Analysis of Botnet Detection

Mrs. Yogita Deepak Mane [#1], Prof. Kailas K. Devadkar [#2]

#1 Department of Computer Engineering, Sardar Patel Institute of Technology, Andheri (W).University of Mumbai, India.
#2 Department of Information Technology, Sardar Patel Institute of Technology, Andheri (W).University of Mumbai, India.

ABSTRACT

BotNets are major threat of the current Internet. It is widespread malware and it arises commonly in today's cyber crime, which results in serious threats to our network. The compromised computer is infected by viruses, worms, or it has become a target of network attacks only when operational state of a network component is shifted from normal state to abnormal state. Thus, prevention and detection of network systems from catastrophic failures is very important.
This paper gives brief idea about Bot, Botnet, life cycle of Botnet and there communication topologies. Paper also includes need of botnet, different methods to detect botnet, existing botnet detection tools and partial listing of major botnets present till date.

Keywords: Bot, botnets, communication topologies, command and control channel.

INTRODUCTION

Currently, the most serious demonstration of advanced malware [1] is Botnet. Botnets have been in existence from more than 20 years; experts have been given warning to the internet user about the malware (threat) posed by botnets for more or less the same period. Nevertheless, the scale of the problem caused by botnets is still underrated and many users have little understanding of the real threat posed by zombie networks. For a better understanding of Botnet, one must know the following terms first, Bot, Botnet and BotMaster.
The term *bot* [2] is derived from "ro-bot ".Bot is a generic term used to describe a script or set of scripts designed to perform predefined functions in automated fashion. Bots are used by search engines to spider online website content & by online games to provide virtual opponents.
Bot is a new type of malware installed into a compromised computer which can be controlled remotely by BotMaster for executing some orders through the received commands. After the Bot code has been installed into the compromised computers, the computer becomes a Bot. Contrary to existing malware such as virus and worm, where their main activities focus on attacking the infecting host, bots can receive commands from BotMaster and are used in distributed attack platform. BotMaster is also known as BotHerder. BotMaster is a person or a group of person which control remote Bots. Botnet is nothing but network consisting of large number of Bots. Bots usually distribute themselves across the Internet by looking for vulnerable and unprotected computers to infect. When they find an unprotected computer, they infect it and then send a report to the BotMaster. The Bot stay hidden until they are informed by their Bot Master to perform an attack or task. Other ways in which attackers use to infect a computer connected in network with Bot includes sending email and using malicious websites. The activities associated

with Botnet can be classified into three parts they are as follows. First is *Searching*, It is used to search vulnerable and unprotected computers. Second one is *Distribution*, It is used to install Bot code to the target computer, and last step is sign-*on* where the Bots connect to BotMaster and become ready to receive command and control traffic.

Difference between Botnet and other kinds of malware is as follows, Botnet works under command and control channel which is used to distribute commands to the bots to perform malicious activities such as form capturing, information grabbing, DDOS attack, spam, and phishing. It has divided into two application classifier one is centralize model (e.g. IRC and HTTP protocol) and other is decentralize model (e.g. P2P (single flux) and DNS (Fast flux)). The main activity of malware is to attack the infected host. Best example of virus and worm is SPAM mails which is spread through email attachment. To avoid such virus one need to scan mail or message and attached file before open it.

LIFE CYCLE OF BOTNET

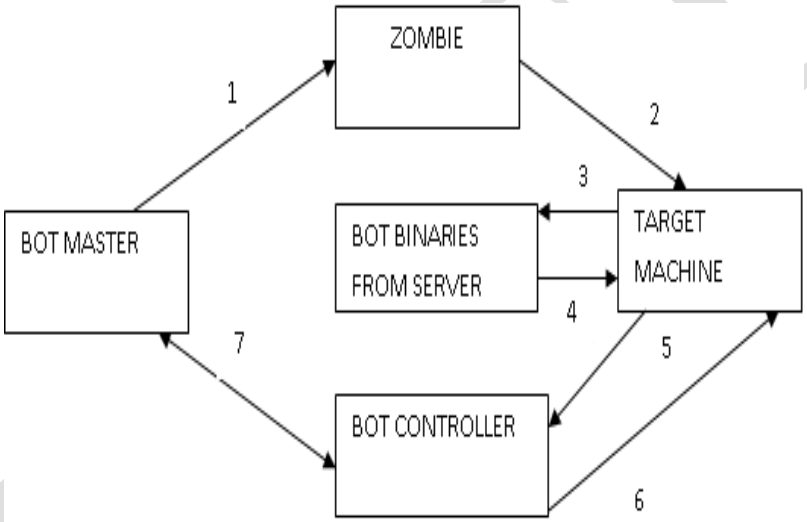


Fig. 1: Lifecycle of botnet

Fig. 1 shows working of Botnet Detection Life cycle. Flow of life cycle is as given in following steps;

1. BotMaster uses a zombie (exploit machine) to send primary infection to the victim machine. This can be done in form of sending email attachments.
2. Victim downloads the attachment and installs it on its machine so that it gets compromised.
3. The malicious Bot program which has been installed onto victim's machine opens network ports and enabling secondary infection.
4. The victim machine downloads the secondary infection through which the machine becomes the part of the Botnet.
5. The victim machine is now programmed to periodically send its status information to the bot.
6. Bot Controller sends a reply back to the victim machine and it also sends new commands from BotMaster.
7. BotMaster sends commands to the Bot controller which in turn passes to all the victim machine.

BOTNET COMMUNICATION TOPOLOGIES

According to the Command-and-Control(C&C) channel, Botnet topologies are categorized into two different models, Centralized model and the Decentralized model. Differences between these two models are as follows.

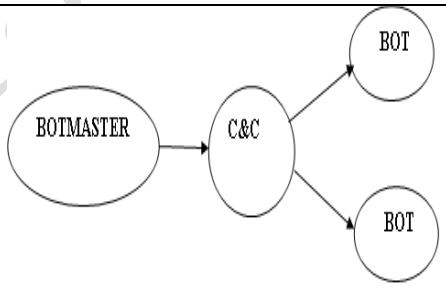
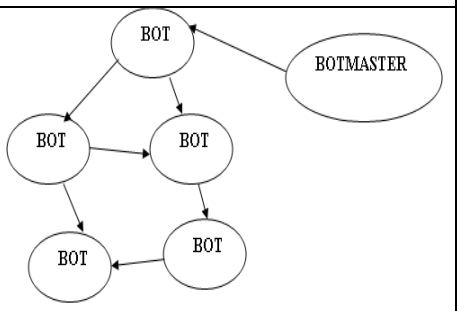
Sr.No	Points	Centralized Model	Decentralized Model
1.	Purpose	In this model, one central point is in charge for exchanging commands and data between the BotMaster and Bots. As shown in fig.2	This model does not depend on any central point. It has Command and Control channel which is used to exchange command and data between BotMaster and Bots. As shown in fig.3
2	Protocol	In this model, server runs on certain network services such as IRC or HTTP.	In Decentralized model, server runs on network services as P2P (Single flux) and DNS (Fast flux)
3	Advantage	It has small message latency which causes BotMaster to easily arrange botnet and launch attack.	1. It doesn't have central point of failure, so it is difficult to discover and destroy botnet. 2. The over-all cost of building and maintaining this type of network is comparatively very less. 3. P2P is more reliable as central dependency is eliminated. Failure of one peer doesn't affect the functioning of other peers.
4	Disadvantage	C & C server is the weak point in this model, if somebody manages to discover and eliminate the C&C server, the entire botnet will become useless and ineffective.	Peer to peer networks are good to connect small number (around 10) of computer and places where high level of security is not required.
5	Figures	 Fig.2	 Fig.3

Table1: comparison between Botnet Communication topologies.

NEED OF BOTNET DETECTION

P2P networks are responsible for handling large amount of traffic on the Internet because many Internet users utilize such network for content distribution. At the same time P2P networks are vulnerable to security threats. Consequently, the detection approaches designed for IRC or HTTP based Botnets may become ineffective against the new P2P based Botnets. Therefore we need to develop a next generation Botnet detection system, which is effective in the face of P2P based Botnets as well.

Botnet are used for various purposes, most of them related to illegitimate activity. Some of their uses include launching distributed denial-of-service (DDoS) attacks, sending spam mails, Trojan and phishing email, illegally distributing pirated media, serving phishing sites, performing click fraud, and stealing personal information [3,4]. They are also the sources of massive exploit activity as they recruit new vulnerable systems to expand their reach. Botnets have developed several techniques in their malware and infrastructure that make them robust to typical mitigation techniques. Due to their sheer volume, diverse capabilities, and robustness they pose a significant and growing threat to the Internet as well as enterprise networks. The threats undermine the reliability and utility of the Internet for commerce and critical applications. Therefore for better understanding of the structure, individual Botnet is needed to formulate appropriate mitigation strategies. So to avoid all these illegitimate activity we need to detect and deactivate Botnet to provide secure network system and to prevent cyber threat and cyber crime.

LITERATURE REVIEW

Network security is a critical issue and a challenge to professional system developers in means of protection against miscellaneous attacks aimed at any resource that is of interest to the attacker. Over the years, with the increasing number of computer systems connected to the global Internet, even the average users must be aware of the external threats and therefore also take some kind of precautions in order to protect themselves from these threats such as installation of antivirus, keeping the system up-to-date, etc. However, from a business' or an organization's point of view, security assessments are of a greater importance and must be acknowledged and valued in order to form the security policies that are associated with an organization or a business.

As shown in Table 2, there are two main existing approaches to detect botnet they are as follows. First approach to detect botnet is Honeynet [13], which is used to track malicious activity. However honeynet is mostly used to understand the botnet characteristics but do not necessarily detect botnet and bot infection. Second approach is Passive network traffic monitoring [13] which is useful to identify existence of botnet. Passive network traffic monitoring is classified into four different techniques they are as follows; signature-based, anomaly based, DNS based and Mining based.

Jin Zhigang, Wang Ying [1], defines Semi-Distributed topology in P2P Botnet Detection and the main idea behind this paper is to find abnormality of botnet computer by using sociality analysis, which is the branch of data mining and analysis of traffic characteristics by using Radial basis function of neural network. By using this technique Researchers has Discovered Photbot and Zeus bot.

Signature Based	Anomaly Based	DNS Based	Mining Based	Network based
1.It is used to Detect only Known bots 2. Zero day attack cannot be detected by this method. 3. **Rishi** and **Snort** tools are used to detect known bots and can applicable only for IRC protocol.	1. This technique is based on following network traffic anomalies; High Network latency, High volume of traffic, traffic on unusual port and Unusual system behavior. 2. Advantage- It is used to detect unknown bot. 3. Disadvantage -It is used only for IRC protocol. It is not used to identify botnet C&C traffic because C&C traffic is not with high volume and does not cause high network latency.	1. This technique is used to Detect DNS traffic by DNS monitoring and can easily detect DNS traffic anomalies 2. It is used to Detect domain name with unusually high or temporally intense of DDNS query. 3. Advantage- It is used to detect DNS traffic anomalies.	1. It is used to identify Botnet C&C traffic. 2. This technique includes machine learning process, classification of data, and clustering to detect botnet. 3. Disadvantage: In this method, it is difficult to detect botnet C&C traffic.	1. This method tries to detect Botnets by monitoring network traffics. 2. Network based is Classified in to two techniques; one is Active Monitoring and second one is Passive Monitoring technique.

Table 2 - Comparison of different Botnet detection Techniques.

Hossein Rouhani, Azizah Bt Abdul Manaf [2, 4] explains the concept of P2P botnet detection based on IRC (Centralized) communication topology. The main idea behind this paper is passive network traffic monitoring. In[4] they define another technique to detect P2P Botnet based on Traffic monitoring by using similar communication pattern and for this researchers have used open source tool such as ARGUS (Audit record Generation & Utilization Tool).

Osman salem, Ali Makke,Jean tajer[5] discovered a technique to detect DDOS Attack. Idea behind this paper is that it defines method of Traffic Monitoring and anomaly detection over high speed network and the result of analysis of large number of traffic flow is stored in Hash table.

Alireza shahrestani, Maryam feily, rodina Ahmad, Sureswaran ramadass[3] , shows a technique of traffic monitoring by using Visual network monitoring system to detect botnet traffic in small and medium size network. This system works under Passive Network traffic monitoring system including Visual threat monitoring. This provides interfacing between botnet traffic and visual threat monitoring by HCI (human computer Interface).

Gu et al. has proposed Botsniffer [7] that uses network-based anomaly detection to identify Botnet C&C channels in a local area network. Botsniffer is based on observation that bots within the same Botnet will likely reveal very strong similarities in their responses and activities. Therefore, it employs several correlation analysis algorithms to detect spatial-temporal correlation in network traffic with a very low false positive rate [7].

Botminer [8] is the most recent approach which applies data mining techniques for Botnet C&C traffic detection. Botminer is an improvement of Botsniffer [7]. It clusters similar communication traffic and similar malicious traffic. Then, it performs cross cluster correlation to identify the hosts that share both similar communication patterns and similar malicious activity patterns. Botminer is an advanced Botnet detection tool which is independent of Botnet protocol and structure. Botminer can detect real-world Botnets including IRC-based, HTTP-based, and P2P Botnets with a very low false positive rate [8].

Geobl and Holz [9] proposed Rishi in 2007. Rishi is primarily based on passive traffic monitoring for odd or suspicious IRC nicknames, IRC servers, and uncommon server ports. They

use n-gram analysis and a scoring system to detect bots that use uncommon communication channels, which are commonly not detected by classical intrusion detection systems [9]. Disadvantage of this method is it cannot detect encrypted communication as well as non-IRC Botnets.

Strayer et al. [10] proposed a network-based approach for detecting Botnet traffic which used two step processes including separation of IRC flows at first, and then discover Botnet C&C traffic from normal IRC flows [10]. This technique is specific to IRC based Botnets.

Masud et al. [11] proposed effective flow-based Botnet traffic detection by mining multiple log files. They proposed several log correlation for C&C traffic detection. They categorize an entire flow to identify Botnet C&C traffic. This method can detect non-IRC Botnets [11].

EXISTING TOOL FOR BOTNET DETECTION

Detail description of existing Botnet detection tools is as follows: Snort [6] is open source Intrusion detection tool. This is used to monitor network traffic to find signature of existing bot. Advantage of sort is to protect the organization network from intrusion and it is used to detect only known bots. Disadvantage of Sort tool is that it is not feasible to detect unknown bots. BotSniffer [7] is anomaly based Botnet detection tool. It is used to identify Bot C&C channel in LAN. BotSniffer is based on observation that bots within same Botnet will likely reveal very strong similarities in their response and activities. Advantages of this tool is that; It uses several correlation algorithms and It has very low false positive rate and Disadvantage of this method is that If Botnet traffic is normal traffic, this type of method cannot detect it and it is used to detect only IRC and HTTP. BotMiner [12] BotMiner is the most recent approach which applies data mining techniques for Botnet C&C traffic detection. BotMiner is an improvement of BotSniffer [7].It clusters similar communication traffic & similar malicious traffic. Then, it performs cross cluster correlation to identify the hosts that share both similar communication pattern & similar malicious activity patterns. Advantage of this method is that; it is used to detect IRC, HTTP and P2P encrypted Bot and it has low false positive rate. Disadvantage for this method is that; If the Challenger finds detection framework and implementation of BotMiner, they might get some ways to avoid detection. For example if challenger does some changes in clustering or in the cross correlation plane. Rishi [9] this technique is discovered by Geobl & Hal. This method detect only well known bot. Rishi uses IRC Bot nickname pattern as signature. The main disadvantage of this method is that it is not used to detect non IRC Bot and encrypted bot. Karasaridis et al[13][15] has study network flows and detect IRC Botnet controllers in a fashion of following steps; in which, the most important one is to identify hosts with suspicious behavior and isolate flow records to/from those hosts. Disadvantage of this method is that it is used to detect only for IRC Botnet. Gu et al.[14][15] has proposed "BotSniffer" that uses network-based anomaly detection to identify Botnet C&C channels in a local area network. BotSniffer is based on observation that bots within the same Botnet will likely reveal very strong similarities in their responses and activities. Therefore it employs several correlation analysis algorithms to detect spatial-temporal correlation in network traffic with a very low false positive rate [7]. Disadvantage of BotSniffer is that it is used only for IRC and HTTP. Bro [16] is an intrusion detection system; that works by passively watching traffic seen on a network link in real time. It is built around an event engine that pieces network packets into events that reflect different types of activity

SR.NO	BOT NAME	YEAR	DESCRIPTION	Protocol Type
1.	GM	1989	It is type of centralized protocol, which assist user to manage their own IRC connection.	Centralized-IRC
2.	EggDrop	December1993	It is recognized as early popular non-malicious IRC bot.	Centralized-IRC
3	GTbot(Global Threat) Variants	April 1998	New capabilities of GTbot are as follows; port scanning, flooding and cloning. It support UDP and TCP socket connections. It also supports IRC Server to run malicious script.	Centralized-IRC
4	Pretty park	May 1999	It was reported in June 1999 in Central Europe Internet Worm. The main purpose of this Trojan is to steal password.	Internet Worm
5	Subseven	1999	It is remote controlled Trojan.	Trojan.
6	Napster	May 1999	It comes under Peer-to-Peer model. It was initially widely used as hybrid Model, next variation was central based and now it is working under peer-to-peer model.	Decentralized –P2P model.
7	Direct Connect	November1999	It is based on Peer-to-Peer model. It is a variation of Napster hybrid model.	Decentralized –P2P model.
8	Gnutella	March 2000	It is decentralized peer-to-peer protocol	Decentralized –P2P model.
9	eDonkey	September 2000	eDonkey is Peer-to-Peer bot. It is used as checksum directory lookup for file resources.	Decentralized –P2P model.
10	Fast Track	March 2001	It made use of super nodes within the peer-to-peer architecture.	Decentralized –P2P model.
11	WinMX	May 2001	It comes under Peer-to-Peer bot. It is a proprietary protocol similar to FastTrack.	Decentralized –P2P model.
12	Ares	June 2001	It is a Peer-to-Peer bot. It has ability to penetrate NATs with UDP punching	Decentralized –P2P model.
13	BitTorrent	July 2001	It is a Peer-to-Peer bot, which uses bandwidth currency to foster quick downloads.	Decentralized –P2P model.
14	SDbot	April 2002	It is Written by Russian Programmer by the name 'SD'. He wrote 40Kb C++ Code, which was malicious bot. It was first publish for hackers via website. This code provides e-mail and chat for support. It also Provides own IRC client for better efficiency.	Centralized-IRC
15	Agobot	October 2002	It is modular update SDBOT. This bot is Incredibly robust, flexible, and has modular design.	Centralized-IRC
16	Spybot or Milkit	April 2003	It is type of malicious bot, which is derived from SDbot. It comes with spyware capabilities. It spread via file sharing applications and has e-mail with extensive feature set, based on Agobot.	Centralized-IRC
17	Rbot	2003	It is backdoor Trojan based on IRC. 1.9 million PCs got affected worldwide by using this bot.	Centralized-IRC
18	WASTE	May2003	It comes under peer-to-peer bot. It uses small VPN-style network with RSA public keys.	Decentralized –P2P model.
19	Sinit	September 2003	It is malicious bot. It is Peer-to-peer bot. it uses random scanning process to find peers.	Decentralized –P2P model.
20	Kademlia	November 2003	It is Peer-to-peer type of bot. It uses distributed hash tables for decentralized architecture.	Decentralized –P2P model.
21	Photbot	March 2004	It is malicious bot. It worked under Peer-to-peer model.	Decentralized –P2P model.
22	MyBot	2005	MyBot is New version of SpyBot. It uses concept of Hybrid coding. This bot is spread via file sharing applications and e-mail attachment.	
23	P2P Based Bot	2006-2007	This is malicious bot. It has 2 generation they are as follows; 1st generation - "March-2006 SpamThru", " April 2006 Nugache" Based on "Gnutella" file sharing 2nd Generation – " January 2007 Peacomm' Pure Distributed P2P	Decentralized –P2P model.
24	"Storm Botnet"	2007	It is truly pure P2P bot, which has no single point of failure. It provides high resilience, scalability and difficulty in tracking.	Decentralized –P2P model.
25	Stuxnet	2010	It spreads via Microsoft Windows, and a target was 'Siemens industrial software and equipment'.	
26	Duqu	September 2011	Duqu is a computer worm discovered on 1st September, 2011.	

BACKGROUND OF ALL TYPES OF BOTS:

Partial listings of bots are illustrated by Table 1.

PROPOSED SYSTEM ARCHITECTURE

Proposed system architecture is shown in fig. 3. It includes following components.

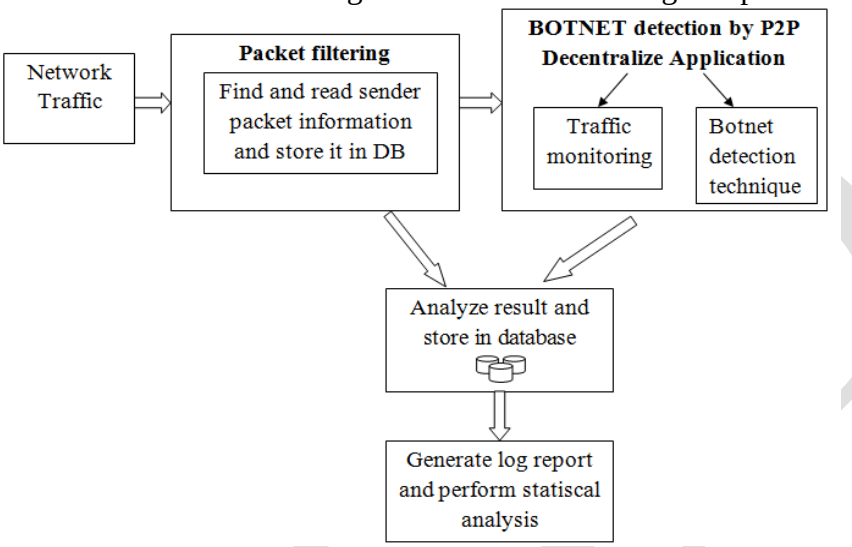


Fig. 3 Proposed System Architecture for Botnet detection

1. Packet Filtering: The main objective of Packet Filtering is to reduce the traffic workload and to make rest of the system perform more efficiently.
2. Traffic Monitoring: It is responsible to identify hosts that are likely part of Botnet during the time that hosts (bots) initiate attack, by analyzing flows characteristics and finding similarities among them. Therefore, this proposed model captures network flows and records some special information on each flow. Each flow record has following information: Source IP (SIP) address, Destination IP (DIP) address, Source Port (SPORT), Destination Port (DPORT), name of Protocol and Active Time.
3. Botnet detection / malicious activity detector: It is used to analyze the traffic from the network and detect the possible malicious activities that machine is performing.
4. Analyze result and store in database: This stage is used to store records regarding packet filtering, traffic monitoring, most access port and malicious activity detector in database.
   Generate log report: This stage is used to generate log report which is used for analysis of victim machine. Log report is in the form of traffic monitoring, most access port information and Bar graph based on most access port

CONCLUSION

Today, botnets are used as main foundation to perform any criminal activity on the internet. Botnets are used as main weapon for cybercriminals. It is very difficult to detect and deactivate Botnet as compared to other kind of malware. The main object of this proposed work is to provide secure network service.

My proposed work is based on anomaly based detection method which is used to Detect and Deactivate P2P Zeus Bot from the victim machine. Detection process mainly based on traffic

monitoring, getting information of most access port number, plotting bar graph for most access port to represent information in graphical way and last to deactivate bot when it has been detected in victim machine.

REFERENCE

[1] Jin Zhigang, Wang Ying "P2P botnet detection based on user Behavior sociality & Traffic entropy function", IEEE 2012 [1].
[2] Hossein Rouhani, Azizah Bt Abdul Manaf," Botnet detection by monitoring similar communication pattern" 2010.
[3] Alireza shahrestani, Maryam feily, rodina Ahmad, Sureswaran ramadass, " Discovery of invariant bot behavior through visual network monitoring system" ,IEEE 2010 .
[4] Hossein Rouhani, Azizah Bt Abdul Manaf, "Botnet Detection based on Traffic Monitoring ", in IEEE 2010
[5] Osman salem, Ali Makke,Jean tajer ,"Flooding Attack detection in Traffic of backbone network" IEEE 2011.
[6] Snort IDS web page. http://www.snort.org, March 2006.
[7] Guofei Gu, Junjie Zhang, and Wenke Lee. "BotSniffer: Detecting Botnet Command and Control Channelsin Network Traffic." In Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08), San Diego,CA, February2008.
[8] G. Gu, R. Perdisci, J. Zhang, and W. Lee, "Botminer: Clustering analysis of network traffic for protocol- and structure independent Botnet detection," in Proc. 17th USENIX Security Symposium, 2008
[9] J. Goebel and T. Holz. Rishi: Identify bot contaminated hosts by irc nickname evaluation. In Proceedings of USENIX HotBots'07, 2007
[10] W. Strayer, D. Lapsley, B. Walsh, and C. Livadas, Botnet Detection Based on Network Behavior, ser. Advances in Information Security.Springer, 2008, PP. 1-24.
[11] M. M. Masud, T. Al-khateeb, L. Khan, B. Thuraisingham, K. W.Hamlen, " Flow-based identification of Botnet traffic by mining multiple in Proc. International Conference on Distributed Framework& Application,Penang,Malaysia.2008
[12]https://www.usenix.org/legacy/event/sec08leb/tech/ full_papers/gu/gu_html/
[13] A.Karasaridis, B.Rexroad and D. Hoeflin, 'Wide-scale botnet detection and characterization', in proceeding of 1st conference on Hot topic in understanding Botnets, Cambrige, MA, 2007.
[14] G.F. Gu, J.J. Zhang, and W.K.Lee, "BotSniffer: detecting Botnet command and control channels in network traffic', In proceedings of the 15th annual network and distributed system security symposium, San Diego, CA, February 2008.
[15] Wei Lu, Mahbod Tavallaee, Goaletsa Rammidi and Ali A. Ghorbani ,' BotCop: An Online Botnet Traffic Classifier ', in IEEE 2009.
[16] http://www.bro.org/bro-workshop-2011/slides/ broverview.pdf