International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

Volumetric, Protocol and Application Layer Ddos Attack Types on Web Servers

[1]Amadi E.C., [2]Ezeji A.E., [3]Okorie D. C., [4]Nnannandu I. J.

[1-4]Department of Information Management Technology, Federal university of Technology, Owerri, Imo State, Nigeria

ec.amadi@gmail.com

ABSTRACT

Distributed Denial of Service (DDoS) flooding attacks are one of the biggest concerns for security professionals. DDoS flooding attacks are typically explicit attempts to disrupt legitimate users' access to services. Developing a comprehensive defense mechanism against identified and anticipated DDoS flooding attacks is a desired goal of the intrusion detection and prevention research community. However, the development of such a mechanism requires a comprehensive understanding of the problem and the techniques that have been used thus far in preventing, detecting, and responding to various DDoS flooding attacks. This paper presents different types of DDOS attack at the volumetric, protocol and applications layer and their possible resolutions available in the internet world.

Keywords: DDoS, Application layer, Volumetric Attack, Protocol, Flooding attack.

1.0 INTRODUCTION

A DDoS attack is a malicious attempt to bring down networks, Web-based applications, and services by overwhelming these resources with too much data or impairing them in some other way. Unlike a denial-of-service (DoS) attack where the source is just a singular computer and connection, a DDoS attack is from multiple sources, and is capable of causing great consequences to a company's brand, reputation and bottom line.

Distributed Denial of Service (DDoS) attacks are a popular way to impact people, organizations, and even nations in malicious ways. DDoS is a non-kinetic weapon that is capable of having an effect that is as devastating, if not more devastating, than a well-placed missile. DDoS attacks have been used as a form of retribution, as a means for activists to further their causes, and even as a strategy for a military to create an advantage during warfare. DDoS attacks are defined and described as "many machines" performing a "coordinated" attack where "access to a computer or network resource is intentionally blocked or degraded."(Harris et al. 2013)

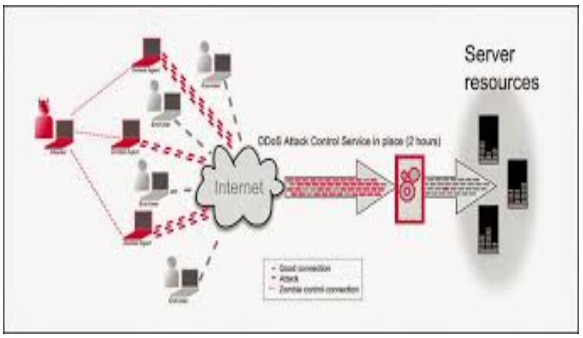

Fig. 1.1 Distributed denial of service attack

DDoS attacks are designed to target any aspect of a business and its resources, and can easily:

- Disable a specific computer, service or an entire network
- Target alarms, printers, phones or laptops
- Hit system resources like bandwidth, disk space, processor time or routing information
- Execute malware that affects processors and triggers errors in computer microcodes
- Exploit operating system vulnerabilities to drain system resources
- Crash the operating system

But DDoS attacks are not all the same.

1.1 Key Concepts and Context

Distributed Denial of Service attacks come in many shapes and sizes. Typically they are classified according to what they do. Whether it is a volume-based attack that saturates the available threads for communication, or a protocol or application-based attack that takes advantage of vulnerabilities inherent in the protocol or application, the intent is ultimately to inhibit the availability of the servers or services provided by those servers that are the target of the attack. One of the reasons these attacks are successful is due to the design of today's Internet.

The Internet is designed for speed in delivery of packets and is less focused on security. The responsibility for ensuring security of information on the Internet is pushed to the sender and receiver. Further, according to some sources, the Internet is not designed to police traffic, and thus vulnerable to IP Spoofing. These design features provide multiple opportunities for various kinds of DDoS attacks. Botnets are often used as the vector of choice to perform DDoS attacks due to the anonymity it provides the attacker as well as the ability to achieve high volumes of traffic with minimal commands being sent. As defined, a botnet is, "a collection of software robots, or bots, which run autonomously and automatically.(Harris et al. 2013).

DDOS attacks can be divided into two categories-

Connection based: This is attack that occurs once a connection between a server and a client has been established via certain standard protocols.

Connectionless: An attack that does not require a session to be formally established before a sender can send data packets(Harris et al. 2013)

1.2 Volumetric Attacks (connectionless)

Also known as "floods," the goal of this type of attack is to cause congestion and send so much traffic that it overwhelms the bandwidth of the site. Attacks are typically executed using botnets, an army of computers infected with malicious software and controlled as a group by the hacker.

Volumetric are the most common types of DDoS attack, making up for about 65% of the total reported cases. These attacks use multiple infected systems which are often part of a botnet to flood the network layers with a substantial amount of seemingly legitimate traffic. This consumes an excessive amount of bandwidth within or outside the network and drives network operations to become painfully sluggish or simply nonfunctional.

Since volumetric attacks essentially "gang rush" a network, they're much more difficult to mitigate than attacks from a single source.

Volumetric attacks come in a variety of forms, including:

- **User Datagram Protocol (UDP) Floods.** Random ports on a server are flooded with UDP packets, causing the server to repeatedly check for and respond to non-existent applications at the ports. As a result of the UDP Flood, the system is unable to respond to legitimate applications.

- **ICMP floods.** A server is flooded with ICMP echo requests from multiple spoofed IP addresses. As the targeted server processes and replies to these phony requests, it is eventually overloaded and unable to process valid ICMP echo requests**.**

1.3 Application-layer attacks

An application layer DDoS attack (sometimes referred to as layer 7 DDoS attack) is a form of DDoS attack where attackers target the application layer of the OSI model. (Anon n.d, 2001). The attack over-exercises specific functions or features of a website with the intention to disable those functions or features. This application-layer attack is different from an entire network attack, and is often used against financial institutions to distract IT and security personnel from security breaches**.**

Application-layer attacks, often referred to as "low and slow" to describe the attacker's goal of staying under threshold detection systems, have exposed weaknesses in netflow and threshold based detection techniques. RUDY (R-U-Dead- Yet) and Slow Loris are two types of application-layer attacks that target the HTTP protocol. R.U.D.Y. (R-U-Dead- Yet) causes the target webserver to hang while waiting for the rest of the HTTP POST request, by initiating simultaneous connections to the server the attacker is ultimately able to exhaust the server's connection table and create a denial-of-service condition.

Slowloris: Developed by Robert RSnake Hansen, is a DDoS attack software that enables a single computer to take down a web server. Due to the simple yet elegant nature of this attack, it requires minimal

bandwidth to implement and affects the target server's web server only, with almost no side effects on other services and ports.Slowloris works by opening multiple connections to the targeted web server and keeping them open as long as possible. It does this by continuously sending partial HTTP requests, none of which are ever completed. The attacked servers opens more connections, waiting for each of the attack requests to be completed.Theattacker seeks to launch a multitude of requests that are difficult to serve back to the requester, depleting application resources and quickly bringing the website down.

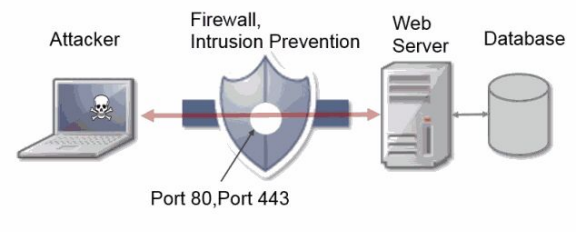

Fig 1.2 Application-layer attack type

Recently, an application-layer exploit targeting the domain name system (DNS) is an amplification attack that recruits DNS servers into the attack path, and leverages DNS methods to increase the attack volume by orders of magnitude. Domain name servers make attractive prey because they are typically very large, run on high-speed Internet connections, and cannot be easily blacklisted. Attackers exploit the DNS by spoofing the target address and sending small queries into the DNS, knowing that the response will be massive. The DNS responds to these spoofed requests with a 10-1,000 times larger answer, flooding the unsuspecting victim with a massive wave of traffic. Taken in isolation, these queries to the DNS are legitimate as the data responses by masquerading as the target.

Method of attack: An application layer DDoS attack is done mainly for specific targeted purposes, including disrupting transactions and access to databases. They require less resource and often accompany network layer attacks. An attack is disguised to look like legitimate traffic, except it targets specific application packets. The attack on the application layer can disrupt services such as the retrieval of information or search function as well as web browser function, email services and photo applications. In order to be deemed a *Distributed* Denial of Service Attack, more than 3-5 nodes on different networks should be used, using less than 3-5 nodes definitely only qualifies as a DoS and not a DDoS

1.4 Protocol Based Attack

Attacks Targeting Server Resources (Kenig et al. 2013).

Attacks that target server resources attempt to exhaust a server's processing capabilities or memory, potentially causing a denial-of service condition. The idea is that an attacker can take advantage of an existing vulnerability on the target server (or a weakness in a communication protocol) in order to cause the target server to become busy handling illegitimate requests so that it no longer has the resources to handle

legitimate ones. But these types of DDoS attacks can target stateful devices such as firewalls and IPSs as well.

TCP/IP Weaknesses: These types of attacks abuse the TCP/IP protocol by taking advantage of some of its design weaknesses. They typically misuse the six control bits (or flags) of the TCP/IP protocol – SYN, ACK, RST, PSH, FIN, and URG – in order disrupt the normal mechanisms of TCP traffic. TCP/IP, unlike UDP and other connectionless protocols, is connection-based, meaning that the packet sender must establish a full connection with his or her intended recipient prior to sending any packets. TCP/IP relies on a three-way handshake mechanism (SYN, An attack is reflective when the attacker makes use of a potentially legitimate third party to send his or her attack traffic, ultimately hiding his or her own identity.

ICMP Flood: Internet Control Message Protocol (ICMP) is another connectionless protocol used for IP operations, diagnostics, and errors. Just as with a UDP flood, an ICMP flood (or Ping Flood) is a non-vulnerability based attack; that is, it does not rely on any specific vulnerability to achieve denial-of-service. An ICMP Flood can involve any type of ICMP message of echo request, once enough ICMP traffic is sent to a target server, it becomes overwhelmed from attempting to process every request, resulting in a denial-of-service condition. An ICMP Flood is also a volumetric attack, measured in Mbps (bandwidth) and PPS (packets per second).

IGMP Flood: Internet Group Management Protocol (IGMP) is yet another connectionless protocol, used by IP hosts (computers and routers) to report or leave their multicast group memberships for adjacent routers. An IGMP Flood is non-vulnerability based, as IGMP allows multicast by design. Such floods involve a large number of IGMP message reports being sent to a network or router, significantly slowing down and eventually preventing legitimate traffic from being transmitted across the target network. An Amplification Attack is any attack in which an attacker is able to use an amplification factor to multiply the power of an attack. For instance, the attacker could use a router as an amplifier, taking advantage of the router's broadcast IP address feature to send messages to multiple IP addresses which the source IP (return address) is spoofed to the target IP. Famous examples of amplification attacks include Smurf Attacks (ICMP amplification) and Fraggle Attacks (UDP amplification).

Another example of a type of amplification attack is DNS amplification, in which an attacker, having previously compromised a recursive DNS name server to cache a large file, sends a query directly or via a botnet to this recursive DNS server, which in turn opens a request asking for the large cached file. The return message (significantly amplified in size from the original request) is then sent to the victim's (spoofed) IP address, causing a denialof-service condition. A connection-oriented attack is one in which the attacker must first establish a connection prior to launching his or her DDoS attack. The outcome of this attack usually affects the server or application resources. TCP or HTTP-based attacks are examples of connection-oriented DDoS attacks.

A connectionless attack, on the other hand, does not require the attacker to open a complete connection to the victim, and therefore is much easier to launch. The

outcome of a connectionless attack affects network resources, causing denial-of-service before the malicious packets can even reach the server. UDP or ICMP floods are examples of connectionless DDoS attacks. 30 SYN-ACK, ACK) where every request creates a half-open connection (SYN), a request for a reply (SYN-ACK), and then an acknowledgement of the reply (ACK).(Zargar et al. 2013). Any attack that attempts to abuse the TCP/IP protocol will often involve sending TCP packets in the wrong order, causing the target server to run out of computing resources as it attempts to understand such abnormal traffic.

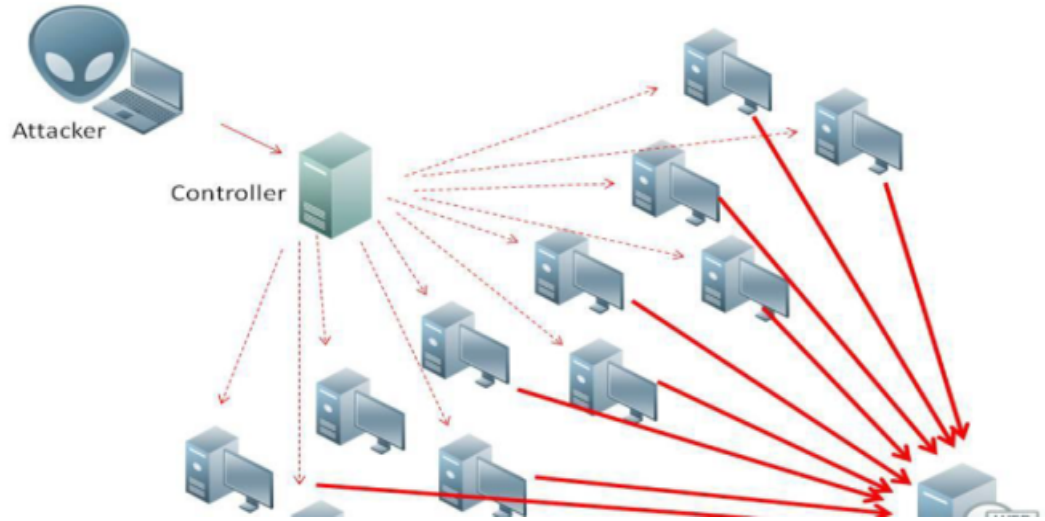

Figure 1.3 Protocol based DDoS attack

Figure 1.4 Slowloris

1.5 The Four Steps to Mitigate a DDoS Attack

There are a number of measures that organizations can undertake to mitigate the risks of a DDoS attack, they include;

Step.1. Over-Provision Bandwidth to Absorb DDoS Bandwidth Peaks

This is one of the most common measures to alleviate DDoS attacks, but it is also probably the most expensive, especially since DDoS attacks can be ten times or even one hundred times greater than standard Internet traffic levels. An alternative to over-provisioning internet bandwidth is to use a security service called scale on-demand to absorb and filter DDoS traffic. DDoS protection services are designed to stop massive DDoS attacks without burdening businesses Internet connections.

Step.2. Monitor Application and Network Traffic

The best way to detect when you are under an attack is by monitoring application and network traffic. Then, you can determine if poor application performance is due to service provider outages or a DDoS attack. Monitoring traffic also allows organizations to differentiate legitimate traffic from attacks. Ideally, security administrators should review traffic levels, application performance, anomalous behavior, protocol violations, and Web server error codes. Since DDoS attacks are almost always executed by botnets, application tools should be able to differentiate between standard user and bot traffic. Monitoring application and network traffic provide IT security administrators' instant visibility into DDoS attack status.

Step.3. Detect and Stop Malicious Users

For application layer DDoS traffic, often times identifying malicious users can be the most effective way to mitigate attacks.

a. Recognize known attack sources, such as malicious IP addresses that are actively attacking other sites, and identifying anonymous proxies and TOR networks. Known attack sources account for a large percentage of all DDoS attacks, because malicious sources constantly change. Organizations should have an up-to-date list of active attack sources.
b. Identify known bot agents; DDoS attacks are almost always performed by an automated client. Many of these client or bot
c. agents have unique characteristics that differentiate them from regular Web browser agents. Tools that recognize bot agents can immediately stop many types of DDoS sources.
d. Perform validation tests to determine whether the Web visitor is a human or a bot. For example, if the visitor's browser can accept cookies, perform JavaScript calculations or understand HTTP redirects, then it is most likely a real browser and not a bot script.
e. Restrict access by geographic location. For some DDoS attacks, the majority of attack traffic may originate from one country or aSpecific region of the world. Blocking requests from undesirable countries can be a simple way to stop the vast majority of

DDoS attack traffic.

Step.4. Detect and Stop Malicious Requests

Because application DDoS attacks mimic regular Web application traffic, they can be difficult to detect through typical network DDoS techniques. (Zargar et al. 2013) However, using a combination of application-level controls and anomaly detection, organizations can identify and stop malicious traffic. Measures include:

a. Detect an excessive number of requests from a single source or user session. Automated attack sources always request Web pages more rapidly than standard users.
b. Prevent known network and application DDoS attacks. Many types of DDoS attacks rely on simple network techniques like
c. Fragmented packets, spoofing, or not completing TCP handshakes. More advanced attacks, typically application-level attacks, attempt to overwhelm server resources. These attacks can be detected through unusual user activity and known application attack signatures.
d. Distinguish the attributes and the aftermath of a malicious request. Some DDoS attacks can be detected through known attackpatterns or signatures. In addition, the Web requests for many DDoS attacks do not conform to HTTP protocol standards. The Slowloris attack, for example, includes redundant HTTP headers. In addition, DDoS clients may request Web pages that do not exist. Attacks may also generate Web server errors or slow Web server response time.

Conclusion

DDoS attacks are destructive weapons that can riun a business. Our reliance on the Internet continues to grow, and the threat of DDoS attacks continues to expand. Organizations need to ensure operational continuity and resource availability with a vigilant DDoS mitigation approach if they want to conduct "business as usual."

There are other techniques that can be used to mitigate DDoS attacks which we didn't capture in this work, example is the incapsula.

References

Anon, Url @ Www.Google.Com.Ng. Available at: https://www.google.com.ng/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&cad=rja&uact=8&ved=0CF0QFjAG&url=http://www.researchgate.net/publication/3342484_Enhancement_of_document_images_using_multiresolution_and_fuzzy_logic_techniques/file/3deec528547a536246.pdf.

Defense Mechanisms Against Distributed Denial of Service (DDoS). Communications Surveys &, 15(4), pp.2046–2069. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6489876 [Accessed June 12, 2016].

DDoS Attack types & Mitigation methods !Incapsulahttps://www.incapsula.com/ddos/ddos-attacks/ (Accessed June 10, 2016).

DDoS Attacks 101: Types, targets, and motivations

http://www.calyptix.com/top-threats/ddos-attacks-101-types-targets-motivations/ (Accessed June 10, 2016).

Harris, B., Konikoff, E. & Petersen, P., Breaking the DDoS Attack Chain. *Institute for Software Research*, (August). 2013.Available at: http://www.cmu.edu/mits/files/breaking-the-ddos-attack-chain.pdf [Accessed June 12, 2016].

Kenig, R. et al., 2013. DDoS Survival Handbook. *Radware*, pp.1–56. Available at: http://security.radware.com/uploadedFiles/Resources_and_Content/DDoS_Handbook/DDoS_Handbook.pdf [Accessed June 12, 2016].

Lee, N. *Counterterrorism and cybersecurity : total information awareness*, Springer.2013

Networks, J., DEFENDING AGAINST APPLICATION-LAYER DDOS ATTACKS, 2006.

Zargar, S.T. et al., 2013a. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS). , 15(4), pp.2046–2069.

Rocky K. C. Chang, Defending against Flooding-Based DDoS Attacks: A Tutorial. 13 October 2009