¿Qué es un ataque DDoS?

Los ataques DDoS son una de las principales preocupaciones de la seguridad de Internet en la actualidad. Conoce cómo funcionan y cómo se pueden detener.

Metas de aprendizaje

Después de leer este artículo podrás:

- Definir un ataque DDoS
- Entender la estructura general de un ataque DDoS
- Diferenciar las tres categorías principales de ataques DDoS
- Conocer varias estrategias de mitigación de DDoS

CONTENIDO RELACIONADO

Mitigación de DDoS

Cómo lanzar un ataque DDoS | Herramientas de ataque DoS y DDoS

¿Qué es un ataque de denegación de servicio (DoS)?

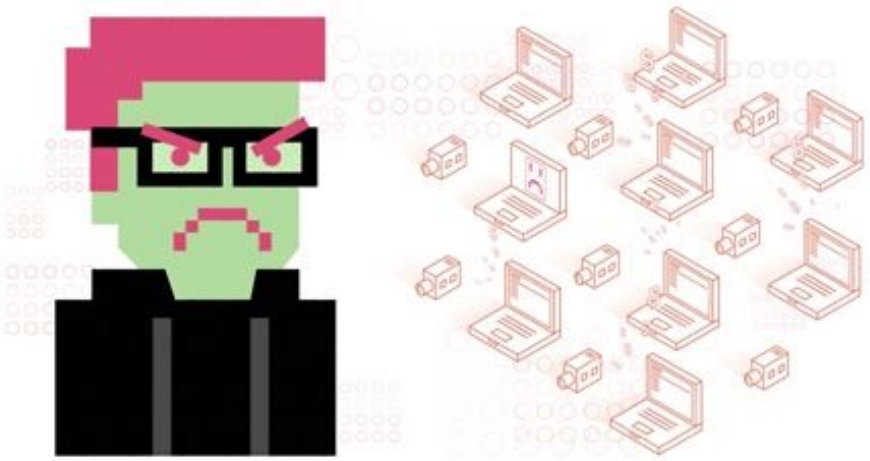
¿Qué es una red de robots (botnet) de DDoS?

¿Qué es la suplantación de IP?

¿Quieres saber más?

Copiar el enlace del artículo

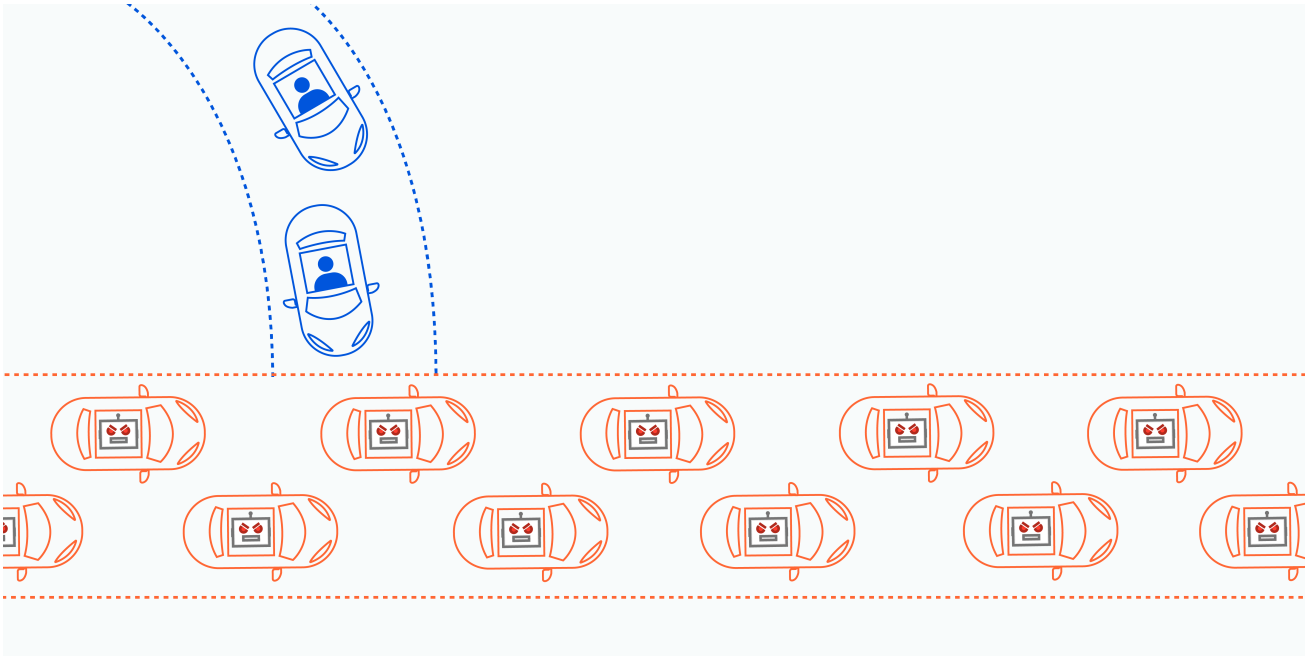
¿Qué es un ataque DDoS?



Un ataque de denegación de servicio distribuido (DDoS) es un intento malicioso de interrumpir el tráfico normal de un servidor, servicio o red determinada, sobrecargando el objetivo o su infraestructura asociada con una avalancha de tráfico de Internet.

La efectividad de los ataques DDoS reside en el uso de sistemas informáticos vulnerables desde los que se origina el tráfico de ataque. Entre los equipos afectados puede haber computadoras y otros recursos de red, tales como dispositivos IoT.

En términos generales, un ataque DDoS es como un atasco de tráfico que impide que llegues al destino deseado.



¿Cómo funciona un ataque DDoS?

Los ataques DDoS se llevan a cabo con redes de equipos conectados a Internet.

Estas redes constan de computadoras y otros dispositivos (como dispositivos IoT) que han sido infectados con malware, lo que permite a un atacante controlarlos de forma remota. Estos dispositivos individuales se denominan bots (o zombis), y un grupo de bots recibe el nombre de botnet o red de bots.

Una vez que se ha establecido una red de bots, el atacante puede dirigir un ataque enviando instrucciones remotas a cada bot.

Cuando el servidor o la red de una víctima es el blanco de la red de bots, cada bot envía solicitudes a la dirección IP del destino, lo que puede llegar a sobrecargar el servidor o la red y, por consiguiente, provocar una denegación de servicio al tráfico normal.

Debido a que cada bot es un dispositivo legítimo de Internet, puede resultar complicado disociar el tráfico de ataque del tráfico normal.

Cómo identificar un ataque DDoS

El indicio más claro de un ataque DDoS es la ralentización de un sitio o servicio, o la falta de acceso a estos. Sin embargo, el aumento legítimo del tráfico es otra de las causas que pueden generar problemas de rendimiento similares, de ahí la necesidad de seguir investigando. Las herramientas de análisis de tráfico pueden ayudarte a detectar algunas de estas señales de advertencia de un ataque DDoS:

- Cantidades sospechosas de tráfico procedentes de una única dirección IP o rango de IP.
- Una avalancha de tráfico de usuarios que comparten un mismo perfil de comportamiento como el tipo de dispositivo, la geolocalización o la versión del navegador web.
- Un aumento inexplicable de las solicitudes a una sola página o servidor.
- Patrones de tráfico raros como picos a deshoras o patrones que parecen anormales (por ejemplo, picos cada 10 minutos).

Hay otras señales más específicas de ataques DDoS que pueden variar según el tipo de ataque.

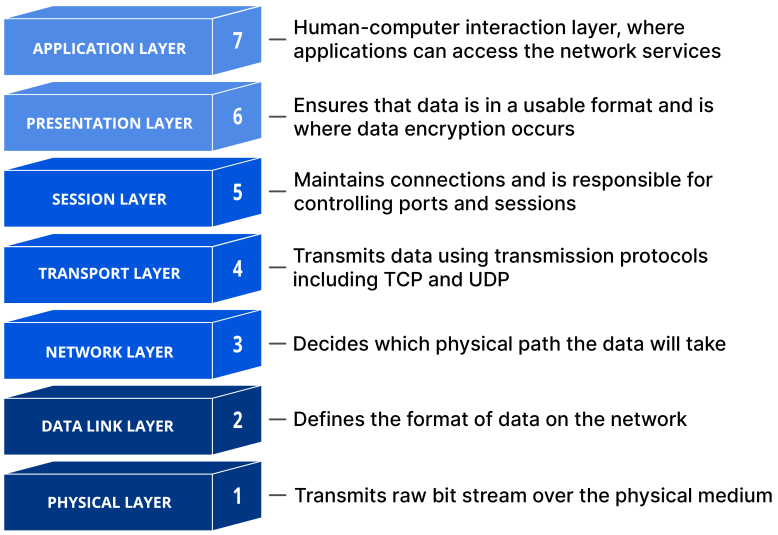
¿Cuáles son los tipos de ataques DDoS más

habituales?

Los diferentes vectores de ataques DDoS tienen como objetivo diversos elementos de una conexión de red. Para poder entender cómo funcionan los distintos ataques DDoS, es necesario saber cómo se realiza una conexión de red.

Una conexión de red en Internet está compuesta por muchos elementos o "capas" diferentes. Es como construir una casa desde sus cimientos, cada capa del modelo tiene un objetivo diferente.

El modelo OSI, que se muestra a continuación, es un marco conceptual utilizado para describir la conectividad de red en 7 capas distintas.



Si bien el objetivo de casi todos los ataques DDoS es sobrecargar un dispositivo o una red determinada con tráfico, estos ataques pueden dividirse en tres categorías. Un atacante puede utilizar uno o varios vectores de ataque diferentes, o bien repetir vectores de ataque en respuesta a las contramedidas adoptadas por el objetivo.

Ataques a la capa de aplicación

El objetivo del ataque:

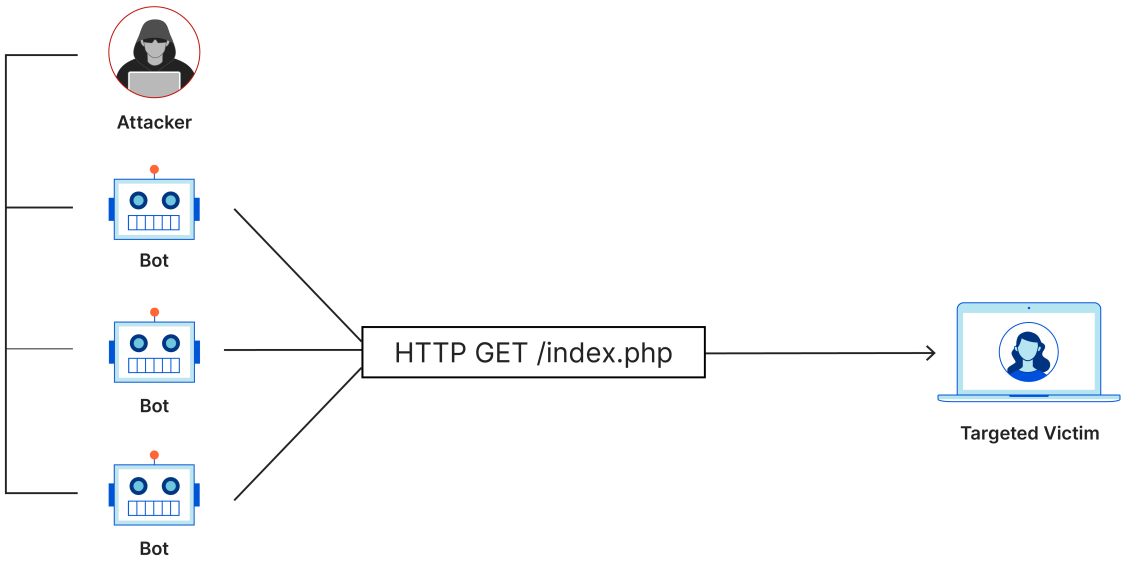
A veces conocido como un ataque DDoS de capa 7 (en referencia a la séptima capa del modelo OSI), el objetivo de estos ataques es agotar los recursos del objetivo para crear una

denegación de servicio.

Los ataques se dirigen contra la capa donde se generan las páginas web en el servidor y se entregan en respuesta a solicitudes HTTP. A nivel computacional, la ejecución de una única solicitud HTTP es fácil en el lado del cliente, pero la respuesta del servidor de destino puede complicarse, ya que este carga a menudo varios archivos y ejecuta consultas de base de datos para crear una página web.

La protección frente a ataques de capa 7 no está exenta de dificultades, ya que diferenciar el tráfico malicioso del tráfico legítimo no es una tarea fácil.

Ejemplo de ataque a la capa de aplicación:



Inundación HTTP

Este ataque es similar a pulsar la tecla de actualización de un navegador una y otra vez en muchos equipos diferentes simultáneamente. El resultado es que un gran número de solicitudes HTTP inunda el servidor, lo que provoca una denegación del servicio.

Este tipo de ataque puede ser sencillo o complejo.

Las implementaciones más sencillas pueden acceder a una URL con el mismo rango de direcciones IP, referencias y agentes de usuario de ataque. Las versiones complejas pueden utilizar un gran número de direcciones IP de ataque, así como dirigirse a direcciones URL al

azar usando referencias y agentes de usuario aleatorios.

Ataques de protocolo

El objetivo del ataque:

Los ataques de protocolo, también conocidos como ataques de agotamiento de estado, provocan una interrupción del servicio al consumir en exceso los recursos de los servidores o los equipos de red, tales como firewalls y equilibradores de carga.

Los ataques de protocolo utilizan las vulnerabilidades de las capas 3 y 4 del conjunto de protocolos para que el objetivo se vuelva inaccesible.

Ejemplo de ataque de protocolo:

Inundación SYN

Una inundación SYN es similar a la situación de un empleado de un almacén que recibe solicitudes de la tienda.

El trabajador recibe una solicitud, va y busca el paquete, y espera la confirmación antes de sacarlo. A continuación, el trabajador recibe muchas más solicitudes de paquetes sin

confirmación hasta que ya no puede llevar más paquetes, se agobia y deja de atender solicitudes.

Este ataque explota el protocolo TCP, la secuencia de comunicaciones por la cual dos equipos inician una conexión de red, mediante el envío a un servidor de un gran número de paquetes de "solicitud de conexión inicial" con marca de sincronización (SYN) con direcciones IP de origen falsificadas.

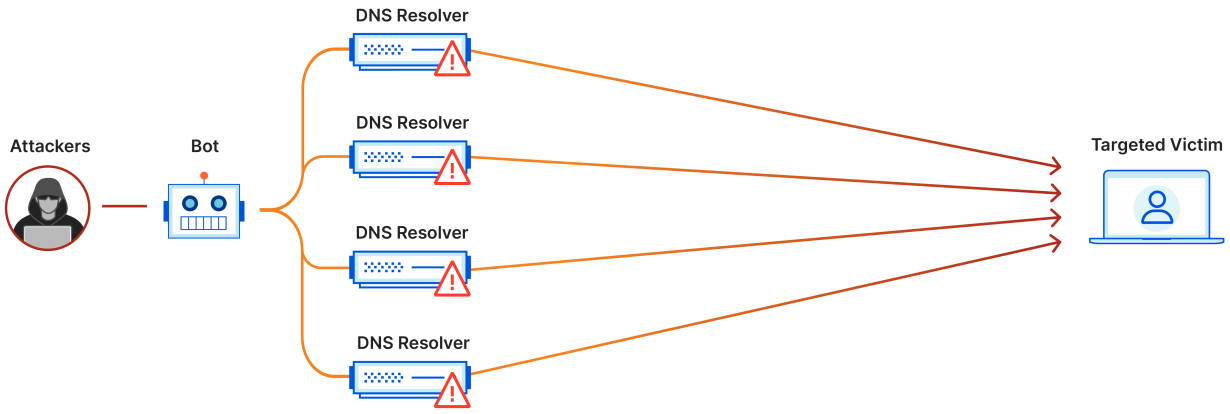
El servidor responde a cada solicitud de conexión y, a continuación, espera el último paso del protocolo de enlace, que nunca se produce, lo que agota los recursos del servidor durante el proceso.

Ataques volumétricos

El objetivo del ataque:

Esta categoría de ataques intenta saturar el tráfico mediante el consumo de todo el ancho de banda disponible entre el objetivo e Internet. Se envían grandes cantidades de datos a un servidor de destino mediante el uso de una forma de amplificación u otro medio de creación de tráfico masivo, como las solicitudes de una red de bots.

Ejemplo de amplificación:



Amplificación de DNS

Una amplificación de DNS es como si un cliente llamara a un restaurante, pidiera todo lo que aparece en el menú y solicitara que le volvieran a llamar repitiendo todo el pedido a un número de teléfono que pertenece a la víctima. Sin apenas esfuerzo, se genera una respuesta larga y se envía a la víctima.

Al enviar una solicitud a un servidor DNS con una dirección IP falsificada (la verdadera dirección IP del objetivo), la dirección IP de destino recibe una respuesta del servidor.

¿Cuál es el proceso para mitigar un ataque DDoS?

La preocupación principal al mitigar un ataque DDoS es diferenciar entre el tráfico de ataque y el tráfico normal.

Por ejemplo, si el lanzamiento de un nuevo producto satura el sitio web de una empresa debido al entusiasmo de los clientes, cortar todo el tráfico sería un error. Si esa misma empresa de pronto experimenta un aumento de tráfico por parte de agentes maliciosos conocidos, es probable que sea necesario intentar mitigar un ataque.

La dificultad radica en diferenciar a un cliente real del tráfico de ataque.

En el moderno ecosistema de Internet, el tráfico DDoS se presenta en diversas formas. Puede variar en diseño, desde ataques únicos sin falsificaciones hasta ataques multivectoriales complejos y adaptables.

Un ataque DDoS multivectorial utiliza varias rutas de ataque para poder sobrecargar al servidor de destino de distintas maneras y potencialmente desviar los esfuerzos de mitigación hacia solo una trayectoria.

Un ataque que se dirige simultáneamente a varias capas del conjunto de protocolos, como una amplificación DNS (que apunta a las capas 3 y 4) combinada con una inundación HTTP (que apunta a la capa 7) es un ejemplo de DDoS multivectorial.

Mitigar un ataque DDoS multivectorial requiere distintos abordajes con el fin de contrarrestar las diferentes trayectorias.

Por lo general, cuanto más complejo sea el ataque, más difícil será distinguir el tráfico normal del malicioso. El objetivo del atacante es disimularlo en la medida de lo posible y hacer que la mitigación sea lo más ineficaz posible.

Los intentos de mitigación que implican excluir o limitar el tráfico de forma indiscriminada podrían acabar excluyendo el tráfico real y el sospechoso. Además, el ataque también se puede modificar y adaptar para eludir las medidas tomadas y contrarrestarlas. Un abordaje por capas será la mejor manera de superar un intento complejo de interrupción del servicio.

Enrutamiento de agujeros negros

Una solución disponible para prácticamente todos los administradores de red es crear una ruta de agujero negro y dirigir el tráfico hacia ella. Dicho de manera simple, cuando se realiza el filtrado de agujeros negros sin criterios de restricción específicos, tanto el tráfico de red legítimo como el malicioso se redirigen a una ruta nula o a un agujero negro y se excluyen de la red.

Si una propiedad de Internet sufre un ataque DDoS, el proveedor de servicios de Internet (ISP) de la propiedad puede enviar todo el tráfico del sitio a un agujero negro a modo de defensa. Sin embargo, no es una solución ideal, ya que el atacante consigue lo que quiere: hacer que la red sea inaccesible.

Limitación de velocidad

Limitar la cantidad de solicitudes que un servidor puede aceptar durante un periodo determinado de tiempo también es una manera de mitigar ataques de denegación de servicio.

Si bien la limitación de velocidad es útil para ralentizar el proceso de apropiación de contenido y mitigar los intentos de inicio de sesión por fuerza bruta, es probable que por sí sola no sea suficiente para controlar de forma efectiva un ataque DDoS complejo.

No obstante, la limitación de velocidad es un elemento útil en una estrategia de mitigación de DDoS eficaz. Más información acerca de la Limitación de velocidad de Cloudflare.

Firewall de aplicaciones web

Un firewall de aplicaciones web (WAF) es una herramienta que puede ayudar a mitigar un ataque DDoS en la capa 7. Al colocar un WAF entre Internet y un servidor de origen, el WAF

puede actuar como proxy inverso y proteger al servidor de destino de determinados tipos de tráfico malicioso.

Al filtrar las solicitudes conforme a una serie de reglas que se utilizan para identificar herramientas de DDoS, se pueden impedir ataques a la capa 7. Uno de los valores clave de un WAF efectivo es la capacidad de implementar rápidamente reglas personalizadas para responder a un ataque. Más información acerca del WAF de Cloudflare.

Distribución de red Anycast

Este enfoque de mitigación utiliza una red Anycast para distribuir el tráfico de ataque a través de una red de servidores distribuidos hasta el punto en el que la red absorbe el tráfico.

Al igual que ocurre con la canalización de un río en canales más pequeños, este enfoque extiende el impacto del tráfico de ataque distribuido hasta el punto en el que se puede administrar, limitando así la capacidad de interrupción.

La fiabilidad de una red Anycast para mitigar un ataque DDoS depende del tamaño del ataque, así como del tamaño y la eficacia de la red. Una parte importante de la mitigación de DDoS de Cloudflare es el uso de una red Anycast distribuida.

Cloudflare cuenta con una capacidad de red de 348 Tbps, que es mayor que el ataque DDoS más grande jamás registrado.

Si actualmente eres víctima de un ataque, puedes tomar medidas para evitar la presión que esto significa. Si ya cuentas con Cloudflare, puedes seguir estos pasos para mitigar el ataque.

La protección contra ataques DDoS que implementamos en Cloudflare es multidimensional con el fin de mitigar todos los posibles vectores de ataque. Más información acerca de la protección DDoS de Cloudflare y cómo funciona.

Búsqueda de nombres de dominio

Sugerencias

Solicitar demostración

Contacta con Ventas

Acerca de los ataques DDoS

Ataques DDoS

Herramientas de ataque DDoS

Glosario de DDoS

Navegación del centro de aprendizaje