International Journal of Engineering &Technology, 7 (1.7) (2018) 194-196

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An effective solution for DDOS attack

Rusheel Raj Panakadan[1], Chitluri Dhanush[2], Dr. Carmel Mary Belinda[3*]

[1,2]Student,[3] Associate professor Department of Computer Science and Engineering,,Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,Avadi, Chennai-62, TamilNadu, India*
[*]Corresponding authors E-mail: carmelbelinda@gmail.com

Abstract

Distributed Denial of Service (DDoS) attacks constitute one of the major threats and among the hardest security problems in today's internet. Defense against these attacks is complicated by spoofed source IP addresses, which gives us a tough task to find out the packets origin. So this paper represents a solution for a DDoS attack. We'll be using wireshark tool to analyze the network traffic of any interface and find malicious activity by hackers. An algorithm is written at the server side so that if any malicious user sends asynchronous requests at a rate of (>=30 requests per second) then a Visual Basic script is sent to the malicious user. The Visual basic script consists of code encapsulated, allowing system administrators to generate and manage computers with error handling, sub routines etc. This .vbs scripts are made to auto run on the computer, thus making a particular service unavailable to the malicious user. Hereby, stopping the server from partial shutdown or preventing it from DDoS attack.

Keywords: *DDoS, Wireshark, Visual Basic scripts, Server, Zombies.*

1. Introduction

The major attacks internet services facing today come from DDoS attack. In computing, denial of services is a cyber attack where the attacker's (hacker) main aim is to make a computer or network resources like servers or printers in the network unavailable to its intended users by temporarily disrupting the services of host connected to the Internet. It's generally accomplished by flooding the targeted machine with enormous request in an attempt to over load system & thereby referring the resources like memory in the targeted machine thus making it unavailable[1].This can be solved by increasing the bandwidth, having protected firewall or by calling the ISP provider. But time taken to stop this DDoS attack is more. So this is not much efficient. DDOS reduces the network resources and bandwidth. The only aim of DDOS is to prevent users from accessing. Sometimes there is a difficulty to differentiate flash crowd and DDOS traffic control [7].This is how a basic DDoS attack work (in diagrammatic way).

Nowadays, every organizations are connected to the internet through broadband. Thereby, using the resources through network has become easy. But traditionally the network principles haven't changed, as they were built by using routers and switches configured by the operators. So, risks such as excessive traffic flow, vulnerabilities arises due to old versioned patches in network devices. Few vulnerabilities in the servers can also be found thus making it hack able.

Security is always a challenging issue and a concern to internet. DDOS is one of them, whereas other common attacks are SQL injections, Execution of malicious software, access control attack and phishing. DDOS is a fast spreading problem for those who are using old technique in configuring the network[8].

Basically, it is classified into two types. One is direct attack whereas other one is reflector attack. In direct attack, the user sends continuous requests to the victim. The packets may be in form of Transport Layer Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol(ICMP) ,whereas in reflector attack the requests are sent from the routers to the server thus making it unavailable. It is known as Distributed Reflection Denial of Service attacks.[9]

Rest of the papers consists of following sections. Section II represents the related work, Section III presents a proposed approach, Section IV represents conclusion.

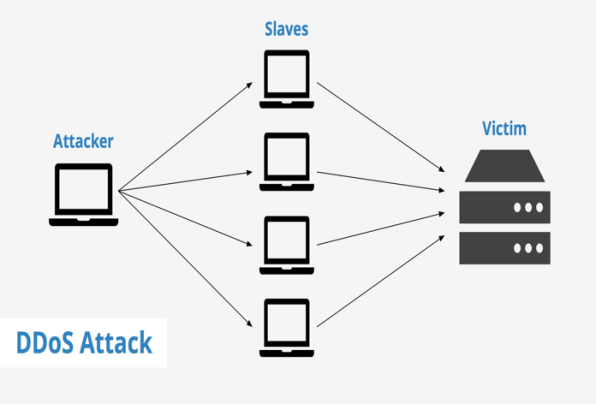


Figure 1: Working of DDOS attack

2. Related Work

Problem faced by DDoS attacks:-

Nowadays, internet plays a vital role in for the socio-economic growth of the society internet has the emergence and attainment for services like banking, education, hospitals, transportation etc. The vulnerabilities of the Internet architecture provides a great chance of attacks thus making internet unavailable. DDoS attack is being a threat to many business & organizations putting them at risk.

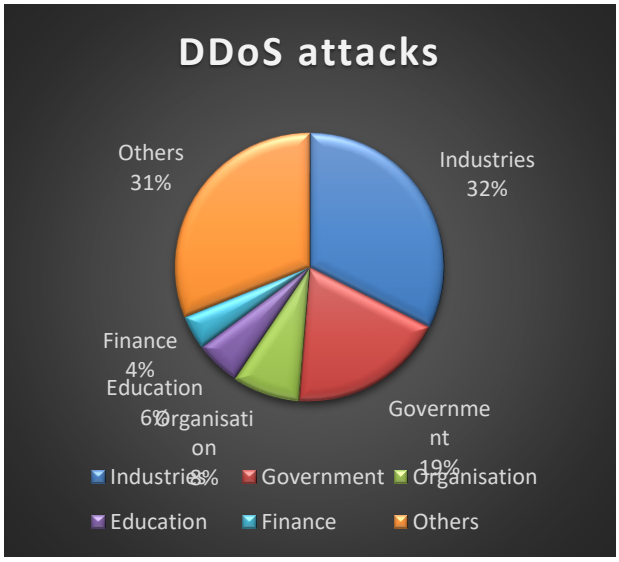


Fig-2: (Pie chart on DDoS attacks as per the survey)

Hospitals are always a main target for the DDoS attacks, as they disrupt internet services for the people in emergency. In organizations & banking sectors, DDoS attacks cause a great loss.[1]

Existing Methodology:

1.IP address filtering
2.Advance protected firewall
3.HoneyMesh concept can prevent happening of DDOS attack, but it causes memory overhead due to large scale of honeypots reduction in speed due to its additional layer and collection of information.[2]
4.Using a network based Intrusion Detection System (IDS) and using port scanning mechanism to find open port on any machine.[4]

3.Proposed Approach

Our proposed solution for DDOS attack:

We continuously analyze the network traffic of an interface(it may be LAN or WIFI) by using wireshark tool, as the malicious user may send asynchronous requests to the server through botnets(compromised computers) also called as "Zombies"[1]. These Zombies are present in large numbers and attack the server thus reducing its bandwidth and consumes its resources.

If it sends asynchronous requests at the rate of > 30 requests per second. For each entry of an attack, we must attain the IP addresses information or all the compromised systems in that DDOS attack at that period of time.
All the zombies IP address information can be obtained, Later organize the bots as per the country code, each entry in the dataset can be denoted by

$vec_j = hcc^j_1 : n^j_1, cc^j_2 : n^j_2, \ldots, cc^j_m : n^j_m i$, (1) where each cc^j_i, i 2 [1 . . . m] which substitutes the country code where the bots are located at time j.

Basically if more requests are received, then it may lead to the blocking of internet pipe from saturation with UDP ,ICMP ,IPV6 ,TCP-SYN packets.

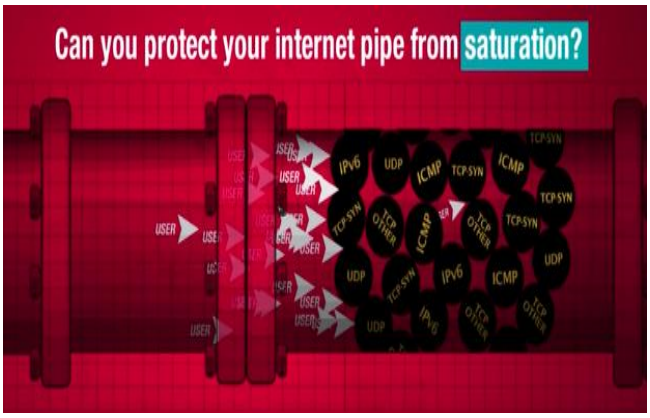
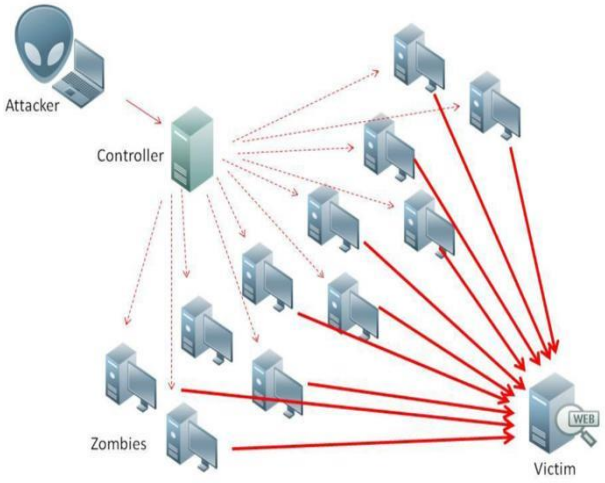


Figure-3: (This is how the packets are flooded)

Sending these huge packets means that the botnets are trying to do or make a conversation with the server, but the server refuses.[4]



The zombies IP addresses are to be found at the server and then the server sends a programmed Vbs scripts(visual basic scripts) to those IP addresses. As the zombies or botnets receives it, the scripts runs automatically in botnets physical machine thus shutting his computer or by killing the internet service .So that requests sent by the malicious user can be stopped or interrupted.

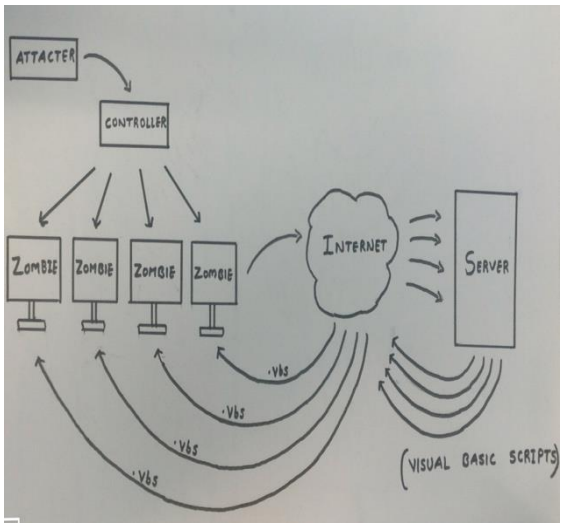


Figure 5

(A diagrammatic representation on how to send scripts to the Zombies or botnets is drawn below):
These can be a case where attackers can use spoofed IP addresses(by hiding their real IP). If this is used then Visual Basic scripts is sent to the spoofed IP addresses and they don't receive it.
In fact, most successful intrusions have a non spoofed components. So attackers use (compromised attacks) i.e. relay hosts to try to make them harder to track down, Therefore spoofing of IP address is hard for TCP connections.

Algorithm:

1.Check the traffic level of the interface.
2.If it is less than L_t (level of the traffic) then increase the bandwidth of the router else go to step 3.
3.Check if any malicious user is sending requests (req> 30).
4.If Yes, then send a control message to the router thereby limiting the rate.
5.Prepare a function at the server, such that a VB Script (Visual Basic Script) is sent at that particular IP address.
6.As soon as it is received at the zombie side (Compromised computers or Controlled Computers), the file is made to run automatically in that physical machine.
7.Thus, disabling the network process or shutting down the machine for a amount of time (as per the time mentioned in the VB Script).

4.Conclusion

The solution for DDoS can be useful for social economic growth of the society, as Internet has the emergence and attainment for services like Banking, Education, Hospitals, Transportation etc., This can solve a serious problem for healthcare providers who need access to the network to provide proper patient care or need access to the Internet to send and receive emails, prescriptions, records, and information. Reputed organizations& Banking sectors can use this solution as this can help them from financial loss that may result to $1 MILLION DOLLARS.

References

[1] Vishal V.Mahale, Nikita P. Pareek, Vrushali U. Uttarwar-2017,Alleviation of DDoS Attack Using Advance Technique.
[2] Alisha Gupta and B.B.Gupta-2017, Honeynettrap:Framework to detect and mitigate ddos attacks using Heterogenous Honeypot
[3] An Lei and Zhu Youchan-2010,The solution of DDOS attack based on Multi-agent
[4] Ved Prakash Mishra, Balvinder Shukla-2017,Development of Simulator for Intrusion Detection System to detect and alarm the DDOS attack
[5] An Wang, Student Member, IEEE, Wentao Chang, Student Member, IEEE, Songqing Chen, Senior Member, IEEE Aziz Mohaisen, Senior Member, IEEE, -2017 A Data-Driven Study of DDoS Attacks and TheirDynamics
[6] PriyankaKamboj, Munesh Chandra Trivedi, Virendra Kumar Yadav, Dr. Vikash Kumar Singh 2017-Detection Techniques of DDoSAttacks:A Survey
[7] Rahul Paul, Anuja Kumar Acharya, Virendra Kumar Yadav, SaumyaBatham-Hiding Large Amount of Data using a New Approach of Video Steganography- In Proc. Fourth International conference Confluence 2013: The Next Generation Information Technology Summit, Sept 27-28, Page(s): 337 – 343 (available at IET and IEEE xplorer).
[8] Shivani, Virendra Kumar Yadav, SaumyaBatham-A Novel Approach of Bulk Data Hiding using Text Steganography- Published in Third International Conference on Recent Trends in Computing (ICRTC 2015) will be held in SRM University, NCR Campus, Modinagar, Ghaziabad, India during March 12th – 13th, 2015. Publisher: Elsevier Procedia Computer Science Journal.
[9] KrishanKumar,A.LSangal,Abhinav Bhandari," Traceback Techniques against DDOS Attacks: A Comprehensive Review",International Conference on Technology(ICCCT),2011. Computer and Communication.