ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

Design and Detection of Social Media Botnets using Event-Driven Analysis

Payal Chandak[1], Prof. H. P. Channe[2]

M.E. Student, Department of Computer Engineering, PICT, Pune, India [1]

Assistant Professor, Department of Computer Engineering, PICT, Pune, India [2]

ABSTRACT: Botnet is a network of compromised computers under the control of a malicious actor. A botnet is a number of Internet-connected computers communicating with other similar machines where components in a network communicate and coordinate their actions by command and control (C&C) or by passing messages to one another like IRC botnets. We are going to develop such social media botnet which will trigger the zombie computer by some particular pre-determined keywords. The detection method will monitor the logs of the network and detect such botnets by event-driven analysis for example attacks from DDoS botnet, a spamming botnet, etc. The network will be monitored and logs will be generated which further will be analysed and perform the detection method depending on the results.

KEYWORDS: Social Media Botnets, Event-Driven Analysis, Twitter and Facebook Botnet detection.

I. INTRODUCTION

A botnet is a number of Internet-connected computers communicating with other similar machines where components in a network communicate and coordinate their actions by command and control (C&C) or by passing messages to one another like IRC botnets. A botnet is a number of internet computers that owners are unaware about and are setup to forward transmissions to other machines on internet. All such machines are referred to as a computer robot that follow their master's commands.

According to reports, botnets pose the biggest threat to internet computers that are most susceptible to such botnet attacks or being included in the zombie army are the ones without firewalls and antiviruses. Most of the home users have high speed internet connection that may be inadequately protected. Zombie is often created through open internet ports through which a trojan program can be left for future activation. Sometimes a botnet army controller can unleash the effects of the army with the help of single command.

The computers that form a botnet can redirect transmissions or packets to a website that can be closed down due to too much traffic handling also known as DDoS attack. The purpose of such a zombie army creator is to defeat a competitor. Zombie masters rely on unprotected computers.

Cyber criminals use social media botnets to spread malicious links, collect intelligence and spread influence. Unlike traditional botnets, social media botnets represent an automated social account instead of an infected computer. This means building a chain of interconnected bots is much easier than traditional methodology botnet creation.

The person controlling the botnets also known as bot herder has two options for building botnets. The first is registering as many accounts as possible that allows the herder to post through this accounts as if they are logged in. The second is to create a botnet thought a registered network application. This is how ISIS built Dawn of Tide Gliding application, which acts as a centralised hub that posts en masse on behalf of all its users. [10]

There are various malicious activities going on without getting noticed generally. Similarly, this type of system is of a Botnets. These systems need to be identified and detected when they are active. Our system tries to find social media botnets which are activated through some predefined keywords. Thus, these kinds of system are yet to be analysed using event driven analysis which involves complete analysis of the traffic in the network by monitoring and recording the data.

A botnet is a number of Internet-connected computers communicating with other similar machines where components in a network communicate and coordinate their actions by command and control (C&C) or by passingmessages to one another like IRC botnets. There are botnets which use social media which is the largest communication platform. These botnets need to be detected because they can cause various attacks. Our system consists of a detection method which will monitor the logs of the network and detect such botnets by event-driven

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

analysis for example attacks from DDoS botnet, a spamming botnet, etc. The network will be monitored and logs will be generated which further will be analyzed and perform the detection method depending on the results.

II. RELATED WORK

A botnet is a number of Internet-connected computers communicating with other similar machines where components in a network communicate and coordinate their actions by command and control (C&C) or by passing messages to one another like IRC botnets. There are botnets which use social media which is the largest communication platform. These botnets need to be detected because they can cause various attacks. Our system consists of a detection method which will monitor the logs of the network and detect such botnets by event-driven analysis for example attacks from DDoS botnet, a spamming botnet, etc. The network will be monitored and logs will be generated which further will be analyzed and perform the detection method depending on the results.

Types of social media botnet attacks:

1. Hashtag Hijacking: Hashtag Hijacking is mainly leveraging a Hashtag to target certain organisation or group by recognising group-specific hashtags, bots spread spam or malicious links that appear in group's circle and news feeds, focusing the attack on that group.[10]

2. Trend-jacking or Watering hole: This method is similar to that of hashtag hijacking where we use hashtags to direct the attack. The top trends are utilised to attack or spread the botnet to as much audience as possible. This way the attacker makes a social watering hole by using the trending keyword for potential victims. This technique is known as watering hole by considering a crocodile at the edge of a watering hole and letting the prey come to him.

3. Spray and pray: In this technique, we post as many links as possible and hope to get few clicks on each link. These bots will generate programmatically text based posts so that they are not detected by social network's terms of service radar. This technique often leverages click bait and is used along with any
of the above technique.

4. Retweet storm: In this method, a tweet is instantly reposted or retweeted by thousands of other bot accounts, thus the name retweet storm. This sort of malicious activities results in the original posting account getting flagged and banned, but the reposts and retweets are not deleted. In this technique, the parent account is known as the martyr bot as it sacrifices itself to spread the malicious bots.

Tzy-Shiah Wang, Chih-Sheng Lin, Hui-Tang Lin, have considered the aspect of Domain Generation Algorithm (DGA) botnet detection mechanism. They propose a defending mechanism for detecting DGA botnets which algorithmically generate domain names to improve their survivability where the hosts and NXDomains are grouped into clusters in accordance with the query behaviours between them, and each cluster is then identified as either malicious or benign depending on social network analysis.[1]

JoakimErsson, EsmiraldaMoradian, in their paper Botnet Detection with Event-Driven Analysis have considered event-driven log analysis software system enables detection of botnet infection on the user's system. Furthermore, to optimize software functionality an experiment that demonstrates how botnet communicates between itself and the command and control is described. The proposed software system was designed to facilitate detection of botnets for users that lack knowledge about botnet analysis. Moreover the system notifies users, i.e. sends a warning message in case of their machines become a part of botnet.[2]

Long Mai and Minho Park, present that K-means gets the best result compared with other algorithms in hybrid model. Mini Batch K-means can also get similar detection rate of K- means clustering but in less time processing. To improve performance, they needed more training data, hence detection rate was higher with better stability.[3][7]

R. A. Al-Dayil and M. H. Dahshan, in their paper "Detecting social media mobile botnets using user activity correlation and artificial immune system," have developed a method to detect mobile botnets that use online social networks such as Twitter as their Command and Control channel. They have developed a full implementation of the system on Android platform and tested it against multiple datasets of randomly generated tweets containing legitimate

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

tweets generated by user, approved applications and bots. The test results have shown that the proposed system can identify the type of tweet with very high accuracy. The accuracy of the detection improves after the signature library of the system has been trained with user input, scoring up to 95 percent.[4]

Naseem F, Shafqat M, Sabir U and Shahzad A, in their paper A Survey of Botnet Technology and Detection, discussed briefly the emergence of botnets, their organization and architecture and botnet life cycle steps. The reputed botnet types; the architecture they use and their different possible detection techniques.[5]

III. PROPOSED ALGORITHM

A. Proposed Problem Definition

To develop and detect social media botnets which use command and control protocols in Client-Server architecture by event-driven analysis.

B. Proposed System Architecture

The system consists of user's machine which are vulnerable and susceptible to attacks and a botnet twitter account. The system has malicious files which contains some keywords. Each keyword has a different functionality related to it. This functionality is actually different kind of attacks to be performed after botnet activation. The twitter account can be created and handled using various twitter APIs which in this project will be restful API. Using the API we can generate the key for the twitter account and then we can operate it from command line. The botnet twitter account will post some tweets which could contain the keywords. Thus, the user system will continuously monitor the twitter account and keep comparing the keywords.

Once the keyword is matched the system will activate the botnet on that machine and perform the corresponding attack. These attacks could be DDoS, spamming attack, keylogger attack, etc. These three attacks will be performed in our project for some corresponding keyword.

After the attack by the botnet, the mechanism used to prevent the botnet attacks consists of a botnet detection software which can be activated and deactivated by the user at any time. This software after being activated will monitor the network traffic and keep the logs. These logs will be analysed and then the pattern is recognised for malicious activities. These activities will be monitored using wireshark software and the analysis can be applied to the packets sent, sender's IP address, packets received from certain sender, packets rerouted, packets sent to international IP address, no. of packets sent, frequency of packets sent, etc. This way the monitoring activity can be performed.

After the monitoring, the logs are analysed and stored in the database. These logs help in determining the botnet activities. After determination of the botnet attack, various actions will be performed depending on the type of the attack. If the attack type is that of a keylogger then the attacker's files will be found and deleted so that no further keylogger actions are recorded.

One can also remove the keylogger data from the clipboard thus entirely preventing the botnet attack as the data is deleted before getting stored into the botnets files.

As the above process results in using different techniques for all the different types of attacks we implement a better method which can help us to remove botnet for all the attacks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

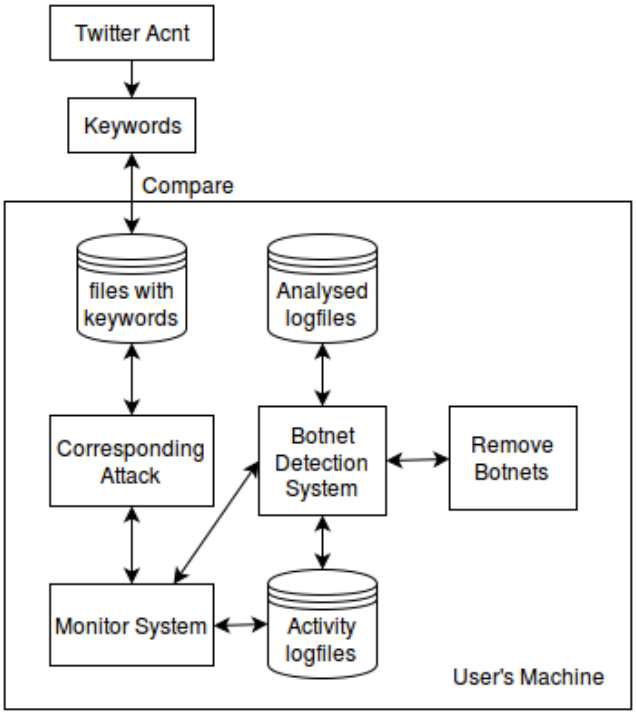

Fig. 1. Social Media Botnet Detection System Architecture

In this system, we are going to use the netstat tool to detect the process which is interacting with the botnet and then we are going to remove the process and the folders associated or modified by the process. This way for all the types of attacks we can directly remove the malware in association with twitter botnet.

IV. SIMULATION AND RESULTS

It is indeed feasible to make an event-based social media botnet detection technique to detect social media botnets. During the evaluation, we notice that in our proposed approach the systems could suffer because of the botnets if there is a delay in detection thus we have subjected the attacks to minimal amount and only sometimes to monitored systems a full-fledged attack is performed. Detection of different types of attacks is performed for different social-media sites.

Following are the results screenshotted of my system:

```
$
$ # 98.158.178.231 is a real C&C server. We are using netcat to make connection to
$ # mentioned C&C server. Here, netcat is acting like a malicious code on victim's
$ # PC and communicating with C&C server.
$
$ netcat -z -v 98.158.178.231 1-1000
netcat: connect to 98.158.178.231 port 1 (tcp) failed: Connection timed out
```

Fig 2. Netcat acting as Botnet Malware connecting to real C&C Server

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 5, May 2017

```
$ # Botnet Detection Algorithm scans all the runnning process in the PC. It
$ # determines the remote server's ip and port that processes are connecting to.
$ # If the process is connecting to known C&C server, then most probably the
$ # process is a malicious botnet code
$
$ python main.py
Local Address       Local Port          Foreign Address     Foreign Port        Process ID          Process Name
192.168.0.127       52152               98.158.178.231      2                   2664                netcat
$
$
```

Fig 3. Detection Algorithm

V. CONCLUSION AND FUTURE WORK

In the proposed system, I have developed a social media botnet which triggers the zombie computer by some particular pre-determined keywords. The detection method monitors the logs of the network and detects such botnets by event-driven analysis for attacks DDoS botnet, a spamming botnet, keyloggers etc. The network is monitored and logs are generated which further are analysed and after detection using netstat tool and analyses of logs are removed along with the botnet controlled files. In future, we can expand the botnets for more social media sites and different types of attacks and detection technique.

REFERENCES

1. T. S. Wang, C. S. Lin and H. T. Lin, “DGA Botnet Detection Utilizing Social Network Analysis”, 2016 International Symposium on Computer, Consumer and Control (IS3C), Xi’an, 2016, pp. 333-336.
2. JoakimErsson, EsmiraldaMoradian, “Botnet Detection with Event-Driven Analysis”, 17th International Conference in Knowledge Based and Intelligent Information and Engineering Systems, Volume 22, 2013, Pages 662-671.
3. Long Mai and Minho Park, “A Comparison of Clustering Algorithms for Botnet Detection Based on Network Flow”, 2016 IEEE, pp. 667-669.
4. R. A. Al-Dayil and M. H. Dahshan, “Detecting social media mobile botnets using user activity correlation and artificial immune system”, 7th International Conference on Information and Communication Systems (ICICS), Irbid, 2016, pp. 109-114.
5. Naseem F, Shafqat M, Sabir U and Shahzad A., “A Survey of Botnet Technology and Detection, International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS”, Vol: 10 No: 01.
6. C. Rossow et al., “SoK: P2PWNED - Modeling and Evaluating the Resilience of Peer-to-Peer Botnets”, 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, 2013, pp. 97-111.
7. T. S. Wang, C. S. Lin and H. T. Lin, “DGA Botnet Detection Utilizing Social Network Analysis”, 2016 International Symposium on Computer, Consumer and Control (IS3C), Xi’an, 2016, pp. 333-336.
8. JoakimErsson, EsmiraldaMoradian, “Botnet Detection with Event-Driven Analysis”, 17th International Conference in Knowledge Based and Intelligent Information and Engineering Systems, Volume 22, 2013, Pages 662-671.
9. Long Mai and Minho Park, “A Comparison of Clustering Algorithms for Botnet Detection Based on Network Flow”, 2016 IEEE, pp. 667-669.
10. R. A. Al-Dayil and M. H. Dahshan, “Detecting social media mobile botnets using user activity correlation and artificial immune system”, 7th International Conference on Information and Communication Systems (ICICS), Irbid, 2016, pp. 109-114.
11. Naseem F, Shafqat M, Sabir U and Shahzad A., “A Survey of Botnet Technology and Detection, International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS”, Vol: 10 No: 01.
12. C. Rossow et al., “SoK: P2PWNED - Modeling and Evaluating the Resilience of Peer-to-Peer Botnets”, 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, 2013, pp. 97-111.

BIOGRAPHY

Payal Chandak is an M.E. Student in the Computer Department, Pune Institute of Computer Technology, Pune University. Her research interests are Cyber Security, Network security, Malwares, etc.

Prof. H. P. Channe is an Assistant Professor in the Computer Department, Pune Institute of Computer Technology, Pune University. Her research interests are Computer Networks, Network Security, Distributed Systems, Wireless Sensor Network, IoT, etc.