What is a DDoS attack? How to Stop DDoS Attacks?

testbytes.net/blog/ddos-attack

December 23, 2019

Security Testing
Monday December 23, 2019

In a world dominated by the digital world, everything seems to be just a click away. Our dependence on digital media has grown manifolds in the past couple of decades. But this dependency has also given birth to many notorious activities, and one of such activity is DDos attack.

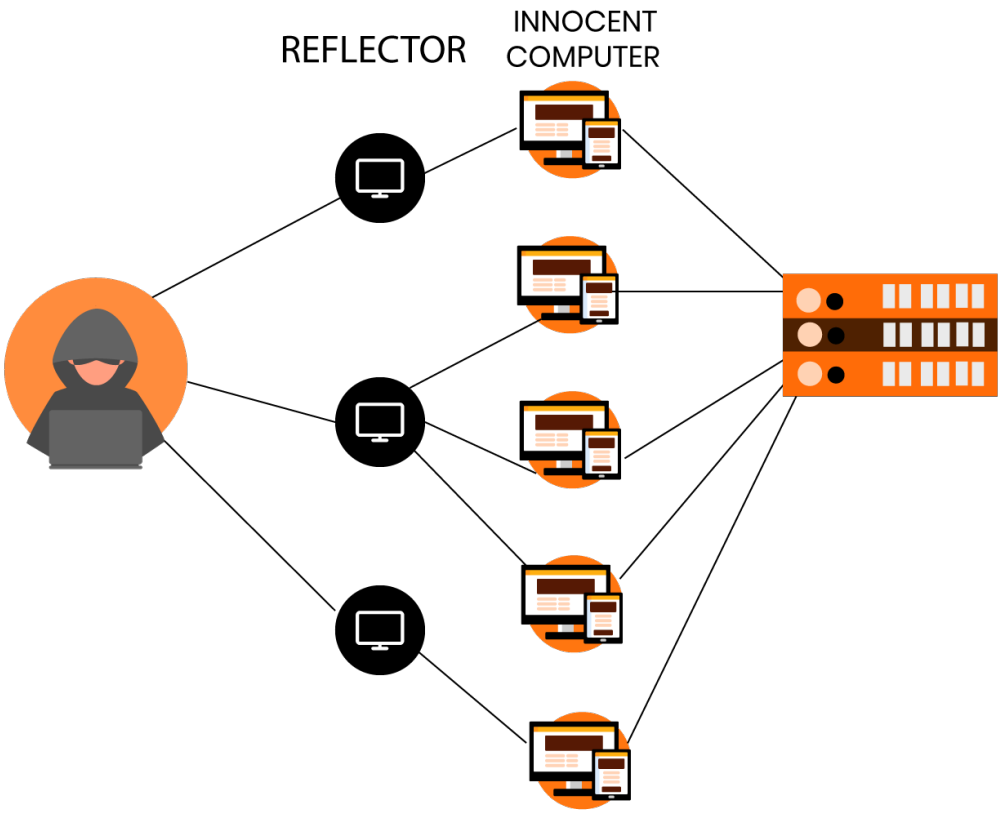
Overview of DDoS Attacks:

In this article, we will learn more about DDoS attacks.

What is a DDoS attack?

DDoS attack or distributed denial of service attack is making it impossible to deliver the service to its end customers. In this kind of attack access to almost everything including s devices, servers, applications, services, networks, etc. is prevented.

The difference between DoS attack and DDoS attack is that in DoS attack malicious data or requests are sent from one system whereas in a DDoS attack it can be sent from multiple systems.



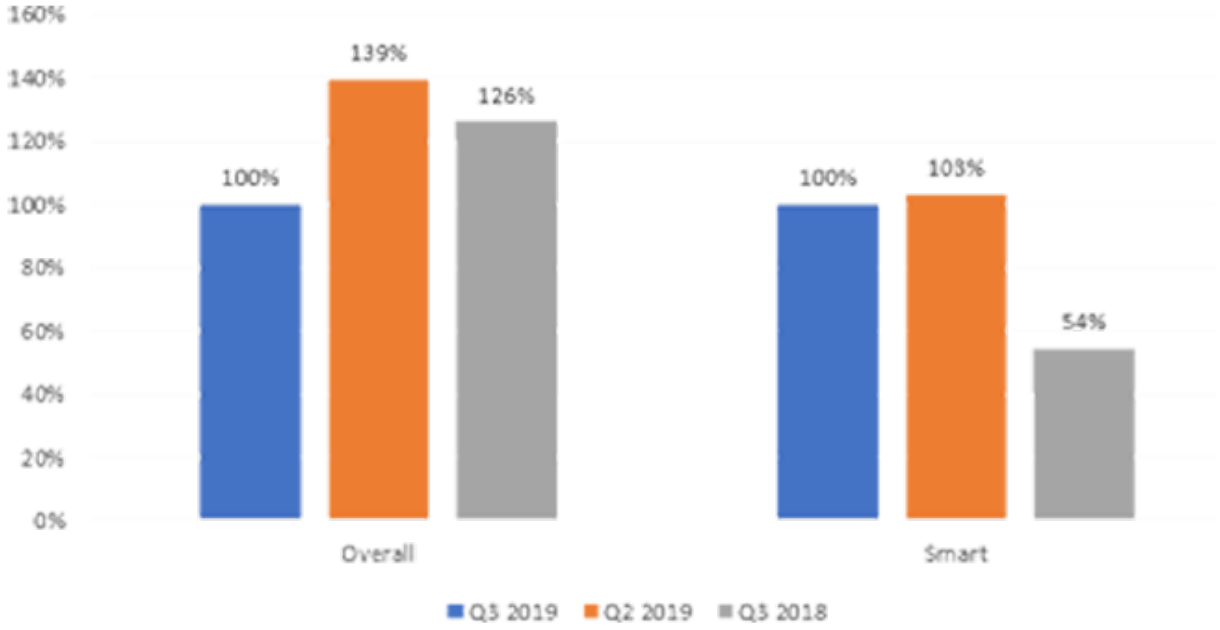
Multiple requests for data are masked to the system to initiate this attack. It could be done by either extensive request to the webserver to serve a page so that it ultimately crashes because of high demand. The other way is to a large number of queries are hit to the database to slow it down and ultimately crash it.

It could result in minor breakdown or disruption in services or the complete breakdown of websites, applications, or taking the complete business offline.

Why DDoS Attack?

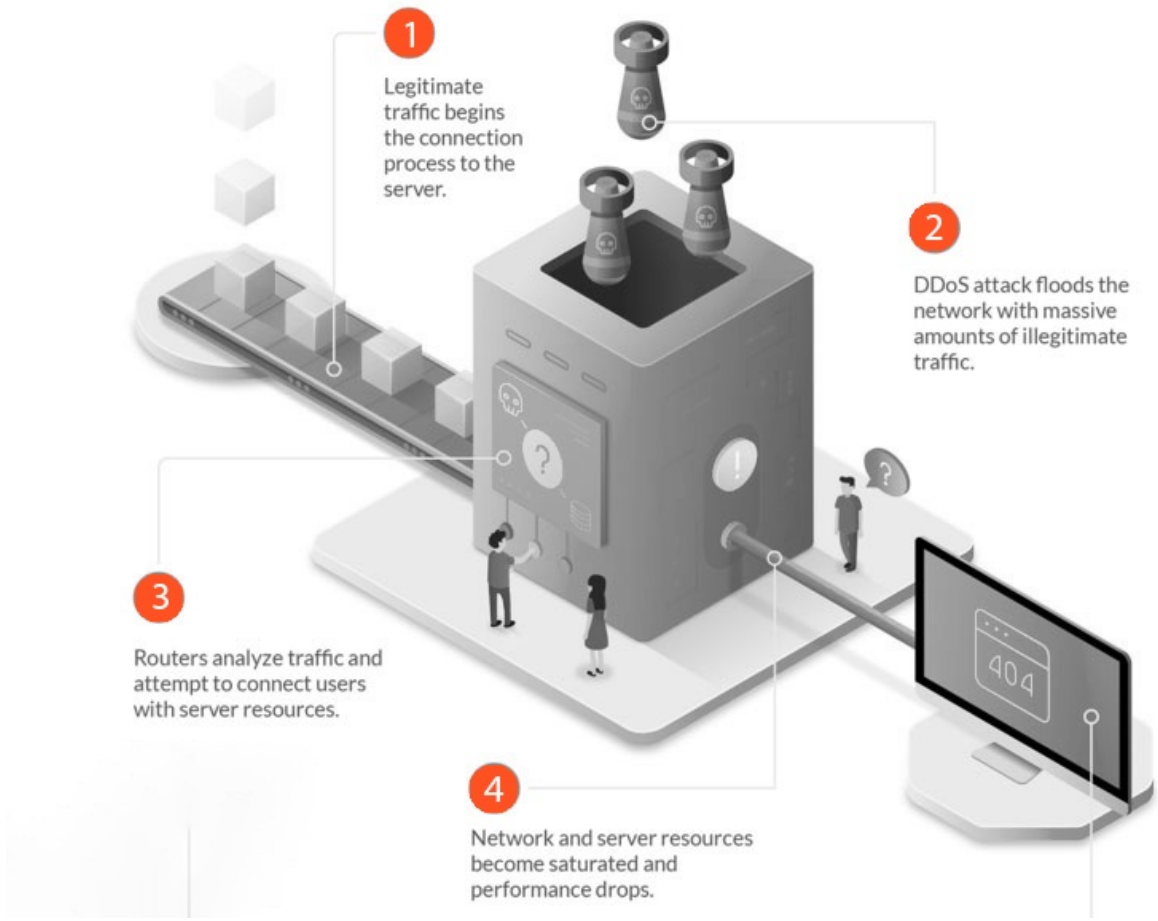
DDoS attacks are initiated to crash the website. The main aim behind such attacks is to make the digital services of the businesses unavailable to its customers.

Duration of DDoS Attack



The duration of the DDoS attack depends on whether the attack is on the network layer or application layer. Network layer attacks can extend up to 48 to 49 hours whereas Application layer attacks can be effective for 60 to 70 days.

DDoS attack Symptoms

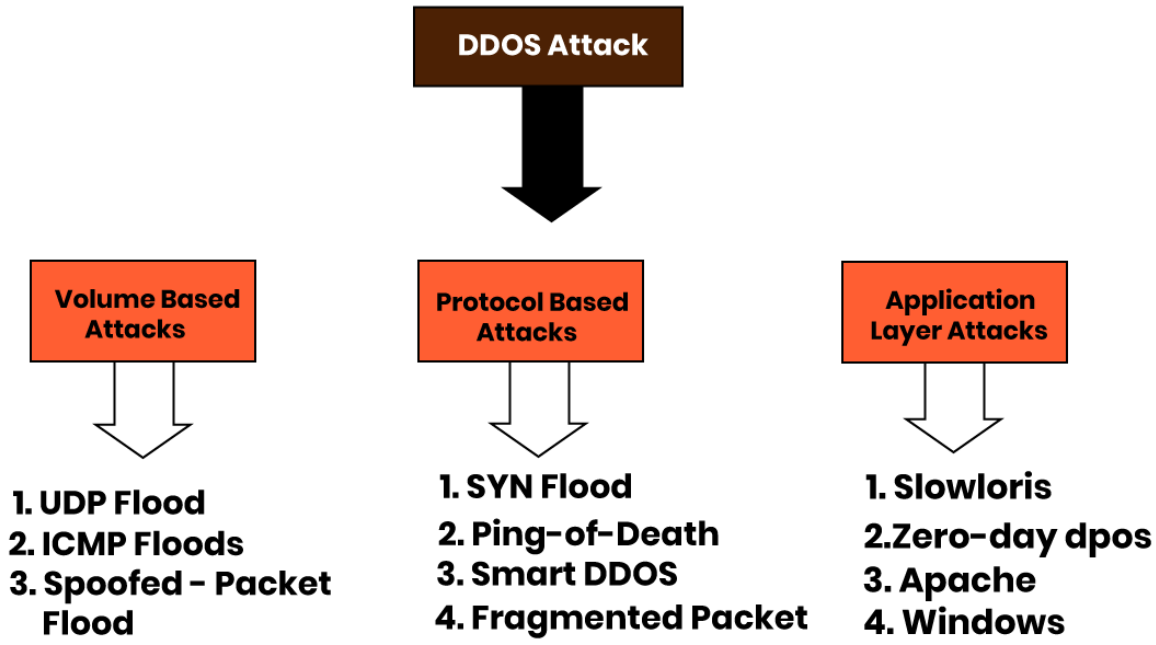


Some of the symptoms of DDoS are:

- Downed server or system
- Too many legitimate requests from legitimate users
- A cut cable.

It might require traffic analysis for precise analysis.

Types of DDoS attack



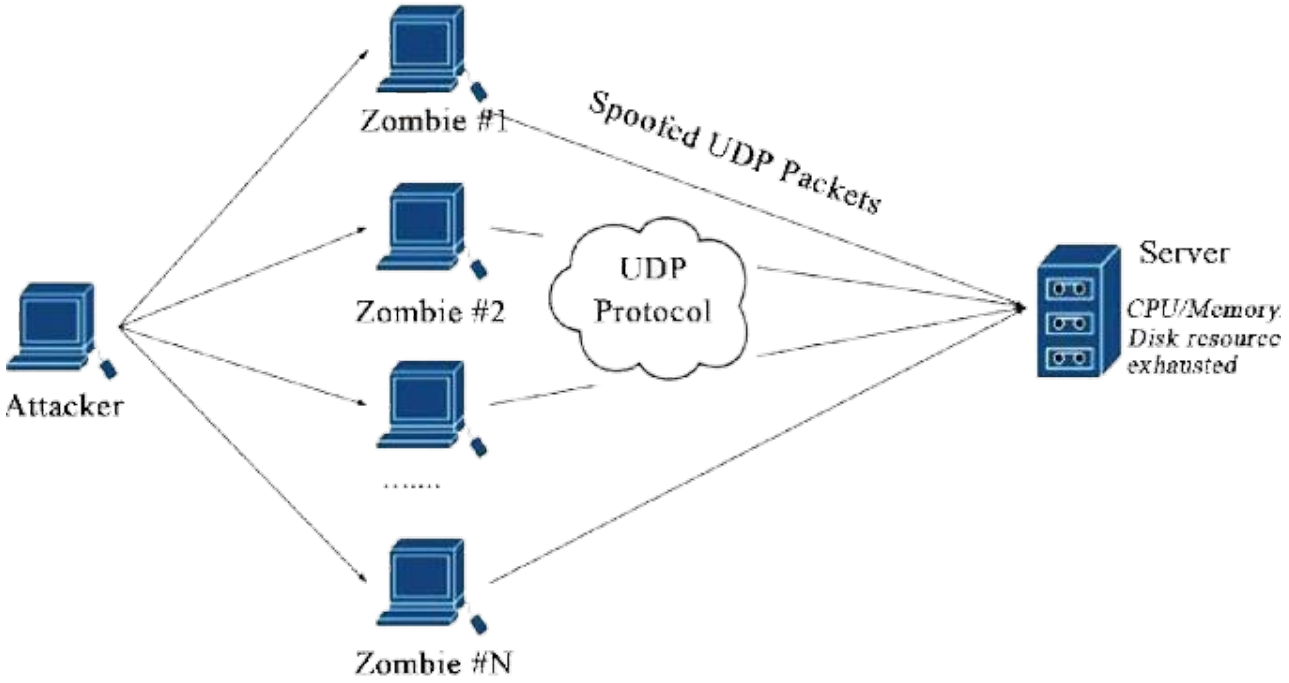
There is a rise in DDoS attacks in the past few years. and even the attacks are now getting stronger and more harmful. In such a scenario it becomes important to take mitigate these attacks to avoid any future security risks.

To avoid these attacks you should be aware of various types of DDoS attacks so that you can protect yourself from them.

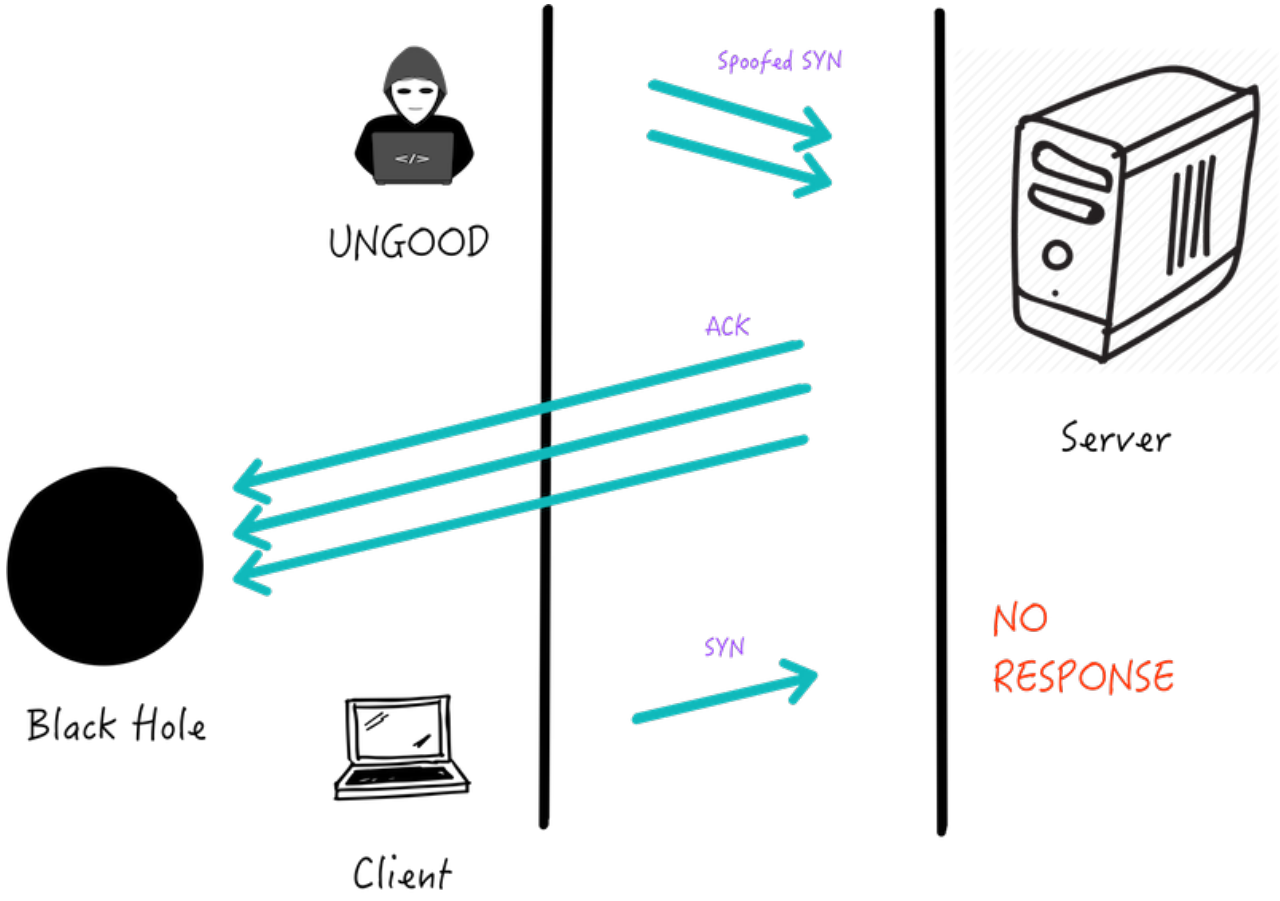
> **Also Read : Why Python is Used For Cyber Security?**

Here are some common types of DDoS attacks:

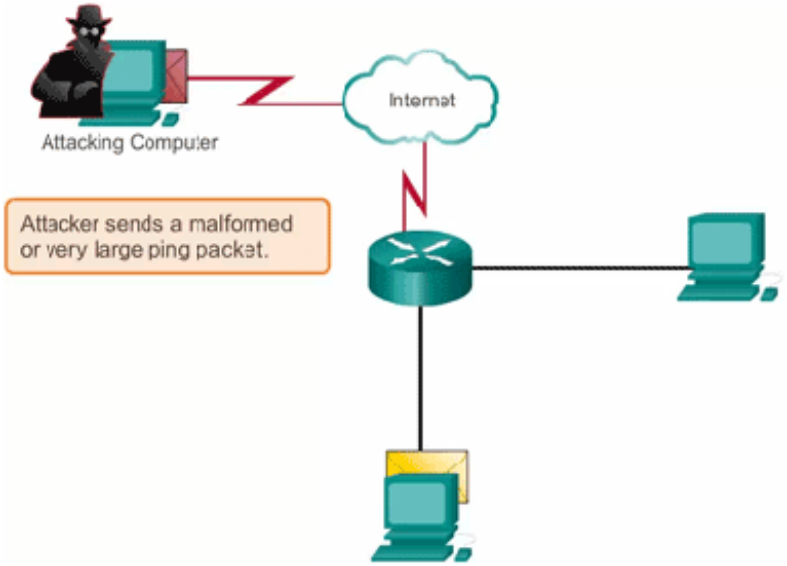
1. UDP Flood: UDP flood or User Datagram Protocol is a common DDoS attack method where random ports on the target machine are flooded with packets.



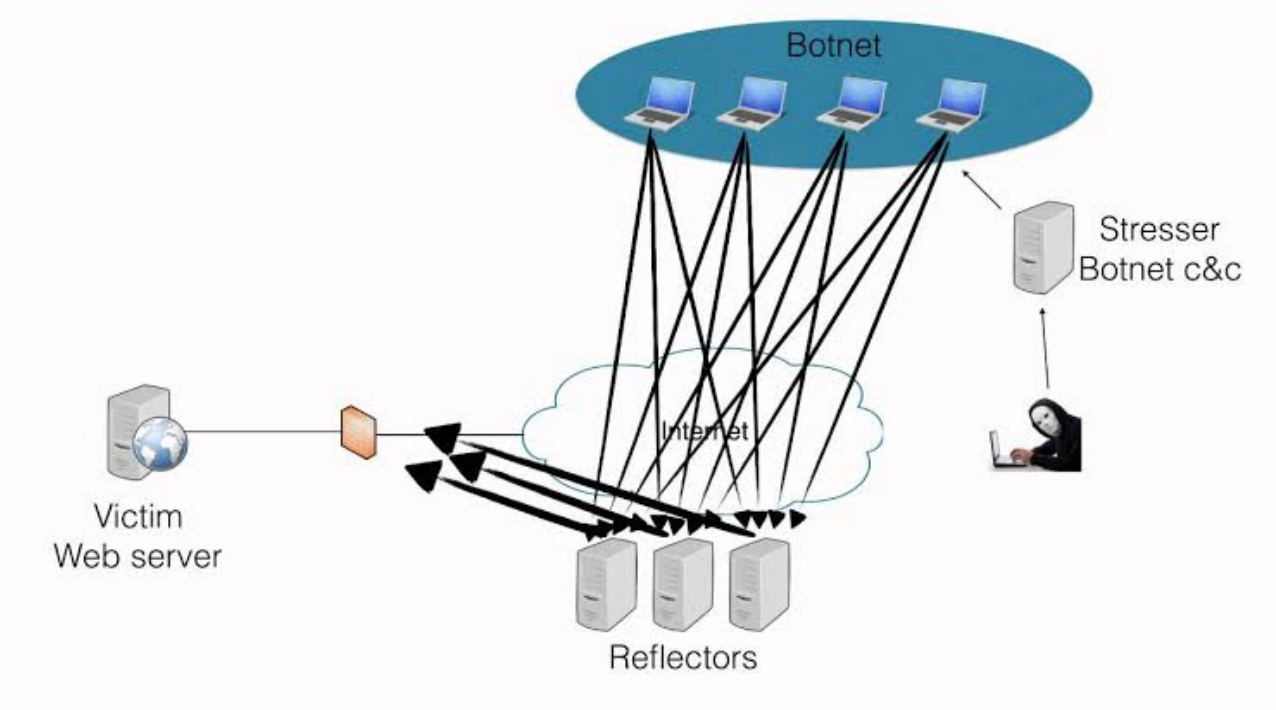
2. SYN Flood: In SYN flood attack repetitive hoaxed requests are sent to a target server from various sources.



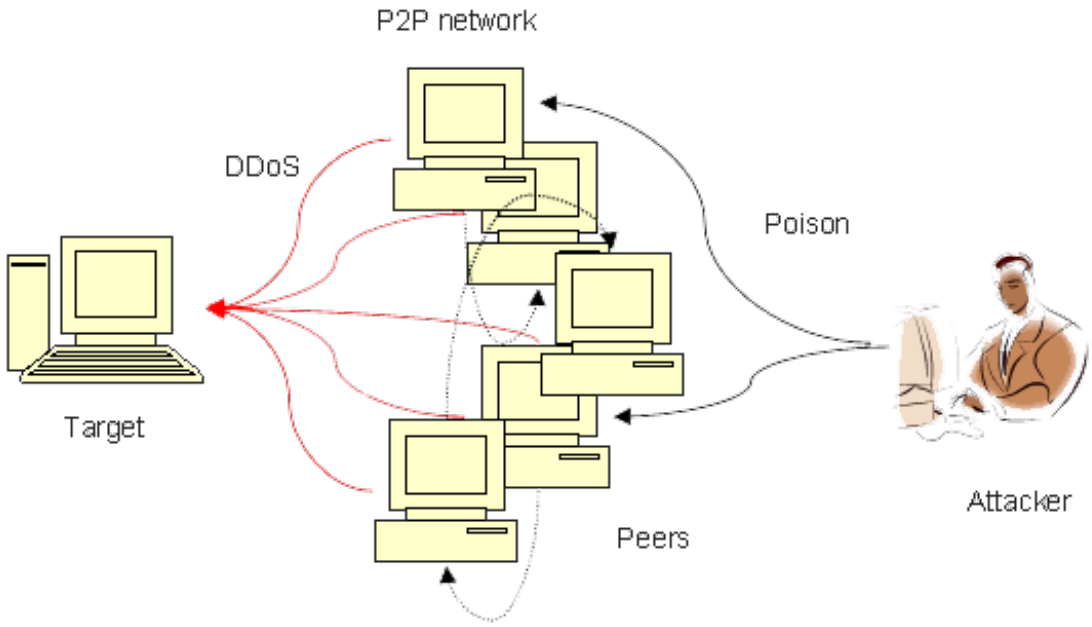
3. Ping of Death: Ping of death (”POD”) sends packets exceeding allowed byte size to manipulates IP protocol.



4. Reflected Attack: A reflected attack is initiated by sending forged packets to multiple computers.

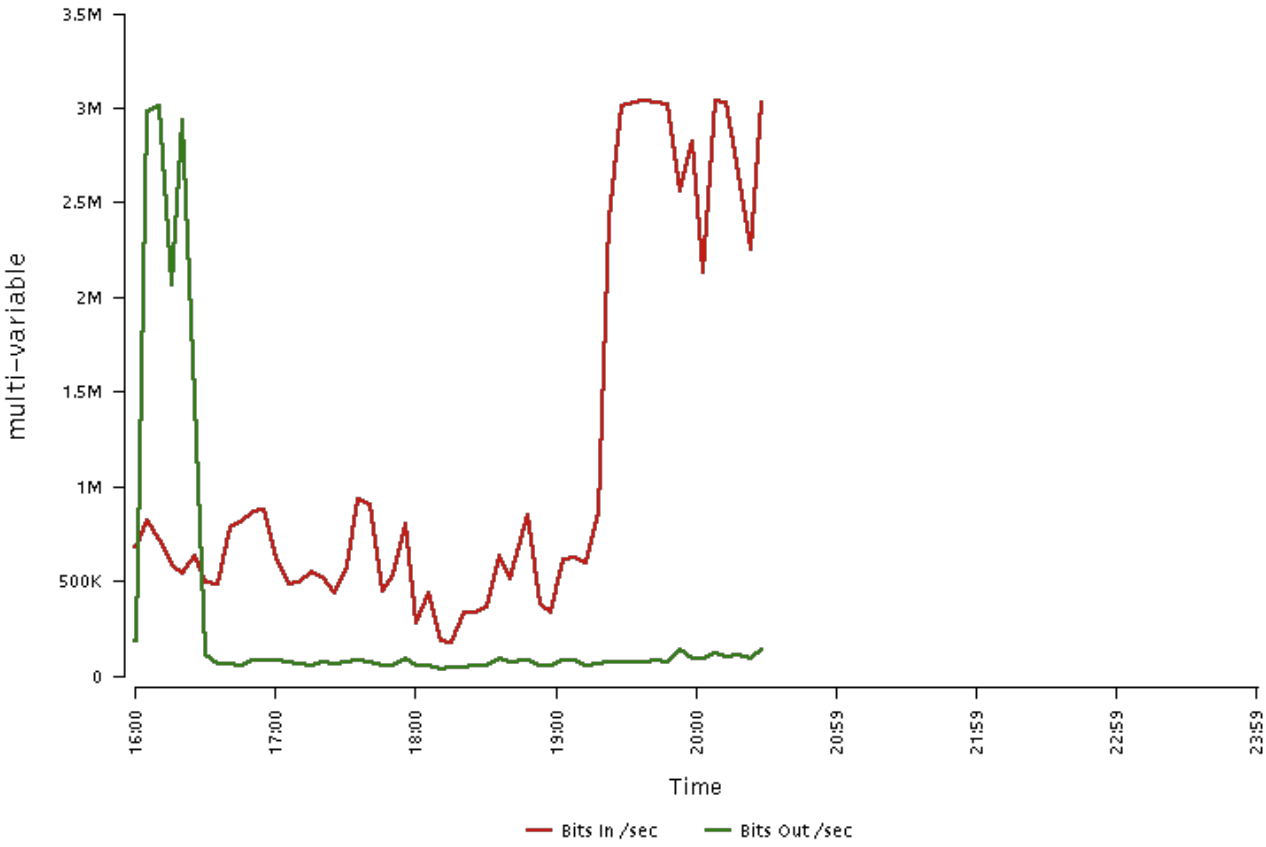


5. Peer-to-Peer Attacks: Peer-to-Peer uses a peer-to-peer server to divert traffic to the target website.

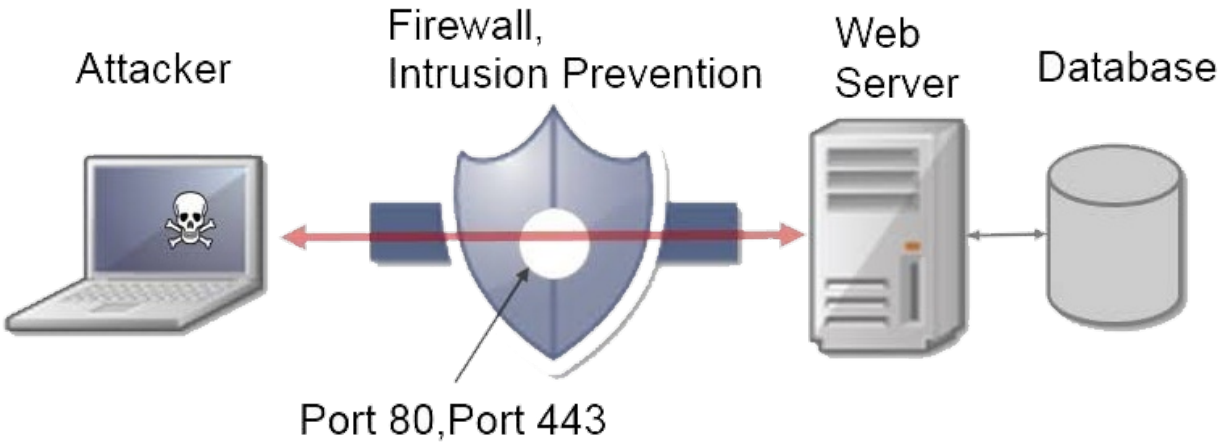


6. Degradation of Service Attacks: Degradation of Service Attacks only slows down the server response times instead of taking the website or server offline.

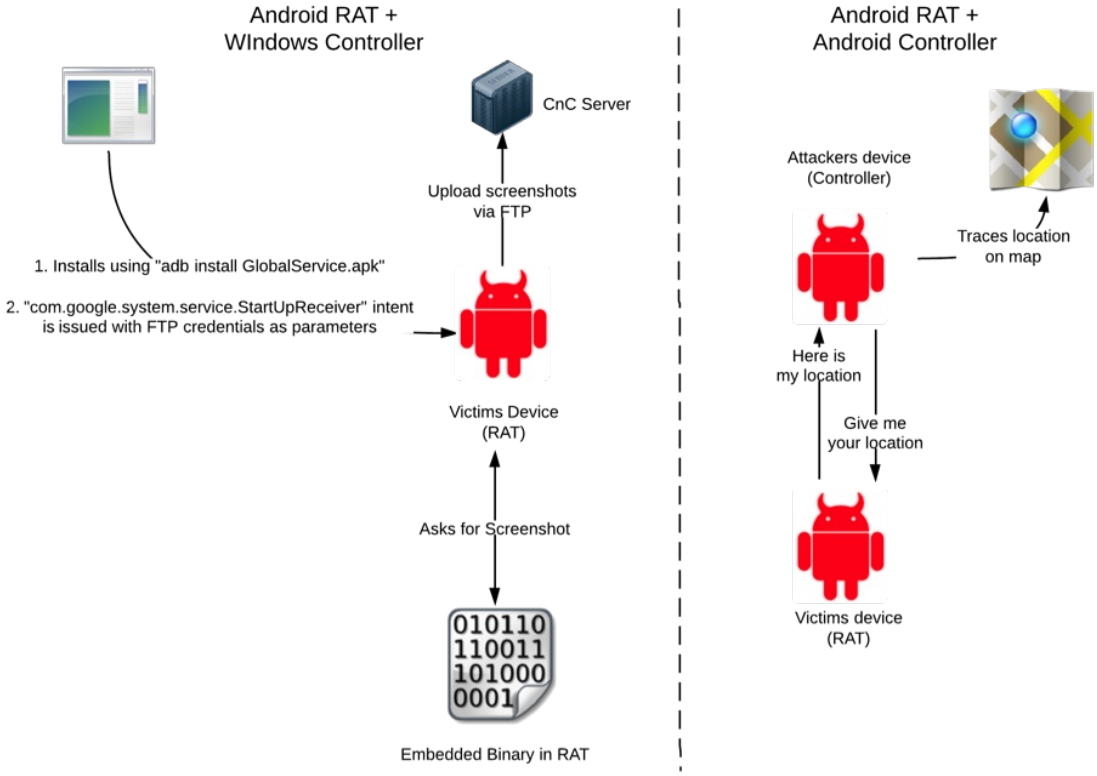
7. Unintentional DDoS: Unintended distributed denial of service refers to congestion in web traffic that causes website/server breakdown.



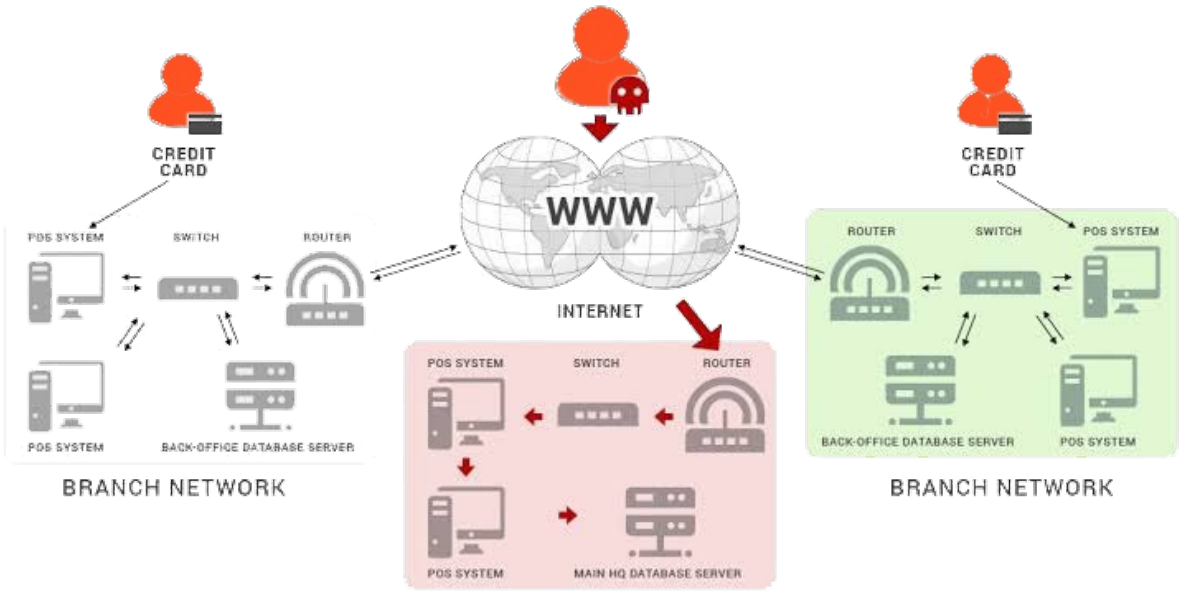
8. Application Level Attacks: Application-level attacks focus on attacking one – or a few – applications.



9. Multi-Vector Attacks: In multi-vector attacks, a group of tools and strategies are used to bring websites and servers offline.



10. Zero-Day DDoS: A “Zero Day” based attack to date has no patches.



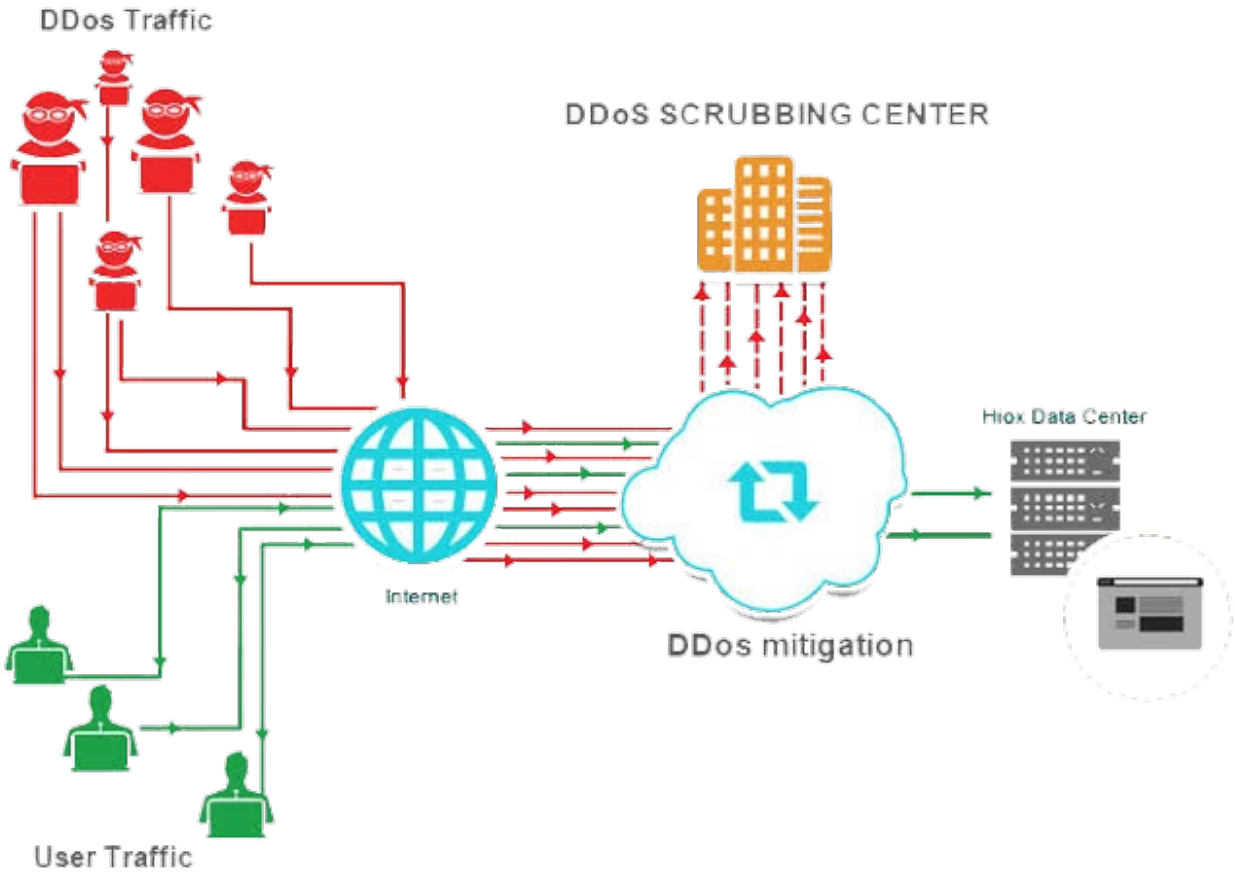
We have seen various DDoS attacks, and all of these can adversely affect your website's performance.

DDoS attack Tools

Various tools are available that can initiate a DDoS attack, some of the common ones are:

1. **HULK:** HTTP Unbearable Load King or HULK is created for research purpose is to initiate attacks on the webserver.
2. **Tor's Hammer:** Created for testing purposes, it helps initiate slow post-attack.
3. **Slowloris Tool:** It helps to make the server down.
4. **LOIC:** Low Orbit Ion Cannon is a free and popular tool that is easy to use.
5. **Xoic:** it is a DDoS tool for small websites.
6. **DDOSIM:** DDoS Simulator simulates the real DDoS attack on the website and network.
7. **RUDY:** R-U-Dead-Yet is a long-form field submission DDoS that initiates the attack through POST method

How to Protect Your Website From DDoS Attacks?



DDoS attacks have become very common in the past few years. India is Among Top 10 Sources for DDoS Attacks in Q2 2015: Akamai

Even the biggest brand has been under the most exceptional cyber-attacks in the history of the internet.

1. Create an Action Plan in Advance

Precaution is always better than cure; prepare an action plan that helps mitigate the DDoS attack risk to a large extent. Though it cannot guarantee 100% security for the risk but can help protect your website to a great extent.

2. Monitor Traffic Levels

Monitoring your traffic levels is another efficient way to protect your website from DDoS attacks. An unexpected and unusual traffic level should raise an alert.

3. Pay Attention to Connected Devices

Connected devices are an easy gateway for hackers to initiate a DDoS attack on your website/server. Keep keen attention to these devices. And for more protection keep changing their passwords regularly and switch them off, when not in use.

4. Ensure You Have Extra Bandwidth

Have an extra bandwidth, it will give a scope to accommodate extra traffic and will give you time to fight the attack.

5. Train Your Customers On Security

Educate your customers to take care of their security. Ask them to follow cyber-security best practices to avoid any such risks.

6. Set up Secured VPS Hosting

Just to save a few bucks, don't go for the lowest price hosting plans. Set up a secured VPS hosting that will provide you with DDoS protection and will reduce the chances of the attack.

7. Drop Packets from Obvious Sources of Attack

Ensure that you have proper arrangements to stop traffic from false sources. Instruct router to drop packets obvious attack source IPS.

8. Purchase a Dedicated Server

Have your own dedicated hosting server to have more bandwidth, control over security, and countless resources.

9. Block Spoofed IP Addresses

Blocking spoofed IP addresses is another way to prevent DDoS attacks.

10. Install Patches and Updates Frequently

Installing updates lessens the DDoS attack risk.

11. Use Proxy Protection

Use of proxy can give you extra protection from DDoS attacks; hence consider it as one of your rescuers.

12. Set up RST Cookies

RST cookies are a good way to protect your website from DDoS attacks.

What's DDoS threat intelligence map and what's it used for?

None can predict the timing of DDoS attacks. All you can do in this kind of situation is to trace the locations where the weaponry is stored in. By knowing so, you can build a defense system that's more effective than anything. The map should have millions of entries that can be changed dynamically to make the map proactive.

The Crime and Punishment of DDoS attacks

Who are behind this devastating attack? Statistics state that most teenagers are behind d such hideous attacks and they are raking millions of dollars as we speak.

What's the punishment for a person who's doing the DDoS attack? First, you need to trace the DDoS attack to put the person who is behind the heinous crime behind bars.

There is another concept behind the attack. Most of the times DDoS attack acts as a mask to perform Phishing and pharming, the most lucrative forms of attack.

> **Know about : Major Cyber Attacks on India (Alarming News)**

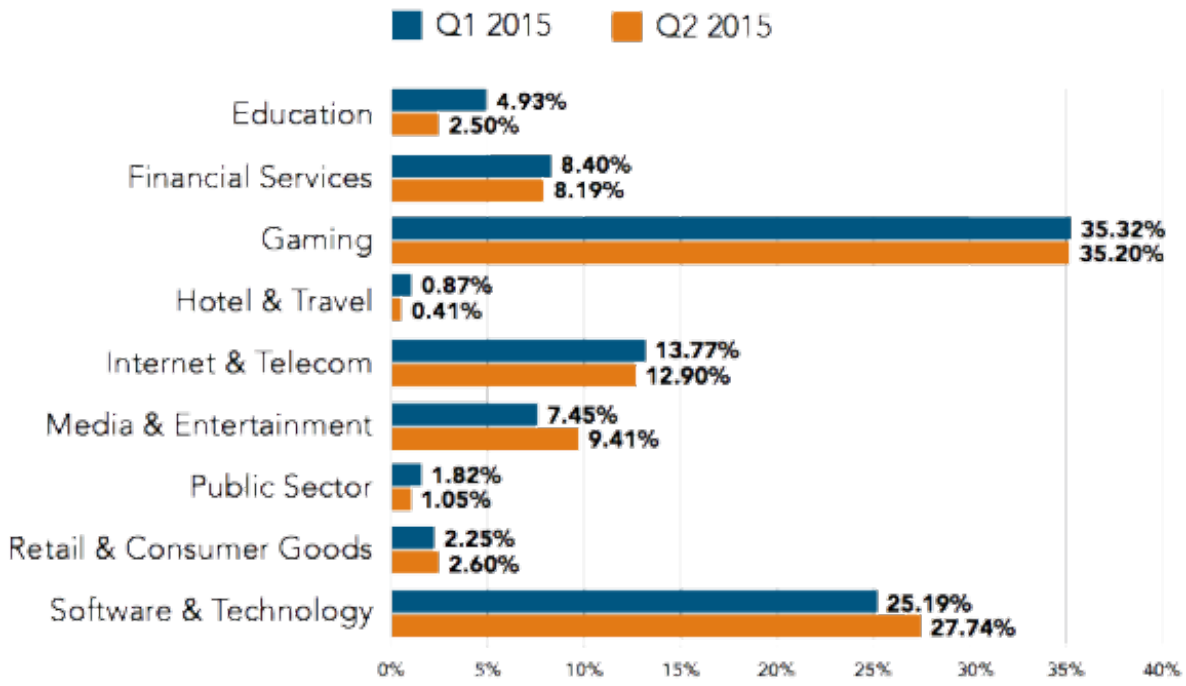
DDoS attacks usually happen by flooding and it's performed by botnets, thousands of them at a time. Owing to the same it's hard to trace such attacks.

However, Just like any other computer and internet-related offenses, performing DDoS attacks with bad intentions punishable under the law of respective countries.

DDoS Attack Frequency by Industry

DDoS attacks are indeed devastating. But wich industry is prone to frequent DDoS attacks?

Have a look

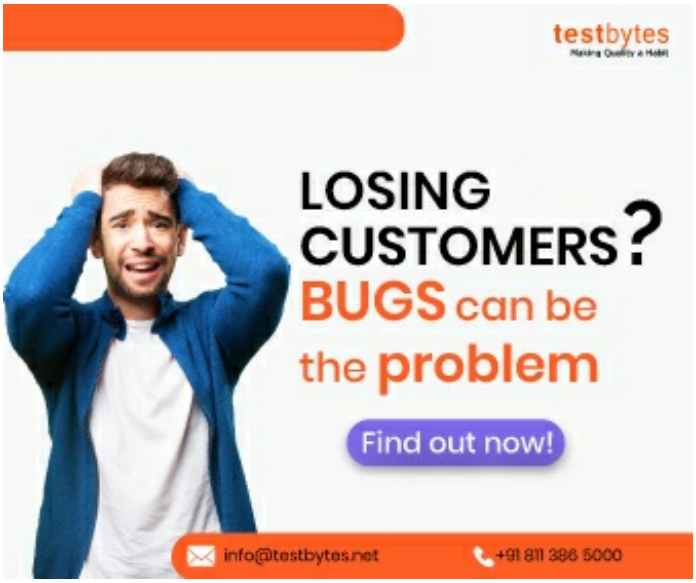


How to identify DDoS attacks?

the worst part about this kind of attack is that there won't be any prior warning before the attack. Since the attack is mainly performed as a masking mechanism to perform another type of attack, unpredictability is the key behind such attacks.

usually what happens is that a website will be bombarded with traffic to an extent where the website will be down for hours or even days.

However, there are certain things you need to monitor that can reveal the attack



For instance,

- An IP address that makes a huge volume of requests at a time
- 503 error

- TTL (time to live) on a ping request
- Slowness issues
- Huge spike in traffic

Conclusion:

Cyber attacks are a big threat to the digital world. There are various types of cyberattacks that possess a threat to the security of individuals /businesses to present online. One such type of attack is DDoS. It overburdens the website /server and makes it impossible for businesses to deliver their services through digital mediums to their customers.