Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Survey of Botnet Based DDoS Attack and Recent DDoS Incidents

Neelam Paliwal
Graphic Era Hill University, India

Ramesh Singh Rawat
Graphic Era University, India

Deepak Singh Rana
Graphic Era Hill University, India

Abstract— DDoS attacks are becoming a major headache for IT professionals because of DDoS attacks are regularly launched by well organized and widely spread botnet computers that are concurrently and accordingly sending large amount of traffic or service request to the target system. The target system either responds so slowly or crashes completely. DDoS attacks allow attackers to launch a much larger and more troublemaking attack. Botnets are superimpose networks built by cybercriminals from hacked the computers. In this paper, we have presented a comprehensive classification of Botnet according to the communication protocol. We also categorized the Botnet based DDoS attack and detection techniques of the Botnet.

Keywords— Botnet, DDoS, IRC, P2P, Web server

I. INTRODUCTION

Denial of Service attacks slow down or totally suspend the service of the system. Attacker sends so many fake messages or request to a server there is the reason server crashes because of heavy load. According to Incapsula report 81 percent of DoS attack seen in 2014.Threat LandScape Report (2013-2014) says that DDoS attacks are becoming a major headache for IT professionals[1].

Botnet is a collection of interconnected bots (bots are autonomous programs automatically perform task absent of real user), receiving and responding to command through Command and Control(C&C) server i.e. IRC or HTTP server. Botnet servers may always communicate and cooperate with other botnet, which is controlled by individual or multiple Botmaster. Command and control server is uses to send instruction to his bots by Botmaster[2].

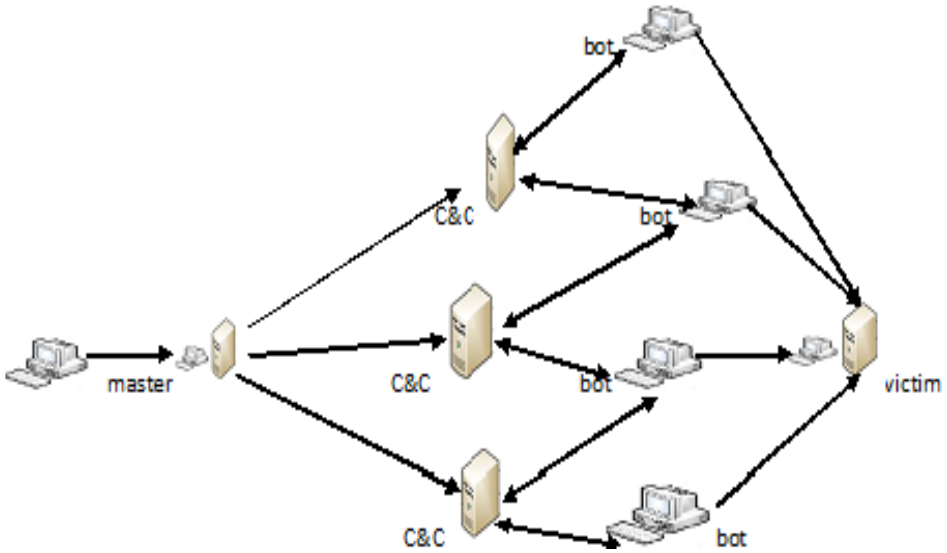

Fig. 1 Botnet based DDoS attack

DDoS attacks use botnet to produce floods of requests that reproduce burst crowds in client traffic. Bots are infected by malware like virus, worms. Some botnet make copies of themselves with the aim to infect many hosts. DDoS defense mechanism more challenging. First, a large number of bots involved in the attack that helps attacker to make the attacks larger and disruptive. Second, attacker use IP spoofing, which makes it very harder to trackback [3] .

DDoS attacks targets web server of companies, media, public and government server especially those providing service to users, control server of national infrastructure (like power or water supplies, traffic and communication industry, etc.) and information infrastructure (like DNS servers, Internet Exchange Points or Data center)[4].

II. MOTIVES OF BOTNET BASED DDOS ATTACK

Botnets are used for different motives like launching distributed denial of service attacks, sending spam, Trojan and phishing email ,illegally distributed pirated media, serving phishing sites, performing click fraud and stealing information among others[5].

- Activism, rivalry and business benefit
- Supports to frauds by disturbing or disabling of the prevention of the fraud
- Use for Extortion, terrorism and warfare
- Real money making business behind
- Most attacks are profit driven
- Revenge

III. COMMUNICATION PROTOCOL OF BOTNET

Botnet servers may always communicate and cooperate with other botnet, which is controlled by individual or multiple Botmaster. Command and control server used by Botmaster to send instruction to his bots. Command and Control sever classified into three categories:

A. IRC –based

IRC is an online text-based message protocol. It has client/server architecture with IRC channel to communicate between multiple servers. Hundreds of clients are connects with multiple server through the IRC. Attackers can use legitimate IRC ports to send command to bots. The use of legitimate IRC ports it make much more difficult to track DDoS command. Additionally, attacker can hide its presence because of IRC server have large traffic [3, 6]. Some IRC-based botnet tools are described:

1) *TRINITY:* The Trinity is one of the most IRC-based DDoS tools. It conducts UDP,TCP SYN, TCP ACK, and TCP NUL flood attacks. The Trinity v3 introduces random flag, TCP fragment floods, TCP established floods and TCP RST packet floods [3, 6].

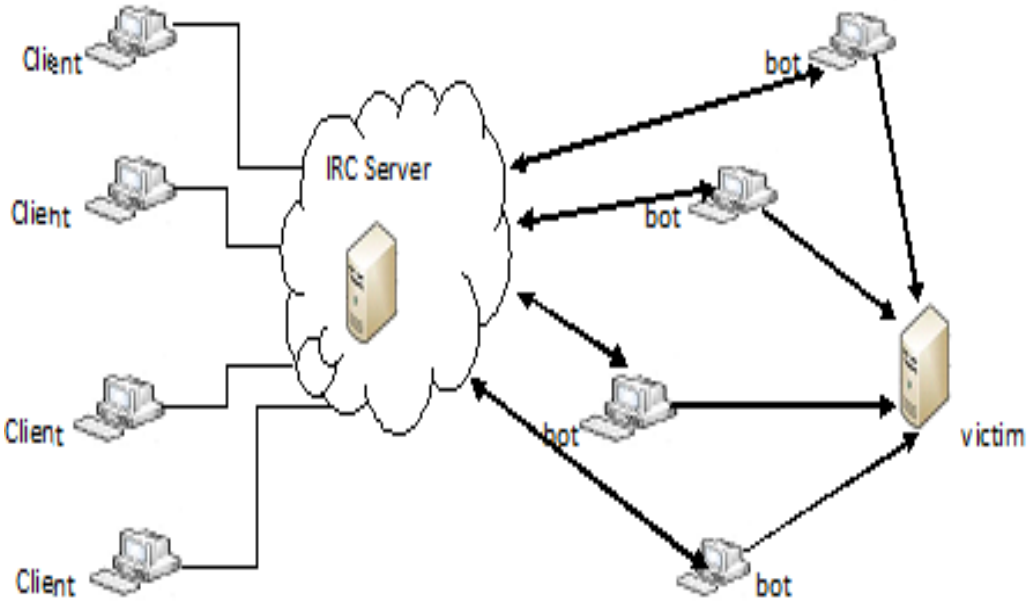

Fig. 2 IRC Protocol

2) *AgoBot:* In [7] , Agobot is a fully developed IRC bot .It has provided following features:

- *Delivery:* When first step exploits succeed, it open a shell on the remote host and download the bot binary. Encoded binary avoid network-based signature detection.
- *Function*: It can steal information of system and monitor local network traffic.
- *Exploits*: It can exploit OS vulnerabilities (e.g. Buffer overflow) and back doors left by other viruses.
- *Recruiting*: It recruits using botmaster restricted horizontal and vertical scanning.

B. Web-based

Attacker can use HTTP as a communication channel to send commands to the bots it makes more difficult to track. Web based botnet periodically downloads the instruction using web request. Instead IRC based botnet maintain the connection with C&C server[3]. In web model bots are reports information to a websites but other bots projected to be configured and controlled through complex PHP scripts. Communication channel is encrypted over 80/443 port and HTTP/HTTPS protocol [6]. Some web based tools are described.

1) BlackEnergy: BlackEnergy is web based distributed denial of service bot used by secretive Russian hacker. Black Energy simply control web based bots using a minimum syntax and structure and initiate the various attacks. Black Energy tool developed by one or more Russian hackers .one of the main feature this tool support in forums is the bot target more than one IP address per hostname. Black Energy C&C is built on PHP, MySQL[8].

2) Clickbot: Clickbot a low-noise click fraud bot. Attacker can launch Clickbot that propagated via email attachment. Botnet uses HTTP protocol as command and control server. Attacker participating in click fraud sends spams[7].

3) Low-Orbit Ion Cannon (LOIC): The LOIC is web based DDoS attack tool that liberates HTTP flooding in the server. Attacker generating large volume of HTTP traffic .This tool has been used by mysterious group to assist malicious traffic by the Zeus botnet, which is complex malware program that cannot be effortlessly removed [6].

C) Peer to Peer based (P2P)

Peer to Peer (P2P) botnet consist of three parts- Botmaster, Servent bots and client bots[9]. Peer to Peer has advantage that communication system is much difficult to disrupt. This means that cooperate of a single bot does not necessarily mean the loss of whole botnet. The peer to peer botnets are distinguishing from conventional botnets in that there is no central C&C server for a P2P[10].

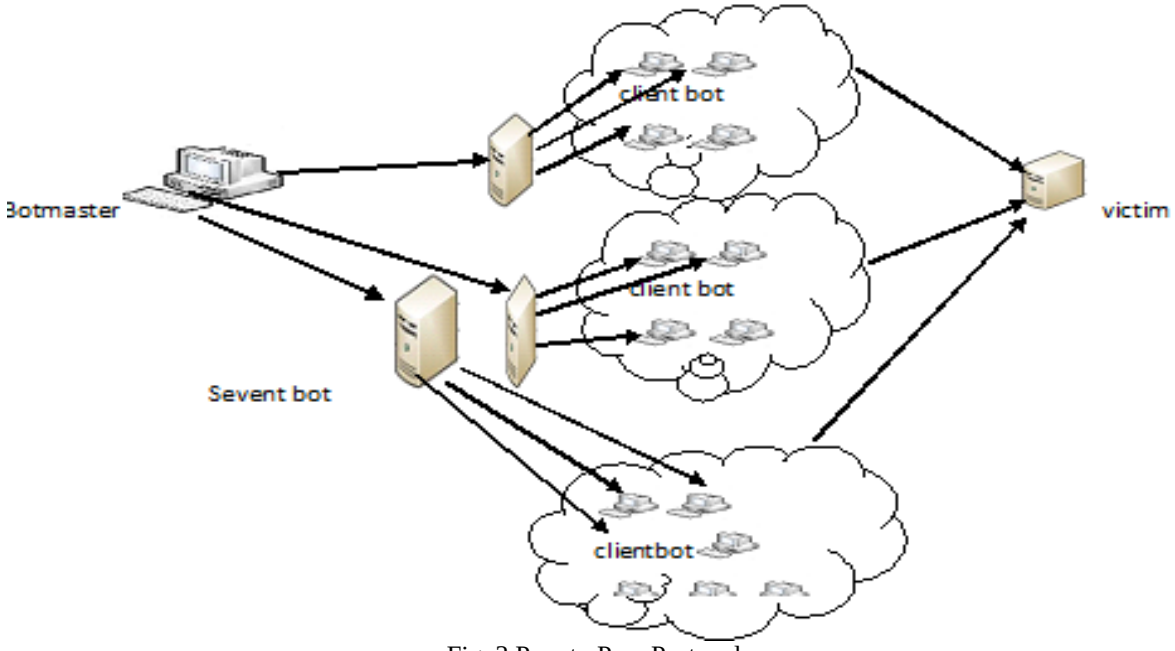

Fig. 3 Peer to Peer Protocol

1) *Zero Access:* ZeroAccess first show in the summer of 2011. ZeroAccess is a Trojan horse that uses higher means to hide itself by creating hidden file systems to store core components, download additional malware, and open a back door on the compromised computer. The primary incentive behind ZeroAccess is financial fraud through pay-per-click (PPC) advertising. It is the largest identified botnet that utilizes a peer-to-peer (P2P) command and control server for communication. There are two different versions of ZeroAccess. In May 2011, the first version (V1) was discovered and in the summer of 2012 the second version (V2) redesign of the Trojan's internals, emerged the ZeroAccessV2 [11].

IV. COMMAND AND CONTROL MODEL OF BOTNET

Attackers speedily send instructions to bot but also do not want that communication to be detected or the source of those commands to be revealed that hide own identity. Command and Control topology are classified in three categories.

A. Centralized

A centralized topology is distinguished by a center point that forwards messages between clients. In centralized system messages sent few well known hops. Message latency of centralized system would low. In centralized System have two major disadvantages. First, they can be easier to detect because of many clients connect the same point. Second, detection of center location can compromise the entire system[9].

B. P2P

Peer to Peer have several advantages over the centralized topology that communication system is much difficult to disrupt. This means that the cooperation of a single bot does not necessarily mean the loss of whole botnet. The peer to peer botnets are distinguish from conventional botnets there is no central C&C server for a P2P[10] .In P2P system have disadvantage C&C communication will experience unpredictable delay and it unsuitable for coordinated, large scale attacks [12].

C. Unstructured

In Unstructured topology, a bot that wanted to send a message that first encrypt the message and then arbitrarily scan the internet and pass the encrypted message when it detected another bot. The design of very simple and discovery of single bot would never compromise the entire botnet. The message latency would be exceptionally high, with no guarantee of message delivery[9].

V. CLASSIFICATION OF BOTNET BASED DDOS ATTACK

Botnet based DDoS attacks are classified into two categories:

A. Typical DDoS Attack

In a typical DDoS attack, an attacker sends attack command to the C&C server who triggers all attack procedures on the bots. Bots are waiting for correct command to start the attack. Then C&C server send command to bots, instruct them to raise DDoS attack against the victim. Bots initiate to send large volume of packets to the victim, exhaust its resources and overflowing its system with useless load[13].

B. Distributed Reflection DDoS Attack(DRDoS)

Distributed Reflection DoS attack architecture consists of C&C server and reflectors. In DRDoS attack attacker send command to C&C server then C&C server instruct the bots to send large volume of packets with victim's IP address as source of IP address to other pure systems (known as reflectors). This insists these reflectors to the victim because they judge that the victim was host that requested it. So that's why there is a large scale of traffic to the victim from reflectors for chance a fresh connection[13]. In January 2002, DRDoS attack had shut down a security research website(www.grc.com) [6].

VI. OVERVIEW OF BOTNET DETECTION

Our survey goes through some related papers to specific area. There are lots of methods and areas that implement the methods to detect the botnet based DDoS attack. However as these schemes are discussed, there are several drawbacks which are further fix and improved by many researchers.

In [14], proposed a two-tier detection foundation that improves the handling process in detecting and mitigating.. In [15], developed NAB("Not-A-Bot") , a system that roughly identify and certify human generated activity. NAB uses a small trusted software component called an attester, which run on client machine. In[16], proposed seven panel comic CAPTCHAs, based on using human ability to understand comic. There are many strategies that can be use to break the CAPTCHAs. Some popular CAPTCHAs cracking service available on the internet that use a combination of Optical Character Recognition and social engineering to bypass all types of CAPTCHAs[17].

In [18], proposed *FireCol,* a system for detection of flooding DDoS attacks. It is performed as close to attack source as possible, providing a protection to user and saving important network resources. *Honeypot[19],*a proactive detection mechanism that are not supposed to receive any legitimate traffic and analysed to divulge vulnerabilities targeted by attackers. In [19], proposed Roaming honeypots scheme to mitigate the effects of service level DoS attacks. In [20], proposed Snort's detection system which is based rules. Snort's based detection system can be real time efficient that counter unreliable DoS attack forms. In [21], proposed the detection model called the ERS, which is a process for recognizing the level type of a sample when compared with the standard values of the ERS index based on the experiential data. In [22], defined HCF (Hop Count Filtering) technique is used to detect the attack and to drop the spoofed IP packet. It can be efficiently implemented inside the Linux kernel. It is a simple and effective solution in protecting Internet servers against spoofed IP packets.

A. Botnet Detection Techniques

Botnet detection techniques are classified into five categories.

1) Anomaly Based

Anomaly based detection to perceive the behavior patterns[23]. This technique does not require any previous knowledge of signature that can discover both the C&C server and infected hosts[24].

- Bot behavior: analyze or detect the behavior of single bot(infected computer) with data.
- Botnet behavior: detect the behavior of groups of infected computers (botnet).
- Temporal behavior: detects behavior of bots or botnet changes over the time include time, size measurements.
- Protocol behavior: detect the behavior of protocol (e.g. peer to peer, HTTP, IRC).

In[24], *BotSniffer* is anomaly based technique that does not need any previous knowledge of signature. BotSniffer has two major components monitor engine and correlation engine. Monitor engine observes network traffic and accumulate various attributes from the observed network.

2) Signature based detection

Signature based approach uses a priori knowledge of signatures. The signatures are constructed by experts analyzing from previous attacks and signatures are used to match with incoming traffic to detect intrusions.. Signature based techniques are only effective in detecting traffic of known DDoS attacks but that technique not effective for new attacks. SNORT and Bro are the two widely used signature based detection approaches[25].

In [20], *SNORT* is signature based open source Intruder Detection system that uses signature set as SNORT rules. This permit the detection system to remove DDoS attacks such as Slowloris attack.

3) Traffic Monitor Based

Traffic monitor based technique collects traffic flow information from many vantage points within network. In [26] to classify traffic into IRC or non-IRC groups. Initially Filter classified traffic flow into good sites and bad sites and also examined flow attributes.

4) Technique Based on SPAM Emails

The techniques analyze the patterns of emails and also get sender or recipient address of these emails. Esbod method classify emails into spam or real emails [24].

5) Nickname Based Detection Technique

In first step establish connection between the botmaster and assign a nickname for bot. Nickname can be helpful detection of Botnet [24].

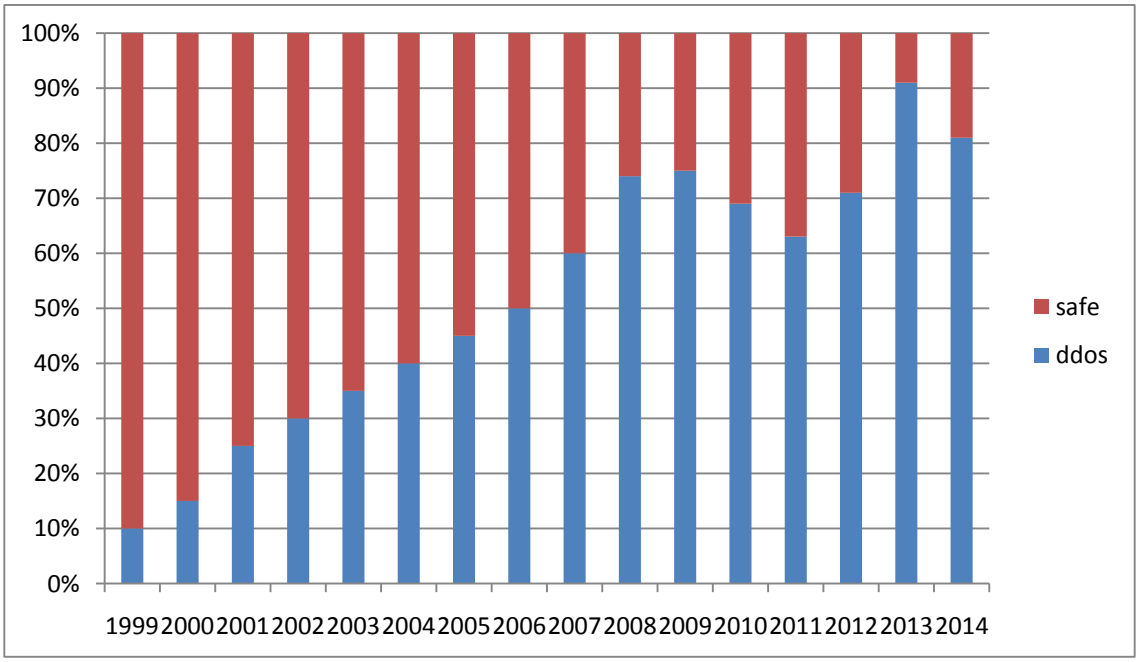

Fig. 4 DDoS Attacks over the year

VII. BOTNET-BASED-DDOS ATTACK INCIDENTS

In the summer of 1991, First DDoS attacks launched against different organizations[3]. In February of 2000, major DDoS attacks harmed several Internet e-com sites. In January of 2001, DDoS attacks disabled Microsoft's name server infrastructure[27]. 1200 attacks were listed against more than 5000 victims in February 2001. In May 2001, Coordinated Center of the Computer Emergency Teem also attacked, for more than two days making the availability of their Website sporadic[6]. In October 2002, the root servers were that provide Domain Name System to internet user shut down for an hour[27]. In February 2004, DDoS flooding attacks made SCO group websites unreachable to user that attacks launched by infected Mydoom virus system[3].

In June 2004, another major DDoS against name servers in the Akamai Content Distributed Network (ACDN)[6].In January 2005, the internet based business service of AI Jazeera provider of Arabic language news services was attacked. In March 2006, Sun Microsystems's Grid computing system that provide text to speech translation application was disabled its opening day[6]. In 2007, e-government, financial services and media were disabled for one to ten hours[4]. In July 2009, government news media and financial websites in South Korea and United States were attacked using Mydoom virus code[3]. In December 2010, Mastercard.com, PayPal, Visa.com and Post Finance organizations attacked by unidentified planed DDoS flooding attacks[3] . The examined DDoS incidents from 2011 to first half 2011 are shown in Table I and various attacks over the year 1999 to first quarter of 2014 are shown in **Fig. 5**.

TABLE II

BOTNET BASED DDOS ATTACK INCIDENT 2011-2014

Date of Attacks	**Details**
3 January 2011	DDoS against Tunisian Government websites included president, prime minister, ministry of industry, ministry of foreign affairs and stock exchange[6] .
30 march 2011	Shut down Blogging Platform Live Journal for over 12 Hours and start again on April 4 and 5, 2011[28].
October 2011	Attacks were launched against websites of National Election Commission of Korea[28]
November(5-12) 2011	The traffic load has been massive with several thou-sands request per second and load the server[28].
1 January 2012	Official websites of the president of Russia to be down for more than 15 hours[28].

19 January 2012	Mysterious attacker who shut down all websites (Justice.gov, MPAA.org, White House, the FBI, BMI.com, Copyright.com, Viacom, Antipriracy.be/nl, Vivendi.fr, Hadopi.fr, and ChrisDodd.com) for 10 minutes[6].
March 2012	DDoS attacks against South Korea websites[28].
18 March 2013	Spamhaus suffered a DDoS attack in which hacker exploited botnet and DNS reflection technologies[29].
27 March 2013	The attack traffic continuously rose from 10Gbps to an 300Gbps, it was largest scale (traffic-wise)[29].
February(9,10) 2014	DDoS attack on 9 February took advantage of insecure network time protocol daemons and 462,621 attacks were observed with the largest single attack of 421 gbps and 122 mbps happening on 10 February [30] .

VIII. CONCLUSION

In this paper we explore the scope of the Botnet based DDoS attack. We classify the some Botnet tools according to the communication protocol of Botnet and categorize the Command and Control model. In this paper we also classify botnet based DDoS attack and botnet detection technique. We are conducting an assessment on DDoS attack over the year and their incidents approved by researchers till now.

REFERENCES

[1] Incapsula, "Botnet based tools and technique of mitigation," *http://www.incapsula.com/ddos/ddos-attacks/botnet-ddos.html*, 2014.

[2] J. Z. Maheeb Abu Rajaab, Fabin Monrose, Andreas Terzis "A Multifaceted Approach to understanding the Botnet Phenomenon," *ACM Conference on Internet Measurement (IMC),*, 2006.

[3] S. T. Zagar, "A Survey of defence Mechanism Against Distributed Denial of Service(DDoS) flooding attacks," *IEEE COMMUNICATION SURVEY & TUTORIALS*, 2012.

[4] V. J. Radunovic, "DDoS - Available Weapon of Mass Disruption," in *21st Telecommunications forum TELFOR 2013* Serbia, Belgrade, 2013.

[5] B. R. Anestis Karasaridis, David Hoefin "Wide-Scale Botnet Detection and Characterization " 2007.

[6] E. Alomari, S. Manickam, B. Gupta, S. Karuppayah, and R. Alfaris, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art," *International Journal of Computer Applications (0975 – 8887)*, vol. 49, July 2012.

[7] Z. Zhu, "Botnet Research Survey," *Annual IEEE International Computer Software and Application Conference*, 2008.

[8] J. Nazario, "BlackEnergy DDoS Bot Analysis," *Arbor Networks*, October 2007.

[9] M. Bailey, "A Surey of Botnet Technology and Defenses," 2008.

[10] H. Y. L. T.T.lu, M.F.Chen, "An Advance Hybrid P2p Botnet 2.0," *World Academy of Science, Engineering and Technology*, vol. 57, 2010.

[11] Symantic, "Security Response," *http://www.symantec.com/connect/symantec-blogs/sr*, 2013.

[12] N. R. R. Sheharbano khattak, "A Taxonomy of Botnet Behavior, Detection, and Defense," *IEEE COMMUNICATION SURVEY & TUTORIALS*, 2012.

[13] S. Yu, "Distributed Denial of Service Attack and Defence," *Springer*, 23 october 2013.

[14] D. Shibin, M. M. Raja, and M. R. Christhuraj, "Detection of DDoS attack using collated strategies and Anteater System" in *International Conference on Information Communication and Embedded Systems (ICICES)*, 2013.

[15] R. Gummadi, "Not-a-Bot(NAB): Improving service availability in the face of Botnet Attacks," 2009.

[16] M. k. Rao, "Using Human Cognitive Abilities to distngish computers and Humans For Preventing Bot Attacks " *International Journal of Computer Science and Engineering* vol. 2, 2013.

[17] M. Serrao, "Cracking Captchas for Cash: A Review of CAPTCHA Cracker " *International Journal of Engineering Research & Technology(IJERT)*, vol. 2, 2013.

[18] J. Francois, I. Aib, and R. Boutaba, "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks," *IEEE/ACM Transactions on Networking*, 2012.

[19] C. S. sherif M. Khattab, Danial Mosse "Roaming Honeypots Mitigating Service-level Denial of Service Attacks " 2004.

[20] M. K. R. S. S.Manjari, "DDoS Counter Measures Based on Snort's detection system " *International Journal for Development of Computer science & Technology*, vol. 1, 2013.

[21] J. W. Weidong Ji, Jun Zhang and Dan Gao, "Based fuzzy pattern recognition methodology for the DDos evaluation," *Journal of Chemical and Pharmaceutical Research*, 2014.

[22] M. P. Sonali Swetapadma Sahu, "Distributed Denial of Service Attacks: A Review," *Modern Education and Computer Science,*, 2014.

[23] A. Z. Sebastian Garcia, Marcelo Campo "Survey on network- based botnet detection methods " *Security and Communication network*, 2013.

[24] V. E. S. E. Haritha.S.Nair "A Study on Botnet Detection techniques," *International Journal of Scientific and Research Publications*, vol. 2, 2012.

[25] A. Srivastava, B. B. Gupta, A. Tyagi, A. Sharma, and A. Mishra, "A Recent Survey on DDoS Attacks and Defense Mechanisms," in *Advances in Parallel Distributed Computing*. vol. 203, D. Nagamalai, E. Renault, and M. Dhanuskodi, Eds.: Springer Berlin Heidelberg, 2011, pp. 570-580.

[26] D. L. T.Strayer, R.Walsh,C.Livadas, "Botnet Detection :Countering the Largest Security Threat " vol. 36, 2008.

[27] C. S. David Moore, Dougles J. Brown, M. Voelker ,Stefan Savage "Inferring Internet Denial of service," *ACM Transactions on Computer Systems*, vol. 24, 2006.

[28] M. S. Daljeet Kaur, Krishan Kumar, "Recent DDoS Incidents and Their Impact," *International Journal of Scientific & Engineering Research*, vol. 3, August-2012.

[29] NSFOCUS, "Mid year DDoS threat report 2013," *http://en.nsfocus.com/SecurityReport/2013%20NSFOCUS%20Mid-Year%20DDoS%20Threat%20Report.pdf*, 2013.

[30] B. L. Communication, "Threat Report," *http://www.blacklotus.net/wp-content/uploads/Black-Lotus-Threat-Report-Volume-I-Issue-3-21-April-2014*, vol. 1, April 2014.

