Cloudflare bloqueó un brutal ataque DDoS de 7,3 TB/s

Ataque tipo DOS:

Este tipo de ataques buscan que un recurso en Internet deje de estar disponible a los usuarios legítimos mediante la saturación de ancho de red o la sobrecarga de los sistemas. Existen multitud de tipos de ataques DOS, en los que se encuentra las inundaciones syn, udp o icmp entre otros, dependiendo del protocolo utilizado, el modo en que se envían o el contenido de los paquetes.

Suceso:

En mayo de 2025 Cloudflare registró un ataque DDOS a una única dirección IP a través de 21.925 puertos, recibiendo 37,4 TB de datos en solo 45 segundos, el mayor ataque de este tipo hasta el momento. La intención no era robar datos o infiltrarse sino dejar inoperativa una empresa de almacenamiento cliente de Cloudflare.

La gran parte del ataque fue de tipo inundación UDP, y lo restante de tipo reflexión y amplificación. En el ataque se usaron 122.145 dispositivos pertenecientes a una red "zombie" distribuida en 161 países.
A pesar de lo intenso del ataque, Cloudflare pudo detener el ataque con éxito

Protección:

- Reducir la superficie expuesta. Abrir al exterior sólo los puertos estrictamente necesarios.
- Implementar cortafuegos y sistemas de detección de intrusos que puedan bloquear conexiones.
- Tener una infraestructura escalable y distribuida.
- Utilizar servicios especializados y monitorear el tráfico en tiempo real.
- Realizar auditorías periódicas.
- Implementar un sistema sólido de control de acceso.