International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 4, 1008–1017, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.4-080

Present Status of Distributed Denial of service (DDoS) Attacks in Internet World

Rajeev Singh
Department of Computer Engineering
College of Technology
G. B. Pant University of Agriculture and Technology, Pantnagar, Uttarakhand, India
Corresponding author: rajeevpec@gmail.com

T. P. Sharma
Department of Computer Science & Engineering
National Institute of Technology Hamirpur, Himachal Pradesh, India
E-mail: teekparval@gmail.com

(Received February 4, 2019; Accepted May 24, 2019)

Abstract
Distributed Denial of Service (DDoS) attack harms the digital availability in Internet. The user's perspective of getting quick and effective services may be badly hit by the DDoS attackers. There are several reports of DDoS attack incidences that have caused devastating effects on the user and web services in the Internet world. In the present digital world dominated by wireless, mobile and IoT devices, the numbers of users are increasing day by day. Most of the users are novice and therefore their devices either fell prey to DDoS attacks or unknowingly add themselves to the DDoS attack Army. We soon will witness the 5G mobile revolution but there are reports that 5G networks are also falling prey to DDoS attacks and hence, the realization of DoS attack as a threat needs to be understood. The paper targets to assess the DDoS attack threat. It identifies the impact of attack and also reviews existing Indian laws.

Keywords- Denial of Service (DoS), Distributed denial of service (DDoS), Botnet, Flooding attacks, IoT attacks.

1. Introduction

In any computer system (standalone or distributed) major security goals are: confidentiality, integrity and availability. These are threatened by various attacks divided into active and passive categories. Attacks that target integrity and availability fall under the active category. The popular techniques in this category involve masquerading, modification of messages, repudiation, replay, and Denial of Service (DoS) attacks. Among these, DoS attacks are the one that hampers & targets availability and are the present domain of discussion in this paper. DoS attack is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and web services. Such attacks are not designed to gain access to the systems. Some of the popular examples includes: i) 'Ping of Death' on a computer that involves sending a malformed or otherwise malicious ping. A ping is normally of 64 bytes in size. Sending a ping which is larger than the maximum IP packet size can crash the target computer, ii) 'Tear drop' in which forged fragmented packets overlap each other during reassembling at the receiving host and possibly crashes it, iii) 'Email-bomb' (a form of net abuse) consisting of sending huge volumes of emails to an address in an attempt to overflow the mailbox (Singh and Sharma, 2015; Kotey et al., 2019; Yusof et al., 2019).

A type of DoS attack in which an attacker uses malicious code installed on various computers to attack a single target is termed as Distributed Denial of Service (DDoS) attack. An attacker uses

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 4, 1008–1017, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.4-080

this method to have a greater effect on the target than is possible with a single attacking machine. This attack can easily cause damage to the victim host or network. It can exhaust the computing and communication resources of its victim within a short period of time (Singh, 2008).

Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb – National Research Council, "Computers at Risk", 1991.

Though this statement made in seminal report of National Research Council in the year 1991 is correct for most of the cyber-attacks but it more appropriately fits for the DDoS Attack. An attacker in this attack hides itself in the distributed Internet and can cause harm to any system anywhere in the world with the help of single terminal/keyboard. Hence, the prediction made approximately 09 years before the first DDoS attack (in the year 2000) was noticed, is very true (Cyber-attacks batter Web heavyweights, 2000). A lot of water has gone under the bridge since then, the DDoS attacks have now entered into terabit age and have more devastating impact on the target. Hence, it becomes imperative to know and review the present status of these attacks.

Figure 1 demonstrates a scenario where the master (the main DDoS attacker) sends control messages (marked in green) though Internet for controlling the slaves. The slaves are the one who unknowingly sends attack packets (marked in red) towards target system. The DDoS attacks are a reality and some of the reasons why these are so frequent in the present Internet world involves: 1) personal reasons (may be for taking revenge) due to which an attacker targets specific computers, 2) prestige gains where the attacker tries to gain respect of hacker community, 3) material gain which can be achieved by blackmailing online companies and, 4) political reasons such as compromising enemy's resources (Mirkovic and Reiher., 2004; Abliz, 2011; Arora et al., 2011).

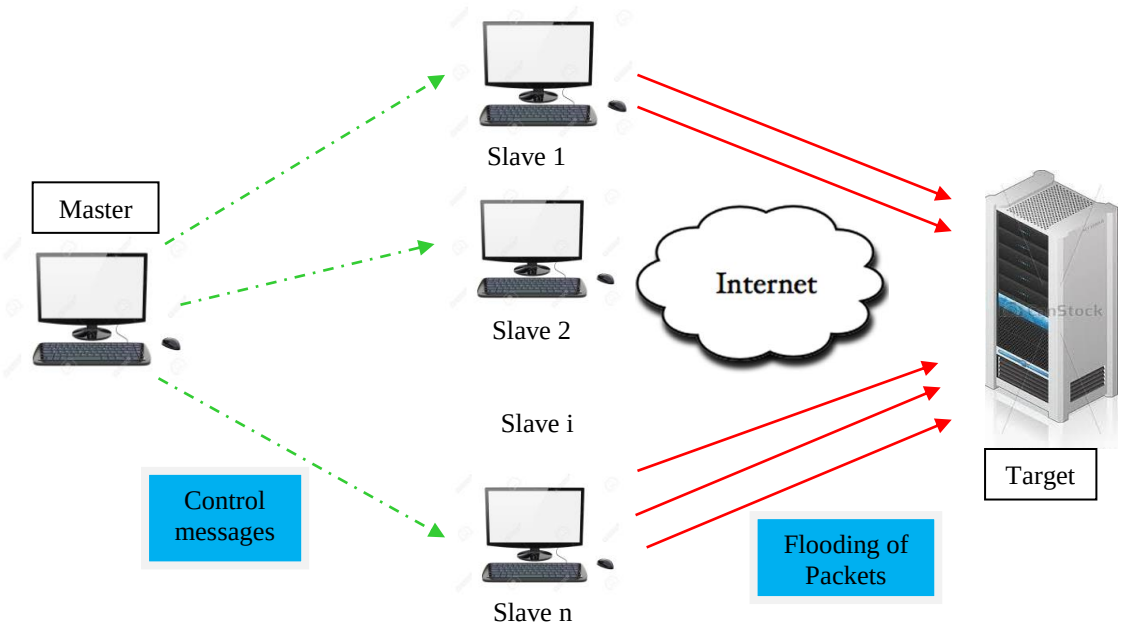

Figure 1. Distributed denial of service attack (Abliz, 2011)

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 4, 1008–1017, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.4-080

DDoS attacks are possible because Internet security is highly interdependent. Security of each host depends on the state of security in the rest of global Internet. Till any of the system in Internet is insecure, the chances of DDoS attacks are there. The attacker may easily slip the attack traffic from a firewall or attacks the firewall itself to make is unusable. Over provisioning also does not helps against DDoS attacks as the attacker can probably get enough resources to overcome any levels of over provisioned resources. Hence, notion of well securing machines in a network, use of firewalls and over-provisioning of servers is of not much use. This is because:1) Internet resources are limited and as such there are not enough resources to match the number of users, 2) there is no accountability enforcement in the Internet and any one can pretend as other via source address spoofing, 3) Control is distributed in the Internet and every networks run according to its local policies. The cost of DDoS attack to an attacker is far less as compared to its benefits. The current defense can only mitigate the attack once it has taken place. An effective defense against it is not visible to date. The solutions are still in infancy stage. Hence, DDoS attacks constitute one of the major threats in today's Internet (Mirkovic et al., 2004; Singh, 2008; Abliz, 2011; Arora, 2011).

Rest of the paper is organized as: Section2 of the paper reports the present status of the DDoS attacks. Section3 provides information about the DDoS attack tools used by the attackers and are easily available on the Internet. Section4 presents DDoS attack cases that have occurred in the past and have raised worries for the users. Section5 and section6 respectively covers cyber laws in India against DDoS attacks and issues and concerns against DDoS attacks. Finally, section7 provides conclusions.

2. Present Status

Prominent types of cyber attacks and their brief description are shown in Table 1. DDoS is listed as one among them. As per (Kardon, 2018), cyber crime has incurred losses amounting to approximately dollar 400 billion in the year 2015 and is expected to reach dollar 2 trillion in the year 2019. The statics of the cyber attacks from January to September 2018 reveals that DDoS attacks contributed 3.57% among various kinds of cyber attacks. The others major shares greater than DDoS attacks were that of Malware (35.61%), Vulnerability (6.41%), Targeted Attack (12.61%), Account Hijacking (17.33%) and Unknown Attacks (16.60%) (Hackmageddon, 2019).

Table 1. Prominent types of cyber attacks (Kardon, 2018)

Attack/concern	**Brief description**
Malware	Software designed with malicious intentions and is designed so as to damage or control a computing device. Popular one includes ransomware that encrypts the files and later demands ransom for unencrypting them.
Phishing	Activity wherein the users are directed especially via emails towards fake websites. The users may give up their passwords and other financial details upon login.
Man-in-the-Middle Attacks	The attacker inserts himself in between the browser and web server and is able to obtain useful information on the way.
Cross-Site Scripting	It involves insertion of malicious code into the website which targets the visitor's browser and causes damage.
DDoS attacks	The army of compromised computing devices overloads the server with data resulting in its shutdown or crashing.
SQL Injection	Refers to corruption of data accessing SQL and make server divulge information like credit card numbers, user names etc.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 4, 1008–1017, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.4-080

Verisign DDoS trends report during Q2 2018 says that 26 percent of DDoS attacks were over 5 Gbps with an average attack peak size of 5.7 Gbps. According to this report, the largest volumetric DDoS attack peaked at 42 Gbps while the highest intensity DDoS attack peaked at 4.7 Mpps. This clearly states the devastating power of present day DDoS attacks. Verisign noticed a 35 percent increase in the number of DDoS attacks when comparing Q2 2018 to Q1 2018. As per the findings, User Datagram Protocol (UDP) floods were the most common attack type (Distributed Denial of Service Trends Report, 2019).

Security vendor Symantec's report in the year 2014 found that 26 percent of all DDoS attack traffic in the world originates from country like India. The love for India by the DDoS attackers is due to low cyber security awareness, lack of adequate security practices and infrastructure. Thus, India is not only affected by DDoS attacks but it also provides a hotbed for launching the large scale DDoS attacks in other countries. The unprotected wireless, mobile and Internet of Things (IoT) devices along with availability of high bandwidth networks (4G/5G) have worsened the things. Thus, assessment of DoS attacks and protection against them in Indian cyber space is the need of the hour (Symantec, 2014).

Akamai trends report finding are that DDoS attacks are remarkably stable. As per the report, the size of the largest attack (bandwidth) grows by about 9% per quarter, which nets out to doubling every two years. This is not continuous growth and whenever the adversary discovers a new attack method then a new peak size is established. This trend is observed including large scale DDoS attacks like Mirai and memcached reflection attacks (Ellis, 2018).

3. Major Attack Tools

The DDoS attack tools may be classified into 4 broad categories: HTTP packet generating - DDoS attack tools, DoS only - attack tools, Mobile - attack tools, Traditional DDoS attack tools. The first category is the most popular these days. This is due to the fact that most of the devices are mainly online most of the time and in working mode, utilizing HTTP based protocols. This category has tools like HTTP Unbearable Load King (HULK), DDOS Simulator (DDOSIM), R-U-Dead-Yet (RUDY), Low Orbit Ion Canon (LOIC) etc. The second category of DoS only - attack tools includes Nemesy, Land and LaTierra, Panther and also Wireless LANs DoS attack tools like Airjack, aircrack-ng which are used in WLANs to bring Access Point or wireless station down. Attacks in this category primarily target the single host. AnDOSid is a mobile based DoS tool which can be used to launch DoS attacks to bring website down from the mobile phone. Trinoo, Tribe Flood Network and Stacheldraht are the popular traditional DDoS attack tools (Singh and Sharma, 2015; Singh and Sharma, 2016; Best DOS Attacks and Free DOS Attacking Tools, 2018; How to DDoS, 2019; Sharma, 2018).

4. DDoS Attack Cases

DDoS attacks became popular in the year 2000 when some popular websites went down due to its impact. This attack was named as Mafiaboy attack. The Mafiaboy was the hacking name of the High School boy Michael Calce. Mafiaboy coordinated and controlled several Universities' networks for conducting the DDoS attack and stopped the services of CNN, Dell, E-Trade, eBay, and Yahoo. Since then DDoS attacks are appearing in news. There are several reports of DDoS attack incidences in the Internet world that have caused devastating effects on the user and web services. One such devastating DDoS attack (popularly referred to as Estonia attack) happened in April, 2007 when the attacker targeted entire country and brought its infrastructure at its knees. The entire country's infrastructure was hit by this attack. This DDoS targeted government, banks,

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 4, 1008–1017, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.4-080

ministries, newspapers and broadcasters web sites of Estonia. 128 unique DDoS attacks (115 ICMP floods, 4 TCP SYN floods and 9 generic traffic floods) were conducted. Attacker used hundreds or thousands of "zombie" computers and pelted Estonian Web sites with thousands of requests a second, boosting traffic far beyond normal levels. Due to attack, the country's network infrastructure got affected resulting in damaging of routers and associated routing tables, overloading of DNS servers and, mail server crashing. As the major attack traffic was coming from outside the country, Estonian ISPs concentrated upon blocking of all the foreign traffic for mitigating the DDoS attacks (Arora, 2011; Famous DDoS Attacks, 2019).

Estonia though a small country but is among the leading countries who adopted the IT based services completely for making the country go paperless. The country has adopted the e-governance and e-voting since last few years. Hence, an attack of such capacity against the IT infrastructure alarmed and raised attentiveness among the other nations who are in their initial stages of adoption of such mechanisms. This attack was considered as the first act of cyber warfare. The reasons of this attack were assumed to be political in nature and were attributed towards the political conflict of Estonia with Russia (Famous DDoS Attacks, 2019).

In 2013, a DDoS attacks against Spamhaus was observed. Spamhaus works against Spaming and its filtering. The attack traffic rate in this attack was 300 Gbps (The attack is referred to as Spamhaus attack). A teenage paid attacker from Britain targeted the Spamhous- who in turn took help of Cloudflare's DDoS protection mechanism for mitigating the attack. Hence, Spamhous was protected but few others like London internet exchange got affected by the attack (Famous DDoS Attacks, 2019).

In August 2015 a DDoS attack was done through unsuspected browsers. This attack fall under browser hijacking wherein a malicious JavaScript was inserted in a popular WebPage Baidu (Chinese web search engine) and all visitors to this website become participants in the DDoS attack. This attack sent 4.5 billion requests using various mobile browsers and was spotted by CloudFlare Researchers. The attack targeted CloudFlare's customer GitHub (An online coding website). Chinese mobile IP addresses were mainly involved in the attack. Xiaomi's MIUI, Safari, Chrome browsers were particularly used. The motivation of the attack is political and it was aimed at the GitHub projects bypassing the Chinese state censorship. The attack lasted several days (www.hackread.com, 2016; Mirai Botnet Linked to Massive DDoS Attacks on Dyn DNS).

In the upcoming October 2016, the DDoS attack named as The Dyn attack was observed. It was performed by the Botnets comprising of compromised IoT Devices. It represented direct attack where the large number of IoT devices targeted the Dyn (network infrastructure company/DNS provider). The attack lasted one day and mainly based upon DNS reflection and amplification (Figure 2). The small requests of the browsers were amplified to large sized responses using DNS resolvers. The amplified responses were used to flood and attack the target named server. The attack was performed by the botnet army consisting of mainly IoT devices like CCTV cameras, DVRs, lightbulbs, and even stuffed animals. The attack utilized approximately 145,000 IoT devices. Thus, the attack turned 'Internet of Things' into 'Botnet of Things'. The attack brought down -Twitter, Amazon, Tumblr, Reddit, Spotify, and Netflix. Compromised IOT devices helped reach attack rate near to 700 Gbps, equivalent to the target streaming 140,000 HD movies simultaneously (Famous DDoS Attacks, 2019).

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 4, 1008–1017, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.4-080

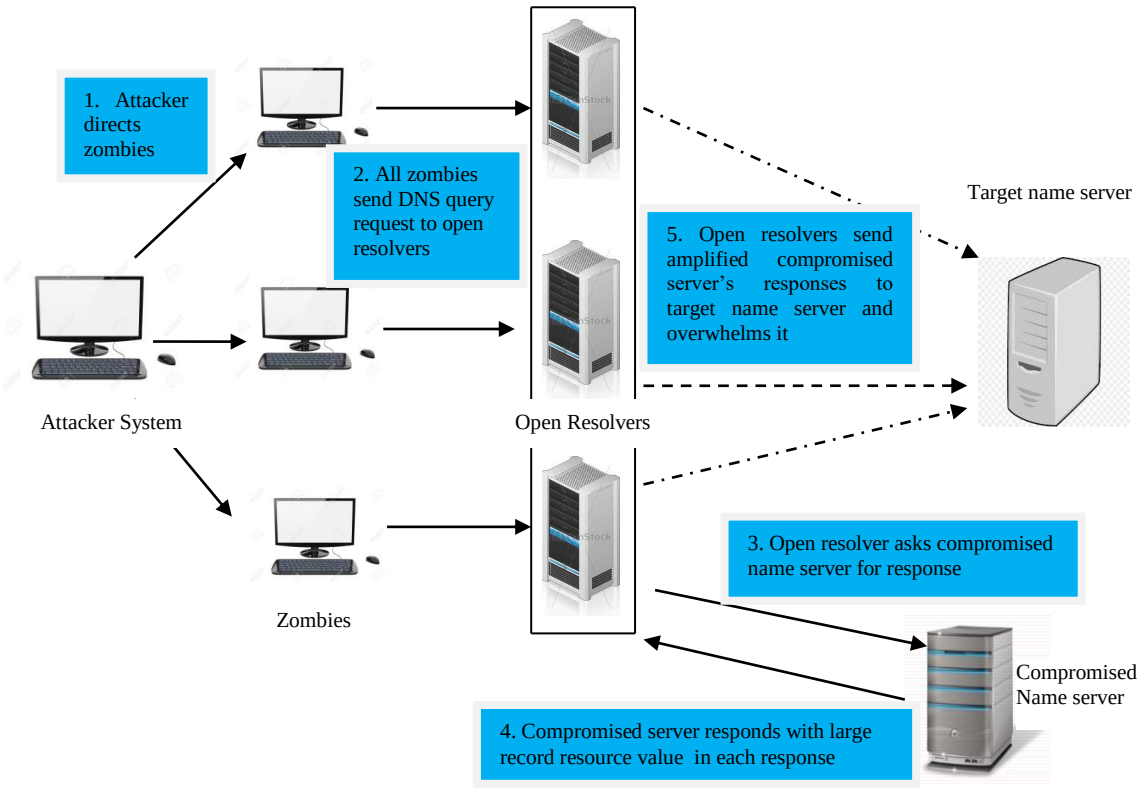

Figure 2. DNS reflection and amplification DDoS attack

In October 2017, DDoS attacks hit Sweden's transportation network causing delays to operations. They crashed the IT system that monitors train's locations as well as taking down associated email systems, websites, and road traffic maps. Customers during this time were unable to make reservations or receive updates on the delays (www.transportsecurityworld.com, 2018; DDoS cyber attack cripples Danish Rail's ability to sell tickets).

NETSCOUT Arbor noticed DDoS traffic surged to 335Gbps and 29.4 million packets per second (Mpps) on 27 February, 2018 in Australia which was approximately 10 times the average traffic flow for the rest of the month (World's Largest DDoS Attack, 2018).

A series of DDoS attacks started building up in the month of February, 2018 and continued in the month of March, 2018. These were noticed by cloud and CDN Company, Akamai. Akamai accordingly alerted its client so as reduce the attacks and associated impacts. These are referred to as Memcached DDoS attack. The most devastating among them was reported on 28 February, 2018. This was largest among series of DDoS attacks in the month of February and March 2018. It was twice the size of Mirai IoT based DDoS attack. The attack traffic rate was of the order of 1.3 terabytes per second (Tbps) and packets rate was of the order of 126.9 million per second. The attack lasted about 20 minutes. Approximately 1000 memcached servers were involved in the attack on 28 Feb 2018 (World's Largest DDoS Attack, 2018).

In memcached DDoS attack an open source data caching tool named as memchaced is used by the attackers. The attackers utilized the extraordinary amplification and reflection of memcached wherein a small amount of 210 bytes may lead to generation of 100MB response i.e., an amplification of 500K. The attack traffic having source port as that of memcached server targeting GiTHub (An online coding website who happens to be a client of Akamai) was filtered by the Akamai servers and the clear traffic was forwarded by the scrubbing centres of Akamai to GiTHub. Hence, very little impact of the attack was noticed on GiTHub. Thus, no botnets involved in the attack. During this attack, the compromised nodes were mainly from United States, Russia, China and India (22.15 percent). Hence, it is again evident apart from the Semantic report (2014) that DDoS attacks needs special attention in counties like India where mobile and Internet users are rising steeply day by day (Nandikotkur, 2014; www.moneycontrol.com, 2018).

On May 14th, 2018 in Denmark a DDoS attack on railway system made it impossible to purchase a ticket via mobile app, website, at ticket machines and in kiosks at the stations hence, posing a real threat in the computer world (www.transportsecurityworld.com, 2018).

5. Cyber Law in India for DoS Attacks

The Information Technology Act, 2000 was inacted by Indian Parliament in the year 2000. The Act states about i) Cyber Contraventions –that may result in civil prosecution and, ii) Cyber Offence – that may result in criminal prosecution. In former, the following two sections provide guidelines for Denial of Service under ***Chapter IX as***

Section 43 (e): causing disruption - *disrupts or causes disruption of any computer resource (computer system or computer network); Preventing normal continuance of computer*
Section 43 (f): denial of access - *denies or causes denial of access to any authorized person by any means; Denial of service attacks*

In these sections, there is provision of imprisonment for a term up to three years or fine up to Rs. five lakhs (to a dishonest/fraudulent person) or both.

In latter, section 66F states about cyber-terrorism. It may attract life imprisonment.

6. Issues and Concerns against DDoS attacks

It is clear that technology alone is insufficient to deter cyber threats and attacks like DDoS will keep on troubling the users. One way to lessen their extent is via spreading the DDoS attack awareness, knowledge and understanding. The users should be told that their devices and networks may be used for the conduction of DDoS attacks, so that users deploy preventive measures in their devices and networks. It is very true that the attackers are becoming stealthier, smarter and more capable day by day. They are doing so by hiding their tracks better. Different governmental legislations are present in different parts of the world for dealing with the DDoS attack cases which complicates the problem further. The anti DDoS solutions exist but are too expensive to implement. Either hardware or software upgrade is required or continuous maintenance is required. Different countries have their own national interests; sometimes they may even favor these attacks under wars and enmity situations. In these attacks, it is ironical that the attacker is not the one who is actually executing the attack rather the attacker is only like a zombie who is acting under the control of the hidden principal attacker. Hence, it is difficult to prove who the real attacker is. Also, it is difficult to prove who used the computer that is used in

the attack at a particular instant of time. In these attacks, usually the consoles are located across international boundaries and hence, law-enforcement problem pose a big challenge. In the past, DDoS has been considered as a nuisance activity conducted by cyber vandals i.e., it has very less socioeconomic aims. But in the future, due to high Return on Investment (ROI), destabilization may be used as the main aim of the attacker instead of the targeting particular targets (Abramson, 2016).

7. Conclusion

Distributed Denial of Service (DDoS) attack harms the digital availability and is a top security threat to service provisioning. The user's perspective of getting quick and effective services may be badly hit by the DDoS attackers. DDoS attack can easily cause damage to the victim host or network. It can exhaust the computing and communication resources of its victim within a short period of time. The cost of attack to an attacker is far less as compared to its benefits. There are several DDoS attack tools available and these are either freely available online or can be purchased for as little as $5(Cluley, 2016). Also, the source code of these attack tools are often released so any cyber criminal can make their own botnet army with ease. In this paper, we have presented the major incidences of DDoS attacks in the Internet World till Jan 2019. The data clearly tell us that these attacks are increasing in number, size and devastating power. These attacks not only targeted the popular web services but also digitally advanced countries and heavily provisioned service providers. Thus, these attacks need to be stopped. If the DDoS attacks like the ones done recently in Denmark, Sweden and Australia were stopped; catastrophe situations in pervasive computing environment may have been prevented. It would have helped the users in maintaining the service connectivity despite of attacks. Hence, it is concluded that DDoS constitute one of the alarming security threats in today's Internet world that needs proper attention.

Conflict of Interest

The authors confirm that this article contents have no conflict of interest.

Acknowledgment

The authors acknowledge and express the gratitude towards their parent institutes for the support.

References

Abliz, M. (2011). Internet denial of service attacks and defense mechanisms. *University of Pittsburgh, Department of Computer Science, Technical Report*, 1-50.

Abramson J. (19 April 2016). DDoS attacks: bigger, stronger, scarier. Retrieved 08Jan, 2019, from https://www.symantec.com/connect/blogs/ddos-attacks-bigger-stronger-scarier

Arora, K., Kumar, K., & Sachdeva, M. (2011). Impact analysis of recent DDoS attacks. *International Journal on Computer Science and Engineering*, *3*(2), 877-883.

Best DOS attacks and free DOS attacking tools (April 26, 2018). Retrieved 08Jan, 2019, from *https://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/#gref*

Cluley G. (May 26, 2016). Hire a DDoS attack for as little as five dollars. Retrieved 08Jan, 2019, from *https://www.tripwire.com/state-of-security/featured/hire-a-ddos-attack-for-as-little-as-5/*

Cyber-attacks batter Web heavyweights (February 9, 2000). Retrieved 08 Jan, 2019, from *http://edition.cnn.com/2000/TECH/computing/02/09/cyber.attacks.01/index.html*

DDoS cyber attack cripples Danish Rail's ability to sell tickets (14 May, 2018). Retrieved 08Jan, 2019, from *https://www.transportsecurityworld.com/ddos-attack-cripples-danish-rails-ability-to-sell-tickets*

Distributed denial of service trends report. Retrieved 04 Feb, 2019, from *https://www.verisign.com/en_IN/security-services/ddos-protection/ddos-report/index.xhtml*

Ellis, A. (2018). State of the internet/security, a year in review (SOTI 2018). *Technical Report Akamai*. *4*(5), 1-16.

Famous DDoS Attacks | The Largest DDoS attacks of all time. Retrieved 04 Feb, 2019, from *https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/*

Hackmageddon. Information security timelines and statistics – cyber attacks statistics. Retrieved 04 Feb, 2019, from *https://www.hackmageddon.com/category/security/cyber-attacks-statistics/*

How to DDoS | DoS and DDoS attack tools. Retrieved 04 Feb, 2019, from *https://www.cloudflare.com/learning/ddos/ddos-attack-tools/how-to-ddos/*

India fourth most targeted country in the world for web application attacks (June 28, 2018). Retrieved 08Jan, 2019, from https://www.moneycontrol.com/news/world/india-fourth-most-targeted-country-in-the-world-for-web-application-attacks-2645941.html

Kardon, L. (June 28, 2018). The 6 types of cyber attacks to protect against in 2018. Retrieved 08Jan, 2019, from *https://pagely.com/blog/cyber-attacks-in-2018/*

Kotey, S.D., Tchao E.T., Gadze, J.D., (2019). On distributed denial of service current defense schemes. *Technologies, 7*(19), 1-24. doi:10.3390/technologies7010019

Mirai Botnet Linked to Massive DDoS Attacks on Dyn DNS (October 22nd, 2016). Retrieved 08Jan, 2019, from https://www.hackread.com/mirai-botnet-linked-to-dyn-dns-ddos-attacks/

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39-53.

Nandikotkur, G. (October 31, 2014). India launches most ddos attacks. Retrieved 08Jan, 2019, from *https://www.bankinfosecurity.in/india-launches-most-ddos-attacks-a-7512*

Sharma, A. (August 7, 2018). Top10 Power Full DoS/DDoS Attacking Tools for Linux, Windows & Android. Retrieved 08Jan, 2019, from *https://thehackerstuff.com/top10-powerfull-ddos-tools-linux-windows/*

Singh, R. (2008). *On prevention of distributed denial of service attacks*. M.Tech. Thesis. Department of Computer Science & Engineering, I.I.T. Roorkee, Roorkee, Uttarakhand, India

Singh, R., & Sharma, T.P. (2015). A location-based method for restricting the flooding DoS effect in WLANs. *Journal of Location Based Services*, *9*(4), 273-295.

Singh, R., & Sharma, T.P. (2015). On the IEEE 802.11 i security: a denial-of-service perspective. *Security and Communication Networks*, *8*(7), 1378-1407.

Symantec: 26% of DDoS attacks this year originated from India (Oct 2014). Retrieved 08Jan, 2019, from *https://www.livemint.com/Industry/V5upm1A2Vb6QIPubzg1I2K/26-of-DDoS-attacks-this-year-originated-from-India-Symante.html*

World's Largest DDoS Attack: US Firm Suffers 1.7 Tbps of DDoS attack (March 6th, 2018). Retrieved 08Jan, 2019, from *https://www.hackread.com/worlds-largest-ddos-attack-us-firm-suffers-1-7-tbps-of-ddos-attack/*

Yusof, A.R., Udzir, N.I. & Selamat, A. (2019). Systematic literature review and taxonomy for DDoS attack detection and prediction. *International Journal of Digital Enterprise Technology*, *1*(3), 292–315.