords- Online Social Network, Social Network Service, security, Botnet.

I. INTRODUCTION

The huge market for open source OS has opened the door for malicious writers to target the Vulnerable features of Open source OS. The survey that the 95% malware application targets the open sources like Android. Other than the mobile malware the new mobile botnet is now popular in the social media. The mobile malware is involving decrease the performance smart phones. Online social networking websites(OSNs), such as Twitter, Facebook and Sina Weibo have play an important part in people's life. By using these social networking services, it is convenient for people to communicate with their friends easily, publish posts about their life freely, and follow hot topics immediate. We have survey that the many detection technology and algorithms are foud in to the detect the bot and Spammers.

The main application of the mobile botnet is follow:-

1. Legal

Most of the time when botnets are in the legal area are commonly used for Distributed computing system which is a field of computer science that studies distributed systems. A distributed system is a software system in which components located on networked computers communicate and coordinate by passing messages. The components interact with each other in order to achieve a common goal. Three significant characteristics of distributed systems are: concurrency of components, lack of a global clock, and independent failure of components. A command and control may be present in the distributed computing but no zombie computer is present in this type of system.

2. Illegal

Botnets sometimes compromise computers whose security defenses have been breached and control ceded to a third party. Each such compromised device, known as a "bot", is created when a computer is penetrated by software from a malware (malicious software) distribution. The controller of a botnet is able to direct the activities of these compromised computers through communication channels formed by standards-based network protocols such as IRC and Hypertext Transfer Protocol (HTTP).Botnets are increasingly rented out by cyber criminals as commodities for a variety of purposes.

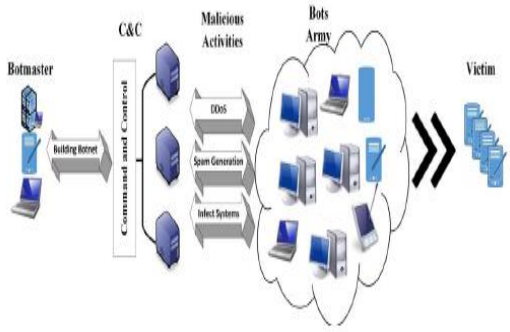

Figure: -1 mobile botnet architecture

Botnet indicates a coordinated attack comprising of various infected machine controlled by a botmaster. A botnet enables unauthorized access of the device and may disrupt the services of the users. Figure 1 shows the basic architecture of a mobile botnet.

II. RELATEDWORK

[1] Reham A. Al-Dayil, Mostafa H. Dahshan proposed "Detecting Social Media Mobile Botnets Using User Activity Correlation and Artificial Immune System"

The proposed method combines the correlation between tweeting and user activity, such as clicks or taps, and an Artificial Immune System detector, to detect tweets caused by bots and differentiate them from tweets generated by user or by user-approved applications. This detector creates a signature of the tweet and compares it with a dynamically updated signature library of bot behavior signatures. The proposed system has been fully implemented on Android platform and tested under several sets of generated Tweets.

The author proposed the detection method that is work like this flow. First step to capture the tweet from twitter. Second step is correlate tweet to user activity. Then third step to create signature from the tweet content. After tweeting event is same as user activity and signature has no match in signature library then assume tweet is valid and accept it. If match in library then go to the user if user accept this tweet sent tweet and delete from library. Otherwise don't sent. If not in library or no relation with user then check the source of the tweet. If it is in approved app then sent tweet. Otherwise ask user to accept tweet and sent.

[2] Pieter Burghouwt, Marcel Spruit, and Henk Sips is proposed the"toward detection of botnet communication through social media by monitoring user activity"

The proposed system In this paper we introduce a new detection mechanism that measures the causal relationship between network traffic and human activity, like mouse clicks or keyboard strokes. Communication with social media that is not assignably caused by human activity, is classified as anomalous. We explore both theoretically and experimentally this detection Mechanism by a case study, with Twitter.com as a Command and Control channel, and demonstrate successful real time detection of botnet Command and Control traffic.

This paper we address the social media based C&C traffic, by introducing mechanism that measures causality between user activity and nework.dificult detection is not the only reason that social media based C&C have most important botnet control mechanism on the internet.

They are use some detector mechanism like honey pots, CAPTHA, NOT A BOT for the detection. First traffic is captured from an inserted network bridges. Then second traffic flow is initiated to social media without keyboard and mouse event. Then that is classified as potential bot generated by detector, The taps implemented to interrupt the keyboard and mouse event.bot go to social media to fetch new interaction or sent harvested info traffic is not triggered by user, this allow detection of botnet traffic to social media.

[3]Ahmad Karim, Rosli Salleh and Syed Adeel Ali Shah proposed "DeDroid: A Mobile Botnet Detection Approach Based on Static Analysis"

In this paper, we propose a static analysis approach called DeDroid, to investigate botnet-specific properties that can be used to detect mobile botnets. Initially, we identify critical features by observing coding behavior of the few known malware binaries having C&C features. Then we compare the identified features with the Drebin dataset of malicious applications and come to the conclusion That Drebin dataset has 35 percent applications which qualify as botnets.

The proposed Dedroid analysis approach first step is examines theC&C features associated with different well known malware family. After taking sample from each malware family a static analysis performed by reverse engineering the application. Then take permission and API calls having close relation with botnets.

They have highlighted potential botnet features for static analysis. After identifying critical botware features in malicious application. The system repeat the process for certain malicious samples and compare. The comparative analysis perform validate that result.

[4] Mohit Agrawal, R. Leela Velusamy proposed "R-SALSA: A Spam Filtering Technique for Social Networking Sites"

Reliability based Stochastic Approach for Link-Structure Analysis (R-SALSA) algorithm has been proposed in this paper for classifying a message being Spam or benign. The dataset collected from popular Netherland's social media named Hyves is used to test proposed algorithm. It has been evaluated with different performance based metrics namely true positive rate, false positive rate, accuracy, and it is found to be performing better than previously proposed unsupervised author reporter model.

The proposed filtering model is based on SALSA algorithm combined with the reliability of reporters and renamed as R-SALSA. The SALSA algorithm uses the links between user and the messages to calculate spam score for each message.

For improving the SALSA algorithm they introduce new parameter namely reliability factor denoted as 'α' which can be calculated as the ratio between correct spam report by reporters to total number of reporters reporting content as spam.

The algorithm creates a bilateral graph of reporters R= {r1, r2, r3,…, rn} and contents C={ c1, c2, c3,…,cn}. Where

one disjoint set of the graph represents reporters and another set represents message content connected by directed edges (E).

[5] Vishnu Teja Kilari, Guoliang Xue, Lingjun Li proposed" Host Based Detection of Advanced MiniDuke Style Bots in Smartphones through User Profiling"

In this paper they proposed innovative C%C that collect the user information in OSNs and combine with username generation algorithm.Then proposed the new sysetm that is identify bot in C%C channel .Our approach involvesbuilding a profile of user based on his web usageand then comparing that profile to subsequent usage to detect malicious behavior .

Before this process they cluster the web usage based on network domain and collect similar features.then they use clssification algorithm to create user profile and compare with domain and user behaviour.if the thresold is crossed over normal user to domain .tat is notify based ob their response model is updated.

III. COMPARATIVE ANALYSIS

Sr. No.	Paper Title	Methods/ Techniques	Advantages	Disadvantages
1.	Detecting Social Media Mobile Botnets Using User Activity Correlation and Artificial Immune System"	detection method using UAC and AIS	Misbehavior in social media is detected .	It is less accurate.
2.	Towards Detection of Botnet Communication through Social Media by Monitoring User Activity	Detector mechanism	Detect the spam messages	This system is slow.
3.	DeDroid: A Mobile Botnet Detection Approach Based on Static Analysis	Static analysis approach called dedroid	Detect and find the bot	It is used only in android system
4.	R-SALSA: A Spam Filtering Technique for Social Networking Sites	Reliability based Stochastic Approach for Link-Structure Analysis	More accurate result compare to other approaches	it is not give efficient performance
5.	Host Based Detection of Advanced MiniDuke Style Bots in Smartphones through User Profiling	Username Generation Algorithm	It is detect the malicious user.	It is used in mobile device.

Table 1. Literature Comparison

IV. CONCLUSION

In this paper, we have survey different method to detect mobile botnets that use online social networks as their Command and Control channel. Our detection method works on mobile devices and detects botnets based on the existence of user activity in addition to checking the content of the tweet itself. The accuracy of the detection improves after the system has been trained with user input.

REFERENCES

[1] Reham A. Al-Dayil, Mostafa H. Dahshan," Detecting Social Media Mobile Botnets Using User Activity Correlation and Artificial Immune System" volume: -109-114 7th ICICS ©2016 IEEE

[2] Burghouwt, Pieter, Marcel Spruit, and Henk Sips. "Towards detection of botnet communication through social media by monitoring user activity." In International Conference on Information Systems Security, pp. 131-143. Springer Berlin Heidelberg, 2011.

[3] Siddiqa, Aisha, Ahmad Karim, Tanzila Saba, and Victor Chang. "On the analysis of big data indexing execution strategies." Journal of Intelligent & Fuzzy Systems (2016).

[4] Mohit Agrawal, R. Leela Velusamy proposed "R-SALSA: A Spam Filtering Technique for Social Networking Sites" Electrical, Electronics and Computer Science (SCEECS), 2016 IEEE Students' Conference.pp-1-7 6th march 2016.

[5] Kilari, Vishnu Teja, Guoliang Xue, and Lingjun Li. "Host Based Detection of Advanced MiniDuke Style Bots in Smartphones through User Profiling." In 2015 IEEE Global Communications Conference (GLOBECOM), pp. 1-6. IEEE, 2015.