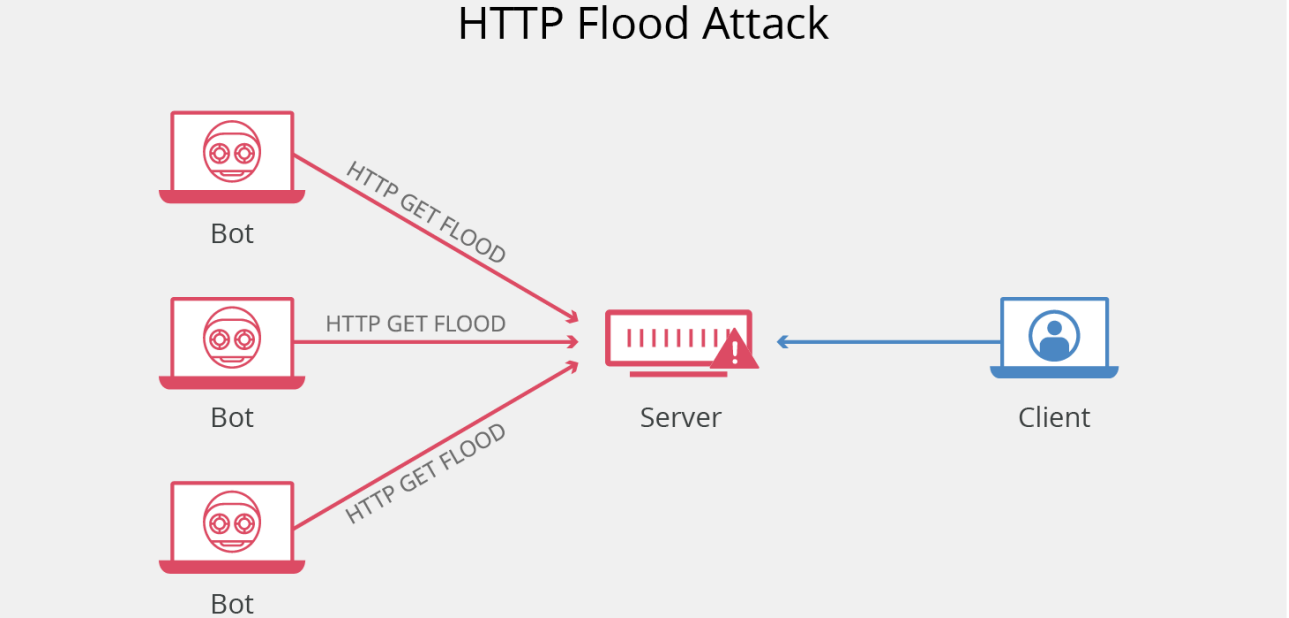
HTTP flood DDoS attack

Archived: 2026-04-06 01:55:29 UTC

What is an HTTP flood DDoS attack?

An HTTP flood attack is a type of volumetric distributed denial-of-service (DDoS) attack designed to overwhelm a targeted server with HTTP requests. Once the target has been saturated with requests and is unable to respond to normal traffic, denial-of-service will occur for additional requests from actual users.



How does an HTTP flood attack work?

HTTP flood attacks are a type of “layer 7” DDoS attack. Layer 7 is the application layer of the OSI model, and refers to internet protocols such as as HTTP. HTTP is the basis of browser-based internet requests, and is commonly used to load webpages or to send form contents over the Internet. Mitigating application layer attacks is particularly complex, as the malicious traffic is difficult to distinguish from normal traffic.

In order to achieve maximum efficiency, malicious actors will commonly employ or create botnets in order to maximize the impact of their attack. By utilizing many devices infected with malware, an attacker is able to leverage their efforts by launching a larger volume of attack traffic.

There are two varieties of HTTP flood attacks:

1. **HTTP GET attack** - in this form of attack, multiple computers or other devices are coordinated to send multiple requests for images, files, or some other asset from a targeted server. When the target is inundated with incoming requests and responses, denial-of-service will occur to additional requests from legitimate traffic sources.

2. **HTTP POST attack** - typically when a form is submitted on a website, the server must handle the incoming request and push the data into a persistence layer, most often a database. The process of handling the form data and running the necessary database commands is relatively intensive compared to the amount of processing power and bandwidth required to send the POST request. This attack utilizes the disparity in relative resource consumption, by sending many post requests directly to a targeted server until it's capacity is saturated and denial-of-service occurs.

How can an HTTP flood be mitigated?

As mentioned earlier, mitigating layer 7 attacks is complex and often multifaceted. One method is to implement a challenge to the requesting machine in order to test whether or not it is a bot, much like a captcha test commonly found when creating an account online. By giving a requirement such as a JavaScript computational challenge, many attacks can be mitigated.

Other avenues for stopping HTTP floods include the use of a web application firewall (WAF), managing an IP reputation database in order to track and selectively block malicious traffic, and on-the-fly analysis by engineers. Having an advantage of scale with over 20 million Internet properties allows Cloudflare the ability to analyze traffic from a variety of sources and mitigate potential attacks with quickly updated WAF rules and other mitigation strategies to eliminate application layer DDoS traffic.

Cloudflare DDoS Protection
