A Review on the Flash Crowd Attack and Its Implications

Pragathi Prasanna
UG BE Student
ECE Department, DSCE
USN : 1DS13EC736

Pavithra G.
Full Time Research Scholar
VTU RRC, Belagavi, Karnataka
USN : 5VZ16PEJ56

Dr. T. C. Manjunath
Prof. & Head of the Dept.,
Dept. of E & C E,
Dayananda Sagar CE, B'lore

***Abstract*:- In this booming digital era, everything is going online. Out of which, online shopping and online retail applications get a mammoth share. Many people shifting their focus towards online shopping to that of brick and mortar shops. So this has made online business a boom. Internet is a global network which provides the various communications for the users. It also provides better scalability and openness. This causes unprotected and unauthorized transaction to users. This feature of internet is useful for attackers to perform some attacks by sending malicious data through malicious and suspicious transactions without bothering for the security. Lack of authorization means that attackers can create a fake identity and send malicious traffic with impunity. Communication privacy has been a growing concern especially with the internet becoming a major hub of our daily interactions. At the same time it is also being threatened by many advanced attacks on these online applications. Flash crowd attack is one such advanced network security attack. This attack concentrates on an online application's website by sending many dummy useless requests to the server, thus putting a lot of pressure on server. Once the flash crowd attack occurs, a response rate increases and it results in web server crashing. This evades even the legitimate clients/ buyers not to access the server. It is found that this attack might cause lot of problems to online buyers in the coming days. Minimizing the flash crowd attack is possible by using wireshark and addressed the problems that are raised by this attack. The work presented in this paper is the UG credit seminar work of the undergraduate student that was undertaken by the UG student & just provides a brief review of the different attacks undergone in online retail applications and is just a review paper, which serves as a basis for all the students, faculties as a base for carrying out the research in this exciting field of network security.**

General Terms:- Flash Crowd Attack, online retail application

Keywords:- DDoS, DoS, FCA.

1. INTRODUCTION

The attacker can try for an illicit entry to the services provided by the network bluffing as a private node and this well known concept could be named as Denial Of Service (DOS) attack. DOS prevents or inhibits the normal use or management of communication facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade the performance. DOS is considered under the active attack that can be easily detected but their prevention is tough.

At a given point of time these processes handle a limited amount of traffic depending upon the performance of hardware, bandwidth and memory usage. Suppose the saturation point of this exceeds, service may not be provided by the servers and the actual traffic is neglected as well as the user cannot access the services. Due to the huge usage of internet for varied applications, technology has enabled low cost and low power consumption WSNs. As a result of this basic nature of networks it is open to many data attacks. These kinds of attacks may be tried on different layers of network, some of them may be preventive and can be resolved using some kind of protocols to prevent the attacks. Truly these attacks are not easy to name and put a stop to.

Online shopping is a form of electronic commerce which allows consumers to directly buy goods or services from a seller over the Internet using a web browser. Consumers find a product of interest by visiting the website of the retailer directly or by searching among alternative vendors using a shopping search engine, which displays the same product's availability and pricing at different e-retailers.

As of 2016, customers can shop online using a range of different computers and devices, including desktop computers, laptops, tablet computers and smartphones. An online shop evokes the physical analogy of buying products or services at a regular "bricks-and-mortar" retailer or shopping center; the process is called business-to-consumer (B2C).

2. OVERVIEW

In the current era, most modified way for an attacker is to attack application. They find a way to distract application assets such as "Flash Crowd Attack". In flash crowd attack, they may act as real application processor by deploying the network and generates legal requests for the applications to override the victim. This type of attack is extremely challenging since it is active in legal resources. So they act like they are legal participants in the network. In order to lower service application they attack the network once in a while. An improved form of traditional DOS attack can be called as Distributed Denial Of Service (DDOS). Flash crowd attack is a form of DDOS. DDOS can be defined as

an attack in which multiple compromised computers systems attack a target, such as a online shopping.
server website or other network resource and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the system forces it to slow down or even crash and shut down, thereby denying service to users. Like the attack may not be on a single machine rather it points on a set of equipments used as a master slave configured machine in a network having multitier configuration. DDOS attack acts as a decisive risk to the network connected. Flash crowd legally issues some of the pop up messages with a fishy wish to attack the server.
Unexpected surges in Web request traffic can exercise server-side resources (e.g., access bandwidth, processing, storage etc.) in undesirable ways. Administrators today do not have requisite tools to understand the impact of such "flash crowds" on their servers. Most Web servers either rely on over-provisioning and admission control, or use potentially expensive solutions like CDNs, to ensure high availability in the face of flash crowds. A more fine-grained understanding of the performance of individual server resources under emulated but realistic and controlled flash crowd-like conditions can aid administrators to make more efficient resource management decisions.

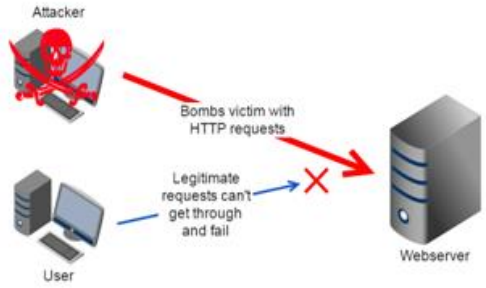

Fig.1. DoS attack representation

3. UNDERSTANDING DDOS AND DOS

DoS : Denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

DDoS : A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.

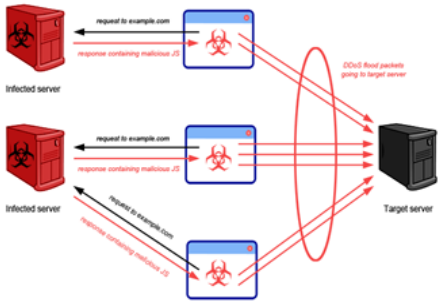

Fig. 2. DDoS attack representation

4. LITERATURE SURVEY

In order to understand the basic concepts involved it is important to conduct the literature survey. Previously published papers were referred and below are the ones that are found to be more relevant and useful for going forward.

[1]. Analysis of a botnet takeover
This article describes an effort to take control of particularly sophisticated and insidious botnet and study its operation for a period of 10 days. It summarizes what the authors learned and reports on what has happened to that botnet since.

[2]. Towards situational awareness of large scale botnet probing events
In this work, it investigates ways to analyze collections of malicious probing traffic in order to understand the significance of large scale 'botnet probes'. This analysis draws upon extensive honeydata to explore the prevalence of different types of scanning, including properties such as trend, uniformity, co-ordination and darknet avoidance.

[3]. Abnormally malicious autonomous systems and their internet connectivity
In this paper, they explore whether some autonomous systems indeed are safe havens for malicious activity. They look for ISPs and Ass that exhibit disproportionately high malicious behavior using 10 popular blacklists, plus local spam data and extensive DNS resolutions based on the contents of the blacklists. Overall they examine the malicious activity as AS granularity can unearth networks with lax security or those that harbor cybercrime.

[4]. Identifying suspicious activities through DNS failure graph analysis
In this paper, they propose a light weight anomaly detection approach based on unproductive DNS traffic namely the failed DNS queries with a novel tool DNS failure graph, which captures the interaction between hosts and failed domain names. They apply a graph decomposition algorithm based on tri-non negative matrix factorization technique to iteratively extract coherent co-clusters (sub graphs) from DNS failure graphs. These co-clusters represent a variety of anomalous activities like spamming, Trojans, bots etc.

[5]. Detecting algorithmically generated domain-flux attacks with DNS traffic analysis

In this paper, they develop a methodology to detect such domain fluxes in DNS traffic by looking for patterns inherent to domain names that are generated algorithmically, in contrast to those generated by humans. They look at distribution of alphanumeric characters as well as bigrams in all domains that are mapped to same set of IP addresses.

[6]. Discriminating DDOS attack from flash crowd using flow correlation co-efficient

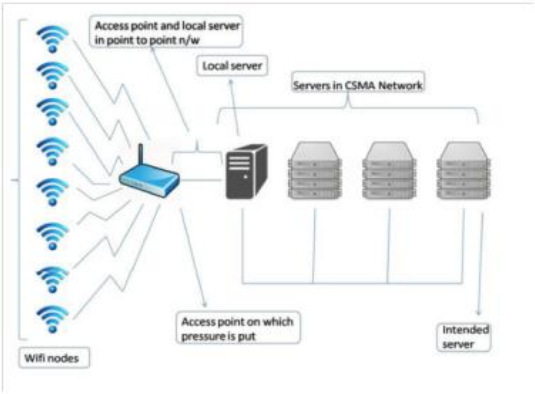

Fig. 3 : A typical scenario of the flash crowd attach model

In this paper, they represent a novel flow similarity based approach to discriminate DDOS attack from flash crowd attack, which remains an open problem to date. DDOS pose a critical threat to the internet. Based on this approach, they proposed a discrimination algorithm using the flow correlation co-efficient as a similarity metric among suspicious flows.

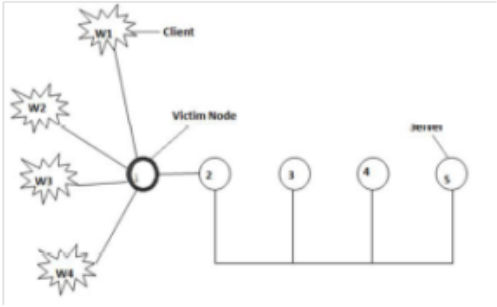

Fig. 4 : Flash crowd attack model

5. FLASH CROWD ATTACK NETWORK MODEL

A gateway will be part of two networks which utilizes different protocols in tele-communications and computer networking. A protocol will be transferred to next one by gateway as depicted in Fig3. In the Fig4, it has integrating the wireless nodes with that of the early simulated point to point and CSMA network. This gives us the network model for the Flash Crowd Attack. The Wi-Fi nodes directly interact with the access point 1, which is the victim node in the flash crowd attack. The access point gets overloaded by the requests of the wireless nodes on it. The above figure depicts the typical scenario of the Flash Crowd Attack model in a real-time application. There are 8 Wi-Fi nodes which are wirelessly connected to the access point. Thus all the requests that the Wi-Fi nodes send, will pass through this access point. So it will incur lot of load from the requests of these Wi-Fi nodes. Then the access point is connected to a local server in a point-to-point connection. Then all these servers are connected in a CSMA network to each other. The server at the end is the intended server. The requests from the Wi-Fi nodes will be served by the intended server.

6. CONCLUSIONS

The conclusion drawn is that the Flash Crowd Attack cannot be controlled entirely, but it can be limited only to a certain extent. We can only minimize its certain effects on the access point by identifying the legitimate clients to that of dummy clients. More the number of clients more will be the load on the access point, and hence some legitimate clients cannot get the services that are intended to have. There is a lot of scope for improvement in this work. Instead of having just one access point to all the clients, we can implement more than one access points. Introduction of more number of access points will reduce the load on one access point, and there will be equal load balancing. Apart from identifying the legitimate clients from that of dummy clients, we can also derive a mechanism on the server

REFERENCES

[1]. William Stallings, “Cryptography and Network Security”, *Pearson Education, Indian branch patparganj Delhi*, 2003, ISBN / ISSN 81-7808-902-5.
[2]. Gururaj H L, Praveen KS, Ramesh B “ Minimizing the impact of flash crowd attack in online retail application”. 2017 11 th International Conference on Intelligent Systems and Control (ISCO)
[3]. M. Edman and B. Yener, "On anonymity in an electronic society: A survey of anonymous communication systems," ACM Comput.Surv., vol. 42, no. 1, 2009.
[4]. B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna, "Your botnet is my botnet: Analysis of a botnet takeover," in Proc.ACMConf Comput. Commun. Security,2009.
[5]. Z. Li , A. Goyal, Y. Chen, and V. Paxson, 'Towards situational awareness of large-scale botnet probing events," IEEE Trans. Inf Forensics Security, vol. 6, no. I , pp. 175- 188, Mar. 2011.
[6]. C. A. Shue, A. J. Kalafut, and M. Gupta, "Abnormally malicious autonomous systems and their intemet connectivity," IEEE/ ACM Trans. Netw., vol. 20, no. I, pp. 220-230, Feb. 2012.
[7]. N. Jiang, J. Cao, Y. Jin, L. E. Li, and Z.-L. Zhang, "Identifying suspicious activities through DNS failure graph analysis," in Proc. IEEE Int. Conf. Netw. Protocols, 2010, pp. 144- 153.
[8]. S. Yadav, A. K. K. Reddy, A. L. N. Reddy, and S. Ranjan, "Detecting algorithmically generated malicious domain names," in Proc. Intemet Meas. Conf., 2010, pp. 48-61..
[9]. http://www.usenix.com ,http://www.wedebugyou.com
[10]. http://www.digitalattack.com