# EXCITINGIP.COM

IT, Networking, Mobile, Camera, Gadgets... Everything that Excites Techies :)

NETWORK SECURITY

## An Introduction to DDoS – Distributed Denial of Service attack

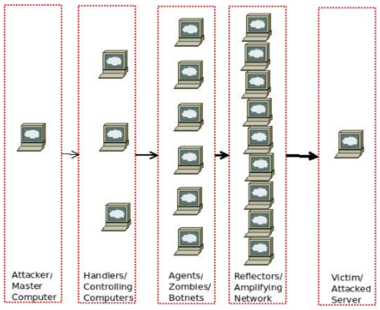
*March 15, 2011*

As you might have heard, the famous blogging service WordPress.com was recently unavailable for around an hour due to a huge Distributed Denial of Service attack carried out by many infected computers on the Internet. In this article, let us look at what a Distributed Denial of Service attack is, why it is hard to detect and mitigate, few types of DDoS attacks & some measures one can take to prevent/ mitigate them.

### What is DDoS – Distributed Denial of Service Attack?

DDoS stands for Distributed Denial of Service attack. It is a form of attack where a lot of zombie computers (infected computers that are under the control of the attacker) are used to either directly or indirectly to flood the targeted server(s) – victim, with a huge amount of information and choke it in order to prevent legitimate users from accessing them (mostly web servers that host websites). In most cases, the owners of the zombie computers may not know that they are being utilized by attackers. In some cases, there is only a periodic flooding of web servers with huge traffic in order to degrade the service, instead of taking it down completely.

### Components & Architecture diagram of a Distributed Denial of Service attack:


Attacker/ Master Computer
Handlers/ Controlling Computers
Agents/ Zombies/ Botnets
Reflectors/ Amplifying Network
Victim/ Attacked Server

**Distributed Denial Of Service Attacks (DDoS) - Architecture Diagram**

As you can see in the above architecture diagram representing Distributed Denial of Service (DDoS) attacks, there maybe up to five components. Two of them are aways there – The attacker/ master computer from where the attacks are initiated and the Victim/ Attacked server which comes under the attack. Presence of just these two components makes it a Denial of Service attack (DOS).

The three components in the middle, make it a Distributed Denial of Service attack! Zombies / botnets are the computers from which the DDoS attacks are carried out. They may either be volunteer computers or in most cases, infected computers of Internet browsing users who download certain malicious software unawares (from bit-torrent sites, etc) which entitles them to be controlled by the attackers. There maybe an additional layer of handlers / controlling computers which issue instructions to the zombies/ agents & a reflector layer which amplifies the number of requests that arrive from zombies, and sends it to the victim servers to cripple it.

### Why are DDoS – Distributed

## Denial of Service attacks difficult to detect and mitigate?

Since unsuspecting user's computers are used as zombies to carry out the attacks against the victim server, it is difficult to trace down the actual attacker. More over, there are no fixed IP addresses/ IP address series for the zombie computers that connect to the Internet using broadband connections, and even if some of attacking zombie computers are identified and blocked, more computers can always be summoned by the attacker.

Sometimes, even zombie computers do not directly communicate with the victim servers – instead they spoof the IP address of the victim server and send requests to large number of reflector computers (which may not be infected). This makes the reflectors to send huge reply packets to victim servers, as they need to reply back to all the requests from what it thinks is the originator!

It might be relatively easier to identify and fend off the bigger attacks from small number of systems like 10 machines sending 1000 requests per second than 1000 machines sending 10 requests per second, which is possible with DDoS attacks.

Some of these attacks are in the range of multiple Gigabits per second (In the case of WordPress.com, it was 4 Gbps). Since most Internet connectivity links to individual organizations are lesser than that, such high magnitude attacks can choke the entire Internet bandwidth.

## Types of Distributed Denial of Service attacks:

There are two types of DDoS attacks – Attacks that target the Network (Internet bandwidth) and choke the Internet bandwidth used by the victim server, so that it cannot accept legitimate requests coming from genuine users through the Internet gateway & Attacks that target the vulnerabilities in applications in order to cripple server resources like CPU, RAM, Buffer memory, etc and make the servers unavailable for handling any legitimate requests.

For example, DNS attack targets the network. In this, many zombie computers query DNS servers simultaneously (with the spoofed IP address of the victim server). Now, the DNS servers need to respond back to the queries, to the source IP address. Since all the source IP addresses are of the victim server, all the responses are sent there – thereby chocking the bandwidth available with the victim server. Likewise, a Syn Flood attack targets applications – It opens multiple connections (using multiple zombie computers) to the victim server using 'Syn' requests. The server responds with 'Syn-Ack' acknowledgement. The zombie computers need to send back an 'Ack' response, for the victim server to close the connection. But they don't do that, resulting in many open connections (which cannot be used by other users) in the server.

The handlers, are a small number of controlling computers which communicate with the numerous zombie computers using command and control signals, which can be intercepted to identify the handlers/ master computer. But sometimes, even those communications are encrypted by attackers.

## Some Steps for prevention/ mitigation of Distributed Denial of Service attacks (DDoS):

As such, the Distributed Denial of Service attacks are difficult to prevent / mitigate. But steps can be taken (based on your environment) to prevent/ identify/ mitigate the DDoS attacks and some of them are given below:

- Identification of **statistical patterns** of DDoS attacks and comparing the same with live traffic, might help in identifying these attacks early. Its possible to identify and **filter illegitimate traffic** while simultaneously allowing legitimate traffic. This requires appropriate filtering systems, and can be automated or done manually.
- Having **alternate network paths** and applying **load balancing** for incoming traffic would reduce the risk posed by DDoS attacks. Having over provisioned/ additional servers/ cloud based resources even if it can be summoned only at the time of DDoS attacks also helps – especially with small DDoS attacks, as **more traffic** can be handled.

- **Rate-Limiting/ Throttling:** The maximum incoming traffic (coming in to a server) can be controlled, and any additional traffic could be throttled to prevent the server from going down. Its beneficial if the source(s) of DDoS attacks could be identified so that the traffic from there could be filtered out. Its possible to send 'null-routes' back to the attacking computers, to confuse them in thinking there is no target server.
- **Honeypots:** Many organizations don't use this, but its a very interesting technique which involves the setting up of dummy servers with maximum vulnerabilities that are exposed to hackers as legitimate servers. When the hackers attack these systems, its possible to study the attack patterns, attack intentions and even find out attack sources.
- **Aggressive Caching:** Caching is a method by which the frequently accessed web pages are stored as separate HTML files and when users request these pages, the HTML files are presented to them instead of the Time/CPU resource consuming database quires. This enables the servers to handle more requests/ per second and hence the smaller DDoS attacks

can be fended off.

- If its a website, it might be better to host it on **cloud infrastructure/ content delivery networks/ managed service providers** etc, who have dedicated network security professionals and devices (if companies don't have them in-house) to manage DDoS attacks. But the cost of such hosting / DDoS mitigation needs to be considered.

- It helps if the zombie computers are **protected** in the first place to ensure that they cannot get infected by attackers and do not participate in the DDoS attacks. This article explains what zombies are and how individual computer users can be safe.

## excITingIP.com

You could stay up to date on the various computer networking and related IT technologies by subscribing to this blog with your email address in the sidebar box that says, 'Get email updates when new articles are published'

components of DDOS | DDOS | DDOS architecture diagram | DDOS attack | DDOS attacks | distributed denial of service | distributed denial of service attacks | mitigation of DDOS | prevention of DDOS | types of DDOS | what is DDOS

*By Rajesh K*

### 2 COMMENTS

**CONZ**
JUNE 26, 2011 AT 4:58 PM

thanks for intro..nice

**KARLY - SERVER SPACE**
JANUARY 28, 2014 AT 7:31 AM

Thanks for sharing Rajesh. You express some valuable insights into DDoS attacks and ways to prevent them. These types of attacks are very real and happen on a daily basis. By controlling so many unsuspecting computers to facilitate the attack, this is a very powerful action indeed.

News Network-Active Network-Passive Wireless Network Voice over IP Video over IP Network Security Network Optimization Data Center Storage Protocols Bandwidth Applications Open Source Server Tech Office Automation Xip Blog
|