International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 4; Issue: 3; March -2015

Response Replicator Unit: To fight DDOS attacks.

Pradeep Sadanand [1], Basavaraj Jakkali [2]

[1] Assistant Professor Dept. of CSE, BMS College of Engineering, Bangalore , India

[2] Associate Professor Dept. of CSE, BMS College of Engineering, Bangalore , India

Abstract: Computer malware infiltrate into computer systems affecting the performance of the system from its intended use. Trojan horse and Botnet are class of malware that have emerged as frontrunners of DDOS attack, disrupting some of the services hosted on the Internet. This paper proposes a system to supplement the existing internet infrastructure to combat possible DDOS attack.

Keyword: DDOS attacks, DDOS Defense mechanism, Computer Malware, Trojan horse and Botnet.

I. Introduction

The term computer malware has been a matter of concern for more than two decades. Computer malware has caused fear, apprehension and hatred ness among computer users. Computer malware are malicious program or script and are classified as Virus, Worms, Ad ware, Spy ware, Botnets and Trojan horse based on their behavior [1]. Two categories of computer malware that deserve immediate attention are Trojan horse and Botnet.

The Trojan horse attacks account to 83 percent of the global malware according to the survey conducted by BitDefender from January to June 2009[2].A Trojan horse is a program or a script (not necessarily malicious) that enters a computer system without the knowledge or consent of the computer user[3]. A Trojan horse is generally transmitted through email with subject titles which usually catch the attention of the recipient. A recipient of such email is usually persuaded to perform actions such as clicking on a hyperlink or open an attachment. If the recipient responds with any of these actions, an appropriate response is generated to deceive the recipient. Meanwhile a Trojan horse is downloaded on to the system behind the scenes. Once resident on a system, a Trojan horse may participate in modifying the data, disrupting the performance of the system or of the entire network, steal valuable data from the

system, invite additional malicious program or become a part of a DDOS attack. DDOS (Distributed Denial of Service) or DOS (Denial of Service) are attacks to disrupt a computer system or computer networks from its intended use. Usually the Trojans that take part in such DDOS attack are controlled by a controller (not necessarily the distributor of the Trojan horse); the controller may be a hacker or an entity with some vested interest. The controllers can scan and locate resident Trojans in the network and use them to his wishes [4].

A Botnet is similar to Trojan horse in various aspects except Botnet propagation. The Botnet replicate and penetrate to multiple systems by harvesting the email addresses or use IRC channels of the compromised system [5]. The collections of such replicated Botnet are controlled by a Command and control (C&C) server. The Command and control (C&C) server can utilize the services of such deployed Botnet for malicious intent including the launch of DDOS attack.

In this paper the focus is on DDOS attacks and defense mechanism in wired networks. The rest of the paper is organized as follows, Section II introduces related work on DDOS attacks and defense mechanism. Section III identifies the problem. Section IV proposes the model to combat DDOS attacks. Section V concludes with some insights for combating comprehensive DDOS flooding attack

II. Related work

A. Srivastava et. al [6] discusses numerous challenges in tackling DDOS attacks. DDOS defense mechanisms can be deployed at source, destination and hybrid approach.

The source defense mechanisms are Ingress/Egress filtering at source edge proposed by P.Ferguson and D.Senie [7]. Utilize firewalls to control the outflow of packets proposed by Mannanet[8]. The Destination based defense mechanisms include History based IP filtering[9] that filters IP packets based on recorded statistics. Packetscore[10] estimates the genuineness of packets before discarding. The hybrid approaches include TRACK[11] combines IP tracebook, packet marking and Packet Filtering. StopIt[12] a network filter to block undesirable traffic

III. Problem Statement

In a typical DDOS attack several distributed computers (ranging from 1000's to millions) at a given instance send service request to a computer system (usually a system providing some service, e.g. http, ftp... etc.). The magnitudes of such distributed requests converge to disrupt the performance of a target system and its associated network to intolerable levels; finishing off with temporarily or indefinitely suspending the system from its intended service. This paper proposes supplementing the internet infrastructure with a new system to combat DDOS attack in order to increase the

availability of the services for its legitimate use.

IV. Proposed Model

Generally DDOS attacks are intended at application's running on the server (i.e. Applications running on the application layer of the TCP/IP protocol stack). Such attacks can be managed by deploying the proposed system called as Response Replicator Unit (RRU) across the internet.

The Response Replicator Units (RRU) consists of a stateful firewall and a set of computer systems for replicating responses. The stateful firewall in the RRU keeps log of requests that arrived before, after and during the DDOS attack. The computers in the RRU are used to dynamically create multiple copies of the predetermined response.

In operation, the stateful firewall monitors the network for possible DDOS attack. On detection of a DDOS attack the stateful firewall will trigger the computer systems in the RRU to create multiple copies of the predetermined response from the server under threat (predetermined response should challenge the authenticity of the request). Such replicated response will serve the flooding DDOS requests.

Since Trojan Horses or Botnets can't authenticate themselves against challenges, the magnitude of the attack scales down gradually allowing only the legitimate requests.

The stateful firewall can now check with the log entries to determine if the subsequent request arriving from a client is due to the responses generated by the RRU. If bona fide the request can be forwarded to the server for processing.

For effective implementation, the replicated response packets should surpass the DDOS requests. This is possible if multiple RRU are scattered across the internet.

V. Future work.

As Internet is home to millions of malware, the extent of the malware deployed for launching DDOS attack can't be estimated. The Computer systems in the RRU might not be able to combat if a full-fledged DDOS attack occurs. Addition of RRU is not just only expensive but also degrades the performance of the available network infrastructure. Though the proposed system might be effective to combat small or medium sized DDOS attack, the scalability of the proposed system for large attacks have to be assessed.

References

[1]. Malware [Online], Accessed at 01 – March-2015, http://en.wikipedia.org/wiki/Malware

[2]. BitDefender malware and spam survey, Accessed at 01 – March -2015,

http://www.bitdefender.com/news/bitdefender-malware-and-spam-survey-finds-e-threats-adapting-to-online-behavioral-trends-1094.html

[3]. Trojan Horse [Online], Accessed at 01 – March -2015, http://en.wikipedia.org/wiki/Trojan_horse_(computing)

[4]. Deconstructing SubSeven, the Trojan Horse of Choice [Online], Accessed at 01 – March -2015http://www.sans.org/reading-room/whitepapers/malicious/deconstructing-subseven-the-trojan-horse-of-choice-953

[5]. Botnet [Online], Accessed at 01 – March -2015, http://en.wikipedia.org/wiki/Botnet

[6]. A. Srivastava, B.B. Gupta , A. Tyagi1, Anupama Sharma, and Anupama Mishra: A Recent Survey on DDoS Attacks and Defense Mechanisms. IEEE Communications surveys and Tutorials, Vol. 15, No. 4, Fourth Quarter 2013

[7]. P.Ferguson and D.Senie, Network Ingress filtering: Defeating Denial of Service Attacks that employ IP source address spoofing, Internet RFC 2827, 2000.

[8]. Mannanet, Reverse Firewall [Online] http://www.cs3-inc.com/pubs/Reverse_Firewall.eps

[9]. T.Peng, C Leckie and K.RammohanRao, Protection from Distributed Denial of Service attacks using history-based IP filtering, ICC '03. May, Vol. 1 pp: 482-486, 2003

[10]. Y.Kim, W.C. Lau, M.C. Chuah and H.J. Chao, Packetscore:A statistics-Based packet filtering scheme against Distributed Denial-of-Service attacks, IEEE Trans. Dependable Secure Computing, Vol. 3, no. 2, pp. 141-155, 2006.

[11]. R.Chen, J.M. Park and R. Mrachany, TRACK: A novel approach for defending against Distributed Denial-of-Service attacks, Technical Report TR-ECE-0602, Dept. of Electrical and Computer Engineering, Virginia Tech, Feb 2006.

[12]. X.Liu, X.Yang, and Y.Lu, To filter or to authorize: network-layer DOS defense against multimillion-node Botnets, in Proc. ACM SIGCOMM conference on Data Communication (SIGCOMM '08), NY, USA, pp. 195-206, 2008.

Pradeep Sadanand is an Assistant Professor in the Department of Computer Science & Engineering at BMS College of Engineering. He has completed his Post Graduation from Vishweswaraya Technological University (VTU), Belgaum, in 2010. His areas of interest include Computer network, Software Engineering and Network Security.

Basavaraj Jakkali is an Associate Professor in the Department of Computer Science & Engineering at BMS College of Engineering. He has completed his Post Graduation from Vishweswaraya Technological University (VTU), Belgaum, in 2002. His areas of interest include Computer Organization, Microprocessors, Theory of Computation, Operating Systems, System Software and Network Security