The Anatomy of a DDoS Attack
Dissecting Large Scale Internet Attacks
// What is a DDoS Attack?
DDoS Attacks Are Like Traffic Jams
Elements of a DDoS Attack

- Malicious attempt to disrupt normal traffic
- Overwhelm target with flood
- Utilize multiple compromised systems
- Motive can be political, social, or financial
- Targets in every industry

Subject: ddos attack

Hi!

If you dont pay 8 bitcoin until 17. january your network will be hardly ddosed! Our attacks are super powerfull. And if you dont pay until 17. january ddos attack will start and price to stop will double!

We are not kidding and we will do small demo now on [XXXXXXXX] to show we are serious.

Pay and you are safe from us forever.

OUR BITCOIN ADDRESS: [XXXXXXXX]

Dont reply, we will ignore! Pay and we will be notify you payed and you are safe.

Cheers!
Cloudflare engineers have witnessed some of the largest DDoS attacks in history unfold.

400Gbps: Winter of Whopping Layer 3 DDoS Attacks

In the winter of 2016, we mitigated the largest Layer 3 DDoS attack to date. We were not only able to mitigate it, but accurately measure and analyze it as well.

Details Behind a 400Gbps NTP Amplification Attack

DDoS attacks take all shapes and forms. In this 400Gbps amplification attack, an attacker used 4,529 NTP servers to amplify an attack from a mere 87Mbps source server.

The DDoS Attack That Almost Broke the Internet

Cloudflare has been fighting historic DDoS attacks for over 5 years. Back in 2013, the 120Gbs on Spamhaus was a “big” attack, and we were able to keep their website online.
The Evolution of DDoS

DDoS Attacks are evolving in size and complexity

- **2012**: 300 Gbps // Volumetric Layer 3/4
- **2013**: 400 Gbps // NTP Reflection
- **2016**: 1 Tbps // IoT Botnet Layer 7 Attack

(C) Cloudflare
How does a DDoS attack work?
Botnet = Robot + Network
Botnet Operations

- Attacker sends instructions to botnet
- Bots send requests to target
- Target server or network overflows capacity
- Difficult to separate good from bad traffic
What are common types of DDoS attacks?
Open Systems Interconnection (OSI) Model

1. **PHYSICAL LAYER**
   - Transmits raw bit stream over the physical medium

2. **DATALINK LAYER**
   - Defines the format of data on the network

3. **NETWORK LAYER**
   - Decides which physical path the data will take

4. **TRANSPORT LAYER**
   - Transmits data using transmission protocols including TCP and UDP

5. **SESSION LAYER**
   - Maintains connections and is responsible for controlling ports and sessions

6. **PRESENTATION LAYER**
   - Ensures that data is in a usable format and is where data encryption occurs

7. **APPLICATION LAYER**
   - Human-computer interaction layer, where applications can access the network services
Layers of DDoS

All attacks degrade availability and performance of applications, websites, and APIs

Types of DDoS Attack Traffic

- **Volumetric DNS Flood**
  - Bots
  - DNS Server
  - Application

- **Amplification (Layer 3 & 4)**
  - Bots
  - DNS Server
  - Server

- **HTTP Flood (Layer 7)**
  - Bots
  - HTTP
  - Application/Login
Volumetric Attacks

DNS Amplification Attack

A DNS Amplification attack is like if someone were to call a restaurant and say “I’ll have one of everything, please call me back and tell me my whole order,” where the callback phone number they give is the target’s number. With very little effort, a long response is generated.
Protocol Attacks

A SYN Flood Attack is analogous to a worker in a supply room receiving requests from the front of the store. The worker receives a request, goes and gets the package, and waits for confirmation before bringing the package out front. The worker then gets many more package requests without confirmation until they can’t carry any more packages, become overwhelmed, and requests start going unanswered.
Application Layer Attacks

HTTP Flood Attack

This attack is similar to pressing refresh in a web browser over and over on many different computers at once – large numbers of HTTP requests flood the server, resulting in denial-of-service.
How are DDoS attacks mitigated?
Black Hole Routing

- Drop traffic from the network
Rate Limiting

- Limiting requests over a time period
Web Application Firewall (WAF)

- Filtering L7 requests with rules
Anycast Network Diffusion

- Scatter attack traffic across distributed servers
// What is a UDP flood attack?
UDP Flood Attack

Normal UDP Traffic

1. Server checks for running programs listening at a specified port.

2. If no programs are receiving packets, server responds with a ICMP (ping) packet to inform sender that the destination was unreachable.
UDP Flood Attack

As a result of the targeted server utilizing resources to check and then respond to each received UDP packet, the target’s resources can become quickly exhausted when a large flood of UDP packets are received, resulting in denial-of-service to normal traffic.
What is a SYN flood attack?
Normal TCP Connection

1. Client sends a SYN packet to the server in order to initiate the connection.

2. Server responds with a SYN/ACK packet, in order to acknowledge the communication.

3. Client returns an ACK packet to acknowledge the receipt of the packet from the server. After completing this sequence of packet sending and receiving, the TCP connection is open and able to send and receive data.
SYN Flood Attack

1. Attacker sends high volume of SYN packets to the targeted server, often with spoofed IP addresses.

2. Server responds to each connection request and leaves an open port ready to receive the response.

3. While the server waits for the final ACK packet, attacker sends more SYN packets. Each new SYN packet causes the server to maintain new open port connection, and once all the available ports have been utilized the server is unable to function normally.
SYN Flood Attack

SYN Flood Mitigations
1. Increasing Backlog queue.
2. Recycling the Oldest Half-Open TCP connection
3. SYN cookies
4. Using a Proxy Service
What is a DNS Flood?
DNS Flood Attack

DNS Flood Mitigation

DNS floods represent a change from traditional amplification based attack methods. With easily accessible high bandwidth botnets, attackers can now target large organizations. Until compromised IoT devices can be updated or replaced, the only way to withstand these types of attacks is to use a very large and highly distributed DNS system that can monitor, absorb, and block the attack traffic in realtime.
Cloudflare DDoS Protection

- 10MM Requests/second
- 10% Internet requests everyday
- 38% of all DNS queries
- 115+ Data centers globally
- 10+ Tbps Network capacity
- 2.5B Monthly unique visitors
- 7M+ websites, apps & APIs in 150 countries
// Thank you!

**Presenter**
Name: Suzanne Aldrich
Email: suzanne@cloudflare.com
Twitter: @SuzanneAldrich