Journal of ICT, Design, Engineering and Technological Science (JITDETS)
VOL. 3, NO. 2, pp. 35-38, 2019
DOI: https://doi.org/10.33150/JITDETS-3.2.3

ORIGINAL CONTRIBUTION

Exhausted Servers Deny Service - HTTP Get Attack

Alvin Prasad [*]

The University of Fiji, Lautoka, Fiji

Abstract— **Hyper Text Transfer Protocol (HTTP) Get attack is the most common type of Denial of Service attacks (DOS) found today. It is common because it is very easy to implement/set up. It disallows the services of an organization to be offered to users by flooding the server with a legitimate request, thus exhausting the server. This prevents the server from providing services to legitimate users, which leads to organizations and businesses losing millions of dollars. Several mitigation techniques are available, but these techniques are still insufficient to detect and combat malicious requests. The objective of this review paper is to provide the readers with information on DoS attacks and the attackers' intention behind these illegal activities. The critical analysis of the current literature provides insights on how to mitigate and prevent these types of attacks. This article suggests limiting the response time for each request from the server, and in dealing with the response, it can use the latest verification system. This research can help the organizations and the solution developers in mitigating and preventing the flooding attack thus, allowing organisations to flourish as information is readily available to the users.**

Index Terms— **DoS, Flooding, HTTP Get attack, No CAPTCHA reCAPTCHA**

Received: 13 September 2019; **Accepted:** 29 November 2019; **Published:** 28 December 2019

I. INTRODUCTION

Researchers continually analyse and develop new strategies to combat computer and network attacks [1]. Attackers on the other hand develop new attacks which bypass the defence systems. As the technological world grows with new and smart infrastructure, IT experts utilizing the new infrastructure created new architecture which leads to a smarter way to do business and share information. Information is a vital resource for everyone whether it's an individual or an organization. Information is used by the top level management to generate knowledge which helps them to make strategic and tactical decision. Individuals which can be specified as ordinary people or the civil society and students need to get information or service to complete day to day activities.

The different types of information which are desired are news, idea and opinions, research, theoretical analysis, telephone number, train or aeroplane timetable, legal information, financial information and many more [2, 3]. Nowadays, most of this information's are stored on networked computer systems; everybody's life now depends on network based computer systems like health sector, government, universities, financial, defence departments and many others. This makes life easy and allows easy and timely access to relevant information's from relevant organizations.

Besides its significant contribution to the organizations and the society as a whole it also has some limitations or threats. One of the major threats associated with information technology is security issues. The vital information's which are available can be stolen or the services can be denied to customers which lead to losses in millions of dollars. According to Neustar Annual DDos attack and impact report, companies loose more than $100,000 per hour during peak hours of business. Companies have reported that the attacks sometime last for a day or so [4]. Just imagine an attack for half an hour with the cost of $500,000!

Attackers target large, middle and small sized organizations, government websites, game sites and public events. According to Cloudflare [5] the biggest DDos attack was suffered by GitHub in February 2018 where the incoming traffic was 1.3 terabytes per second and lasted about 20 minutes. In one of the other major attacks reported on a high profile company was when the attackers took its toll on yahoo in year 2000 [6] where huge amount of traffic was noted on the web server. Recently other major attacks were reported where in 2012, major banks websites in the United States suffered slowdowns and customers were unable to get the service provided by these banks [7]. According to the report these attacks were the largest ever recorded. In one of the other massive attack in March 2015, GitHub, the largest public code repository organization was attacked [8]. Where the service provided by the organisation was shut down for five days. Coingeek in an article [9] also reports latest frequent attacks on their services recently. In 2018 according to the Netscout intelligence report the average attack size has gone up [10], which warns the society to be more vigilant.

The attack scenarios mentioned above are the DoS attack and Distributed Denial of Service attack (DDoS) which are very popular and easy to setup. In DoS one computer is used to conduct the attack whereas in DDoS multiple devices are used. In this article we have discussed about DoS attacks and DDoS attack, the attackers and the intention behind the attack lastly, provided suggestion to mitigate these types of attacks.

[*] Corresponding author: Alvin Prasad

[†] Email: aly157@gmail.com

II. DOS ATTACK

DOS attacks are attacks where the users are unable to receive the service or use the resources which they were using from any information technology architecture on a day to day basis for a period of time. The main intention behind this type of attack is to prevent the legitimate user from using a particular service as well as prevent the service provider from providing service. DOS attacks are very powerful and harmful. This type of attack mostly consumes the server resources which lead to the server unable to provide its services. The server resource can be CPU, sockets, disk bandwidth, database bandwidth, input/output bandwidth, memory, etc.

III. DDOS ATTACK

DDOS is another type of DOS attack which is mostly preferred by attackers. This type of attack occurs when more than one system located at different time zone flood the resources of a targeted system. This is because DDOS attack source is very difficult to identify.

There are several stages that attackers carry out to accomplish this type of attack. The attacker first searches the networked systems for security gap. This process takes some time to complete. After multiple systems are found the attackers penetrates into these systems and plants malicious code or bad bots into the systems which allows the attacker to take control of the infected system remotely, once they are infected they are also known as zombie. Bot, which is the short form of robot, is a computer program that does any task on command. These collections of infected computers when connected are known as Zombie army or Botnet. The victims are unaware of these intrusions into their system. The attacker conducts this activity through many techniques example taking advantage to vulnerability, user opening infected documents or emails, user visiting malicious websites, etc.

Once the Botnet is formed and the attackers are happy with the number in the group, they use the power of all to perform the Distributed attack. They send multiple numbers of requests to the target machine at once which leads to the system to respond very slowly which is unusable or it crashes and do not respond at all.

IV. ATTACKERS AND INTENTIONS

The DOS attack into the system and the network can be from a competitor, professional groups (hackers), enemy, terrorist or bragger. According to (Zadelhoff, 2016) the major threat to company information is from an insider. A competitor tries to deny the service which other organizations are providing so that users tend to choose their companies for service. This way the victim looses customers and reputations as they are unable to satisfy or provide service to the customer.

Professional groups or hackers do this to directly earn money after attacking a particular service and demanding money to avoid the attack. Enemy will try to take revenge and cause damage to the business or to obliterate the brand name. Moreover, other type of attacks is targeted to the government or political parties. This attack initiates with a disagreement between political parties. Here the political parties or individuals want to protest or show criticism against government or other parties. Sometimes the organizations and the government fall victim accidently. This happens when there is cyber warfare between two groups and the organizations are caught in the crossfire.

Furthermore, some attacks are initiated by individual who try to test their knowledge and boast that they are elegant. Some attacks are done in a fun context and are not aware of the damage it causes. Attacks from inside the business is very catastrophic can cause a lot of damage, as these attackers are holding or have held top most positions in the company and have access to all the important resources saved on the computer or network systems. Again this is done for personal gain, or is done to earn money by selling information to other businesses. This insider can be an employee of the organization or a former worker.

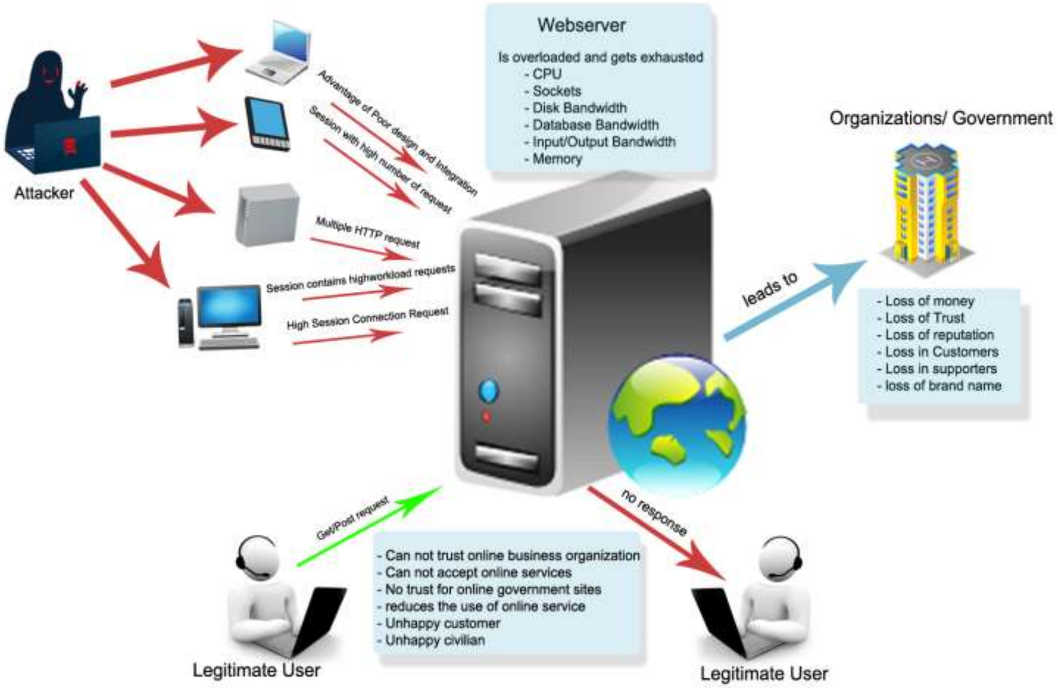
Webserver
Is overloaded and gets exhausted
- CPU
- Sockets
- Disk Bandwidth
- Database Bandwidth
- Input/Output Bandwidth
- Memory
Attacker
Advantage of Poor design and Integration
Session with high number of request
Multiple HTTP request
Session contains highworkload requests
High Session Connection Request
Organizations/ Government
leads to
- Loss of money
- Loss of Trust
- Loss of reputation
- Loss in Customers
- Loss in supporters
- loss of brand name
Get/Post request
no response
- Can not trust online business organization
- Can not accept online services
- No trust for online government sites
- reduces the use of online service
- Unhappy customer
- Unhappy civilian
Legitimate User
Legitimate User

Fig. 1. HTTP DOS attack

IV. HTTP DDOS ATTACK

HTTP is the application layer protocol used by the World Wide Web to help in managing the web requests. HTTP is responsible for controlling, arranging and directing messages from a web browser (user) to the web server and then back to the user. HTTP acts as a medium to transfer or transport hypertext documents. Hypertext documents are documents which contains text, images, video, audio, animation and hyperlinks. IT is based on a number of request methods including POST, GET, PUT, DELETE and more but web browsers normally use GET and POST.

HTTP is defined as a connectionless and stateless protocol, this means that the browser sends a request to the server and disconnects and waits for a response meanwhile the server processes the request and reconnects with the client and sends the response. Hence, it is also called a stateless protocol where the server does not require storing any session information for any of the request. It treats every request as independent.

HTTP DOS (HDOS) attack is an attack designed against websites where attackers attempt to make the web server's services unavailable to the legitimate users. These attacks are used against large organization sites, government sites, activist sites, competitor sites and other small, medium and large business sites.

These attacks can easily be conducted where the attacker can overload the web server with multiple web service requests which leads the web server unable to respond on time. The requests are generally valid or legitimate requests. As the server is responsible to provide service to all legitimate requests, it tries to process multiple request but gets exhausted and finds it difficult to provide the service to other new legitimate requests. One advantage of HTTP DOS attack from the attackers point of view is that it is very easy to setup.

HDOS attack can be categorized into different types depending on the method used to generate the attack on the web server. These attacks can be conducted using one computer device, as well as multiple devices controlled by one person.

V. HTTP GET

HTTP GET attack is a very effective layer 7 attack type where individual machine or a zombie (many machines) send a legitimate request to the web server requesting services from the server (Imperva Incapsula, 2017). In simple terms a user using the web browser sends a request to get any content like image, definition, services from the web server where the server fulfils the request. The request can be multiple per second which leads the responding server to get exhausted while responding and apparently stop working.

In an article Pauli [11] reported an attack where the organization received 4.5 billion requests in a day from 650,000 IP addresses which is 275,000 requests per second. This creates a lot of havoc to the victim environment as they are unable to provide the necessary services to its clients. Moreover detecting these types of attacks is difficult as the request is very difficult to separate from the legitimate request. Analysing and comparing the transactions for a service is not the way to detect the attacks now, as the characteristics of requests whether normal or malicious are the same.

Different solutions have been suggested from different authors. Chwalinski et al. [12] suggest to use clustering and information theoretical metrics to detect http get attack. In this study, a new algorithm is used which examines the interest of different users and differentiates between legitimate and malicious requests. Another research by Lim [13] proposes the idea of using a Software Defined Network (SDN) based system which blocks the unwanted traffic and redirects it to another additional domain which prevents the attack. Analysing the parameters of the incoming transactions and categorizing them into normal and attack transactions using the Naïve Bayes classifier algorithm is another solution provided in a research [14].

The literature provides information and suggestion which are effective in some cases and do not work in others. As this type of attack is easy to setup, attackers design new ways to attack a new organization. We would also like to suggest some points which can be incorporated by solution designers who develop methods to mitigate or prevent the attack.

VI. DISCUSSION

"Completely Automated Public Turing test to tell Computers and Humans Apart" which is well known as CAPTCHA is a verification technique that allows the machine to differentiate between another machine and human [15]. This technique of verification was very popular till AI took its toll where algorithms were designed which can solve the simple text based captcha.

Our suggestion in regards to the HTTP-GET attack is to limit the response time for each request from the server and when dealing with response use a "No CAPTCHA reCAPTCHA" verification system.

If we put this in a scenario it means, first the server should take maybe a second to respond to only a certain number of requests say x. As soon as the server receives more than x number of requests, a cluster can be formed with the current number of request and the new request can stack in another cluster. As the server responds to the current cluster, the other request can go to another cluster which will also has a limit of about x number of requests. As the requests from the first cluster are fulfilled the request from the second cluster can flow in to the first one giving in space for the new request in the second cluster.

Concurrently, while the server is responding to the requests for the first cluster it should first check the IP address of the first cluster. If more than 1 request is coming from 1 IP within a second, send a reply to the same address using a "No CAPTCHA reCAPTCHA" verification system with a response time limit.

Which will allow administrators and the machine to determine if the requester is a malicious code or a human. At the same time the server should do the same if the packet size for each of the request coming in sequence is of the same size as mostly it will be same. Those suspicious requests can be diverted to another server or group which can deal with those requests and this will not affect the normal flow of the day to day activities.

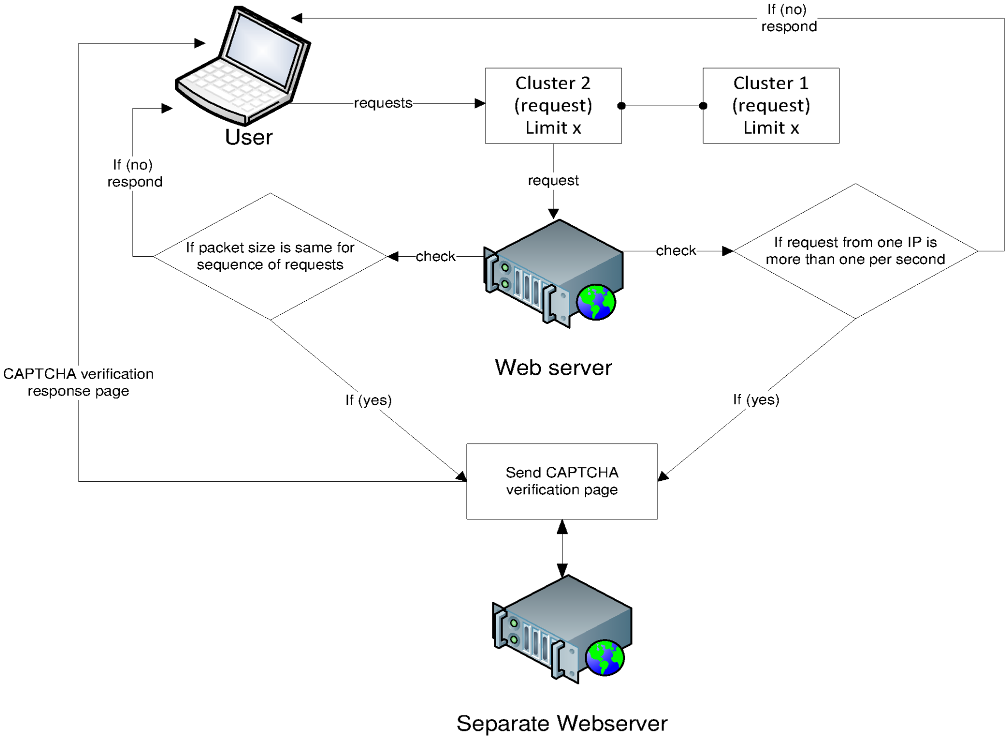

Fig. 2. Suggestion flowchart

VII. CONCLUSION

As the setup for a DDoS and DOS does not require much, it is growing and becoming very common in the current stint. Hence, this easy to setup attack brings large organizations to its knees for hours or even weeks. This leads to a significant loss of money, reputation, trust, supporters, customers, brand name and many more. Keeping these in mind this paper suggest some important points which can be incorporated by solution developers and policy makers.

Declaration of Competing Interest

The authors declare that they have no conflict of interest.

References

[1] E. Uma and A. Kannan, ``Self-aware message validating algorithm for preventing XML-based injection attacks,'' *International Journal of Technology and Engineering Studies*, vol. 2, no. 3, pp. 60-69, 2016. doi: https://doi.org/10.20469/ijtes.2.40001-3

[2] The Open University. (2017) Understanding information. [Online]. Available: https://bit.ly/2UUaDaL

[3] N. Ugtakhbayar, B. Usukhbayar, S. H. Sodbileg, and J. Nyamjav, ``Detecting TCP based attacks using data mining algorithms,'' *International Journal of Technology and Engineering Studies*, vol. 2, no. 1, pp. 1-4, 2016. doi: https://doi.org/10.20469/ijtes.2.40001-1

[4] Neustar. (2017) Neustar DDoS and cybersecurity report. [Online]. Available: https://bit.ly/3d9GYAJ

[5] Cloudflare. (2019) Famous DDoS attacks. the largest DDoS attacks of all time. [Online]. Available: https://bit.ly/2CcBOHp

[6] A. Hermida. (2000) Yahoo attack exposes web weakness. [Online]. Available: https://bbc.in/2NdOP5G

[7] D. Goldman. (2012) Major banks hit with biggest cyberattacks in history. [Online]. Available: https://cnn.it/2YcgRF1

[8] S. Anthony. (2015) Github battles "largest DDoS" in site's history, targeted at anti-censorship tools. [Online]. Available: https://bit.ly/2UZE5fP

[9] B. Beatty. (2018) More ddos attacks on bitcoin (bch-sv) friendly websites. [Online]. Available: https://bit.ly/2ARIOt5

[10] H. Modi. (2018) Netscout threat intelligence report. [Online]. Available: https://bit.ly/2UX73gq

[11] D. Pauli. (2015) Mobile advertising DDoS javascript drip serves site with 4.5bn hits. [Online]. Available: https://bit.ly/2YezhFb

[12] P. Chwalinski, R. Belavkin, and X. Cheng, ``Detection of HTTP-GET attack with clustering and information theoretic measurements,'' in *Foundations and Practice of Security*. Berlin, Germany: Springer, 2013, pp. 45-61.

[13] S. Lim, J. Ha, H. Kim, Y. Kim, and S. Yang, ``A SDN-oriented DDoS blocking scheme for botnet-based attacks,'' in *6th International Conference on Ubiquitous and Future Networks (ICUFN)*, Shanghai, China, 2014.

[14] N. A. Singh, K. J. Singh, and T. De, ``Distributed denial of service attack detection using naive bayes classifier through info gain feature selection,'' in *Proceedings of the International Conference on Informatics and Analytics - ICIA-16*, Pondicherry, India, 2016.

[15] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, ``CAPTCHA: Using hard AI problems for security,'' in *Lecture Notes in Computer Science*. Heidelberg, Germany: Springer, 2003, pp. 294-311.