DDoS Attacks & Mitigation Strategies

[1]Vikas Kumar Jain, [2]Rajesh Pokhriyal, [3]Rajesh Patil
[1]Sr Manager, [2]Manager, [3]Manager
[1]Data Center,
[1]Railtel Corporation of India Ltd., Gurugram, India

Abstract: A denial of service (DoS) attack is any attack that prevents a legitimate user from accessing a network resource. A distributed denial of service (DDoS) attack is one that uses numerous network resources as the source of the specific attack vector. The use of multiple resources is primarily intended as a method to amplify the capabilities of a single attacker, but it can also help to conceal the identity of an attacker and complicate mitigation efforts. Most DDoS attacks leverage a "botnet", which is a network of Internet connected computer systems centrally controlled by an attacker. Botnets can range in size from a handful of systems to tens of millions. Most botnets use compromised computer resources without the knowledge of the owner.

IndexTerms **- DDoS, botnet, Mitigation, Smokescreen, extortion, ISP, CDN**

1. INTRODUCTION

Businesses lose billions of money to malicious hackers every year, with DDoS emerging as one of the most prevalent techniques used to attack websites. Thankfully, there are steps that can be taken to lessen the risk. There's a process for implementing DDoS mitigation. This starts with understanding about DDoS Impact, Attacker motivation; DDoS attacks types, Mitigation strategies and benefit of implementing DDoS mitigation.

2. DDOS IMPACT

2.1 Damage to Reputation

Due to DDoS attack on application / Network, attacker can cause an outage and can negatively impact the reputation of a company.

2.2 Direct Revenue Loss

Due to outage to a network that directly generates revenue, such as E-commerce or online media, can directly impact an organization.

2.3 Lost Productivity

A DDoS attack often prevents employees to do their activities and act as a decoy to distract IT staff.

2.4 Attack Smokescreen

Various shows that DDoS attacks are often align with other threat vector. Business needs to be aware of full threat landscape and prepare to deal with multiple types of activity at a time.

A DDoS attack is generally used to hide other nefarious activities from information security personnel.

3. ATTACKER MOTIVATIONS

3.1 Extortion

A common motivation for DDoS attacks is the extortion of money from the targeted company. In a typical DDoS extortion scheme, the attacker will anonymously contact the victim organization to request a specific amount of money to be paid to prevent a future attack. Often the attacker will prove their capabilities by performing a limited DDoS attack at a specific time. The anonymous transfer of funds is usually carried out using the Bitcoin virtual currency. A cyber-criminal gang known as DD4BC was exposed in December 2015 for operating a massive DDoS extortion ring.

3.2 Hacktivist

Within the scope of DDoS, "hacktivism" is the use of DDoS to promote a specific political agenda. An attack of this type will often be preceded by a public statement from the attacker on social media or other public forums detailing a specific grievance or manifesto. Victims of these attacks are often well established brands or companies that are likely to suffer substantial reputation damage from the associated enterprise impact and news coverage. The most well-known example of this type of attacker is the loose hacktivist collective "Anonymous," which has claimed responsibility for DDoS attacks targeting Bank of America, Visa, MasterCard, the Church of Scientology and many others.

3.3 State-sponsored/Cyber terrorism

A cyber terrorism campaign involves a nation or terrorist organization performing a DDoS attack. The primary goal is often the silencing of speech from certain sources, or the substantial disruption to the target's telecommunications infrastructure and commerce. These types of DDoS attacks are generally much larger and better orchestrated due to the significant resources of the attacker. A suspected example occurred in March 2015 when a DDoS barrage originating from China targeted specific anti-China resources hosted on GitHub. Other examples include a three week DDoS attack in the spring of 2007 targeting the country of Estonia, which effectively disconnected the country from the Internet. The attack was linked to a political dispute with Russia.

3.4 Personal Vendetta

The historical origins of DDoS are primarily from online disputes between individuals or small groups. These types of attacks grew in popularity during the late 1990s in online chat systems. The primary purpose of these attacks is to "punish" someone for a perceived wrong, or silence their speech. These types of attacks are still prevalent today.

3.5 Business Rivalry

The purpose of these attacks is to cause financial impact or embarrassment to a business competitor. These attacks are typically long in duration, and target resources responsible for revenue generation, such as E-commerce systems. The advent of DDoS-for-hire services, where someone can purchase a DDoS attack for less than $20, has facilitated and made this type of attack more common.

4. TYPE OF ATTACKS

4.1 Layer 7 Attacks

4.2 Protocol Attack

4.3 Bandwidth Attack / Volumetric / Reflection Attacks

(fig 4.1- types of DDoS attacks)

5. MITIGATION STRATEGY FOR ENTERPRISES TO HANDLE DDOS ATTACK IN COMBINATION OF ISP CLEAN PIPE AND CDN PROVIDER

5.1 On premises Appliance

Why Network parameter security devices are failed in protocol attack and Why CPU and Memory are exhausted on server where application resides.

Network Security devices like Firewalls are primary entry point in network. They have limitation in their core design

A. Total concurrent session
B. New Sessions per second

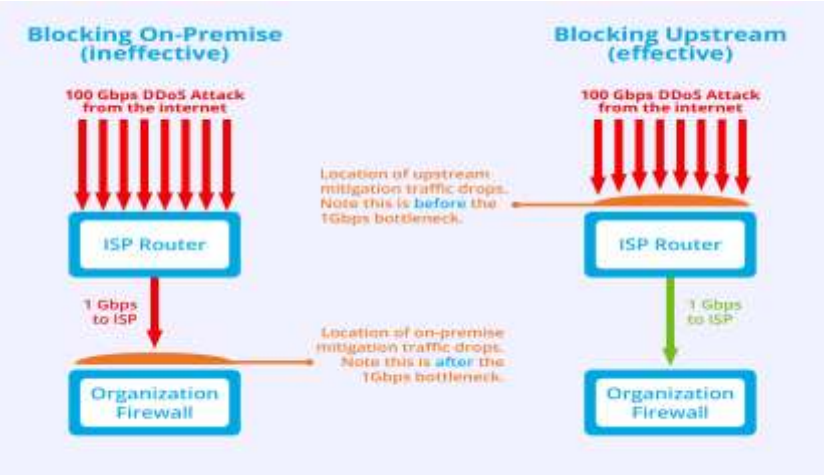
If attacker is able to exhaust these two limitations of firewall then he can stop functioning of entire operations of business.

Excessive request and connection are performed in in Layer 7 attacks which will sudden increase in CPU or memory utilisation.

Then only one solution to enterprise is to deploy Anti DDoS solution on premises

Limitation

Solution is enough to handle these kinds of layer 7 and protocol 7 attacks. On premises solution is ineffective In case of Bandwidth / Reflection attack, enterprise has to take ISP clean pipe service.



(fig 5.1-ISP DDoS mitigation)

5.2 Cloud signaling to ISP DDoS solution

On premises appliance /application may use IETF Open Threat Signaling to signal information relating to current threat handling to other device in ISP cloud. ISP can mitigate DDoS in their cloud by using various DDoS mitigation countermeasures.

5.3 CDN based application security + DDoS

Enterprises can choose application security integrated with DDoS solution form CDN provider to mitigation threat of Layer 7 DDoS attack instead of mitigating layer 7 DDoS on premises solution.

6. BENEFITS OF SERVICE

A. Reduce the risk of downtime
B. Ensure high performance during attack
C. Minimize cost by avoiding needs of deploying dedicated hardware

REFERENCES

[1] Shui Yu.2004. Distributed Denial of Service Attack and Defense
[2] David Dittrich, Peter Reiher, Sven Dietrich.2005.Internet Denial of Service: Attack and Defense Mechanisms
[3] Francois Encrenaz.blog. http://francois-encrenaz.net