Detection of Botnet Attacks By Filtering And Monitoring

Indu R
Dept. of Information Technology
Amal Jyothi College of Engineering
Kottayam, India

Monisha K. S
Dept. of Information Technology
Amal Jyothi College of Engineering
Kottayam, India

Joan George
Dept. of Information Technology
Amal Jyothi College of Engineering
Kottayam, India

Sneha Gandhi
Dept. of Information Technology
Amal Jyothi College of Engineering
Kottayam, India

***Abstract*— Today the term botnet is used to describe army of computers that are under the control of malicious conquering party. Botnets have been identified as the one of the most serious threats to network security. This is because there are increased cybercriminals coming up as there are lots of opportunities and advantages to them financially mainly. Bot attacks happen without the knowledge of the user and because of this it's a serious threat as it leads to many disadvantages to the user such as loss increased internet charge, private information being compromised, decrease in internet speed. This paper discusses the way in which botnet attacks can be detected by using filtering and monitoring.**

***Keywords*— Botnets, P2P, hackers, cybercriminals, DDoS**

I. INTRODUCTION

Bots and botnets have become a major concern for many organizations, including federal agencies. A bot is a computer that has been infected with malware and has specialized malicious tools installed so that it can attack other computers as directed by a hacker. Botnets are used every day in various types of attacks, they can compromise other computers and make them generate phishing e-mails and committing financial fraud.

In this paper we are trying to detect botnets on the basis of behavioral analysis (monitoring communication in a network for behaviors that are known to be exhibited by botnets).

Bot activities are often, although not always, closely coordinated with DDoS attacks and time-sensitive spam and phishing attacks, as evidenced by a sharp correlation in the timing of their networks activities.[1] For example, the controller instructs all bots to start sending their pump-and – dump spam payload at the same time. Network activity for individual bots are usually silent for much of the time, but tend to have a very high number of connections in a short period of time.

II. HISTORY

A botnet is a special kind of network that cybercriminals create by making one compromised system at a time. Hackers create botnets by sending a virus or malware to attack your computer or other device and turning it into a "zombie computer" by leaving a small program called a "bot" on it. Once the bot is on your system, it is no longer your system; it is under the control of the hacker. After you have lost control like the cybercriminal can use the system to send spam and phishing messages. But while your computer or device may be powerful enough for what you need, by itself it is not enough for the big business of cybercriminals. The cybercriminals take compromised systems and use them to build a vast and powerful network of systems at their command. Taken as a whole this network is called a botnet. Botnets have become the biggest sources of money for hackers and greatest dangers for the Internet. Anti-malware can help protect you and the Internet against virus and malware attacks by removing bots if they get on your system.

A. Peer to peer

A P2P computer network is one in which each computer in the network can act as a client or server for the other computers in the network, allowing shared access to various resources such as peripherals, and sensors without the need for a central server. [2] P2P networks can be used for sharing content such as audio, video, data, or anything in digital format. [2]

P2P is a distributed application architecture that partitions tasks or workloads among peers. [2] Peers are in the application who are equally privileged. Each computer in the network is referred to as a node. Peers are both suppliers and consumers of resources in contrast to the traditional client-server supply, and client consume data.

B. HOW BOTS ATTACK A NETWORK?

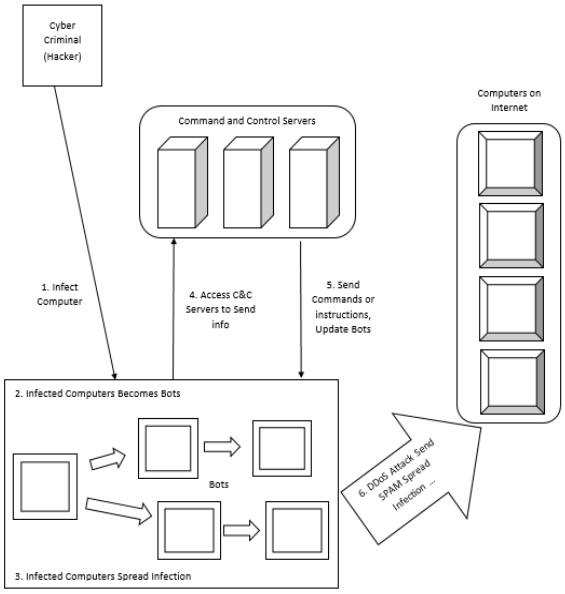

Fig.1 Botnet operation

The first stage of the bot attack is done by an external hacker. Usually the hacker attacks the weakest system (whether it is a stand-alone system or a systems in a network).This paper focuses on systems in a network which are attacked by an external hacker until the firewall breaks. When a system in a network (say A) is compromised by the hacker, system A and the hacker together attacks the next weakest system in that network. The weakest system will continuously get attacked until it is compromised and the network will become a group of bots called botnet.

Previously bots were used to help military personnel in controlling stand-alone computers from an external location. The personnel did not have to be there in person and dangerous situations could be avoided. Botnets also helped in sending of useful information to a group of computers.

Now botnets are used for generating phishing e-mails and committing financial fraud.

III. PROPOSED SYSTEM

The proposed system is a server-client system, where the server captures the packet and the client helps for detecting the bot. Any packet coming from an external source should be captured, monitored and checked whether it is a bot or not. Packet are transmitted through three modules. Transmission module, detection module and filtering module. The transmission module catches the packet, the detection module detects whether it is a bot or not and filtering module filters the packets in certain list namely black list and gray list.

IV. FIREWALL SYSTEM STRUCTURES

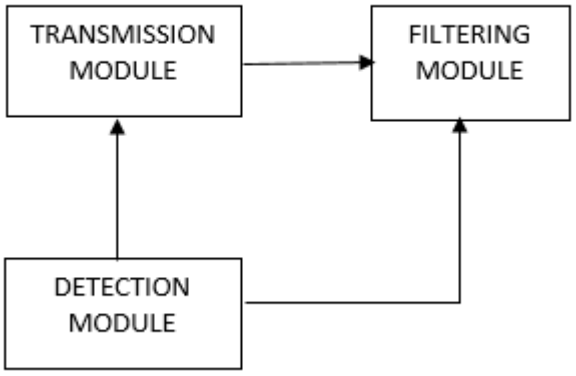

Fig.2 System

The main modules in this system consists of Transmission module, Detection module and Filtering module.

TRANSMISSION MODULE

Transmission module catches the packages from the network. It sends the package to the detection module for finding out whether or not it's a bot.

DETECTION MODULE

The detection module is where the detecting of a bot is done. In order to detect the bots we first check the frequency packets being sent. Once the number of packets being sent reaches a certain frequency we are able to check the packets to determine whether or not they are bots. After the frequency check we do the standard deviation using the following formula:

$$S_i = \sqrt{\frac{\sum_{i=1}^{n}(x_{ij}-\bar{x})^2}{n-1}}$$

S_i = standard deviation of packet
X_{ij}= time difference between the packets
$\bar{x}$ =mean difference of packets
n=number of packets

A repeated standard deviation is also performed using the following formula:

$$S_r = \sqrt{\frac{\sum_{i=1}^{p} s_i^2}{P}}$$

S_r= repeated standard deviation
P= number of samples
S_i=standard deviation

FILTERING MODULE

The filtering module filters the packets into gray list which contains the details of each and every packets which are captured by transmission module and black list which contains the details of affected packets.

V. OVERALL SYSTEM FLOW

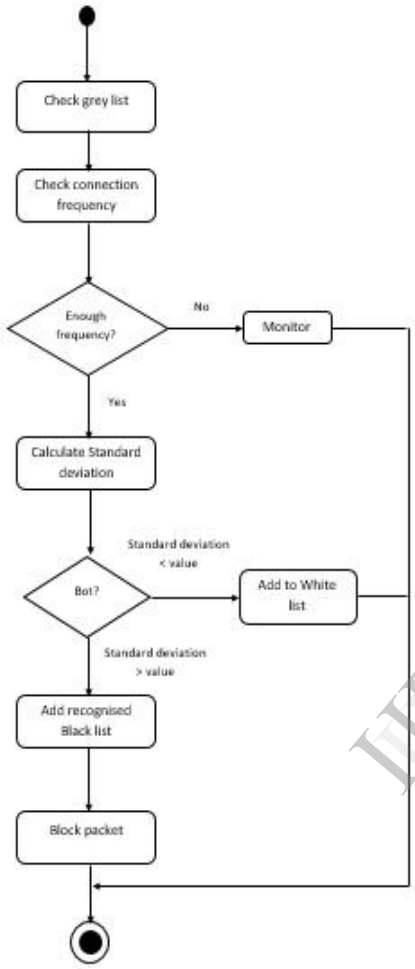

Fig.3 Process flow

In this system, when a package enters a system, the packet is put into the gray list and from there it is called to the proposed module. The proposed module then checks the connection frequency. If the connection frequency is not enough then the corresponding packet will be monitored. If the frequency is enough, then the proposed module calculates first the standard deviation then the repeated standard deviation (S_r). It checks whether the package is a bot or not. If it is an infected http bot the detection system will notify the user about the packet.

VI. EXPERIMENTAL STUDY

As a part of our project we have conducted a study on bots. We have implemented it on P2P network. It helped to detect the bot at early stage.

In the study we monitor the packets arriving to a particular system and if that corresponding packet is from a bot affected system then the details of that packet is given to black list which gives the details like ip address and hardware address of that corresponding packet. If not then we consider the packet as not being a bot and place it in the gray list and continue monitoring it.

Table 1. Black list

ip address	Hardware address
192.168.1.102	17:8cc:107:ab
192.168.1.100	17:8cc:108:ab
192.168.1.103	17:8cc:106:ac

The table above shows the details about the bot which contains ip address and hardware address.

VII. CONCLUSION

This system gives protection against attacks from external hackers. Botnet defense monitor will help the internet users to make a network bot free and protect the internet users. Our paper explains the effects of a bot and how best to detect bots in a network.

VIII. FUTURE WORK

In future we trying to implement prevention method which helps us to detect the origin of bot and how to destroy it completely .Not only bot but also all malicious programs can be detected and removed. It will be a complete network security system.

IX. REFERENCE

1. Microsoft Security Intelligence Report, http://www.microsoft.com/security/sir/story/default.aspx#!botnetsection_detecting
2. Antivirus.com, http://www.antivirus.com/security-software/definition/ botnets-detection/index.html
3. Guo-Quan Wei, Hung-Chang Chang, Tung-Ming Koo, “Construction of P2P firewall HTTP-Botnet defense mechanism”, IEEE 2011