Scrutinize of distributed denial-of-service and Alleviation

#1Amira Abdullah Al-Jaafariya, #2Sumaiyh Bani Oraba, #3Malak Saleh Al-Hizami, #4Dr.Ramesh Palanisamy
Department of Information Technology,
University of Technology and Applied Sciences-IBRA,
Sultanate of Oman.
[1]36S1565@ict.edu.om, [2]36S1568@ict.edu.om, [3]36S1547@ict.edu.om, [4]palanisamy@gmail.com.

***Abstract*-Cybercrimes are becoming one of the most crucial threats of the new millennium, Distributed Denial of Services is one type of such cyber attacks that affects the use of the internet by users, hence, this paper will discuss the definition of Distributed Denial of Services, how it works, its types, goals and measurements. The analytical methodology will be applied to meet the objectives of this paper.**

Keywords:Cybercrimes,DDoS,Crypto.

1. INTRODUCTION

DDoS is the shortcut of Distributed Denial of Services that is considered a type of cyber attacks that aiming at the destruction of network resource or host's services that is connected to the internet. This type of attack takes the advantage of a special power limits that apply to any network resources, such as the infrastructure that enables a corporate website. Moreover, DDoS attacks can send multiple requests to the attacked web resource, with the goal of bypassing the website's ability to handle multiple requests and consequently preventing it from functioning properly. In addition, it is a type of malicious attack carried out by the attacker or a group of attackers with the aim of taking the computer or the resources of the targeted networks out of service for a limited period or permanently. In this type of attacks, attackers usually flood target devices with requests more quickly than these devices can respond, or by sending requests specifically designed to consume the target devices' resources such that these devices are no longer able to respond to benign requests.

However if, for example, a malicious group targeted a web page of politicians with this attack, none of

The blog users will be able to preview the content during the attack, and maybe even after it.

As the machine behind the blog will be overloaded with requests (visit requests, for example) that come from the malicious party and will not be Able to respond to either these malicious requests or benign requests, and this could result in the computer being out of operation.

2. LITERATURE SURVEY

A number of studies have discussed the topic of DDoS attacks and cyber attacks in general, for example Argyro P. Karanasiou, 2013 in his article entitled " The Changing Face of Protests in the Digital Age: On Occupying Cyberspace and Distributed-Denial-of-Services (DDoS) Attacks" has stated that the real protests that the world has been suffering from are now also available online, thanks to the " unprecedented phenomenon of global protesting activity" that was created by the internet and its online platforms, in this regard, DDoS is playing the role of " online civil-disobedience."[1] Similarly, Slocombe Geoff in the Asia-Pacific Defense Reporter, wrote an article entitled "World’s Largest Publicly Revealed Distributed Denial of Service Attack " 2018, the author has assumed that the Distributed Denial of Services Attacks are one of the "published cyber operations categories under state-sponsor" consequently he assumed that more DDoS attacks are expected in the coming years. Hence, he suggested that more critical infrastructures with full protection are needed.[2]

1. CYBER CRIME

Cybercrime is defined as " a criminal activity that either targets or uses a computer, a computer network or a networked device." [3] It has different types that are related to email, personal identity, financial cards, Cyber extortion, Crypto jacking and Cyber extortion. Hence, it considers a serious threat that both governments and individuals are suffering from as it is able to stop users use the system or a network with a number of attacks such as Malware attacks, Phishing and Distributed DoS attacks which is discussed in this paper.[4]

2. THE GOALS OF THE DDOS ATTACK

It is not easy to predict or understand the motivations or goals behind DDoS attacks. However, normally the DDoS attacks have some targets such as Government websites, competing companies, online shopping sites, online casinos and any kind of companies or organizations that rely on providing online services over the Internet. [5] In addition, there are number of theories that explain the main reasons and goals behind the occurrence of the DDoS attacks.

3. HOW DOES A DDOS ATTACK WORK?

Network resources, such as web servers, are subject to certain limits in terms of the number of requests that can be serviced simultaneously. In addition to server capacity limits, the channel connecting the server to the internet will also have a limited bandwidth or power. Whenever the number of requests exceeds the capacity limits of any infrastructure component, the level of service is likely to decline either by response to requests will be much slower than usual, or some, or all, of user requests will be completely ignored.[6]

However, usually the ultimate goal of an intruder is to completely prevent the normal **functioning of the web resource, that is, to "block service" altogether. The intruder may also request money to stop the attack. In some cases, a DDoS attack may be an attempt to discredit or harm a competitor's business.**[7]

“Empirical Evaluation of the Ensemble Framework for Feature Selection in DDoS Attack.” *2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)*

[6] Hussain, B., Q. Du, B. Sun, and Z. Han. 2021. “Deep Learning-Based DDoS-Attack Detection for Cyber-Physical System Over 5G Network.” *IEEE Transactions on Industrial Informatics, Industrial Informatics, IEEE Transactions n, IEEE Trans. Ind. Inf* 17 (2): 860-70.

[7] Bhattacharyya, Dhruba Kumar, and Jugal Kumar Kalita. 2016. *DDoS Attacks : Evolution, Detection, Prevention, Reaction, and Tolerance*. CRC Press.

4. MEASURE THE SEVERITY OF A DENIAL-OF-SERVICE ATTACK

The severity of a denial-of-service attack is measured by the volume of data that reaches the target of the attack per second, while the volume of data is measured in the bit. In addition to that, the units of measurement derived from bps, such as Kbps (kilo bits per second), as well as Mbps and Gbps, and Tbps (short for Megabits per secon), Giga bits per second, and Tera bits per second. Usually the maximum value reached by the intensity of an attack of this type is used during a given event or attack.

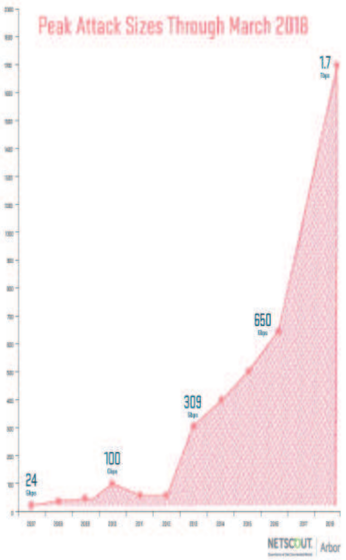

Figure (1) the greatest value reached by the largest denial of service organization

distributed between January 2007 and March 2018

Types of DDos Attacks : There are different types of the DDos attacks such as: Application Layer Attacks, Protocol Based Attacks, Volumetric Attacks, Low and Slow Attacks, Flood Attacks and Reflection-based Attacks.

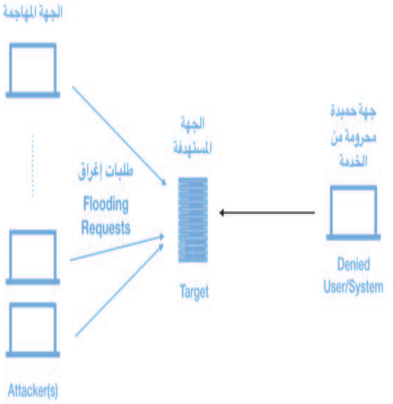

Figure (2) Low and Slow Attacks

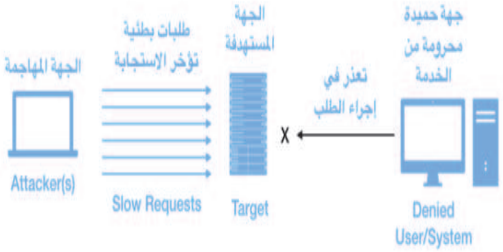

Figure (3) Flood Attacks

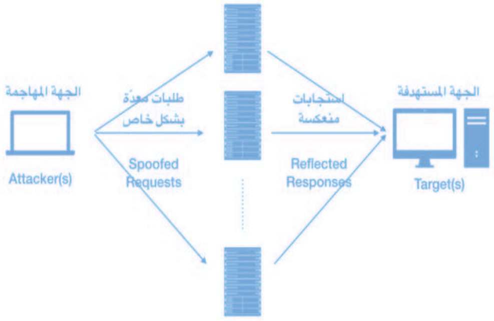

Figure (4) Reflection-based Attacks

1. CONCLUSION

To conclude, the paper has discussed the issue of DDos Attacks by representing its definitions and how it causes a heavy traffic flow to a specific website, and relation to the cyber crimes, and then the types of DDos Attacks were represented with supported graphs. Furthermore, the way it works was explained briefly, in addition to its goals and measurements. However, it is possible to say that it is one of the most important issues that must be handled in order to protect the users and to prevent all its disadvantages. Also, users should be aware of how they can protect themselves from such attacks by for example updating the operating system, using anti-virus software; putting strong passwords and avoiding open attachments in the spam.

REFERENCES

1) *Bhattacharyya, Dhruba Kumar, and Jugal Kumar Kalita. 2016. DDoS Attacks : Evolution, Detection, Prevention, Reaction, and Tolerance. CRC Press. http://search.ebscohost.com/login.aspx?direct=true&db=cat05400a&AN=crc.CAH0KE32827PDF&site=eds-live&scope=site.*
2) *http://search.ebscohost.com/login.aspx?direct=true&db=edsgao&AN=edsgcl.633375503&site=eds-live&scope=site*
3) *Das, Saikat, Deepak Venugopal, Sajjan Shiva, and Frederick T. Sheldon. 2020. "Empirical Evaluation of the Ensemble Framework for Feature Selection in DDoS Attack." 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable*
4) *Cloud (EdgeCom), 2020 7th IEEE International Conference On, August, 56–61. doi:10.1109/CSCloud-EdgeCom49738.2020.00019.*
5) *Hussain, B., Q. Du, B. Sun, and Z. Han. 2021. "Deep Learning-Based DDoS-Attack Detection for Cyber–Physical System Over 5G Network." IEEE Transactions on Industrial Informatics, Industrial Informatics, IEEE Transactions on, IEEE Trans. Ind. Inf 17 (2): 860–70. doi:10.1109/TII.2020.2974520.*
6) *Jia, Y., F. Zhong, A. Alrawais, B. Gong, and X. Cheng. 2020. "FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks." IEEE Internet of Things Journal, Internet of Things Journal, IEEE, IEEE Internet Things J 7 (10): 9552–62. doi:10.1109/JIOT.2020.2993782.*
7) *Karanasiou, Argyro P. 2014. "The Changing Face of Protests in the Digital Age: On Occupying Cyberspace and Distributed-Denial-of-Services (DDoS) Attacks." International Review of Law, Computers & Technology 28 (1): 98–114.*
   Slocombe, Geoff. 2018. "World's Largest Publicly
   Revealed Distributed Denial of Service Attack." Asia-
   Pacific Defence Reporter (2002) 44 (3): 30–31.