STUDY AND EVALUATION OF RECENT DDOS TRENDS OF ATTACK ON WEB SERVER

[1]Amadi E.C., [2]Anakenyi D., [3]Njoku C., [4]Abanobi G.
[1-4]Department of Informaion Management Technology, Federal University Technologyi Owerri (FUTO), Nigeria

ABSTRACT
Distributed Denial of Service (DDoS) attacks have become a major threat to the Internet community because 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. These attacks not only congest a Server, but also affect the performance of other Servers on the entire network also, which are connected to Backbone Link directly or indirectly. The focus of this study, based on existing literature, covers the architecture or models of DDoS attacks and DDoS attack tools, propose taxonomies to characterize the scope of DDoS attacks and categorize it based on their types, and also the recent trends of DDoS attacks on web server are studied and evaluated.

Keywords: Distributed Denial of Service (DDoS), DDOS attacks, DDOS Incidents, Web Server.

1.0 INTRODUCTION

Denial of Service (DoS) attack which is an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, web service, or computer system, have been known to the network research community since the early 1980s. In the summer of 1999, the Computer Incident Advisory Capability (CIAC) reported the first Distributed DoS (DDoS) attack incident (Criscuolo P. J., 2000) and most of the DoS attacks since then have been distributed in nature. In February of 2000, one of the first major DDoS attacks was waged against Yahoo.com, keeping it off the Internet for about 2 hours, costing it lost advertising revenue (Wired.com, 2000). DDoS stands for "Distributed Denial of Service." A DDoS 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 (Lai S. and Wang M. 2014). Distributed Denial of Service (DDoS) attacks add the many-to-one dimension to the DoS problem making the prevention and mitigation of such attacks more difficult and the impact proportionally severe. DDoS exploits the inherent weakness of the Internet system architecture, its open resource access model, which ironically, also happens to be its greatest advantage. DDoS attacks are comprised of packet streams from inherently different sources. These attacks engage the power of a vast number of coordinated Internet hosts to consume some critical resource at the target and deny the service to legitimate clients. The traffic is usually so aggregated that it is difficult to distinguish legitimate packets from attack packets. More importantly, the attack volume can be larger than the system can handle. Unless special care is taken, a DDoS victim can suffer from damages ranging from system shutdown and file corruption, to total or partial loss of services (Christos D. and Aikaterini M. 2004). Today, DDoS attacks are often launched by a network of remotely controlled, well organized, and widely scattered Zombies or Botnet computers that are simultaneously and continuously sending a large amount of traffic and/or service requests to the target system. The target system either responds so slowly as to be unusable or crashes completely (Mirkovic and Reiher 2004; Chang 2002). Zombies or computers that are part of a botnet are usually recruited through the use of worms, Trojan horses or backdoors (Puri R, 2003; Todd B, 2000; CERT 2001). Employing the resources of recruited computers to perform DDoS attacks allows attackers to launch a much larger and more disruptive attack. Furthermore, it becomes more complicated for the defense mechanisms to recognize the original attacker because of the use of counterfeit IP addresses by zombies under the control of the attacker (Liu J. et al,2009). In this, hackers send control instructions to masters, which then communicate it to zombies for launching attack. As shown in Figure 1, typical DDoS attack has two stages, the first stage is to compromise susceptible systems that are accessible in the Internet and then install attack tools in these compromised systems. This is known as turning the computers into "zombies." In the second stage, the attacker sends an attack command to the "zombies" through a secure channel to launch a bandwidth attack against the targeted victim(s). The current attacks on some web sites like Amazon, Yahoo, e-Bay and Microsoft and their resultant disruption of services have uncovered the weakness of the Internet to Distributed Denial of Service (DDoS) attacks (Daljeet K. and Monika S. 2014).

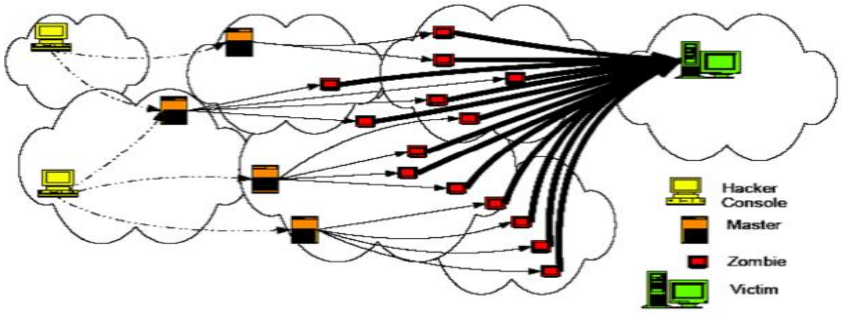

Figure 1. Attack Modus Operandi (Daljeet and Monika 2014).

2.0 CONCEPT OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

Distributed Denial of service (DDoS) attacks is designed to disrupt network services, by intentionally blocking or degrading the available resources used by them (Monika et al, 2010). DDoS attacks mainly take advantage of the Internet architecture and that is what makes them even more powerful. The Internet was designed with functionality, not security, in mind. Its design opens several security issues that can be exploited by attackers. More analytically

• **Internet security is highly interdependent.** No matter how secure a victims system may be, whether or not this system will be a DDoS victim depends on the rest of the global Internet (CERT Coordination Center 2001).

• **Internet resources are limited.** No Internet host has unlimited resources that sooner or later can be consumed by a sufficient number of users.

• **Many against a few.** If the resources of attackers are greater than the resources of the victims then the success of the attack is almost definite.

• **Intelligence and resources are not collocated.** Most of the intelligence needed for service guarantees is located in end hosts. At the same time in order to have large throughput high bandwidth pathways are designed in the intermediate network. This way, attackers can exploit the abundant resources of an unwitting network in order to flood a victim with messages.

2.1 Steps for Conducting a DDOS Attack

The following steps take place while preparing and conducting a DDoS attack (Christos D. and Aikaterini M. 2004):

1. **Selection of agents:** The attacker chooses the agents that will perform the attack. These machines need to have some vulnerability that the attacker can use to gain access to them. They should also have abundant resources that will enable them to generate powerful attack streams. At the beginning this process was performed manually, but it was soon automated by scanning tools.

2. **Compromise:** The attacker exploits the security holes and vulnerabilities of the agent machines and plants the attack code. Furthermore he tries to protect the code from discovery and deactivation. Self propagating tools such as the Ramen worm and Code Red soon automated this phase. The owners and users of the agent systems typically have no knowledge that their system has been compromised and that they will be taking part in a DDoS attack. When participating in a DDoS attack, each agent program uses only a small amount of resources (both in memory and bandwidth), so that the users of computers experience minimal change in performance.

3. **Communication:** The attacker communicates with any number of handlers to identify which agents are up and running, when to schedule attacks, or when to upgrade agents. Depending on how the attacker configures the DDoS attack network, agents can be instructed to communicate with a single handler or multiple handlers. The communication between attacker and handler and between the handler and agents can be via TCP, UDP, or ICMP protocols.

4. **Attack:** At this step the attacker commands the onset of the attack. The victim, the duration of the attack as well as special features of the attack such as the type, length, TTL, port numbers etc, can be adjusted. The variety of the properties of attack packets can be beneficial for the attacker, in order to avoid detection.

2.2 Reasons for DDoS Attacks

The main aim of a DDOS attack is to harm on victim, either for personal reasons like against home computer or for revenge purpose, for secret information Theft by damaging victim's resources. Some attacker also experiment this attack to gain popularity by making successful attack on popular web servers

which give them fame in the hacker community. Sometimes attackers usually belongs to the military or terrorist organizations of a country and they are politically motivated to attack a wide range of critical sections of another country (Dhruv & Petal 2014). So, we can categorize DDOS attack based on motivation of the attackers into following categories which includes Financial/Economical gain; Revenge; Ideological belief; Intellectual challenge and Cyber warfare.

2.3 DDoS Attack Architectures and Tools

The attacker is hidden behind the layers of multiple zombies. There exist multiple DDoS attacker communication models that have emerged in past decade. DDoS attack networks fall under three categories, namely, the Agent-Handler model, Internet Relay Chat (IRC)-based model and the Web-based models.

2.3.1 Agent-Handler mọdèl/DDoS Attack Tools: The Agent-Handler model of a DDoS attack composed of four elements (Raghav et al, 2015) as shown in Fig. 2.

a. Attacker: The main source that starts the attack.

b. Handler: Malicious software installed on the system which works according to the attacker.

c. Agent: The handler (software) when installed on the system makes that system an agent (bots/zombies) spread the attack on to the other machines.

d. Victim: Primary victim or main server under attack.

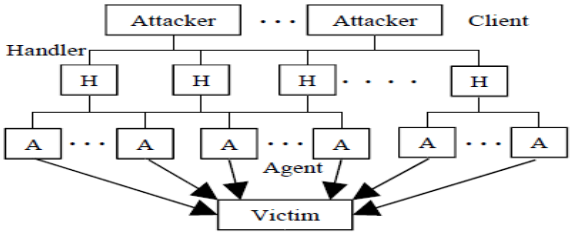

Figure 2. Agent Handler Model of DDoS Attack (Specht and Lee, 2004)

Agent-based DDoS attack tools are based on the agent–handler DDoS attack model comprising handlers, agents, and victims. Examples of agent-based DDoS tools are Trinoo, Tribe Flood Network (TFN), TFN2K, Stacheldraht, Mstream, and Shaft (Gupta et al, 2010). Among the above mentioned agent-based DDoS tools, Trinoo (Criscuolo 2000) is the most popular and the most widely used for its capability for bandwidth depletion and for launching UDP flood attacks against one or numerous Internet protocol (IP) addresses.

2.3.2 IRC based DDoS Attack/Attack tools: In IRC based DDoS attack model, attacker communicates with the agents through IRC channel. It is difficult to track this type of DDoS attack as attackers use legitimate ports for sending commands to agents. Moreover, high volume of traffic in IRC channels help attackers to hide their presence (Raghav et al, 2015).

Figure 3. IRC Model of DDoS Attack

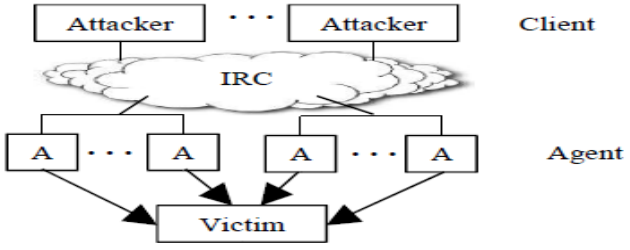

Figure 3. IRC Model of DDoS Attack (Specht and Lee, 2004)

IRC-based DDoS attack tools were developed after the emergence of agent–handler attack tools. More sophisticated IRC-based tools have been developed, and these tools include the important features of several agent-handler attack tools. The Trinity is one of the best-known IRC-based DDoS tools on top of UDP, TCP SYN, TCP ACK, and TCP NUL packet floods. The Trinity v3 (Hancock 2000) introduces TCP random flag packet floods, TCP fragment floods, TCP established floods, and TCP RST packet floods. Along with the development of the Trinity came the myServer (Sven Dietrich et al 2010), that rely on external programs to conduct DoS and plague to simulate TCP ACK and TCP SYN flooding. Knight

(Bysin 2001) is another light-weight and powerful IRC-based DDoS attack tool that can perform UDP flood attacks and SYN attacks. Knight can be considered an urgent pointer flooder (Specht and lee, 2004). An IRC-based DDoS tool based on Knight is Kaiten (Bysin 2001), which conducts UDP, TCP flood attacks, SYN, and PUSH+ACH attacks.

2.3.3 Web-based DDoS attack/Attack tool: More recently, botnets have started using HTTP as a communication protocol to send commands to the bots making it much more difficult to track the DDoS command and control structure. Web-based botnets do not maintain connections with a C&C server like IRC-based botnets do. Instead, each Web bot periodically downloads the instructions using web requests. Web-based botnets are stealthier since they hide themselves within legitimate HTTP traffic. Bots are configured and controlled through complex PHP scripts and they use encrypted communication over HTTP (port 80) or HTTPS (port 443) protocol. The following are the advantages of Web-based controls over IRC (Company 2006):

- Ease of set-up and website configuration;
- Improved reporting and command functions;
- Less bandwidth requirement and the acceptance of large Botnets for the distributed load;
- Concealment of traffic and hindrance of filtering through the use of port 80/443;
- Resistance to Botnet hijacking via chat-room hijacking; and
- Ease of use and of acquisition.

Web-based DDoS attack tools were recently developed with the purpose of attacking the application layer, especially the Web server. IRC-based DDoS attack tools with the HTTP/S flooding function are used to attack a Web server, thus proving that attackers are increasingly adopting various tools to introduce DDoS attacks (McPherson 2011). Unlike currently popular attack tools that can launch DDoS attacks, most organizations are unaware of the broad development over the last few years and are vulnerable to attackers. There are three Web-based DDoS attack tools namely: BlackEnergy, Low-Orbit Ion Cannon (LOIC) and Aldi Botnet

2.4 Taxonomy of DDoS Attack

There are a wide variety of DDoS attacks. In this paper propose a taxonomy of the main DDoS attack methods in Figure 4.

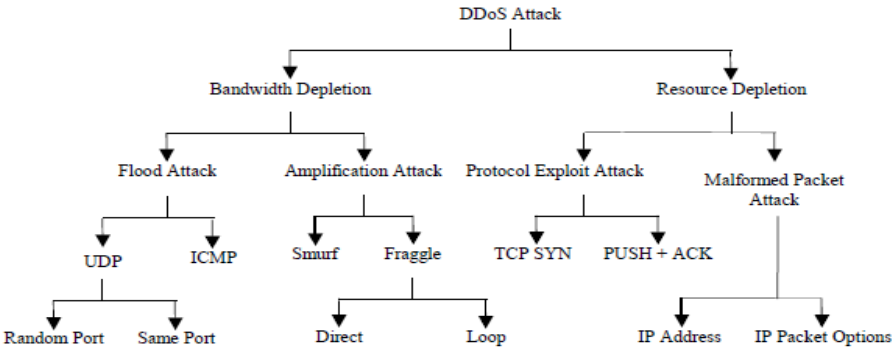

Figure 4: DDoS Attack Taxonomy (Specht and Lee, 2004)

There are two main classes of DDoS attacks: bandwidth depletion and resource depletion attacks. A bandwidth depletion attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the primary victim. A resource depletion attack is an attack that is designed to tie up the resources of a victim system making the victim unable to process legitimate requests for service (Specht and Lee, 2004).

1. Bandwidth Depletion Attacks

Bandwidth depletion attacks can be characterized as flood attacks and amplification attacks.

Flood Attacks. A flood attack involves zombies sending large volumes of traffic to a victim system, to congest the victim system's network bandwidth with IP traffic. The victim system slows down, crashes, or suffers from saturated network bandwidth, preventing access by legitimate users.

Amplification Attacks. An amplification attack involves the attacker or the zombies sending messages to a broadcast IP address, using this to cause all systems in the subnet reached by the broadcast address to send a reply to the victim system.

2. Resource Depletion Attacks

Resource depletion attacks involve the attacker sending packets that misuse network protocol communications or are malformed. Network resources are tied up so that none are left for legitimate users. This attack can be characterized as Protocol Exploit Attacks and Malformed Packet attacks. Table 1 gives a brief description of various types of attacks and their impacts on different layers of TCP/IP.

Table 1. DDoS Attacks and Their Impact

DDOS ATTACK	DDOS TYPES	ATTACKED LAYER	ATTACK DESCRIPTION
TCP-SYN Attack	Resource Depletion	Transport layer-This type of attack uses transport layer protocols i.e. TCP-SYN and thereby reaching limits of bandwidth and connection of hosts.	It exploits the weakness of three way handshake sequence of TCP connection. SYN request is sent with spoofed source address is sent to victim. Victim unknowingly accepts the request and sends a SYN+ACK only to be kept waiting for a cross confirmation from the source which in real sense has been spoofed to some other IP address. Hence, it results in denial of service because of binding of resources of the victim.
UDP Flood Attack	Bandwidth Depletion	Transport layer-UDP is another transport layer protocol that is used for DDoS attack.	UDP packets flood the random or specified ports of the victim system for unknown applications and if the application is not found then the victim replies with the ICMP Destination Unreachable Packet resulting in system slowdown.
ICMP Flood Attack	Bandwidth Depletion	Network layer- Uses ICMP (which is a network layer protocol) to block the network bandwidth and firewall with extra load.	ICMP ECHO REQUEST packets flood the victim's system i.e. sending m /packets as fast as possible without waiting for the reply. Hence, it saturates the bandwidth of victim's network connection.
PUSH+ACK Attack	Resource Depletion	Transport layer	In this attack multiple agents send TCP packets to the victim system with PUSH and ACK bits set to zero. Hence, victim unloads all the data in the TCP buffer which leads to system crash.
Ping of Death	Resource Depletion	Network layer- Packets which are Protocol Data Units (PDU) of network layer are used for making erroneous fragments.	In Ping of Death attack victim system ends up with the IP packets which are larger than 65,535 bytes when reassembled from the malicious fragments.
IP address and packet options attack	Resource Depletion	Network layer	Attacker sends ICMP ECHO REQUEST packets (with return address spoofed to victim's IP address) to network amplifier and which again sends the packets to the systems within the broadcast address range. These systems send the ICMP ECHO REPLY to the victim which saturates the bandwidth of connection.
Smurf Attack	Bandwidth Depletion Amplification Attack	Network layer	Attacker sends ICMP ECHO REQUEST packets (with return address spoofed to victim's IP address) to network amplifier and which again sends the packets to the systems within the broadcast address range. These systems send the ICMP ECHO REPLY to the victim which saturates the bandwidth of connection.
Fraggle Attack	Bandwidth Depletion Amplification Attack	Transport layer	Attacker sends UDP packets (with return address spoofed to victim's echo service port) to ports of the system which supports character generation. Thus the network falls in infinite loop in which system sends character generated to the echo service of the victim and receives echo reply which again leads to the same process. Hence this attack blocks the bandwidth of the connection.
NTP Amplification	Bandwidth Depletion	Transport and Application layer	Attackers attack the victim servers with UDP traffic with the help of Network Time Protocol(NTP)

			servers.
HTTP Flood Attack	Resource Depletion	Application layer-Overloads the specific services of Application level infrastructure.	This attack uses HTTP GET or POST requests to block the resources of the web server or application. For instance, a request to download a large file from bot to server can significantly consume victim's resources.
SIP Flood Attack	Resource Depletion and Bandwidth Depletion	Application layer-Targets login pages with random user Ids and passwords.	Attackers flood the Session Initiation Protocol(SIP) proxy servers with SIP INVITE packets with the help of Botnet. It consumes the network bandwidth and server resources of the server making it incapable of providing VOIP service.
Distributed Reflector Attacks	Resource Depletion and Bandwidth Depletion	Application layer	It hides the sources of attack and makes the attack even more distributed in nature. Attacker attacks the zombies which again floods traffic on the victim via third parties. Hence, making it difficult to identify the attack sources. For instance, DNS(Domain Name System) Amplification attack.
Slowloris Attack	Resource Depletion	Application layer-Uses high volume HTTP GET Flood or HTTP POST Flood to crash the server.	It targets the victim server by sending partial requests. It constantly sends HTTP headers without completing the request. Hence, victim's connection remains open for a long time which later leads to denial of legitimate connections from clients.
ARP Poisoning	LAN Attack	Network and Data link layer- It disrupts legitimate flow of data with the help of malicious MAC frames.	Address Resolution Protocol(ARP) Spoofing Attack is carried when attacker sends false ARP packets to gateway informing that its MAC address should be associated with the target's IP address. Hence, allowing attacker to drop or not forwarding the packets to the destination.

(Source Raghav et al, 2015)

3.0 DDOS ATTACK INCIDENTS

3.1 Early Trends of DDoS Attacks

A DDoS attack is a major Internet threat as it can create a huge volume of unwanted traffic.The first reported large-scale DDoS attack occurred in August, 1999, against the servers of University of Minnesota was accounted for rendering 227 systems unusable for a couple of days university. Many DDoS flooding attacks had been launched against different organizations since the summer of 1999 (Alomari et al,2012). Most of the DDoS flooding attacks launched to date have tried to make the victims' services unavailable, leading to revenue losses and increased costs of mitigating the attacks and restoring the services. In February 2000, Yahoo, eBay, Amazon, Datek, Buy, CNN, ETrade, ZDNet and Dell were among the high-profile targets of a 15-year old Canadian nicknamed "Mafiaboy". The attack, which reached the rate of 1GB/sec caused unprecedented financial damage and changed the public perception regarding DoS. From then on, DoS and in general Internet crime, started moving from the IRC networks to e- commerce (Loukas & Oke 2009). Analysts estimated that during the three hours Yahoo web site was down; it lost about 500,000 USD. According to the bookseller Amazon, the DDoS attack was a reason for losing 600,000 USD during the 10 hours of downtime. Likewise, during the DDoS attacks against eBay, eBay.com availability was degraded from 100% to only 9.4% (Mohammed &Azizah, 2009). "Mafiaboy" was sentenced in September 2001 for causing over $1.7 billion damages. In January 2001, The first major attack involving DNS servers as reflectors occurred in January 2001 targeted towards Register.com. This attack, which forged requests for the MX records of AOL.com lasted about a week before it could be traced back to all attacking hosts and shut off. It used a list of tens of thousands of DNS records that were a year old at the time of the attack. In February 2001, over 12,000 attacks were registered against more than 5,000 distinct victims over a three-week period (ITworld.com, 2001). The Coordination Center of the Computer Emergency Response Team was also attacked in May 2001, making the availability of their Website intermittent for more than two days (Alomari et al,2012). Microsoft also lost approximately 500 million USD over the course of a few days from a DDoS attack on its site. In October 2002, 9 of the 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. Another major DDoS flooding attack occurred in February 2004 that made the SCO Group website inaccessible to legitimate users. This attack was launched by using

systems that had previously been infected by the Mydoom virus (Zargar et al, 2012). The virus contained code that instructed thousands of infected computers to access SCO's website at the same time. Another major DdoS attack was launched on June 15, 2004 against name servers on Akamai's Content Distribution Network (CDN), which blocked nearly all access to many sites for more than two hours. The affected sites included Apple computer, Google, Microsoft, and Yahoo. These companies have outsourced their DNS service to Akamai to enhance service performance(Gonsalves, 2007). 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 (Alomari et al,2012). As proof of these disturbing trends, 2003 to 2006 FBI/CSI surveys (Cichardson, 2007; Gordon et al, 2006) concluded that DdoS attacks are one of the major causes of financial lossesas depicted in Figure 5. Large-scale attacks cause substantial financial damage to companies relying on the Internet for their daily business. Direct (e.g., revenue loss during the attack) and indirect (e.g., customer loss attributed to degraded reputation) damages are also experienced. E-commerce and stock exchange sites spend millions of dollars to recover from these attacks, whereas other companies allocate a huge amount of money to defend themselves from possible hackers. As indicated by the survey of VeriSign respondents, expenditures reach up to $2.5 million (Kerner 2011).

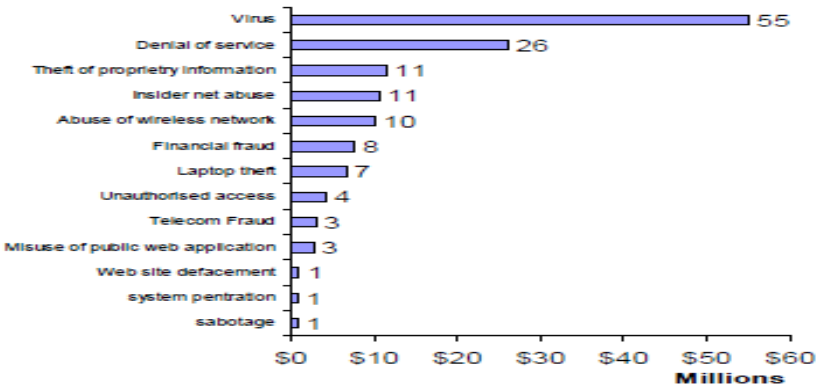

Figure 5. Financial losses incurred due to attack incidents (Monika et al, 2010)

3.2 Recent Trends of DDoS Attack Incidents

DDoS attacks occur almost daily. Even well-known websites, such as Twitter, Facebook, Google, and other popular search engines, cannot escape these attacks that affect countless users. In 2007, e-government, financial services and media were disabled for one to ten hours (Radunovic, 2013). In the weeks leading up to the five-day 2008 South Ossetia war, a DDoS attack directed at Georgian government sites containing the message: "win+love+in+Rusia" effectively overloaded and shut down multiple Georgian servers. Websites targeted included the Web site of the Georgian president, Mikhail Saakashvili, rendered inoperable for 24 hours, and the National Bank of Georgia. While heavy suspicion was placed on Russia for orchestrating the attack through a proxy, the St. Petersburg-based criminal gang known as the Russian Business Network (R.B.N), the Russian government denied the allegations, stating that it was possible that individuals in Russia or elsewhere had taken it upon themselves to start the attacks (Usman et al, 2012). In July 2009, government news media and financial websites in South Korea and United States were attacked using Mydoom virus code (Zargar et al, 2012). An eye-opener case was the DDoS incident that targeted the White House, FBI, DOJ (FBI, 2012), the Recording Business Association of America, Universal Music Websites, and the Hong Kong Stock Exchange (Headlines, 2012). A total of 80 computers were compromised by the Botnet and up to 250,000 were infected with malware during the attack. The attack traffic consumed 45 gigabytes per second according to the 7th Annual Report from the Arbor Company 2011(McPherson, 2010). The outage lasted for seven days. On December 2010, a group calling themselves "Anonymous" orchestrated DDoS flooding attacks on organizations such as Mastercard.com, PayPal, Visa.com and PostFinance (Guardian, 2010). In 2011, There were several attacks such as DDoS attack against Tunisian Government websites, shutting down Blogging Platform Live Journal, launching attack against South Korea National Elaction Commission website and flooding traffics of Asian E-commerce Company. Most recently, In January 2012 official website of Russia president was down for hours, since September 2012, online banking sites of 9 major U.S. banks (i.e., Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, Fifth Third Bank, BB&T, and HSBC) have been continuously the targets of series of powerful DDoS flooding attacks launched by a foreign hacktivist group called "Izz ad-Din al-Qassam Cyber Fighters" (Kitten, 2013). Consequently, several online banking

sites have slowed or grounded to a halt before they get recovered several minutes later. Figure 6 illustrate summary of DDoS Attacks over the years since the first noticeable incident while Table 2 summarizes the recent trends of DDoS attacks:

Figure 6. Summary of DDoS attacks over the Years

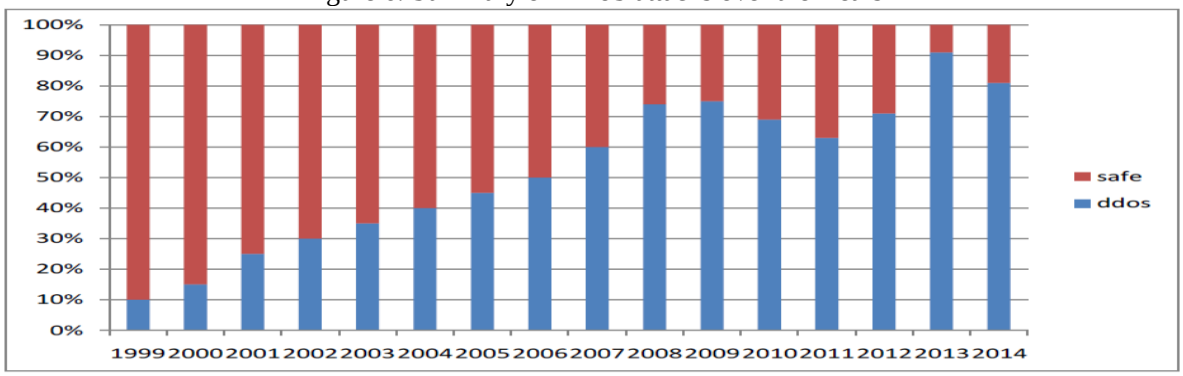

Figure 6. Summary of DDoS attacks over the Years (Paliwal et al., 2014)

Table 2. Recent DDoS Incidents

Date of Attacks	Details of Attacks
February 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 (B. L. Communication 2014).
March 2013	Spamhaus suffered a DDoS attack in which hacker exploited botnet and DNS reflection technologies andThe attack traffic continuously rose from 10Gbps to an 300Gbps, it was largest scale (traffic-wise) (NSFOCUS 2013).
October 2012	Web site of Capital One Bank. The incident was the second attack allegedly waged by a hacktivist group against the bank,
March 2012	DDoS attacks against South Korea websites (Daljeet & Krishan 2012). and United states Websites. It is similar to those launched in 2009.
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 (Alomari et al, 2012) and also Official websites of the president of Russia to be down for more than 15 hours (Daljeet & Krishan 2012).
November 2011	Asian Ecommerce Company. Flood of Traffic was launched and 250,000 Computers are infected with malware Participated. The traffic load has been massive with several thousands request per second and load the server (Daljeet & Krishan 2012).
October 2011	Attacks were launched during the morning when citizens would look up information and attack leads to fewer turnouts against websites of National Election Commission of Korea (Daljeet & Krishan 2012).
April 2011	Attack on Operation Sony that lead to an outage of the Play Station Network (Takahashi 2011) .
March 2011	Attack on NEW YORK (CNN Money) which hit the company‘s data centers with tens of millions of packets per second [49], serious functionality problems and Shutting down Blogging Platform Live Journal for over 12 Hours and start again on April 4 and 5, 2011 (Daljeet & Krishan 2012).
January 2011	DdoS attack against Tunisian Government websites included president, prime minister, ministry of industry, ministry of foreign affairs and stock exchange (Alomari et al, 2012), FINE GAEL‘s News Web site (www.finegael2011.com) which causes One-night content outage by an anonymous attacker using the LOIC tool The journal.ie 2011) and also on Egyptian government websites which causes the site to go offline from the beginning of the revolution until the president stepped down (Somaiya 2011).
December 2010	Master Card, PayPal, Visa and Post Finance. Attack was launched in support of WikiLeaks.ch and its founder. Attack lasts for more than 16 hours.
February 2008	15 minutes of outage on WordPress.com, they were 246 attacks, 6 Gigabits of incoming traffic and also 170 attacks reported on Onlinecasino.com.
January 2008	30 minutes of outage on Sciencetology.org . 220Mbps of incoming

	Traffic.
December 2007	DSL.com suffered an attack, 48MBps of malicious data, although traffic was less, attack was more of open connection request from an ever-growing list of I GBps.
July 2007.	2 days of outage on Castlecops.com. 1 GBps of traffic loss of more than $160,000.

4.0 CONCLUSION

DDoS attack incidents are increasing day by day. Not only, that DDoS incidents are increasing tremendously but it present a serious problem in the Internet and challenge its rate of growth and wide acceptance by the general public, skeptical government and businesses. These DDoS attacks can pose a serious threat to the web server, which can lead to high data and economic losses. In evaluating the recent trends of DDoS attacks, this paper provides a clear view of the DDoS attack problem, by evaluating reasons and steps for conducting DDOS attack, assessing various DDoS attacks architecture and tools, classifying these attacks based on its type depending on the vulnerability of exploitation and reviewed DDoS incidents over the past years.

REFERENCE

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

Arora K., Kumar K., Sachdeva M., (2011). "Impact Analysis of Recent DdoS Attacks", International Journal of Computer Science and Engineering., ISSN 0975-3397,Vol. 3,pp 877-884.

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

Bysin, (2001). "knight.c sourcecode,". Available at: http://packetstormsecurity.org/distributed/knight.c

CERT, (2001) 'Denial of Service Attacks' available at http://www.cert.org/tech tips/denialofservice.html

CERT Coordination Center, (2001)Trends in Denial of Service attack technology, Available from http://www.cert.org/archive/pdf/DoS_trends.pdf.

Chang R. K. C., (2002) Defending against flooding-based distributed denial of service attacks: A tutorial, Computer journal of IEEE Communications Magazine, Vol. 40, no. 10, pp. 42-51.

Christos D. and Aikaterini M. (2004). "DDoS attacks and defense mechanisms: classification and state-of-the-art" Available at http://www.sciencedirect.com. Computer Networks pg. 643–666.

Cichardson R., (2007). "Computer Crime and Security Survey," available at http://www.crime-research.org/news/11.06.2004/423.

Company V., (2006) "Distributed Denial of Service (DDoS) and Botnet Attacks," An iDefense Security Report.

Criscuolo P. J., (2000), Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory.

Daljeet K., Monica S., Krishan K., (2012) "Recent DDoS Incidents and Their Impact," International Journal of Scientific & Engineering Research, vol. 3.

Daljeet K. and Monika S. (2014). "Impact Analysis of DDoS Attacks on FTP Services", Proc. of Int. Conf. on Recent Trends in Information, Telecommunication and Computing, Journal of Association of Computer Electronics and Electrical Engineers pg. 220-228.

Dhruv A. P., Prof Patel H. (2014). Detection and Mitigation of DDOS Attack against Web Server, International Journal of Engineering Development and Research, vol. 2.

FBI, "Justice Department Charges Leaders of Megaupload with Widespread Online Copyright Infringement," 2012. Available at: http://www.fbi.gov/news/pressrel/press-releases/justice-department-charges-leaders-of-megaupload-with-widespread-online-copyright-infringement.

Gonsalves C., (2007). Akamai. DDoS Attack Whacks Web Traffic, available at http://www.eweek.com/article2/0,1895,1612739,00.Asp.

Gordon A., Loeb P., Lucysgyn W., and Richardson R., (200) CSI/FBI Computer Crime and Security Survey, CSI Publications.

Gupta B. B., Joshi R. C., Misra M., (2010). Distributed Denial of Service Prevention Techniques, International Journal of Computer and Electrical Engineering (IJCEE), vol. 2, number 2, pp. 268-276.

Headlines, (2012) "DDoS Attacks Against Government and Entertainment Websites Escalate,". Available at: http://www.infosecisland.com/blogview/19543-DDoS-Attacks-Against-Government-and-Entertainment-Websites-Escalate.html.

Hancock B., (2001) "Trinity v3, a DDoS tool, hits the streets," Computers & Security, vol. 19, pp. 574-574.

ITworld.com. (2001) "CERT hit by DDoS attack for a third day,". Available at: http://www.itworld.com/IDG010524CERT2

Kerner S.M., (2011). "DDoS Attacks on the Rise," 2011. Available at: http://www.esecurityplanet.com/trends/article.php/3932976/DDoS-Attacks-on-the-Rise.htm

Kitten T., DDoS: Lessons from Phase 2 Attacks, available at http://www.bankinfosecurity.com/ddos-attacks-lessons-from-phase-2-a-5420/op-1

Lai S. and Wang M. (2014) "Principal Analysis and Defense Technologies of Application Layer DDos Attacks". Journal of International Conference on Mechatronics, Electronic, Industrial and Control Engineering, pg. 564.

Laurie Segall, (2011). "Wordpress hammered by massive DdoS attack,". Available at: http://money.cnn.com/2011/03/03/technology/wordpress_attack/index.htm.

Liu J., Xiao Y., Ghaboosi K., Deng H., and Zhang J., (2009). Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures, EURASIP Journal on Wireless Communications and Networking, vol. 2009, Article ID 692654, 11 pages.

Loukas G. and Oke G. (2009). Protection against Denial of Service Attacks: A Survey.

McPherson D., (2010). "Worldwide Infrastructure Security Report," Arbor Networks, available at: http://ipv6.org.sa/sites/default/files/World_Infrastructure_Security_Report_ 2011.pdf.

Mirkovic J., and Reiher P., (2004) A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53.

Mohammed A. S. and Azizah A., (2015). Denial of Service and Distributed Denial of Service Attacks, A Novel Protective Framework for Defeating HTTP-Based available at http://dx.doi.org/10.1155/2015/238230

Monika S., Gurvinder S., Krishan K., and Kuldip S., (2010). DDoS Incidents and their Impact: A Review, The International Arab Journal of Information Technology, Vol. 7, No. 1.

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

Operation Payback cripples MasterCard site inrevenge for WikiLeaks ban, Dec. 8, 2010, available at http://www.guardian.co.uk/media/2010/dec/08/operation–payback–mastercard–website–wikileaks.

Paliwal N. Singh R. Deepak R. and Rana S. (2014) Survey of Botnet Based DDoS Attack and Recent DDoS Incidents International Journal of Advanced Research in Computer Science and Software Engineering, pp. 1452-1458)

Puri R., (2003) 'Bots and Botnet – an overview' available at http://www.giac.org/practical/GSEC/RamneekPuriGSEC.pdf.

Radunovic V. J., (2013) "DDoS - Available Weapon of Mass Disruption," in 21st Telecommunications forum TELFOR 2013 Serbia, Belgrade.

Raghav V., Nitika C. and Jyoteesh M. (2015). Impact Evaluation of Distributed Denial of Service Attacks using NS2, International Journal of Security and Its Applications Vol.9, pp.303-316 http://dx.doi.org/10.14257/ijsia.2015.9.8.27 Somaiya R., (2011). "Hackers Shut Down Government Sites," Available at: http://www.nytimes.com/2011/02/03/world/middleeast/03hackers.html?_r=2.

Specht S M. and Lee R. B., (2004). Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures. Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550.

Sven Dietrich N.L., Dittrich D., (2000) "Analyzing Distributed Denial 0f Service Tools: The Shaft Case," Proceedings of the 14th Systems Administration Conference (LISA 2000), New Orleans, Louisiana, USA, pg. 12.

Takahashi D., "Hackers deny involvement in PlayStation Network outage,". Available at: http://venturebeat.com/2011/04/22/as-playstationnetwork-outage-continues-hackers-deny-involvement

The journal.ie, (2011). "Fine Gael website defaced by Anonymous _hacktivists',". Available at: http://www.thejournal.ie/fine-gael-website-defaced-byanonymous-hacktivists-2011-01.

Todd B., (2000) 'Distributed Denial of Service Attacks', available at http://www.linuxsecurity.com/resourcefiles/intrusiondetection/ddos–whitepaper.html.

Usman T., Yasir M., Bessam A., (2012). Defense and Monitoring Model for Distributed Denial of Service Attacks, The 2nd International Workshop on Internet of Ubiquitous and Pervasive Things (IUPT 2012).

Wired.com, (2000). "Yahoo on Trail of Site Hackers". Available at http://www.wired.com/news/business/0,1367,34221,00.html.

Zargar S. T., Joshi J., and Tipper D., Senior (2012) "A Survey of defence Mechanism Against Distributed Denial of Service(DDoS) flooding attacks," IEEE Communication Survey & Tutorials.