BotDefender: A Framework to Detect Bots in Online Social Media

Neharika Singh [1], Madhumita Chatterjee [2]
[1, 2] Department of Computer Engineering, University of Mumbai, PCE, New Panvel, Maharashtra, India.

Abstract – Online social network is the most popular and efficient platform for billions of users and their activities. Hundreds of billions of active users all around the world are using online social network (OSN) like Facebook, twitter, LinkedIn etc. OSNs act as platform for the user to interact, communicate and group with other people. Recently OSNs have become a favorite place of attackers to perform many illegal activities such as launch distributed denial of service attack, phishing, covert channel communication and click fraud to extract personal information from the infected victim machine by using Botnet. In this paper, we propose a novel botnet detection method in online social media (OSM) - BotDefender, which will help to differentiate non-malicious and malicious users by analyzing user behavior.

Index Terms – Online Social Media, Online Social Network, Social Network Bots, Botnet Detection, BotDefender.

1. INTRODUCTION

Threats to modern society are nothing but malware. There are multiple types of malware out of them botnet is the most important and biggest problem to the security of Internet. The bot is an intelligent program that operates automatically as an agent for different goals. Bots term denotes Zombies and botnet term denotes Zombies armies.

Bots are controlled by nodes called 'Botmaster'. The main distinction between Botnet and another type of malware abbreviates in existence of Command-and-Control (C&C) organization. Recently botnet in more active on social networking sites to perform illegal activities like settling personal information. Therefore it is very important to detect botnet at the early stage to avoid all the harmful activities on the social networking sites.

2. LITERATURE REVIEW

This section presents the relevant literature surveyed for various techniques of Botnet attack detection.

Distinguishing the legitimate user is not easy when it comes to detect botnet. Therefore it is necessary to detect botnet at the initial stage.

Yuede Ji [2] has proposed a social bot Behavioral detecting approach in the end point machine. Bot identification is in 6 stages:(1)Infection (2)Predefined host behaviours (3)Establishment of C&C (4)Receive the commands of Botmaster (5)Execution of social bot commands (6)Evaluation. Based on specific behaviours, system consists of three components:(1)Host behaviour monitor (2)Host behaviour analyser (3)Detection approach. It gives 29.9%False Positives and 4.5% False Negatives.

Mansoureh Ghanadi, Mahdi Abadi,in their paper [5], used a negative reputation subsystem to analyse images shared by users of social network.A negative reputation score is generated for every single user, based on the previous records of suspicious group activities participation.

Md Sazzadur, Ting-Kai Huang, Harsha V.Madhyastha and Michalis Faloutsos, [6], 2012, this is the first tool focused on detecting malicious apps on facebook. First, it will identify a set of features that help use distinguish malicious apps from benign one. It can detect malicious apps with 99.5\% accuracy with no false positive and a low false negative rate 4.1%.

3. ARCHITECTURE

The proposed system aims of bot attack by combining two approaches viz., Bot-User Profile Identification and Monitoring Activities (Uploading and Downloading). The architecture of proposed detection system that can detect malicious users from normal users refers Figure 4.1.

The proposed model has two parallel approaches to identify the legitimate users from malicious users. It has separate modules for identifying fake user and will check the image at the time of upload or download to identify whether it contains any malicious code or not.

3.1. Bot-User Profile Identification

Bot User Profile identification can be divided in 3 modules: Behavior Monitor, Detection Approaches and Report Generation. Bot User Profile Identification generates report, where it will classify the user in two categories Normal User and Malicious User. If the user is malicious, it will send to the suspended user module otherwise it will allow user to continue. All these reports are stored in the database.

1. Behavior monitoring

There are 3 modules in this Stage :(1) Keyboard/Mouse monitoring (2) Monitoring Host behavior (3) Monitoring Network behavior. Out of all the module Network behavior records inflows and outflows in live network.

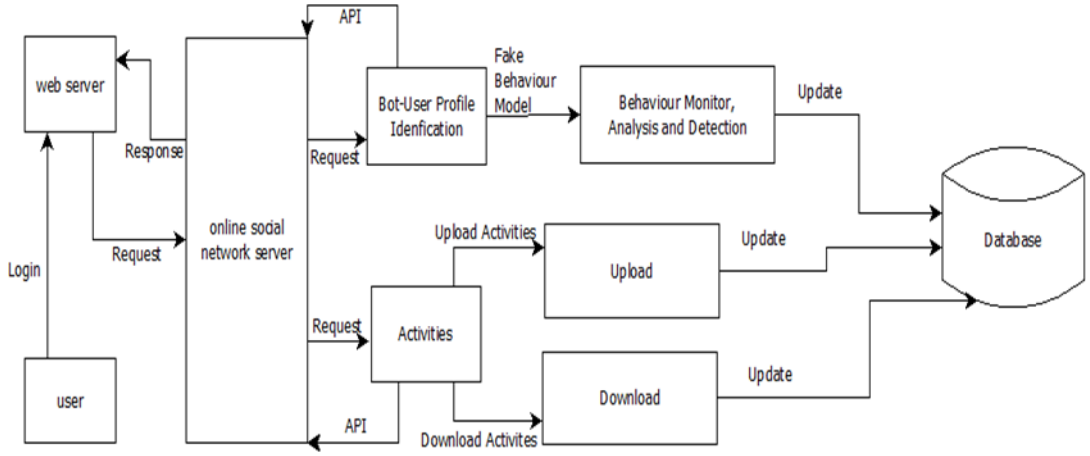

Fig 4.1 Overview of Proposed System

2. Behavior analyzer

Behavior Analyzer analyses bot user profile behavior and generates analysis report. Genuine and bot profiles have certain patterns in them. For the detection of Stegobot, we focus on the different patterns or characteristics. In order to efficiently detect bot, features like Followers, Trust Friends will be used.

3. Detection module

In Detection Module, it will first construct the behavior tree. The result is produced by this tree matching with template library.

4. Report

Once the Behavior Tree Based approach generates the similarity report, it will categorize the user as malicious and as the normal user. Malicious user list is then forwarded to next module.

5. Suspend user

In this module, malicious user's access to account is suspended. This doesn't delete the user's profile or data such as documents, calendar events, or email messages. However, the user can no longer sign-in to the account. To suspend a user, email-id will be blocked so that user can't recreate their account

3.2. Activities

Activities are divided into two categories:

1. Upload Activities

Upload Activities go through 4 phase - Detection Model, Negative Reputation, Detection Report and Remove Malicious Code refer Figure 4.2.

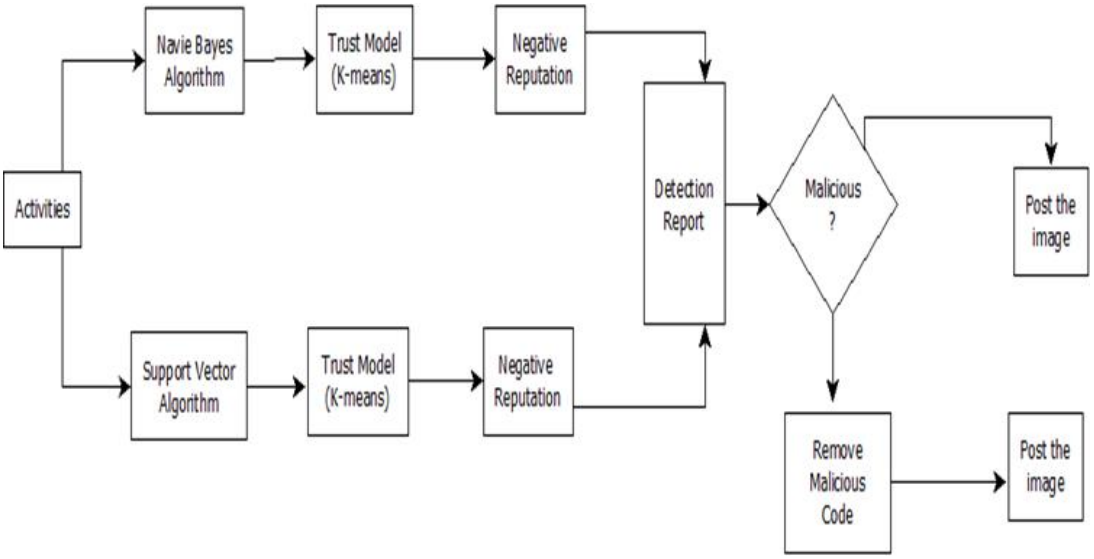

Fig 4.2 Upload Architecture in detail

1. Detection Model

This module analyzes activities using algorithms, Support Vector Machine Algorithm and Navie Bayes. Each of them uses a different set of features. Output of this module is sent to negative reputation.

2.Negative Reputation

This module with assign negative reputation to malicious activities[5].

3.Detection Report

It will compare same individual user using both algorithms and generate one report. While comparing it requires threshold value to generate one result with low false positive rate. Detection Report can use two different averaging operators: - an order weighted averaging or simple weighted averaging. It is necessary to select the optimal threshold value for generating an optimal result. The system will continue monitoring the normal distribution of malicious and legitimate users.

4.Remove Malicious Code

This module will remove the malicious code behind the uploaded media and then allows to post them. While removing malicious code it maintains the digital quality of uploaded items. It is very easy to identify malicious command like Base64 and JavaScript which might be hidden in fields such as size, date, format, etc.

3.3. Download Activities

This module will check whether an image belongs to the original user or not with the help of image metedata. It will also help to distinguish normal user from malicious users.

4. CONCLUSION

The existing approaches focus mainly on detection of a botnet. So there is a need to come up with a solution that incurs minimal overhead and validates the user input and response from the server. The proposed system can detect bot before getting uploaded to social networking platform and generates fake identification report of the individual user.

REFERENCES

[1] Binkley R, Singh S,"An Algorithm for Anomaly-Based Botnet Detection", Global Information Assurance Certification (GIAC), August 8, 2014.

[2] YuedeJi, Yukun He, Xinyang Jiang and QiangLi,"Towards Social Botnet Behavior Detection in the end host", IEEE, 2014.

[3] Reema Sharma,Deepshikha, "Social Networking Sites: A New Platform for Botnets A short Case Study to prove that how today's Social Networking is a New Platform for Cyber Criminals", International Journal of Emerging Technology and Advanced Engineering, Volume 4 ,Special Issue 1, 2014.

[4] Natarajan Venkatachalam, R.Anitha, "A Multi-feature approach to detect Stegobot: a covert multimedia social network botnet", Springer, 2016.

[5] MansourehGhanadi, Mahdi Abadi,"SocialClymene: A Negative Reputation System for Covert Botnet Detection in Social Network", IEEE, 2014.

[6] MdSazzadur, Ting-Kai Huang, HarshaV.Madhyastha and MichalisFaloutsos,"FRAppE: Detecting Malicious Facebook Applications", IEEE, 2012.

[7] EhsanAhmadizadeh, ErfanAghasian, Hossein Pour, RoohollahFallahNejad,"An Automated Model to Detect Fake Profiles and botnets in online social network using steganography technique",IOSR Journal of Computer Engineering, Volume 17, Issuse 1, Feb 2015.

[8] V.Natarajan, Shina Sheen, R.Anitha, "Multilevel Analysis to detect covert social botnet in multimedia social networks", The Computer Journal, Volume 58, 2015.

[9] Zhang J,Lee w,"Botsniffer: Deetecting Botnet command and control channels in network traffic", Network and Distributed System Security Symposium(NDSS), 2008.

[10] Freiling , Holz T and Wicherski G,"Botnet Tracking: Exploring a Root Cause Methodology to prevent Distributed Denial of Service Attacks", European Symposium of Research in Coumputer Security(ESORICS), 2005.

[11] Zhang J, Gu G,"BotMiner: Clustering Analysis of Network traffic for Protocol and Structured Independent Botnet Detection", Distributed Framework and Application(DFMA), 2008.

[12] Richard Carbone, Pierce M Gibbs,"Botnet Tracking Tool", Global Information Assurance Certification(GIAC), August 8, 2014.

[13] Joe, M. Milton, and B. Ramakrishnan. "Enhancing security module to prevent data hacking in online social networks." Journal of Emerging Technologies in Web Intelligence 6.2 (2014): 184-191.

[14] Joe, M. Milton, B. Ramakrishnan, and R. S. Shaji. "Prevention of losing user account by enhancing security module: A facebook case." journal of emerging technologies in web intelligence 5.3 (2013): 247-256.

[15] Joe, M. Milton, and B. Ramakrishnan. "Novel authentication procedures for preventing unauthorized access in social networks." Peer-to-Peer Networking and Applications 10.4 (2017): 833-843.