Distributed Denial-of-Service (DDoS) Attack - Technical Description

Description

A Distributed Denial-of-Service (DDoS) attack attempts to make a server or network resource unavailable to legitimate users by flooding it with overwhelming traffic from multiple sources. In network layer DDoS attacks, the network pipes get fully clogged, making the network unavailable. In Application Layer DDoS attacks, the network remains available, but the application and server resources, such as CPU, memory or disk space, are exhausted.

Since intermediate security devices can easily blacklist IP addresses, DDoS attacks require the attacker to build a network of computers to generate traffic to overwhelm the targeted server from multiple different IP addresses. The network, called a “botnet,” is created by exploiting vulnerabilities in PCs via drive-by-downloads, phishing, spear phishing or other attacks. The compromised computers (called "zombies") can be controlled remotely by the attacker and used as a legion to launch an attack against any target resource.

DDoS attacks can be categorized into three types:

- **Volumetric Attacks** - Volumetric DDoS attacks saturate the bandwidth of the attacked website, leaving applications and services nonfunctional with no available bandwidth to utilize. Volumetric attacks are Layer 3 / 4 / 7 DDoS attacks that target the network, transport and application layers in the OSI Model. These attacks include: UDP floods, ICMP floods, high bandwidth web traffic from bots, etc.
- **Protocol Attacks** – Protocol attacks consume the actual server resources, or connection state tables that are present in load balancers, firewalls, application servers and other infrastructure components. Protocol attacks include: SYN floods, Ping of Death, fragmented packets attack, etc.
- **Application Attacks** – Application attacks overload specific aspects/elements of an application or service. These attacks can be effective with a single attacking machine generating a low traffic rate, where the traffic resembles legitimate website traffic, making them difficult to detect and mitigate. Application attacks are also known as Layer 7 attacks. These attacks include: Slowloris, R-U-Dead-Yet (RUDY), Apache Range Header attack, etc.

Effects

If these attacks succeed at overloading the system with high traffic volume and consuming critical resources such as bandwidth, disk storage, CPU memory, database connections, etc., the attacker can prevent legitimate users from using the system, When the business and brand depend on the Internet, an extended downtime could be very costly. E-criminals commonly demand ransom to stop DDoS attacks. Hacktivists and cyber terrorists, on the other hand, normally indulge in DDoS attacks as a revenge for perceived injustice or to garner publicity.

Method

For application layer DDoS attacks, bots can be designed to send/receive slow HTTP/HTTPS requests by slowly sending only part of an HTTP/HTTPS request. For example:

- HTTP Headers
- HTTP Content
- URL Parameters

Because these requests appear legitimate, they avoid triggering protocol timeouts, and are hard to detect.

Example

DDoS attack sending slow HTTP Request Slow Header/Slow Content:

==========

Slow Header:

POST /index.html HTTP/1.0

Content-Length: 5

Header1: Value1

[sleep for few seconds]

Header1: Value1

...

Slow Content:

POST /index.html HTTP/1.0

Content-Length: 5000

B [sleep for few seconds] a [sleep for few seconds] r [sleep for few seconds] r [sleep for few seconds] a [sleep for few seconds] c [sleep for few seconds] u [sleep for few seconds] d [sleep for few seconds] a [sleep for few seconds] .....

Prevention

Slowloris or RUDY attacks are difficult to detect, because they are legitimate requests to the server. At times, genuine requests from real users are slow. The Barracuda Web Application Firewall has the capability to detect and prevent Slowloris attacks, using an advanced slowloris detection algorithm, and recognize the pattern of slow requests/responses from attackers, preventing it from degrading web application performance.

See Also

CWE 941, CWE 400, OWASP

Barracuda Active DDoS Prevention Service