What is Application Layer Attack?

Application Layer Attack - application layer attacks or Layer 7 (L7) DDoS attacks refer to a type of malicious behavior designed to target the 'top' layer in the OSI model where it occurs. Common Internet requests like HTTP GET and HTTP POST.

These layer 7 attacks, in contrast to network layer attacks like DNS Amplification, are particularly effective because they consume server resources, in addition to network resources.

Application Layer Attack targets the 'top' layer in the OSI model where common Internet requests like HTTP GET and HTTP POST occur.

How does Application Layer Attack work?

The fundamental effectiveness of most DDoS attacks comes from the difference between the amount of resources needed to perform an attack versus the amount of resources needed to process or mitigate the attack. While this still happens with L7 attacks, the effect of affecting both the targeted host and the network requires less total bandwidth to achieve the same disruption effect. An application layer attack produces more damage with less total bandwidth.

To explore why this is the case, consider the relative resource consumption difference between a client making a request and a server responding to the request. When a user submits a request to log into an online account such as a Gmail account, the amount of data and resources that the user's computer must use is minimal and does not match the amount of resources used in the process of checking login credentials, loading relevant user data from a database, then resubmit a response containing the requested website.

Even without login information, many times the server receives a request from the client to do database queries or other API calls to create a web page. When this discrepancy is increased due to multiple devices targeting a

single web property, as in a botnet attack, the effect can overwhelm the targeted server, leading to denial of translation. service against legitimate traffic. In many cases, simply targeting an API with an L7 attack is enough to bring the service offline.

Why is it so difficult to prevent application layer DDoS attacks?

It is very difficult to distinguish between attack traffic from normal traffic, especially in the case of an application layer attack, such as a botnet that performs an HTTP Flood attack against a victim's server. Because every bot in the botnet makes seemingly legitimate network requests, the traffic is not tampered with and can emerge from 'normal' origin.

Application layer attacks require an adaptive strategy that includes the ability to limit traffic based on specific sets of rules that can change frequently. Properly configured tools like WAF can minimize the amount of bogus traffic being sent to the root server, greatly reducing the impact of the DDoS attack attempt.

With other attacks like SYN Flood or NTP Amplification, strategies can be used to reduce traffic quite effectively, as long as the network itself has the bandwidth to receive them. Unfortunately, most networks cannot withstand a 300Gbps host amplification attack, and there are even few networks that can route and serve the volume of application layer requests that an L7 attack can. create more.