Botnet Detection using Coarse Grained Algorithm

Pooja G P[1], Preethi K M[1], Rajini Y S[1], Shwetha S[1], Ms. Monika Nag K J[2]
[1]*Student, ISE/The National Institute of Engineering, Mysuru, Karnataka, India*
[2]*Assistant Professor, ISE/The National Institute of Engineering, Mysuru, Karnataka, India*
(E-mail: shwethavsrinivas79@gmail.com)

Abstract- BOTNET is a collection of private computers infected with hostile software which scans the very large segment of the Internet's address space for various motives, such as impair or distorting hosts, enlisting hosts into a botnet. These BOTNET's are usually controlled by remote attacker (the botmaster) using a command and control(C&asmp;C) channel. This paper deals with the designing of new network defence system for detection and prevention of peer-to-peer botnets using coarse grained algorithm. This paper deals with the subsequent 2 observations, 1. As a result of the convey with several alternative nodes botmaster or attack targets are easier to identify and 2. The infected machines activities interacts with one another than those of traditional machines.

Keywords*: Botnet, Botmaster, C&C channel, Coarse grained algorithm.*

I. INTRODUCTION

BOTNETs acts as the main channel for different types of cyber-crimes, such as junk email(sending unwanted emails), distribution denial of-service (DDoS) attacks, identity theft, fraud activities, etc. The Command and Control channel is an important part of a botnet because bot masters usually depends upon the Command and Control channel to send commands to their bots and receive information from the infected machines. Botnets can create their Command and Control(C&C) channel in different ways, hence we propose a Coarse-Grained [2] Detection of peer to peer [5] Bots Technique. This technique provides a pure security for the users to share their files. Here a server is maintained to track the number of data packets transferred in a network and an Admin module to check the log of attacker's and tracks the attacker's profile and IP address and cleans the attacks or block the IP address and attacker's profile. Here the blocking of BOT's or attacker's module works as an antivirus in the network. Hence we are presenting a novel botnet detection system

I. Existing System

Exiting methods does not depend on any transport layer used by which can be easily brutal by Peer to Peer applications .It is due to the fact that the web traffic profile Of a bot-infected host might be completely damaged by the legitimate Peer to Peer application running on it simultaneously. For example, in our experiments, when a Waledac and a Bitorrent application is running by host simultaneously, we require a flow clustering-based analysis approach to find out the hosts that runs Peer to Peer applications. A bot-infected host might be completely distorted by the legitimate Peer to Peer application running on it simultaneously

B. Proposed System

We concentrate on a different type of botnet scan that performed under the command and control of the botmaster, taking place over a well-delimited interval. In this paper we concentrate on detailed dissection of the scanning behaviour of the botnets, inclusive of normal methods to correlate, envision, and extends the behaviour of botnet across the global Internet. Before detecting Peer to Peer botnets in variance to our approach can detect and profile various Peer to Peer applications. We also recognise the performance of our botnet system and its scalability optimised. We presented a novel botnet detection system that is able to identify stealthy botnets, whose malicious activities may not be observable.

II. ARCHITECTURE

The system architecture construct the basic structure of the system, defining the important core design characteristics and components that produce the framework. The architecture view of the user's vision is also provided by the system architecture. Below figure shows the user login to the account and user can upload or download a file which are available in server. Login entity has two attributes Server IP address and port number for Server Botmaster. This is used to Connect Servant bots to Botmaster. Botmaster gives command to connected Servant bot, and give traffic for the Client bots. Deep packet inspection inspect the traffic for Servant, creating traffic for Client bots.

Initially botmaster will generate the bot files using bot generator module which is a file used to introduce undesirable behaviors in other systems. The generated bot files are sent to targeted users through the network channel called as BOTNET. When the targeted user receives the files, the appropriate action given in the bot files are performed in the user's system. Botmaster [3] can perform several actions which he wants to perform in the user system such as deleting a particular file, auto browsing, crash the user's system, and can reboot the system.

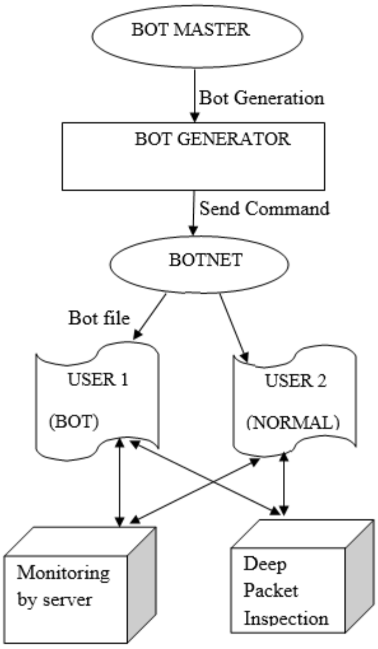

Fig. 1.0 Architecture

III. METHODOLOGIES

In this paper we present six modules which comprises of theoretical analysis of the following methods.

A. User Interface Design

A user interface (Window) has been designed for our project. The main function of these windows is to establish a communication between the two peers where one peer can send the message to another peer. In this module the Swing packages which are available in java are used to design the User Interface. In Java, Swing packages are Widget toolkits and it is part of Sun Microsystems' Java Foundation Classes (JFC) and also they are API for designing a graphical user interface (GUI) for Java programs.

B. Coarse Grained Peer-to-Peer Detection

In this module we mainly concentrate on the component which is responsible for identifying Peer to Peer [1] clients by examining the remaining network flows after traffic filters the component. For each one of the host, within the supervised network we recognized two different flow sets, indicated as Stcp(h) and Sudp(h), which includes the flows associated to successful outgoing Transmission Control Protocol(TCP) and User Datagram Protocol(UDP) connections respectively. Here we examined successful Transmission Control Protocol connections with a completed acknowledged handshake, SYN, SYN/ACK and those User Datagram Protocol (virtual) connections for which there was at least one "request" packet and a corresponding to that a "response" packet.

C. File Uploading and Sending

This method is used to transfer the appropriate file from storage devices to user account and then to transfer the file into destination account. There are many contrasting types of files are available for example: data files, text files, program files, directory files, and so on. Due to the availability of different types of file we can store different and huge amount of information which are necessary.

D. Bot Detection

Since bots are malignant programs used to accomplish commercial malignant activities, they constitute precious parts for the bot master, who instantly try to extend the utilization of bots. In the case of Peer to Peer bots, an appropriate number of peers needs to be online in order to have functional network (BOTNET), which means, the active time of a bot should be proportional with the active time of the underlying infected system.

E. Clustering and Eliminating

The Euclidean distance of the two equitable vectors is referred to as the distance between two flows. To separate the group of flows into a defined collection of clusters we apply a clustering algorithm [4]. Each one of the acquired flows of clusters, *Cj (h)*, constitute a collection of flows with same size. For each one of these *Cj (h)*, we determine a set of destination Internet Protocol addresses analogous to the flows in the clusters, we also review the BGP (Border Gateway Protocol) prefix for each one of these Internet Protocol.

F. Detection of Attacker IP Address

Based on the Internet protocol addresses, the geographical location of the website visitors can be recognized by this method for applications such as fraud detection.

IV. CONCLUSION

This implementation of the proposed system will help to detect the infected or compromised host efficiently compared to other techniques and also the proposed algorithm is accurate and cost effective. Botnets usually scans very large part of the internet address space for different activities such as impair or distorting hosts, enlisting hosts into a botnet. Here we come up with several methods to defend networks and computer systems against these malicious activities. The methods either aim at breaking the communication flow between bots and the Control and command server, or detecting signs of a successful invasion. Hence we come up with a novel botnet detection systems which are able to recognize a surreptitious peer to peer botnets, whose malignant activities cannot be observable.

V. REFERENCES

[1] P. Wang, S. Sparks, and C. C. Zou. “An advanced hybrid peer-to-peer botnet”. IEEE Transactions on Dependable and Secure Computing, 7(2), pp. 113-127, April-June 2010.

[2] T. Kocak, I. Kaya, "Low-power Bloom filter architecture for deep packet inspection", *IEEE Commun. Lett.* vol. 10, no. 3, pp. 210-212, Mar. 2006.

[3] X. Wang, D. Ramsbrock, *Live Botmaster Traceback*, Sep. 2009.

[4] Abdullah Al-Dhelaan, Mznah Al-Rodhaan, "An efficient and scalable density-based clustering algorithm for datasets with complex structures", *Neurocomputing*, 2015

[5] P. Wang, S. Sparks, C. C. Zou, "An advanced hybrid peer-to-peer botnet", *IEEE Trans. Depend. Secure Comput.* vol. 7, no. 2, pp. 113-127, Apr. /Jun. 2010.