DDoS

**What is a DDoS Attack?**

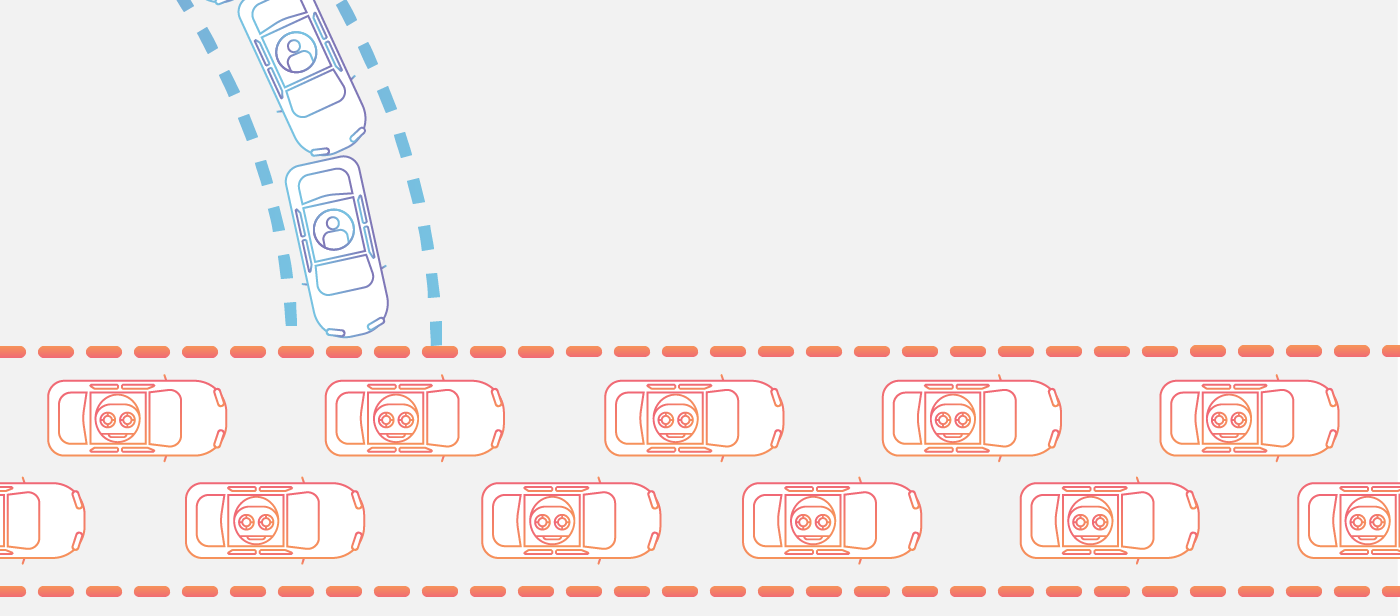
A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like a traffic jam clogging up with highway, preventing regular traffic from arriving at its desired destination.

**DOS VS. DDOS**

The differences between regular and distributed denial of service assaults are substantive. In a DoS attack, a perpetrator uses a single Internet connection to either exploit a software vulnerability or flood a target with fake requests—usually in an attempt to exhaust server resources (e.g., RAM and CPU).

On the other hand, distributed denial of service (DDoS) attacks are launched from multiple connected devices that are distributed across the Internet. These multi-person, multi-device barrages are generally harder to deflect, mostly due to the sheer volume of devices involved. Unlike single-source DoS attacks, DDoS assaults tend to target the network infrastructure in an attempt to saturate it with huge volumes of traffic.

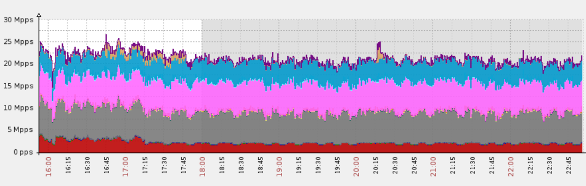
DDoS attacks also differ in the manner of their execution. Broadly speaking, denial of service attacks are launched using [homebrewed scripts or DoS tools](https://www.incapsula.com/ddos/ddos-attack-scripts.html) (e.g., [Low Orbit Ion Canon](https://www.incapsula.com/ddos/attack-glossary/low-orbit-ion-cannon.html)), while DDoS attacks are launched from botnets — large clusters of connected devices (e.g., cellphones, PCs or routers) infected with malware that allows remote control by an attacker.



**DENIAL OF SERVICE ASSAULT TYPES:**

DoS attacks can be divided into two general categories:

1)Application layer attacks (a.k.a., layer 7 attacks) can be either DoS or DDoS threats that seek to overload a server by sending a large number of requests requiring resource-intensive handling and processing. Among other attack vectors, this category includes [HTTP floods](https://www.incapsula.com/ddos/attack-glossary/http-flood.html), slow attacks (e.g., [Slowloris](https://www.incapsula.com/ddos/attack-glossary/slowloris.html" \t "_blank) or [RUDY](https://www.incapsula.com/ddos/attack-glossary/rudy-r-u-dead-yet.html)) and [DNS query flood](https://www.incapsula.com/ddos/attack-glossary/dns-flood.html) attacks.

Gaming website hit with a massive DNS flood, peaking at over 25 million packets per second

The size of application layer attacks is typically measured in requests per second (RPS), with no more than 50 to 100 RPS being required to cripple most mid-sized websites.

2. Network layer attacks (a.k.a., layer 3–4 attacks) are almost always DDoS assaults set up to clog the “pipelines” connecting your network. Attack vectors in this category include [UDP flood](https://www.incapsula.com/ddos/attack-glossary/udp-flood.html), [SYN flood](https://www.incapsula.com/ddos/attack-glossary/syn-flood.html), [NTP amplification](https://www.incapsula.com/ddos/attack-glossary/ntp-amplification.html) and [DNS amplification](https://www.incapsula.com/ddos/attack-glossary/dns-amplification.html) attacks, and more.

Any of these can be used to prevent access to your servers, while also causing severe operational damages, such as account suspension and massive overage charges.

DDoS attacks are almost always high-traffic events, commonly measured in gigabits per second (Gbps) or packets per second (PPS). The largest network layer assaults can exceed 200 Gbps; however, 20 to 40 Gbps are enough to completely shut down most network infrastructures.

**How does a DDoS attack work?**

A DDoS attack requires an attacker to gain control of a network of online machines in order to carry out an attack. Computers and other machines (such as IoT devices) are infected with [malware](https://www.cloudflare.com/learning/ddos/glossary/malware/), turning each one into a bot (or zombie). The attacker then has remote control over the group of bots, which is called a [botnet](https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/).

Once a botnet has been established, the attacker is able to direct the machines by sending updated instructions to each bot via a method of remote control. When the [IP address](https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/) of a victim is targeted by the botnet, each bot will respond by sending requests to the target, potentially causing the targeted server or network to overflow capacity, resulting in a [denial-of-service](https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/) to normal traffic. Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.

**What are common types of DDoS attacks?**

Different DDoS attack vectors target varying components of a network connection. In order to understand how different DDoS attacks work, it is necessary to know how a network connection is made. A network connection on the Internet is composed of many different components or “layers”. Like building a house from the ground up, each step in the model has a different purpose. The [OSI model](https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/), shown below, is a conceptual framework used to describe network connectivity in 7 distinct layers.

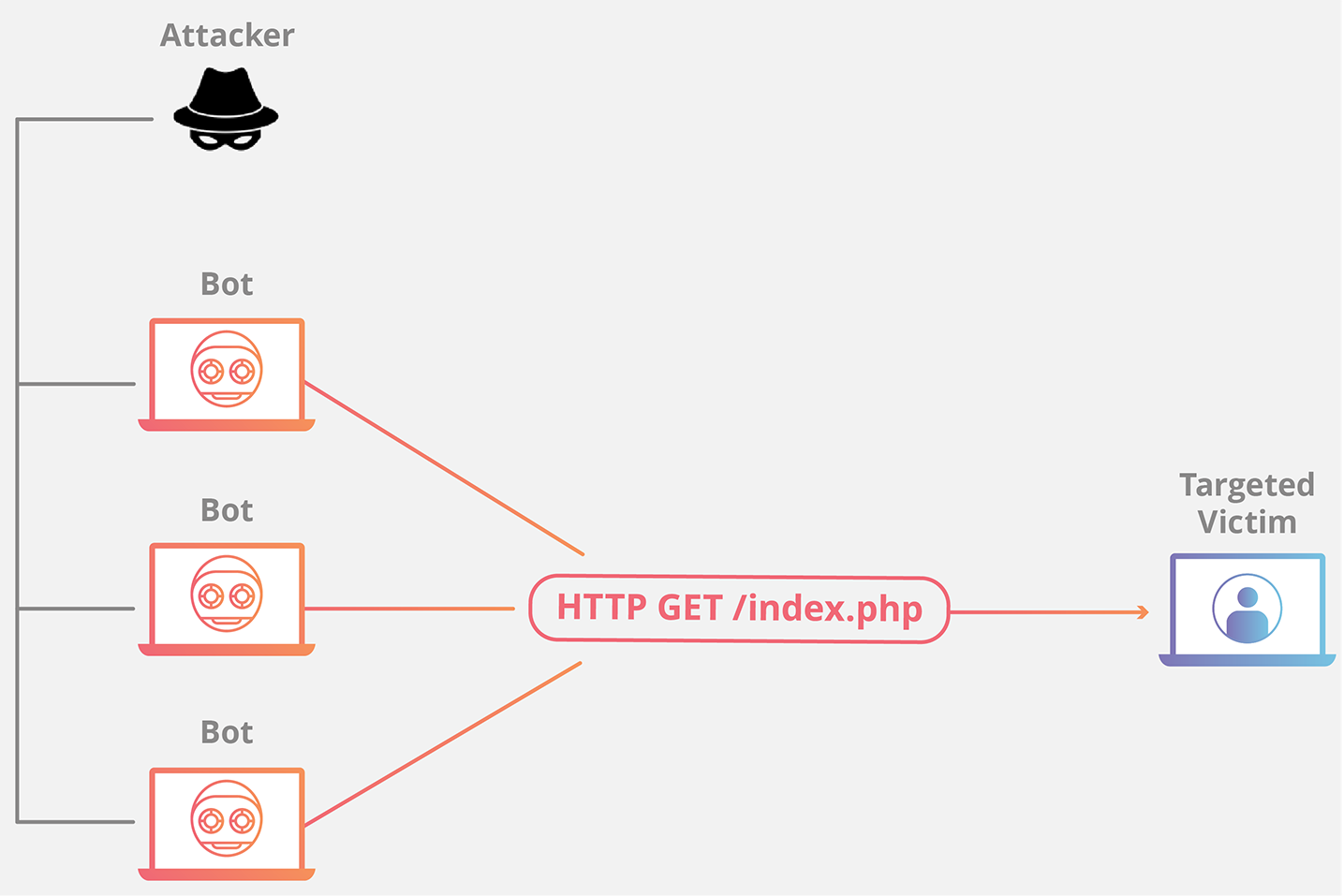
While nearly all DDoS attacks involve overwhelming a target device or network with traffic, attacks can be divided into three categories. An attacker may make use one or multiple different attack vectors, or cycle attack vectors potentially based on counter measures taken by the target.

**1)Application Layer Attacks**

The Goal of the Attack:

Sometimes referred to as a layer 7 DDoS attack (in reference to the 7th layer of the OSI model), the goal of these attacks is to exhaust the resources of the target. The attacks target the layer where web pages are generated on the server and delivered in response to [HTTP](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http) requests. A single HTTP request is cheap to execute on the client side, and can be expensive for the target server to respond to as the server often must load multiple files and run database queries in order to create a web page. Layer 7 attacks are difficult to defend as the traffic can be difficult to flag as malicious.

Application Layer Attack Example:



HTTP Flood

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.

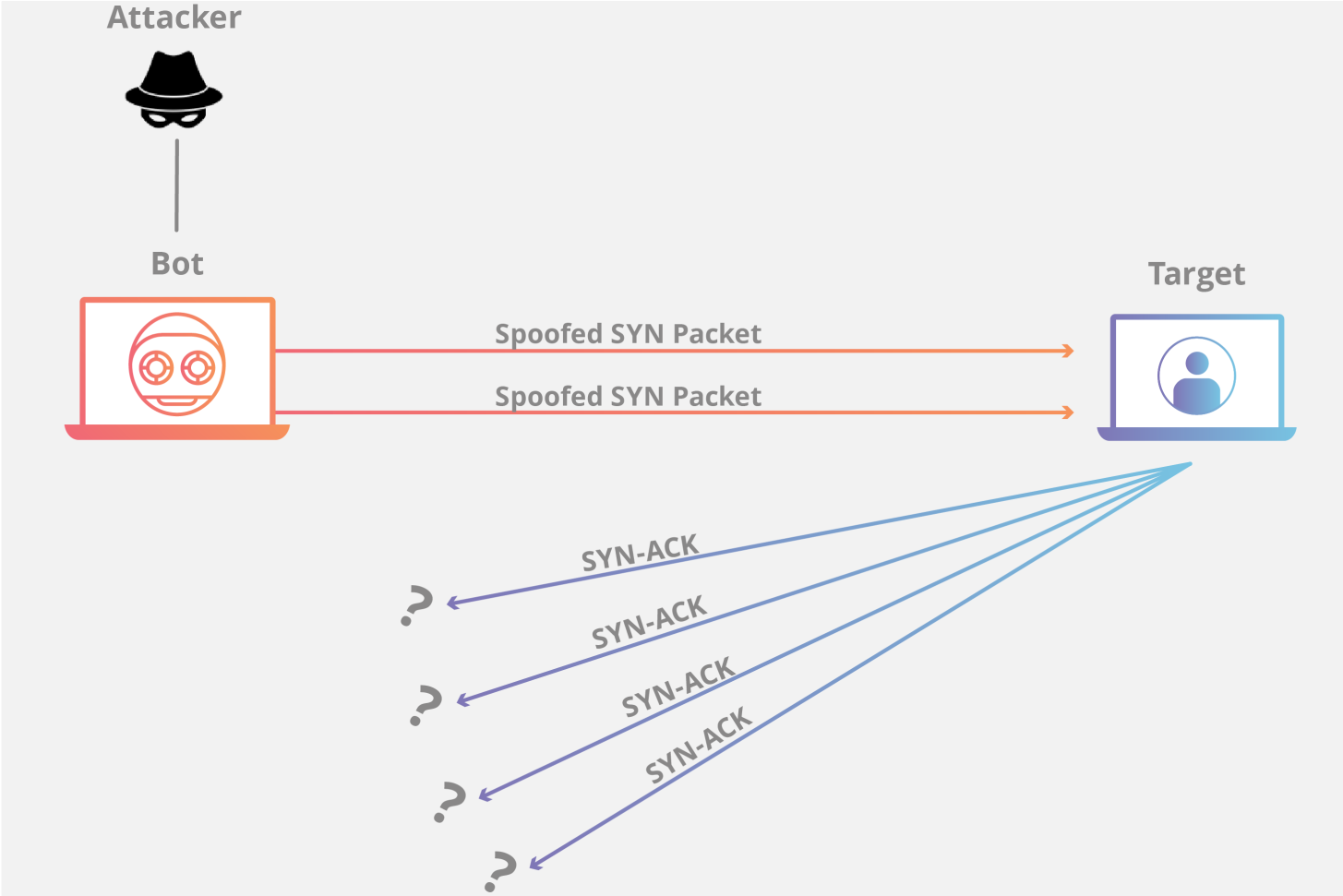
This type of attack ranges from simple to complex. Simpler implementations may access one URL with the same range of attacking IP addresses, referrers and user agents. Complex versions may use a large number of attacking IP addresses, and target random urls using random referrers and user agents.

**2)Protocol Attacks**

The Goal of the Attack:

Protocol attacks, also known as a state-exhaustion attacks, cause a service disruption by consuming all the available state table capacity of web application servers or intermediate resources like firewalls and load balancers. Protocol attacks utilize weaknesses in layer 3 and layer 4 of the protocol stack to render the target inaccessible.

Protocol Attack Example:



**3)SYN Flood**

[A SYN Flood](https://www.cloudflare.com/learning/ddos/syn-flood-ddos-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.

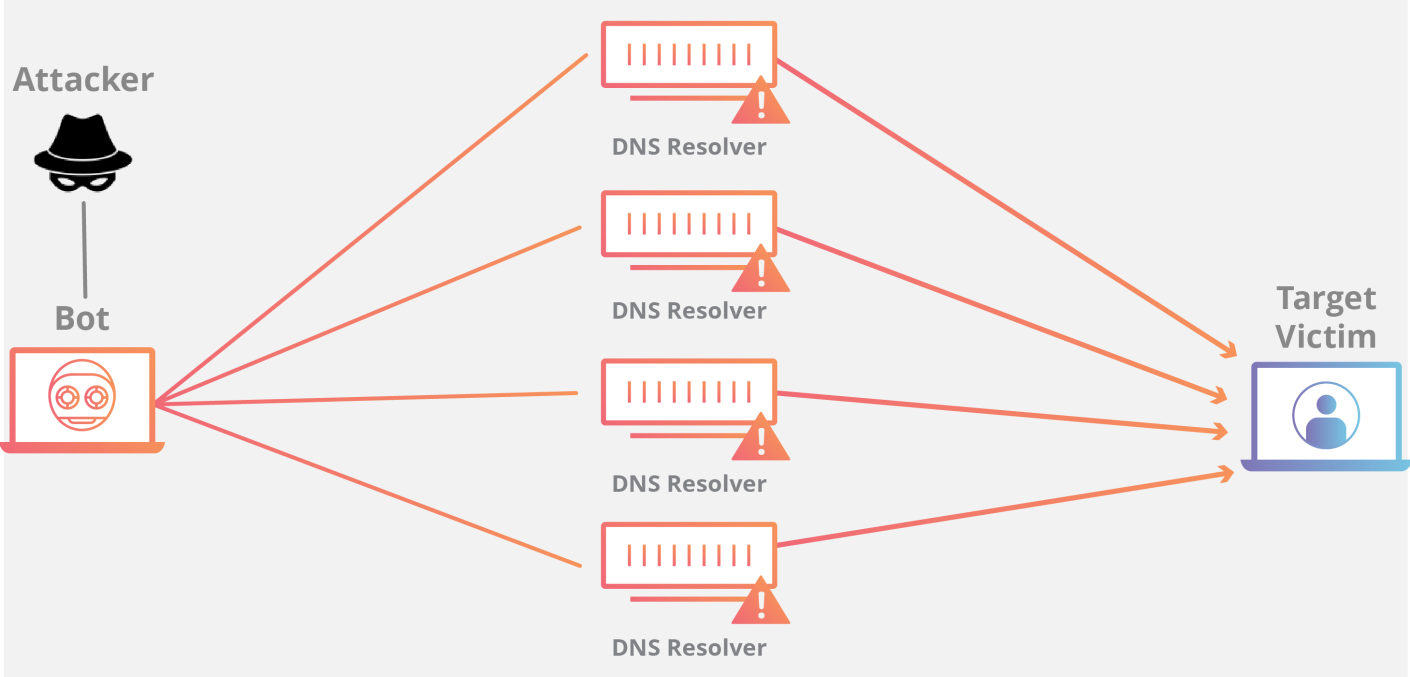
This attack exploits the [TCP handshake](https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/) by sending a target a large number of TCP “Initial Connection Request” SYN packets with [spoofed](https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/) source IP addresses. The target machine responds to each connection request and then waits for the final step in the handshake, which never occurs, exhausting the target’s resources in the process.

**4)Volumetric Attacks**

The Goal of the Attack:

This category of attacks attempts to create congestion by consuming all available bandwidth between the target and the larger Internet. Large amounts of data are sent to a target by using a form of amplification or another means of creating massive traffic, such as requests from a botnet.

**5)Amplification Example:**



**6)DNS Amplification**

A [DNS Amplification](https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-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.

By making a request to an open [DNS](https://www.cloudflare.com/learning/ddos/glossary/domain-name-system-dns/) server with a spoofed IP address (the real IP address of the target), the target IP address then receives a response from the server. The attacker structures the request such that the DNS server responds to the target with a large amount of data. As a result, the target receives an amplification of the attacker’s initial query.