International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 8 (2015) pp. 20959-20971

http://www.ripublication.com

Distributed Denial of Service (DDOS) Attack, Networks, Tools and DEFENSE

K.Vinoth Kumar and Dr.S.Bhavani

Research Scholar, Karpagam University.
Professor & Head, Department of ECE ,
Karpagam University, Coimbatore.

Abstract

Distributed denial of service (DDoS) attacks continues to grow as a threat to organizations worldwide. According to the CIAC, the first DDoS attacks occurred in the summer of 1999. DDoS attacks have a history of flooding the victim network with an enormous number of packets, hence exhausting the resources and preventing the legitimate users to access them. Even after having standard DDoS defense mechanisms, still attackers are able to launch an attack. These inadequate defense mechanisms need to be improved and integrated with other solutions. The purpose of this paper is to study the characteristics of DDoS attacks, various network models, different kinds of tools and Countermeasures to defend against DDoS attacks.

Keywords: Attack, CIAC, DoS, DDoS, Defense Mechanism, Legitimate, Victim.

Introduction

A. Denial of Service (DoS) Attack

A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet. DoS attacks are low-cost, and difficult to counter without the right tools [1].

B. Distributed Denial of Service (DDoS) Attack

DDoS attack is a distributed, large scale coordinated attempt of flooding the network with an enormous amount of packets which is difficult for victim network to handle, and hence the victim becomes unable to provide the services to its legitimate user and also the network performance is greatly deteriorated. This attack exhausts the resources of the victim network such as bandwidth, memory, computing power etc. The system which suffers from attack or whose services are attacked is called as “primary victim” and on other hand “secondary victims” is the system that is used to originate the attack. These secondary victims provide the attacker, the ability to wage a more powerful DDoS attack as it is difficult to track down the real attacker [1, 2].

In DDoS attack, the attacker selects the compromised machine (i.e. those machines which have loopholes) and network of the compromised machines are called botnet. These botnets are further instructed to execute commands in order to consume all the resources available on victim’s system [3]. Fig. 1 shows the basic structure of DoS and DDoS attack.

C. Difference between DoS and DDoS Attack

It is important to differentiate between Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. In a DoS attack, one computer and one internet connection is used to flood a server with packets, with the aim of overloading the targeted server’s bandwidth and resources.

A DDoS attack, uses many devices and multiple Internet connections, often distributed globally into what is referred to as a botnet. A DDoS attack is, therefore, much harder to deflect, simply because there is no single attacker to defend from, as the targeted resource will be flooded with requests from many hundreds and thousands of multiple sources [4].

Rest of the paper is organized as follows: Section II describes DDoS attacker’s motivation factors and history of DDoS attacks, Section III presents DDoS attack characteristics and models, Section IV describes DDoS attack types and mechanism, Section V presents DDoS attack toolkit, Section VI describes how DDoS attacks are performed using botnet, Section VII presents defense against DDoS attack, Section VIII concludes the paper.

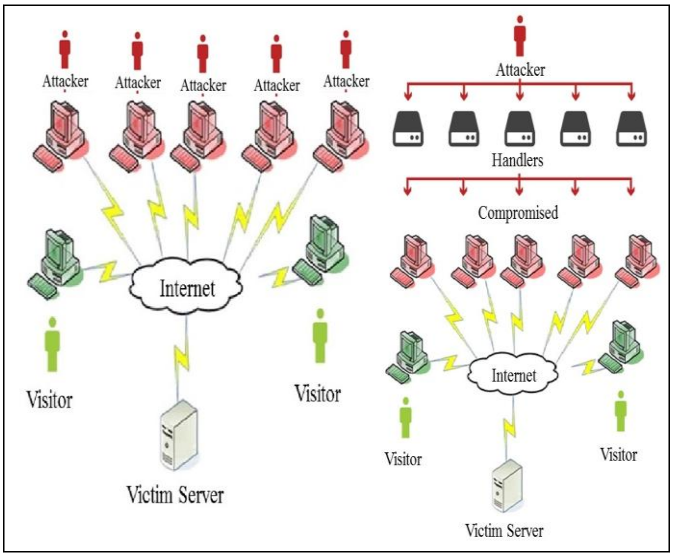

Figure 1: Basic Structure of DoS and DDoS Attack

DDOS Attack Motivation & History

A. DDoS Attacker's Motivation Factors

Human beings are not born to become an attacker. They are enough motivated due to some reasons to launch the attack. Based on some obvious reasons and facts, the motivation factor can be categorized as [6]:

- Financial Benefit: The attackers of this category are highly skilled and hard to be detected. They only concern here is to have financial gain.
- Professional Skills: The attackers target systems for experiment purpose to check their vulnerabilities and strength of security mechanism. The attackers who are very much enthusiastic and ready to face challenges fall into this category.
- Payback Attitude: In this category, the attackers are usually very much frustrated and low skilled persons, perform attack only to take revenge.
- Cyber Warfare: In this category, attackers are usually high skilled and intellectual person who generally belong to military or terrorist organizations of a country. They attack to defend their country or their organizations [7]. Table I shows some serious DDoS attack incidents in history.

B. DDoS Observations

The ideology of an attacker and the method chosen for attacks is not correlated. It is found that there is specific geographic pattern of DDoS attacks. Easily accessible tools that helps to make successful attacks on small websites, suggests that distressed individuals may use DDoS as a weapon for building score or making a political point.

DDOS Attack Characteristics and Network Models

A. Characteristics of DDoS Attack

Following are the different ways to characterize the distributed denial of service attack:

- Disruptive/Degrade Impact: After being a part of attack, the victim either to stop providing services to the client or the services are degraded that means some of the services are still being provided to the client even the victim's system is under the attack.
- Exploiting Vulnerability: Network of machines which follows the instructions of master attacker to send request for a service on a victim's machine to consume its all the resources.
- Dynamic Attack Rate: Sometime attacker make down the websites very quickly by sending large no of request more than its capacity, is known as constant attack rate. While some times attacker takes time to make it down by sending packets in variable length of request that is not constant, known as variable attack rate.

- Automated Tools: Attackers can be classified by automated tools also and their skills. Attack can be performed manually; semi-automated or fully-automated tools.

B. DDoS Attacks Components

Fig. 2 describes the component of DDoS attack, who initiates the attack by selecting vulnerable system as agents and further the agents use botnet to exhaust the victim's system.

Table 1: DDOS Attack Statistics

Year	**Incidents**
2013	The Czech financial sector was targeted in cyber attacks on Wednesday, at the same time on the national bank and stock exchange websites which get disrupted by dedicated denial of service (DDoS) attacks—London, 8 March, 2013.
2012	US and UK Government Sites Knocked Down by Anonymous—April 16, 2012. DDoS Attack Impacts Canadian Political Party Elections—March 24, 2012.
2011	A DDoS attack on Sony was used—April 16-20 2011.
2010	PayPal Transaction is suspended over WikiLeaks website after attacked by DDoS—December 3-5, 2010.
2009	The Mydoom virus code was re-used to launch DDoS flooding attacks against major government news media and financial websites in South Korea and the United States in July 2009 [8].
2008	BBC hit by DDoS Attack, two DDoS attacks on Amazon.com and eBuy.
2007	Estonia Cyber Attack [9].
2006	US Banks have been targeted for financial gain.
2004	SCO Group website inaccessible to legitimate users.
2003	Mydoom defiled thousands of victims to attack SCO and Microsoft [10].
2002	13 root servers that provide the Domain Name System (DNS) service to Internet users around the world shut down for an hour because of a DDoS flooding attack [11].
2001	First major attack involving DNS servers as reflectors. The target was Register.com. The Irish Government's Department of Finance server was hit by a denial of service attack carried out as part of a student campaign from NUI Maynooth.
2000	Yahoo! Experienced one of the first major DDoS flooding attacks that kept the company's services off the Internet for about 2 hours incurring a significant loss in advertising revenue [12].

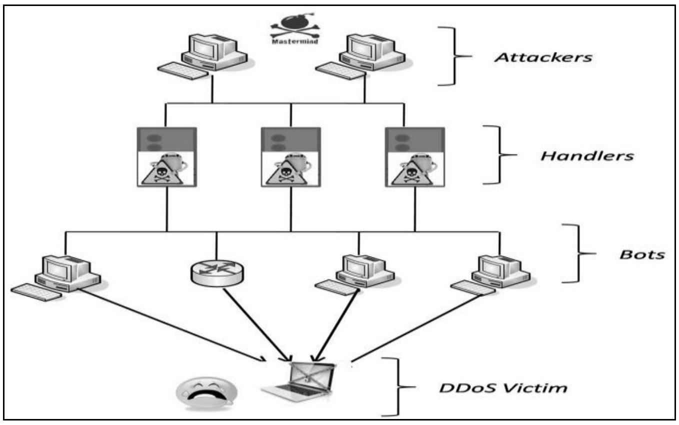

Figure 2: Components of DDoS Attacks

1. Master Mind/Planner: The Original Attacker, who creates reasons and answers for, why, when, how and by whom the attack will be performed.
2. Controller/Handler: Co-ordinator of original attacker, who may be one or more than one machine, is used to exploit other machines to process DDoS attack.
3. Agents/Zombies/Botnets: Agents, also known as slaves or attack daemons, sub ordinates are programs that actually conduct the attack on the victim. These programs are usually deployed on host computers. These daemons influence both the machines: target and the host computers. It facilitates the attacker to gain access and infiltrate the host computers.
4. Victim/Target: A victim is a target host that has been selected to receive the impact of the attack.

C. DDoS Network Models

Two types of DDoS attack networks have emerged: the Agent-Handler model and the Internet Relay Chat (IRC) based model.

The Agent-Handler model of a DDoS attack: It consists of agents, handlers and client. Fig. 3 shows the Agent-Handler Model, in which the Agent and handler knows each-others identity. The client is the interface where the attacker/mastermind communicates with the rest of the DDoS Components. The handlers are software packages distributed all over the Internet so that it helps to client to convey its command to the agents. The agent software's are vulnerable systems, compromised by the handlers and actually launch the attack on victim's machine. The agent's status and schedule for launching attack can be upgraded by the handler when it is required. Communication relation between agent and handler is either one to one or one to many. Most Common way to attack is by installing handler instructions either on compromised route on network layer or on network server. This makes it difficult to identify messages exchanged by the client-handler and between the handler-agents.

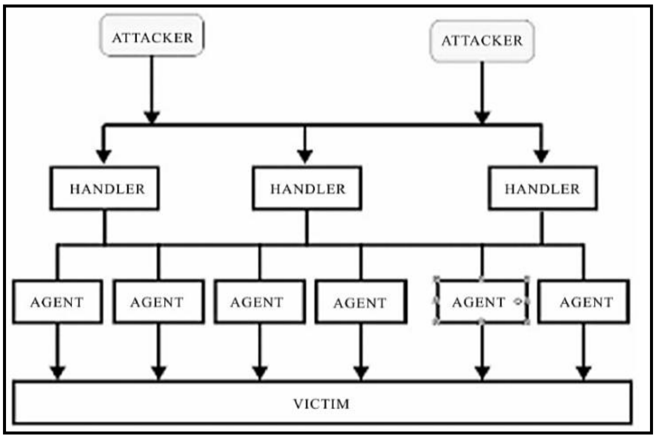

Figure 1: Agent-Handler Model

IRC-based DDoS attack: IRC i.e. Internet Relay Chat, Fig. 4 shows the architecture of this model where attacker and agent does not know their identity. It is a communication channel to connect the clients to the agents, which provides some additional benefits to the attacker such as use of IRC ports to send the commands to the agents. Because of this, tracking the DDoS command packets becomes difficult. In addition to that, because of heavy traffic going through IRC servers attacker can easily hide its presence. As the attacker has direct access of IRC server, the attacker has access to a list of all available agents [13]. The attacker does not need to have a list of the agents. The agent software that installed in the IRC network which communicates to the IRC channel, notifies the attacker on when the agent is up and running.

DDOS Attack Types And Mechanism

A. Types of DDoS Attacks

DDoS attacks can divided in three types:

- Volume Based Attacks - This type of attack includes UDP floods, ICMP floods, and other spoofed packet floods. The goal of this DDoS attack is to saturate the bandwidth of the attacked site. The magnitude of a volume-based attack is usually measured in Bits per second.
- Protocol Attacks - This type of DDoS attack consumes the resources of either the servers themselves, or of intermediate communication equipment, such as routers, load balancers and even some firewalls. Some examples of protocol attacks include SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. Protocol attacks are usually measured in Packets per second.
- Application Layer Attacks - Perhaps the most dangerous type of DDoS attack, application layer attacks are comprised of seemingly legitimate and innocent requests. The intent of these attacks is to crash the web server. Some examples of application layer attacks include Slowloris, Zero-day DDoS attacks, DDoS

attacks that target Apache, Windows or OpenBSD vulnerabilities and more. The magnitude of this type of attack is measured in Requests per second.

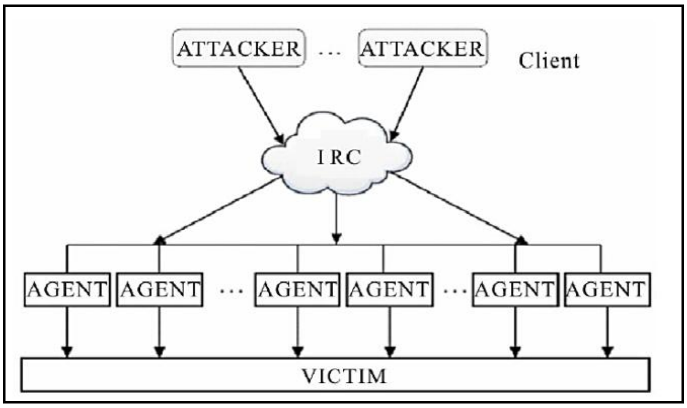

Figure 2: IRC Model

B. DDoS Attacks Mechanism

Some of the most famous standard DDoS attacks are summarized as follows:

- Apache 2: This attack is build up against an Apache Web server where the client asks for a service by sending a request with many HTTP headers. Upon receiving the large amount of HTTP request Apache Web server cannot outface the load and it crashes.
- ARP Poison: Address Resolution Protocol (ARP) Poison attacks claims the attacker to have key in to the victim's LAN. The attacker spoof the hosts of a specific LAN by providing them with wrong MAC addresses for hosts with already-known IP addresses. This can be done by the attacker through the following procedure: The network is monitored for "who has" requests type which is an ARP request. The moment such a request is received; the malevolent attacker tries to respond as fast as feasible to the questioning host so that it can mislead it for the requested address.
- Back: In Back type of attack the requests are send an apache Web server, where the server is flooded with requests containing a large number of front-slash (/) characters in the URL description. When the server tries to process all these requests, it becomes unable to process other legitimate requests and hence it denies service to its legitimate user.
- CrashIIS: The CrashIIS attack is commonly a projected towards Microsoft Windows NT IIS Web server. The attacker sends the victim a malicious GET request, which causes the Web server to crash.
- Land: In this type of attack the attacker sends TCP SYN packet to the victim that contains the same IP address as the source and destination addresses. Such a packet completely blocks the victim's system.
- DoS Nuke: This kind of attack is launched against the Microsoft Windows NT victim is inundated with "out-of-band" data (MSG_OOB). The packets that are sent by the attacking machines are flagged "urg" because of the

MSG_OOB flag. This causes the target to get down, and this leads to displays a “blue screen of death” on the victim machine.

- Mail bomb: In this type of attack, the victim’s mail queue is flooded by a huge amount of messages, causing system failure.
- SYN Flood: A SYN flood attack take place during the three-way handshake that marks the onset of a TCP connection. In the three-way handshake, a client sends a TCP SYN packet to a server requesting for a new connection. Thereby, the server sends a SYN/ ACK packet back to the client and places the connection request in a queue. As a final point, the client acknowledges the SYN/ACK packet. When an attack takes place, however, the attacker sends an abundance of TCP SYN packets to the victim, forcing it for both: 1) To open a lot of TCP connections and 2) To respond to them. Then the attacker does not execute the final step of the three-way handshake that follows, exposing the victim that is not capable to accept any new incoming connections, since its queue is full of half- open TCP connections.
- Ping of Death: In Ping of Death attacks, the attacker creates a packet that contains more than 65,536 bytes, which is out of the limit of the IP protocol. This packet can produce different kinds of damage to the machine that receives it, that results in crashing and rebooting.
- Process Table: This attack use the feature of some network services to generate a new process each time a new TCP/IP connection is set up. The attacker considers making as many uncompleted connections to the victim as possible in order to force the victim’s system to generate as many as processes. For this reason, as the number of processes that are running on the system cannot be very much large, the attack renders the victim unable to serve any other request.
- Smurf Attack: In a “smurf” attack, the victim is thronged with Internet Control Message Protocol (ICMP) “echo-reply” packets. The attacker sends voluminous ICMP “echo-request” packets to the broadcast address of numerous subnets. These packets have the source IP address field updated with victims address. Every machine that is associated with any of these subnets responds by sending ICMP “echo-reply” packets to the victim. Smurf attacks are very alarming, because they are intensely distributed attacks.
- SSH Process Table: This attack makes large amount of connections to the victim with the Secure Shell (SSH) Protocol without carrying out the login process. In this way, the zombie contacted by the SSH on the victim’s system is indulged to start so many SSH processes that it is fatigued.
- Syslogd: In this type of attack the Solaris 2.5 server is banged by sending large amount of messages with illegal source IP address.
- TCP Reset: In TCP Reset attacks, the network is scrutinized for “tcp connection” requests which are send to the victim. The moment such a request is found; the malicious attacker sends a spoofed TCP RESET packet to the victim and obliges it to lay off the TCP connection.
- Teardrop: A Teardrop attack causes a stream of IP fragments with their offset field overloaded. As a packet travels from the source machine to the

destination machine, it is broken up into smaller sections or fragments, through the process of fragmentation. The destination host that tries to reassemble these abnormal fragments in the long run clangs or reboots.

- UDP Storm: In a User Datagram Protocol (UDP) connection, when it receive a UDP packet, a character generation (“chargen”) service generates a series of characters, while an echo service echoes any character it receives. Manipulating the above two services, the attacker sends a packet to another machine with the source misleading to be that of the victim. Then, the echo service of the anterior machine echoes the data of that packet back to the victim’s machine and the victim’s machine, consecutively, responds in the similar fashion. Hence, a constant stream of unserviceable load is created that problems the network [14].

DDOS Attack Toolkit

With time the attackers are using sophisticated tools to materialize the attacks, this sections lists the tool kits used in some of the attacks.

1. Trinoo: It uses TCP to communicate between attacker and control master program. The communication between the trinoo master and daemon is held using UDP packets. It implements UDP flood attack against victim. The master and daemons are password protected and prevent system administrators to take control of the trinoo network.
2. Win Trinoo: This is a variant trinoo that works on Windows platform. It sends large amount of UDP packets to the victim as an action of attack.
3. MStream: The mstream program which is based on the “stream.c” attack, includes a “master controller” and a “zombie”. As the name indicates master controller controls all of the zombie agents. There is no encryption in the communications between the client, master, and zombie. An attacker connects to the master controller using Telnet to control the zombies. The zombie can slow a computer down by using up CPU cycles via a modified version of stream’s attack .The attack consumes network bandwidth when the target host tries to send TCP RST packets to non-existent IP addresses in addition to the incoming ACK packets which cause Routers to return ICMP host/network unreachable packets to the victim, consequential the starvation of bandwidth. This consumes large amount of network bandwidth and at the same time distributed method of attack multiplies the effect on the CPU.
4. Tribe Flood Network (TFN): In this technique, a command line interface is used to communicate between attacker and control master program. The communication between the two is done through ICMP Echo reply packets. Following attacks are implemented through TFN’s attack daemons: Smurf attack, SYN flooding, UDP flood and ICMP flood attack [15,16].
5. Stacheldraht: Stacheldraht is another master/slave DDoS attack toolkit based on TFN attack. But unlike TFN, it uses an encrypted TCP connection to communicate between attacker and master control program. Communication between master and daemon is held using TCP and ICMP and it involves an

automatic update technique for attack daemons. Following attacks are implemented through stacheldraht attack daemons: smurf, UDP flood, ICMP flood attacks, SYN flood [17].

6. Shaft: It is modeled after trinoo. But unlike trinoo, the communication between control master program and attack daemons is achieved using UDP packets and they communicate via a simple TCP Telnet connection. An important feature of shaft is its ability to switch control master servers and ports in real time and hence making detection by intrusion detection tools difficult. Hence, attacks implemented through Shaft are difficult to detect [18].
7. TFN2K: Uses TCP, UDP, ICMP or all three to communicate between control master and program and the attack daemons. Communication between the real attacker and control master is encrypted using key based CAST-256 algorithm.

DDOS Attack Using Botnet

Botnets implement under a command and control (C & C) management infrastructure and compromise a network of machines with programs referred as bot, zombie, or drones. The Botnets affects a series of systems using various tools and by installing a bot that can remotely control the victim using IRC. Present botnets are most frequently used to spread DDoS attacks on the Web [19]. Moreover, the attackers can change their communication approach during the creation of the bots. Majority of bots varied its potentials to participate in such attacks. The most classic and generally implemented Botnet attack on application layer is the HTTP/S flooding attack, which launches bots created by the HTTP server. Such bots are thus called, Web-based bots [20]. Fig. 5 shows a botnet attack in cloud services.

The goal of a Botnet based DDoS attack is to entail damage at the victim side. In general, the mysterious in- tention behind this attack is personal which means block the available resources or degrade the performance of the service which is required by the target machine. There- fore, DDoS attack is committed for the revenge purpose. Another aim to perform these attacks can be to gain popularity in the hacker community.

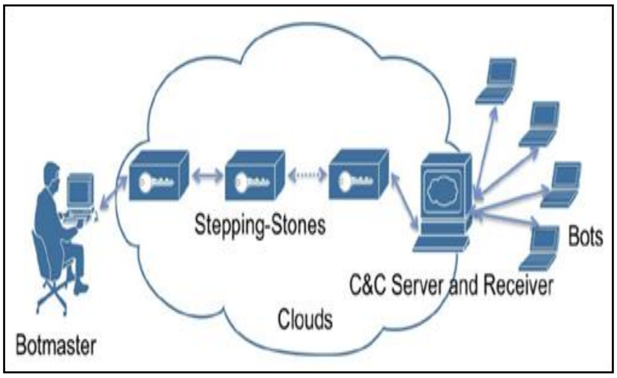

Figure 1: Botnet Attack

Defense DDOS Attack Using Botnet

Defending the DDoS attacks involves three phases: before the attack, during the attack and after the attack. The first one is prevention, which needs a process to deploy the network to guard against attack. During the attack, signature-based and anomaly based techniques are used to detect the attack and identify the attack sources before it reaches the target. Defense after the attack makes use of mitigation techniques.

We divide the DDoS defense into following sub-problems:

1. The *detection* problem consists of designating those points in time at which network is experiencing an attack. An effective algorithm for solving detection problem should have high detection probability and a low false alarm probability.
2. The *identification* or characterization problem consists of selecting the true attacks from a set of possible candidate attacks. The method we propose is extensible to a wide variety of attacks.
3. The *mitigation* is the problem of estimating total attack traffic targeted towards the network and reducing the effects of the attack.
4. The *filtering* of attack flows requires with high confidence that these flows are identified as attacks to minimize collateral damage [21].

Conclusion

DDoS attacks are quite advanced methods of attacking a network system to make it unusable to legitimate network users. These attacks are an annoyance at a minimum, and if they are against a critical system, they can be severely damaging. Loss of network resources costs money, delays work, and cuts off communication between network users. The negative effects of a DDoS attack make it important that solutions and security measures be developed to prevent these types of attacks. Detecting, preventing, and mitigating DDoS attacks is important for national security.

In this paper, we tried to scope the DDoS problem by describing taxonomies of DDoS attacks, attack networks, attack techniques and attack tools. This may help in facilitating research into more comprehensive, multi-tiered solutions, rather than just designing specific countermeasures for a specific attack.

References

[1] Denial-of-service attack ,Wikipedia, http://en.wikipedia.org/wiki/Denial-of-service_attack

[2] CERT Statistics, URL: http://www.cert.org/stats/cert.

[3] L. Garber, Denial-of-service attacks rip the Internet, IEEE Computer 33 (4) (2000) 12–17.

[4] K.J. Houle, G.M. Weaver, N. Long, R. Thomas, "Trends in denial of service attack technology," Technical Report Version 1.0, *CERT Coordination Center*, Carnegie Mellon University, 2001.

[5] J. Mirkovic, P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communications*, Review 34 (2) (2004) 39–53.

[6] A. ALmomani, T.-C. Wan, B. B. Gupta, A. Altaher, E. A. Lmomani and S. Ramadass, "A Survey of Phishing Email Filtering Techniques," *IEEE Communications Surveys* & *Tutorials*, Vol. PP, No. 99, 2013, pp. 1-21.

[7] S. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks," *Communications Surveys & Tutorials*, *IEEE*, Vol. PP, No. 99, 2013, pp. 1-24. doi:10.1109/SURV.2013.031413.00127

[8] K. Zetter, "Lazy Hacker and Little Worm Set off Cyber war Frenzy," 2009. http://www.wired.com/threatlevel/2009/07/mydoom/

[9] L. Greenemeier, "Estonian Attacks Raise Concern over Cyber "Nuclear Winter"," Information Week, 2007. http://www.informationweek.com/estonian-attacks-raise-concern-over-cybe/199701774

[10] J. Vijayan, "Mydoom Lesson: Take Proactive Steps to Prevent DDoS Attacks," 2004. http://www.computerworld.com/s/article/89932/Mydoom_lesson_Take_proactive_steps_to_prevent_DDoS_attacks?%20taxonomyId=017

[11] "Powerful Attack Cripples Internet," 2002. http://www.greenspun.com/bboard/q-and-a-fetch-msg.tcl msgid=00A7G7

[12] Yahoo on Trail of Site Hackers," Wired.com, 2000. http://www.wired.com/techbiz/media/news/2000/02/34221

[13] J. Lo, *et al*., "An IRC Tutorial," 1997. http://www.irchelp.org/irchelp/irctutorial.html#part1

[14] Mstream Distributed Denial of Service Tool (Zombie Detected) (DDosMstreamZombie)," 2013. http://www.iss.net/security_center/reference/vuln/ddos-mstream-zombie.htm

[15] D. Dittrich, "The Tribe Flood Network Distributed Denial of Service Attack Tool," University of Washington, Seattle, 1999. http://staff.washington.edu/dittrich/misc/tfn.analysis.txt

[16] J. Barlow and W. Thrower, "TFN2K—An Analysis," Axent Security Team, 2000. http://security.royans.net/info/posts/bugtraq_ddos2.shtml

[17] D. Dittrich, "The Stacheldraht Distributed Denial of Service Attack Tool," University of Washington, Seattle, 1999. http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt

[18] D. Dittrich, S. Dietrich and N. Long, "An Analysis of the 'Shaft' Distributed Denial of Device Tool," *USENIX Systems Administration Conference*, March 2000. http://www.soscholar.net/detail?paper_id=2bb7f2f9-2ed7-3422-78d2-e938aaaf44af

[19] E. Alomari, S. Manickam, B. 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*, Vol. 49, No. 7, 2012, pp. 24-32.

[20] F. Freiling, *et al.*, “Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of- Service Attacks,” *Computer Security-ESORICS* 2005, Milan, 12-14 September 2005, pp. 319-335.

[21] S. Anjali , J. Ramesh, “An auto-responsive honeypot architecture for dynamic resource allocation and QoS adaptation in DDoS attacked networks” *Computer Communications 32* (2009) 1384–1399.

[22] T. Shweta, G. Brij, A. Ammar, M. Anupama and V.Suresh, “Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks,” *Journal of Information Security*, 2013, 4, 150-164. doi:10.4236/jis.2013.43018.