What Is a Distributed Denial of Service (DDoS) Attack?

blog.netwrix.com/2021/08/18/ddos-atttack

Kevin Joyce

The term DDoS attack refers to a malicious actor or group of actors intentionally trying to overwhelm a victim's computer network with traffic. The large influx of network traffic being directed at the target can cause serious issues for legitimate traffic, such as regular users who need to access websites, data or services.

Everyone from gamer sites to large enterprises fears the threat of distributed denial of service attacks. So, how can a malicious actor generate enough traffic to slow or even paralyze a system? Botnets. A botnet is a group of internet devices or systems that have been compromised by malicious actors. When the attackers want to perform a DDoS attack, they instruct all members of the botnet to send traffic to the target.

Handpicked related content:

[Free Guide] Network Security Best Practices

DDoS Attack Example

Some of the most notable DDoS attacks leveraged a botnet created by using the Mirai malware to compromise devices running Linux (routers, network-attached security cameras and other IoT devices). One specific attack was against Rutgers University; it prevented students from accessing the internet for an extended period of time. Rutgers allegedly spent over $1,000,000 to recover from the attack and harden their security posture.

DDoS Attack Types

There are a few different of DDoS attacks, including the following:

Flooding

Flooding attacks attempt to send so much traffic to a system or network that it overwhelms the service. There are three common types of flooding attacks based on the protocol they use:

- **User Datagram Protocol (UDP)** — Packets are sent to random ports on a system, which causes the system to check for services or applications listening on the port, determine that there isn't one, and send back a response. This waste of resources can cause issues with the services or applications the system is hosting.
- **Internet Control Message Protocol (ICMP)** — Pings are sent to a system in an extremely rapid manner. Trying to respond to all the requests can hurt the performance of the system.

- **Hypertext Transfer Protocol (HTTP)** — An attacker queries a web server or application with a high number of expensive interactions, rendering the web server unusable.

Ping of Death

In a Ping of Death attack, an attacker sends ping requests in way similar to an ICMP flood attack, but the ping itself is a malicious set of data. This attack abuses the fact that large packets are sent in chunks; when those chunks are re-assembled, they can be malicious and exploit vulnerabilities to cause systems to crash.

DNS Amplification

A DNS amplification attack exploits vulnerabilities in domain name system (DNS) servers to turn the attacker's small queries into much larger payloads that can diminish available bandwidth and overwhelm the server.

Handpicked related content:

Top 10 Most Common Types of Cyber Attacks

DDoS vs DoS

The difference between a DDoS attack and a denial of service (DoS) attack is scale. A DDoS attack comes from multiple sources, often a botnet. In a DoS attack, a single source is used to attempt to overwhelm a target system or network, so DoS attacks generally have less of an impact.

DDoS FAQ

1. How can an organization spot a DDoS attack?

To identify DDoS attacks, you must understand what constitutes normal traffic in your environment. The more you know about what usually occurs, the easier it is to spot that something is amiss. Some things to pay attention to include:

- Traffic coming from a lot of abnormal sources, or a lot of traffic from a single source that you normally don't receive traffic from
- An unusual increase in traffic to a specific system
- Other abnormal traffic patterns

2. How long does a DDoS attack last?

A DDoS attack can last as long as an attacker is able to expend resources sending requests to your system or network. There have been DDoS attacks that lasted minutes, hours, days and even weeks.

3. What should an organization do after a DDoS attack?

The most important thing to do after a DDoS attack is to analyze it is carefully. Understanding how it occurred can help you determine how to detect attacks in the future and prevent your systems from being overwhelmed. Questions you may want to ask yourself include:

- What type of attack was used?
- How long did it last?
- Which systems were targeted?

Also review the impact of the attack on your business or service, including which customers or users were affected and for how long. Quantifying the damage in financial terms can help you make decisions about how much attention and budget to spend on preventing future attacks.

Kevin Joyce
Senior Technical Product Manager at Netwrix. Kevin is passionate about cyber-security and holds a Bachelor of Science degree in Digital Forensics from Bloomsburg University of Pennsylvania.