Ataque DDoS con Slowloris

El ataque slowloris intenta sobrecargar un servidor objetivo al abrir y mantener muchas conexiones HTTP simultáneas al objetivo.

Metas de aprendizaje

Después de leer este artículo podrás:

- Definir un ataque DoS con Slowloris
- Explicar cómo funciona un ataque Slowloris
- Entender varias estrategias de mitigación para un ataque Slowloris

CONTENIDO RELACIONADO

Ataque bajo y lento

R U Dead Yet? (R.U.D.Y.)

¿Qué es un ataque DDoS?

High Orbit Ion Cannon

Ataque de amplificación de NTP

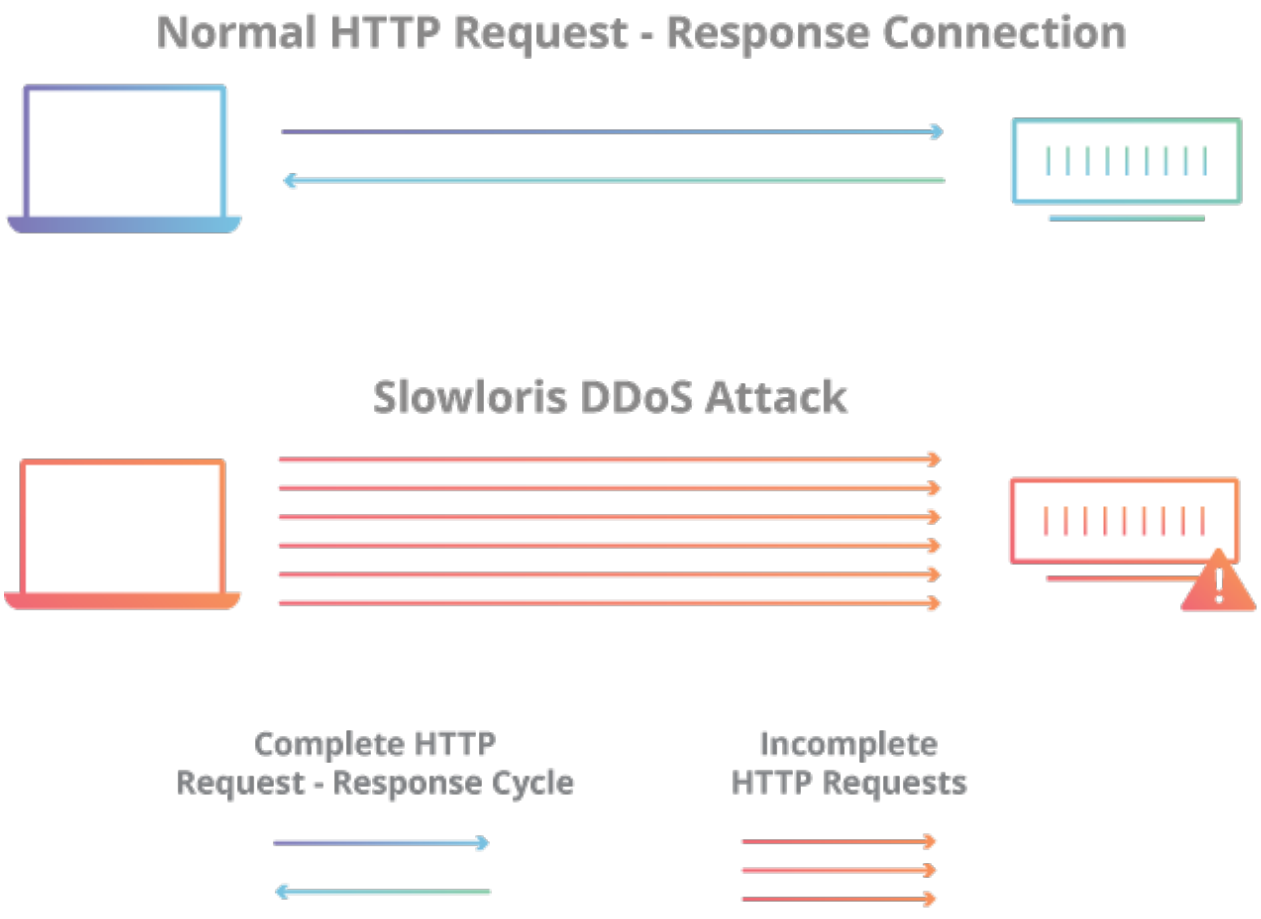
¿Quieres saber más?

Suscríbete a theNET, el resumen mensual de Cloudflare sobre las ideas más populares de Internet.

Copiar el enlace del artículo

¿Qué es un ataque DDoS con Slowloris?

Slowloris es un programa de ataque de denegación de servicio que permite que un atacante sobrecargue un servidor objetivo al abrir y mantener muchas conexiones simultáneas HTTP entre el atacante y el objetivo.



¿Cómo funciona un ataque Slowloris?

Slowloris es un ataque a la capa de aplicación que opera utilizando peticiones HTTP parciales. El ataque funciona al abrir conexiones a un servidor web objetivo y mantener esas conexiones abiertas todo el tiempo que pueda.

Slowloris no es una categoría de ataque, sino que es una herramienta de ataque específica diseñada para permitir que una sola máquina derribe un servidor sin utilizar mucho ancho de banda. A diferencia de los ataques DDoS basados en la reflexión que consumen ancho de banda como amplificación NTP, este tipo de ataque utiliza una baja cantidad de ancho de banda, y en su lugar tiene como objetivo utilizar los recursos del servidor con solicitudes que parecen más lentas de lo normal, pero que por lo demás imitan el tráfico regular. Entra en la categoría de ataques conocidos como ataques "bajos y lentos". El servidor atacado solo tendrá un número determinado de hilos disponibles para gestionar conexiones concurrentes. Cada hilo del servidor intentará mantenerse en servicio mientras espera a que se complete la solicitud lenta, lo cual nunca ocurre. Cuando se haya superado el máximo de conexiones posibles del servidor, no se responderá a cada conexión adicional y se producirá una denegación de servicio.

Un ataque Slowloris se produce en 4 pasos:

1. Primero, el atacante abre múltiples conexiones al servidor objetivo mediante el envío de múltiples encabezados de solicitudes HTTP parciales.

2. El objetivo es abrir un hilo para cada solicitud entrante, con la intención de cerrar el hilo una vez que se haya completado la conexión. Para ser eficiente, si una conexión tarda demasiado, el servidor agotará el tiempo de la conexión excesivamente larga, liberando el hilo para la siguiente solicitud.

3. Para evitar que el objetivo agote las conexiones, el atacante envía periódicamente encabezados de solicitud parciales al objetivo para mantener activa la solicitud. Básicamente, dice: "¡Todavía estoy aquí! Solo soy lento, por favor, espérame".

4. El servidor objetivo nunca es capaz de liberar ninguna de las conexiones parciales abiertas mientras espera a que termine la solicitud. Una vez que todos los hilos disponibles están en uso, el servidor será incapaz de responder a las solicitudes adicionales realizadas desde el tráfico regular, provocando una denegación de servicio.

La clave tras un Slowloris es su capacidad de causar muchos problemas con muy poco consumo de ancho de banda.

¿Cómo se mitiga un ataque Slowloris?

Para los servidores web que son vulnerables a Slowloris, hay formas de mitigar parte del impacto. Las opciones de mitigación para los servidores vulnerables pueden dividirse en 3 categorías generales:

1. **Aumentar la disponibilidad del servidor** - Aumentar el número máximo de clientes que el servidor permitirá en cualquier momento aumentará el número de conexiones que el atacante debe hacer antes de poder sobrecargar el servidor. Siendo realistas, un atacante puede escalar el número de ataques para superar la capacidad del servidor, independientemente de los aumentos.

2. **Limitar la velocidad de las solicitudes entrantes** - Restringir el acceso en función de ciertos factores de uso ayudará a mitigar un ataque Slowloris. Técnicas como la limitación del número máximo de conexiones que puede realizar una única dirección IP, la restricción de las velocidades de transferencia lentas, y la limitación del tiempo máximo que un cliente puede permanecer conectado son enfoques para limitar la eficacia de los ataques bajos y lentos.

3. **Protección basada en la nube** - Usa un servicio que pueda funcionar como proxy inverso, protegiendo el servidor de origen.

¿Cómo mitiga Cloudflare un ataque Slowloris?

Cloudflare almacena en búfer las solicitudes entrantes antes de empezar a enviar nada al servidor de origen. Como resultado, el tráfico de ataque "bajo y lento", como los ataques Slowloris, nunca llega al objetivo previsto. Más información sobre cómo la protección contra DDoS de Cloudflare detiene los ataques de Slowloris.

Para empresas

Compara planes

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