International Journal of Scientific & Technical Development
(A Peer-Reviewed Bi-Annual Journal) ISSN: 2348-4047

STUDY OF FLASH EVENTS AND RECENT DDOS ATTACKS -A REVIEW

***Daljeet kaur, **Dr V K Joshi**
*Department of Computer Sc& Engineering, SBS State University (Punjab) India 152004
**Department of Computer Engineering, Desh Bhagat University (Punjab) India 147301
Corresponding Author EmailID: daljeetkaur617@gmail.com

Abstract

Recent Distributed denial of service (DDoS) attacks have evolved to become a serious threat to the smooth running of both business and government applications on the Internet. Because both are dependent on web servers for their day-to-day work and transactions. A DDoS attack involves flooding a target system with internet traffic so that it is rendered unusable. The web services are either degraded or completely disrupted by DDoS attacks by sending a flood of packets in the form of legitimate looking requests towards the victim web servers. These attacks are virulent, relatively new type which effect availability of Internet services and resources. Another event which is very similar to DDoS attack is a Flash event (FE), which is an overload condition caused by a large number of legitimate requests. In this paper, an overview of DDoS & Flash event problem is given, brief detail of most recent Flash event and DDoS incidents on online organizations is highlighted.

Keywords:DDoS, Flash events, Web servers, Legitimate, Flood of packets.

1. INTRODUCTION

The "availability" means that the information, the computing systems, and the security controls are all accessible and operable in committed state at some random point of time [1]. Threat to theInternet availability is a big issue which is hampering growth and survival of E-business and other Internetbased applications. Internet failures can be accidental or intentional. The Internet design concentrates mainly onproviding functionality though a little attention has been given on designing strategies for controlling accidentalfailures. On the other hand, intentional attacks by malicious users have no answer in the original Internet design.

A denial-of-service (DoS) is such an intentional attempt by malicious users / attackers to completely disrupt or-degrade (compromise) availability of service/resource to legitimate/authorized users [2].Some well-known DoS attacks are SYN Flood, Teardrop, Smurf, Ping of Death, Land, Finger Bomb, BlackHoles, Octopus, Snork, ARP Cache Poisoning and the Misdirection. DoS attacks exploit weaknesses in Internetprotocols, applications, operating systems, and protocol implementation in operating systems.

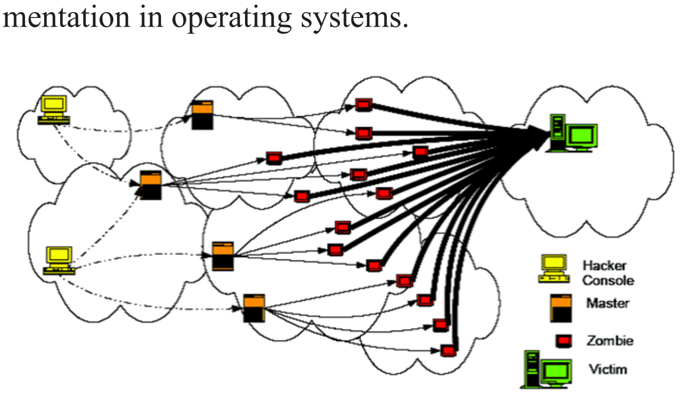
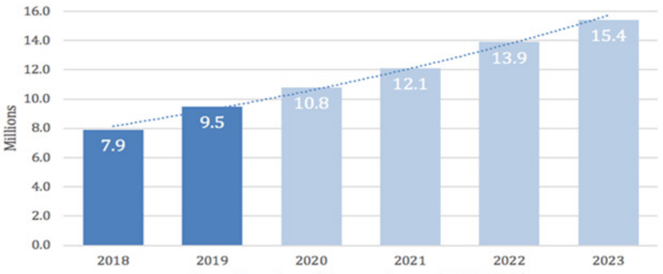


Fig.1 DDoS attack Scenario

Distributed denial-of-service attacks (DDoS) degrade or completely disrupt services to legitimate users by expending communication and/or computational resources of the target. [3] and [4] described DDoS attacks as amplified form of DoS attacks, where attackers direct hundreds or eventhousands of compromised hosts called zombies against a single target. There are varieties of DDoS attacks asclassified in [3] and [5]. However, the most common form of DDoS attacksis a packet-flooding attack, in which a large number of seemingly legitimate TCP, User Datagram Protocol(UDP), or Internet Control Message Protocol (ICMP) packets are directed to a specific destination.As per [6] defending against these attacks is challenging for mainly two reasons. First, thenumber of zombies involved in a DDoS attack is very large and deployment of these zombies spans largegeographical areas. The volume of traffic sent by a single zombie might be small, but the volume of aggregatedtraffic arriving at the victim host is overwhelming. Second, zombies usually spoof their IP addresses under thecontrol of attacker, which makes it very difficult to trace the attack traffic back even to zombies. According tothe Internet architecture working group [7], the percentage of spoofed attacks is declining, but thesheer volume and distributed nature of DDoS attack traffic still the design of an effective defence. The zombie machinesunder control of masters/ handlers (running control mechanism) as shown in Figure 1 transmit attack packets,which converge at victim or its network to exhaust either its communication or computational resources.

The first known distributed denial of service attack occurred in 1996 when Panix, now one of the oldest internet service providers, was knocked offline for several days by a SYN flood, a technique that has become a classic DDoS attack. Over the next few years DDoS attacks became common and Cisco predicts that the total number of DDoS attacks will double from the 7.9 million seen in 2018 to something over 15 million by 2023[8].



Data: Cisco Annual Internet Report (2018–2023)

Fig.2Cisco's analysis of DDoS total attack history and predictions

Apart from detecting of DDoS attacks, there is an another kind of network traffic which is gaining popularityamong security researchers, and which causes a denial ofservice to legitimate users of a web service, is a FlashEvent (FE). As per [9], an FE is similar to high-rate DDoS(HR-DDoS) attack wherein thousands of legitimate userstry to access a particular computing resource such as awebsite simultaneously. This sudden surge in legitimatetraffic is mainly due to some breaking news happeningaround the world like the publishing of Olympic scheduleor new product launch by companies like Apple, Samsung,etc. It causes the untimely delivery of responses from webservice and thus, require immediate action. It can also occur in case of a natural disaster or a terrorist attack (example: 9/11 attack on America). Sometimes, a low efficiency server is linked to a very popular website like Slashdot or reddit, which may cause huge growth in traffic. Such a flash event is known as Slashdot effect [10]. As there areonly a few parametric differences between DDoS attacksand FE traffic, it is very challenging to discriminate thetwo [11].

In this paper, we have presentedthe recent flash events and recent DDoS attacks.

2. RECENT FLASH EVENTS

[12] Many FEs have occurred in recent times which have leadto the untimely responses to the legitimate users. Someof the famous examples of FEs are:

- In August 2016, millions of users simultaneously accessed the Australian census website to fill their personnel details. The lack of sufficient resources on theweb server causes the website to crash down [13].
- In February 2016, a new phone was launched with a
- lowest ever price of INR 251 named as freedom251. It attracted millions of people in a short span of timeand lead to the crash down of the web server in fewhours.
- In November 2014, the announcements of attractive schemes by leading online shopping vendors likeAmazon, Flipkart, Snapdeal, etc. resulted in theshutdown of their shopping website for about anhour.
- In June 2014, a unique breakdown occurred at Microsoft office, when their products like Exchange &Lync, MS Office 360 were not available online. Theleading traffic peaks overwhelmed the huge amountof network elements, which results in unavailabilityof the functionality of Lync for a longer time.

3. RECENT DDOS ATTACKS

Many DDoS attacks have been occurred in recent times which have disturbed to the legitimate users. Some of the famous DDoS attacks are:

Amazon Web Services (AWS) (February 2020)According to an article by ZDNet, in February of 2020, "Amazon said its AWS Shield service mitigated the largest DDoS attack ever recorded, stopping a 2.3 Tbps attack." Prior to this attack, the world record for largest recorded DDoS attack was 1.7 Tbps (Terabits per second), which itself supplanted the record set by the GitHub attack that will be mentioned below.

The ZDNet article doesn't name the AWS customer, but it did mention that "the attack was carried out using hijacked CLDAP web servers and caused three days of 'elevated threat' for [Amazon's] AWS Shield staff." CLDAP stands for Connection-less Lightweight Directory Access Protocol, which is a protocol for connecting, searching, and modifying shared directories on the internet.It is also, according to ZDNet, a protocol that "has been abused for DDoS attacks since late 2016" and that "CLDAP servers are known to amplify DDoS traffic by 56 to 70 times its initial size."

GitHub (February, 2018)

A popular online code management service used by millions of developers, GitHub is used to high traffic and usage. What it wasn't prepared for was the then record-breaking 1.3 Tbps of traffic that flooded its servers with 126.9 million packets of data each second. The attack was the biggest recorded DDoS attack at that time, but the onslaught only took GitHub's systems down for about 20 minutes. This was largely due to the fact that GitHub utilized a DDoS mitigation service that detected the attack and quickly took steps to minimize the impact.

Unlike many recent DDoS attacks, the GitHub attack didn’t involve botnets. Instead, the DDoS attackers used a strategy known as memcaching, in which a spoofed request is delivered to a vulnerable server that then floods a targeted victim with amplified traffic. Memcached databases are commonly used to help speed up websites and networks, but have recently been weaponized by DDoS attackers.

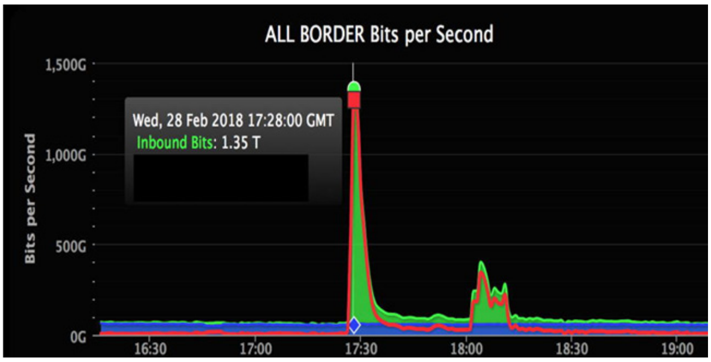


Fig.3 Chart of the February 2018 DDoS attack on GitHub.

Undisclosed NETSCOUT Client (March 2018)

Not long after the 1.3 Tbps DDoS attack against GitHub, NETSCOUT reported that one of their customers was targeted by a 1.7 Tbps DDoS attack. This particular attack was described by NETSCOUT as being “based on the same memcached reflection/amplification attack vector that mad up the Github attack.”

However, despite the massive size of the attack, “no outages were reported because of this,” according to NETSCOUT. This can serve as an example of how being prepared for a specific type of attack can make a major difference in the impact of that attack.

Dyn (October, 2016)

As a major DNS provider, Dyn was crucial to the network infrastructure of several major companies, including Netflix, PayPal, Visa, Amazon, and The New York Times. Using a malware called Mirai, unidentified hackers created a massive botnet incorporating internet of things (IoT) devices to launch what was at the time the largest recorded DDoS attack. The assault had massive trickle-down effects, as many of Dyn’s customers found their websites crippled by DNS errors when Dyn’s servers went down. Although the problems were sorted out and service restored by the end of the day, it was a frightening reminder of the fragility of network infrastructure.

BBC (December, 2015)

On the last day of 2015, a group called “New World Hacking” launched a 600 Gbps attack using its BangStresser application tool. The attack took the BBC’s sites, including its iPlayer on-demand service, down for about three hours. Aside from its sheer size, which was the biggest DDoS attack on record at that time, the most noteworthy aspect of the BBC attack was the fact that the tool used to launch it actually utilized cloud computing resources from two Amazon AWS servers. For IT security professionals who had long trusted Amazon’s reputation for security, the notion that DDoS attackers had found a way to leverage the bandwidth of a public cloud computing service to power their assault was particularly troubling.

Spamhaus (March, 2013)

In 2013, Spamhaus was an industry-leading spam filtering organization, removing as much as 80% of spam emails. This made them an attractive target for scammers, who ultimately hired a teenage hacker in Britain to launch a massive offensive to take down Spamhaus’s systems. Clocking in at 300 Gbps, this assault was the biggest DDoS attack recorded at that time. When Spamhaus responded to the threat by turning to a DDoS mitigation service, the attacker shifted focus to try to bring it down as well, which caused network disruptions throughout Britain as other companies were caught in the crossfire.

Bank of America/JP Morgan Chase/US Bancorp/Citigroup/PNC Bank (December, 2012)

In September and October of 2012, a group identifying itself as “Izz ad-Din al-Qassam Cyber Fighters” launched several DDoS attacks against US banks, allegedly in response to a controversial film trailer on YouTube. Later that year, the group promised to expand the scope of its attacks. In December, it followed through by hitting six prominent banks over the course of three days, disrupting services and causing severe slowdown. While the attack was larger than those from a few months prior, the earlier wave left cybersecurity experts better prepared to deal with the botnet tactics the group deployed. At its peak, the attacks reached 63.3 Gbps.

As recent DDoS attacks continue to evolve, cybersecurity experts are working hard to counter their effects and diminish their impact. While a DDoS attack is still something every company should be concerned about, there are many ways to safeguard operations against them, from DDoS mitigation services to data center options like blended ISP connectivity. These efforts may not be able to make DDoS attacks a thing of the past, but they're making them a less effective strategy for disrupting operations and services.

4. COMPARISON OF FLASH EVENTS AND DDOS ATTACKS

DDoS and Flash Event are voluminous, bursty and unstable. They both cause high rise in network traffic and lead to disruption of services to legitimate users. Studying the differences between the two, help develop effective prediction and defence mechanism.

According to [14], flash events and DDoS have following differences. During Flash events, clients can be effectively aggregated into clusters. In fact, many have been registered in logs. In case of DDoS, the distribution of DoS attackers is geographically distributed in form of Zombies. Very few previouslyseen clusters are involved.

There is a decline in per client request rate during flash event but in case of DDoS there is no change in per client request rate during the surge. In case of flash event, the volume of traffic generated fluctuates and forms random zigzag wave as there is dynamic changein users, whereas the volume of DDoS attack remainsstable throughout the attack[15].

Figure 4 and Figure 5 consist of model graphs of Flash Events and DDOS Attacks showing its various features. Difference in the traffic pattern in case flash event and DDoS attack is clearly visible in the figures, thus, helping to understand theircharacteristics.

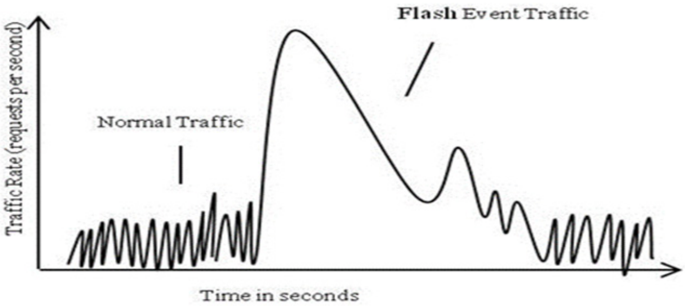


Fig.4 Model Graph for Flash Events

Figure 4 shows that flash events grow rapidly and die out gradually. This is because the Event like any breaking news gets the requests suddenly. As soon as the user realizes the slow response rate, it stops accessing theaffected server. After sometime, the Flash crowd declines. Also, after certain time, the news has been known and accessed by all interested users. So, the news no longer attracts users, thus, decreasing the traffic. Figure 5 shows the DDoS model graph depicting sudden rise and sudden fall of requests. It is so because DDoS attacks are conducted using botnets. In short, the Flash events occur when there is breaking news or a world-wide event. In such a case, large numbers of users throughout the world, send requests to the web server for information. The sudden demand of information leads to outage or crash in the system. DDoS attacks are, however, well planned andprogrammed using the compromised systems known as zombies/ slaves. Therefore, the starting time and ending time are already defined.

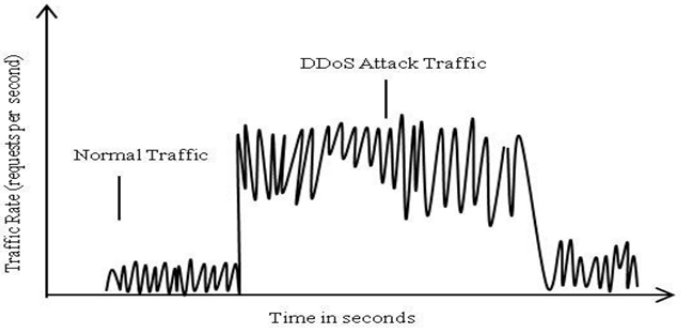


Fig.5Model Graph for DDoS Attacks

5. CONCLUSION

Studyingabout flash events helps us to know the features of flash events and helps us how FE differs from DDoS attacks. The discrimination of high-rate DDoS attacks from asimilar looking legitimate traffic called a flash event (FE)is a real challenging issue in the network security research.In this paper, we have comprehensive reviewed the recent flash events and DDoS attacks. We have alsoshown graphically the difference between both. As part of the future work, we shall work onframework which would discriminate the DDoS attacks from flash events.

REFERENCES

[1] Tipton, H. F. and Krause, M., "Information Security Management Handbook", CRC Press, 2004

[2] Criscuolo, P.J, "Distributed Denial of Service Trin00, Tribe Flood Network, Tribe Flood Network 2000, andStacheldraht CIAC-2319", Department of Energy computer Incident Advisory (CIAC), UCRL-ID-136939,Rev. 1, Lawrence Livermore National Laboratory, February 14, 2000. http://ftp.se.kde.org/pub/security/csir/ciac/ciacdocs/ciac2319.txt.

[3] Mirkovic, J., and Reiher, P., "A Taxonomy of

DDoS Attack and DDoS Defense Mechanisms," ACM-SIGCOMM Computer Communications Review, Volume 34, No. 2, pp. 39-53, April, 2004.

[4] Chen, R., Park, J., and Marchany, R., "A Divide-and-Conquer Strategy for Thwarting Distributed Denial-ofService Attacks," IEEE Transactions on Parallel and Distributed Systems, Vol. 18, No. 5, pp. 577-588, May2007.

[5] Douligeris, C. and Mitrokotsa, A., "DDoS attacks and defense mechanisms: classification and state-of-theart," Computer Networks, Vol. 44, No. 5, pp. 643–666, April 2004.

[6] Moore, D., Shannon, C., Brown, D. J. , Voelker, G., and Savage, S., "Inferring Internet Denial-of-ServiceActivity," ACM Transactions on Computer Systems, Vol. 24, No. 2, pp. 115–139, May 2006

[7] Handley, M., Internet Architecture WG: DoS-resistant Internet subgroup report, 2005.http://www.communications.net/object/download/1543/doc/mjhdos-summary.pdf.

[8] https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

[9] A. Bhandari, A. L. Sangal, and K. Kumar, "Characterizing flash events and distributed denial-of-serviceattacks: an empirical investigation," Security and Communication Networks, 2016.

[10] H.Izycka, "Flash Crowd prediction", Vrije Universiteit Amsterdam, Master's thesis, available at http:// www.globule.org/ publi/ FCP_master2006.pdf.

[11] S. Bhatia, G. Mohay, A. Tickle, and E. Ahmed,"Parametric differences between a real-world distributed denial-of-service attack and a flash event,"in Sixth IEEE International Conference on Availability, Reliability and Security (ARES'11), pp. 210–217,2011.

[12] S. Behal, K. Kumar, M. Sachdeva," Discriminating Flash Events from DDoS Attacks:A Comprehensive Review"International Journal of Network Security, Vol.19, No.5, PP.734-741, Sept. 2017 (DOI: 10.6633/ IJNS.201709.19(5).11)

[13] D. Braue, Attack on Australian Census SiteDidn't Register on Global DDoS Sensors, Aug. 11,2016. (http://www.cso.com.au/article/604910/ attack-australian-census-site)

[14] J. Jung, B. Krishnamurthy, M. Rabinovich, "Flash Crowds and Denial of Service attacks: characterization and implications for CDNs and web sites," available at http:// www2. research.att.com/ ~bala/ papers/www02-fc.html

[15] K.M. Prasad, A.R.M. reddy, K.V. Rao, "Discriminating DDoS attack traffic from Flash Crowds on internet threat monitors (ITM) using entropy variations", AJC & ICT, IEEE, vol.6 6 No.2, June 2013