A Survey on Characterization of Defense Mechanisms in DDOS Attacks

Rajeshwari.S, Malathi.K, Regina.B

Abstract- Distributed Denial of Service (DDoS) Attack is a poisonous threat to our security professionals. DDoS Attack is defined as the attack which targets one or more systems using multiple systems which are compromised usually by Trojan Horse at the same instance of time. DDos Attack does not allow legitimate users to access their resource and their services by taking advantage of the system vulnerability .DDoS Attack is independent of the protocols used .The goals of DDoS Attack is Twofold. First it overloads the server which may lead to crash and the second goal is to acquire and steal the bandwidth by generating a large scale of traffic.The attack is set up by a Master called as BotMaster by controlling armies of system to attack which is injected by malware called as Botnets. Effective and Collaborative Defense Mechanisms for DDoS Attack in Wired Network Systems is the main Scope of Intrusion Detection.

Exploration of defense mechanisms for DDoS Flooding Attack in Wired Network Systems along with their classification and study of various structures of Botnets is discussed in this paper. We also highlight all the techniques already used before the attack, during the attack and after the attack. As application level attacks are common and stealthier when compared to network /transport level attacks we focus more on http DDoS flooding attacks.

Index Terms - DDoS (Distributed denial of service) Attacks ,TrojanHorse ,BotMaster, Collaborative Defense Mechanisms, Http DDoS flooding attacks, Intrusion Detection, application level attacks.

I. INTRODUCTION

We can categorize the interest and motivation of the attackers into 5 types.

1) Financial/economical gain: This type mainly targets on big websites which have large revenue and this is hosted by technically strong hackers with good experience.
2) Ideological belief: Attackers are motivated by their ideological beliefs to paralyze the target system. The incident of this type is WikiLeaks in the year 2010 [1} and Iran in the year 2009 [2]
3) Revenge: Attackers with bad technical skill implement a attack to the injustice happened to them.
4) Intellectual Challenge: Attacker are young hackers who wants to experiment their talent by using tools and implementing small botnets.
5) *Cyber warfare*: Attackers of this type are well trained with lots of resources. They attack due to political views and paralyze other country intellectual properties. Some of the targets are government offices, bank and telecommunication services.

Zombies are implemented with the help of worms, Trojan Horse and Backdoors. First Armies evolution of Zombies are very simple scripts which compromised IRC(Internet Relay Channel) protocol in the internet .This protocol was used in active messaging of text through the internet. Zombies hide their identity by spoofing their IP Address. The main impact of DDoS flooding attack is to make all the services unavailable and make a drastic revenue Loss to the websites. It also takes time to recover and increases Mitigation Cost. For instance YAHOO was attacked in 2002 and its service was unavailable for 2 hours[3].The other famous attack was the shutdown of Domain Name System in 2002.DDoS Flooding attack made 9 root system to crash[4].

MyDoom Virus code was reused to attack SCO website in 2004 which accessed the website at the same instance of time [5] in figure 1.Again in 2009 MyDoom Virus attacked South Korea financial Websites [6][7]. On December 2010 Mastercard.Com, Visa.com was hit by Anonymous group[8].Other Major attacks are on the banking sites of U.S in September 2012[9]. Survey of Arbor Networks gives the statistics that 69% of attack is between 2009 to September 2010[10]. Prolexic Technologies, which are service providers against DDoS Flooding attack gives a statistics that 7000 Attack takes place daily and increasing at a very high speed [11].

II. DDOS FLOODING ATTACK CATEGORIZATION

Major classification is divided under layer categories. First is the Network/Transport DDoS Flooding Attacks [12], [15] which is subdivided into 4 types.

i) Flooding Attacks: The bandwidth of Network is consumed and it uses UDP flood which can be spoofed or non-spoofed [13], [14].
ii) Amplification Flooding Attacks: The traffic is amplified towards the victim by generating multiple messages [13], [15].
iii) Protocol Exploitations Attacks [13],[14]:Victim Resources are controlled by creating the bugs in the protocol.eg RST Flood, TCP SYN Flood.
iv) Reflection Flooding Attack [13], [15]: Request is forged to the reflectors and all the replies are directed towards the victim that consumes the resources of Victim.eg Smurf attack.

Manuscript received December, 2013

Rajeshwari.S, AssistantProfessor(OG),Computer Science &Engineering Department, Saveetha School of Engineering, Saveetha University, Chenna, India.

Malathi.K,Assistant Professor(OG), Computer Science and Engineering Department, Saveetha School of Engineering, Saveetha University, Chennai, India.

Regina.B, Assistant Professor(SG), Computer Science and Engineering Department, Saveetha School of Engineering, Saveetha University, Chennai, India.

Rajeshwari.S is pursuing her PhD in the area of Network Security under the guidance of Dr. P. Shankar, Professor and Principal, Saveetha school of engineering, Saveetha University.

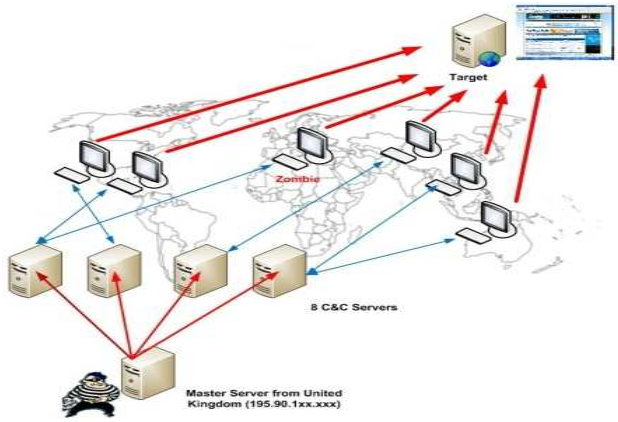

Fig. 2 MyDoom Botnet in U.K

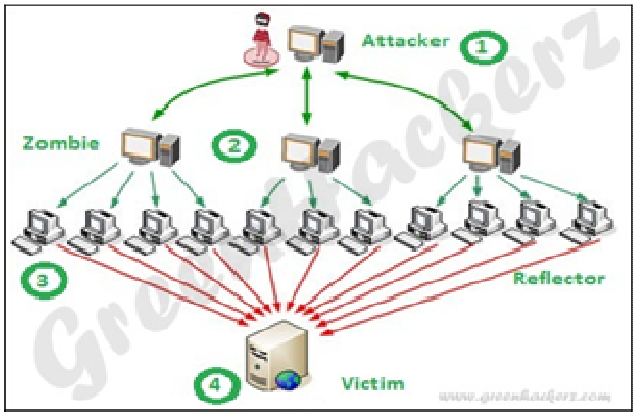

Fig. 2 Reflection Based Attack

Second is the Application level based Flooding Attack which consumes server resources like CPU and its memory. Famous type of attack under this category is SIP (Session Initiation Protocol) [17], DNS and HTTP. Application level based Flooding Attack [17] is divided into two types.

i) Reflection/Amplification based flooding attacks [12], [15]: Large number of request is send to the reflectors and this request is initiated from application level protocol that is forged. These requests are also amplified by sending multiple requests leading to the consumption of server's resources. DNS Amplification is the famous one and the forged request query sent by spoofed IP address consumes large resources for the respond from DNS. This large scale of traffic paralyses the target systems. Other types of attacks are VOIP Flooding Attack [14] and this attack is difficult to trace back as it shows a legitimate traffic. Figure 2 depicts the flow of attack.

ii) HTTP Flooding Attacks [3], [14], [16], [18]: This type of attack is classified into four types.

a) Session Flooding Attacks: The request for the Session Request becomes higher which leads to large consumption of the resource of servers. One of the famous attacks is HTTP Request get Attack. Botnets are used for this attack which has the efficiency to generate 10 attacks per second and therefore less no of botnets can launch successful attacks.

b) Asymmetric Flooding attacks [14]: Sessions used by the attackers will be overloaded with request. This is classified into two types

b.1) Multiple Http get/post flooding attacks [14]: This attack takes place in one HTTP Session and many request is present in one packet. The attack rate of the traffic is low which hides the attacker.

b.2) Faulty Applications [14]: This Attacker mainly focuses on poorly designed websites with vulnerability. The newly opened websites which does not have proper implementation and integration with their databases are selected as Zombies. SQL Injection is used to generate requests.

c.) Request Flooding Attacks [14]: This attack consists of many requests than the normal request rate .But attacker can cheat the defense mechanisms easily.

d.) Slow Request/Response Attacks [19]: This attack opens many new TCP connections without any data to communicate and also sets the receiver a smaller buffer size. The attack reads the response slowly instead of sending the request in a slow fashion.

III. STRUCTURE OF BOTNETS

Botnet Architecture along with the strongly designed tools initiates the DDoS Flooding Attacks.A good defense Mechanisms should deal with two properties which was defined by Peng et al [13]. First it should tackle large scale of zombies that creates drastic traffic. Second the defense Mechanisms should trace back the zombies with spoofed IP address. The ingredients of Botnets are BotMaster who executes the Attack, the Agents who spread the infection also called as zombies and the handlers are the hidden programs in the device through which Botmaster communicates. Main channel used for DDoS Attack are IRC (Internet Relay Chat) through which all commands are executed.

Bots are classified into three types. They are IRC based, Web based and P2P based .

i) IRC based [20]: This uses Architecture of client sever for communication. This protocol is based on messaging of text in the Internet. IRC communicate with hundreds of clients using multiple servers. IRC channels are used as handlers and master bot takes the help of IRC port to communicate with their agents (a .k .a zombies). Malicious codes are easily shared using IRC and the attackers hide their identity easily due to large scale of traffic which server has on the channel. Due to the infrastructure of Centralized command and Control (C&C) we can easily shutdown the entire botnets by capturing the C&C servers. The famous botnets tools under this category are Kaiten[22] and trinity v3[21].The attackers take the control of IRC servers to monitor the list of botnets rather than creating the list in the local system.

ii) Web based [23]: This type of Botnets uses HTTP protocol to command the agents. Web based Botnets doesn't have any connection with C&C Servers and they hide easily in the legitimate HTTP as the traffic is more stealthier. PHP scripts are used to control the Bots and the communications are encrypted through the port80 (HTTP). Famous Botnets tools are Black Energy [24] and Aldi[25].Botnets under this category have self Destructive characters in nature when they are traced. Malicious code is present in the payload which Erases all the data present in the hard drive to kill the traced host [27]

IV. DDOS DEFENSE MECHANISMS-CLASSIFICATION [12], [28], [13], [29], [15], [26]:

DDoS Flooding attacks makes all the resources such as memory, time required to process the task useless. As soon as the DDoS Attack is detected only minimal time is present to disconnect the infected systems. The Defense mechanisms

should be efficient to stop the attack near to the source machine. But the attack accuracy is high near the victim.

Defense mechanisms are classified into two major categories. First one on the location where the defense mechanisms are placed and second one is based upon on the time when attack takes place.

1) Location Based: This is again divided into two major types depending on the layer where the defense mechanisms are placed. They are

i) Network/Transport level :In this layer it can be placed in the source and Destination. Therefore it is subdivided into four subtypes. They are

a) Source Based
b) Destination Based
c) Network Based
d) Hybrid

ii) Application Level: Network based attack is not possible here as the attack traffic in application level cannot be given access to the devices in the lower layers.

Figure 3 Depicts the layer attacks. They are subdivided into two types.

a) Destination Based
b) Hybrid

2) Time based: This is classified into three stages of the attack. They are

i) Before the attack: This can be analyzed using prevention Techniques.

ii) During the attack: This can be analyzed using Detection Techniques.

iii) After the attack: This can be analyzed using Mitigation Techniques

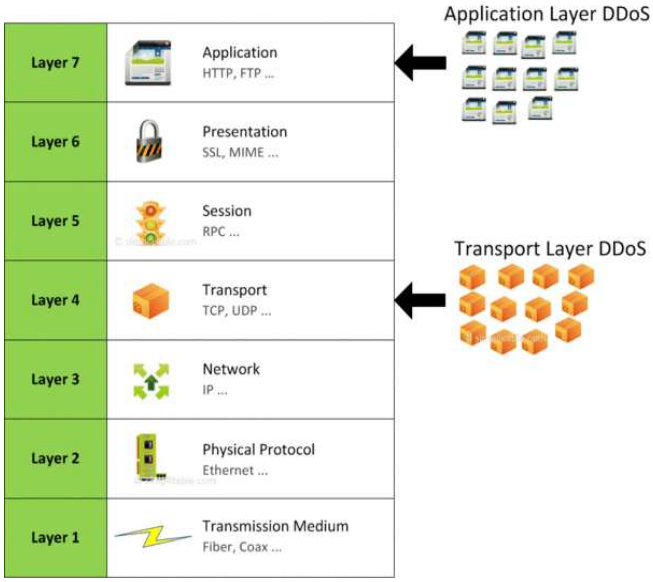

Fig. 3 DDoS in different layers

V. CONCLUSION

We have presented a summary of classification and scope of DDos Flooding attacks Detection methods in Wired network. Even though we have many defensive mechanisms, a effective mechanisms is the need of the time. Research work can be focused on creative and efficient model for authentication of legitimate users to filter the hackers easily. Collaborative model should be designed to control the attacks at different layers simultaneously. As Botnets are great threat to the society, which creates revenue losses to the government websites we need to create a optimal solution for this problem. The work can also find the solutions by predicting the motivation of the attacks and creating a strong Prevention DDoS Systems. Future attacks and their detection can give scope for these DDoS Attack problems.

REFERENCES

[1] [online] http://techcrunch.com/2010/11/28/wikileaks-ddos-attack/
[2] [online] http://isc.sans.edu/diary.html?storyid=6622
[3] Yahoo on Trail of Site Hackers, Wired.com, Feb. 8, 2000, [online] http://www.wired.com/news/business/0,1367,34221,00.html
[4] Powerful Attack Cripples Internet, Oct. 23, 2002, [online]http://www.greenspun.com/bboard/q–and–a–fetch–msg.tcl?msgid=00A7G7
[5] Mydoom lesson: Take proactive steps to prevent DDoS attacks, Feb. 6, 2004, [online]
[6] Lazy Hacker and Little Worm Set Off Cyberwar Frenzy, July 8,2009,[online] http://www.wired.com/threatlevel/2009/07/mydoom/
[7] New ”cyber attacks” hit S Korea, July 9, 2009,[online]http://news.bbc.co.uk/2/hi/asia-pacific/8142282.stm
[8] Operation Payback cripples MasterCard site in revenge for WikiLeaks ban,Dec.8,2010, [online]http://www.guardian.co.uk/media/2010/dec/08/operation–payback–masterc ard–website–wikileaks
[9] T. Kitten, DDoS: Lessons from Phase 2 Attacks, Jan. 14, 2013, [online]http://www.bankinfosecurity.com/ddos-attacks-lessons-from-phase-2-a-5420/op-1
[10] Worldwide Infrastructure Security Report: Volume VI, 2011 Report, Arbor Networks, Feb. 1st, 2011, [online] http://www.arbornetworks.com/report
[11] Prolexic Technologies, [online] http://www.prolexic.com/index.phpknowledge–center/frequently–as k ed–questions/index.html
[12] J. Mirkovic and P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, April 2004.
[13] T.Peng, C.Leckie, and K.Ramamohanarao, Survey of network-based defense mechanisms countering the DoS and DDoS problems, ACM Comput. Surv. 39, 1, Article 3, April 2007.
[14] RioRey, Inc. 2009-2012, RioRey Taxonomy of DDoS Attacks, RioReyTaxonomyRev2.32012,2012. [online]http://www.riorey.com/xresources/2012/RioRey Taxonomy DDoS Attacks 2012.eps
[15] “C. Douligeris, and A. Mitrokotsa, DDoS attacks and defense mechanisms: classification and state-of-the-art, Computer Networks, Vol. 44, No. 5, pp. 643-666, April 2004.”
[16] “S. Ranjan, R. Swaminathan, M. Uysal, A. Nucci, and E. Knightly, DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer attacks, IEEE/ACM Trans. Netw., Vol. 17, No. 1, pp. 2639, February 2009.”
[17] Arbor Application Brief: The Growing Threat of Application-LayerDDoS Attacks, Arbor Networks, Feb. 28, 2011, [online]http://www.arbornetworks.com/component/docman/doc download/467-the-growing-threat-of-application-layer-ddos-attacks ?Itemid=442.
[18] BreakingPoint Labs, Application-Layer DDoS Attacks Are Growing: Three to Watch Out For, Oct. 4, 2011, [online]http://www.breakingpointsystems.com/resources/blog/application-layer-ddos-attacks-growing/
[19] S. Shekyan, Are you ready for slow reading?, Jan. 5, 2012, [online]https://community.qualys.com/blogs/securitylabs/2012/01/05/slow-ad
[20] J. Lo et al., An IRC Tutorial, April, 2003, irchelp.com 1997, [online]http://www.irchelp.org/irchelp/irctutorial.html#part1.
[21] “B. Hancock, Trinity v3, a DDoS tool, hits the streets, Computers & Security, Vol. 19, no. 7, pp. 574-574, Nov., 2000.”
[22] Bysin, knight.c sourcecode, 2001, [online]http://packetstormsecurity.org/distributed/ knight.c.
[23] Team-cymru Inc., A Taste of HTTP Botnets, July, 2008, [online]http://www.teamcymru.com/ReadingRoom/Whitepapers/2008/httpbotnets.Eps
[24] J. Nazario, BlackEnergy DDoS Bot Analysis, Arbor Networks, 2007, [online]http://atlaspublic.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.eps

[25] C. Wilson , DDoS and Security Reports: The Arbor Networks Security Blog, Arbor Networks, 2011, [online]http://ddos.arbornetworks.com/2012/02/ddos-tools/.
[26] "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding AttacksSaman Taghavi Zargar, Member, IEEE, James Joshi, Member, IEEE, and David Tipper, Senior Member, IEEE"
[27] [online] http://infosecisland.com/blogview/12395–DDoS–Attack–Utilizes–Self–Destructing–Botnet.html
[28] "L. C. Chen, T. A. Longstaff, and K. M. Carley, Characterization of defense mechanisms against distributed denial of service attacks, Computers & Security, vol. 23, no. 8, pp. 665-678, December 2004"
[29] "U. Tariq, M. Hong, and K. Lhee, A Comprehensive Categorization ofDDoS Attack and DDoS Defense Techniques, ADMA LNAI 4093, pp. 1025-1036, 2006"

Rajeshwari .S graduated her bachelor of engineering in SRM Valliammai engineering College under Anna University. She Graduated her masters of engineering in St.Joseph College of engineering under Anna University and she got a scholarship from the college for being the topper in the Department. She has also received ARINGAR ANNA Award from St.Joseph college of engineering for being the best outgoing student of the year. She is now doing her PhD under Dr.Chandrasekar ,HOD of Lab Affairs in St.Joseph college of engineering and Dr.P.Shankar, Principal of Saveetha School of Engineering. She is at present working as assistant professor in Computer Science department of SSE, Saveetha University.