Cloudflare anunció el jueves que bloqueó de forma automatizada el mayor ataque de denegación de servicio distribuido (DDoS) del que se tenga registro, alcanzando una velocidad máxima de 7.3 terabits por segundo (Tbps).

El ataque fue detectado a mediados de mayo de 2025 y tuvo como blanco a un proveedor de hosting cuya identidad no ha sido revelada.

> *«Los servicios de alojamiento y componentes esenciales del ecosistema de Internet se han convertido en objetivos frecuentes de ataques DDoS. Este ataque de 7.3 Tbps transfirió 37.4 terabytes en tan solo 45 segundos»,* explicó Omer Yoachimik, de Cloudflare.

En enero de este año, la empresa especializada en seguridad y servicios web informó que contuvo un ataque DDoS de 5.6 Tbps dirigido contra un proveedor de Internet del este asiático. Dicha ofensiva tuvo su origen en un botnet basado en una variante de Mirai, en octubre de 2024.

Posteriormente, en abril de 2025, Cloudflare también se defendió exitosamente de una oleada de 6.5 Tbps que se atribuye al botnet Eleven11bot, conformado por unas 30,000 cámaras IP y grabadores de video. Este ataque de alta intensidad se extendió por aproximadamente 49 segundos.

En contraste, la ofensiva de 7.3 Tbps se centró en una única dirección IP del proveedor de alojamiento, atacando en promedio 21,925 puertos de destino por segundo, con picos de hasta 34,517 puertos distintos.

El ataque empleó múltiples vectores y utilizó una combinación de técnicas como inundación por UDP, ataques de reflexión QOTD, echo, y NTP, además de variantes del botnet Mirai, ataques portmap y amplificación basada en RIPv1. La mayoría del tráfico malicioso (99.996%) correspondió a la modalidad de UDP flood.

Cloudflare destacó que la arremetida provino de más de 122,145 direcciones IP únicas, distribuidas entre 5,433 sistemas autónomos en 161 países. Entre los principales países de origen del tráfico malicioso se encuentran Brasil, Vietnam, Taiwán, China, Indonesia, Ucrania, Ecuador, Tailandia, EE. UU. y Arabia Saudita.

> *«Se observó un promedio de 26,855 IPs únicas por segundo, con un máximo registrado de 45,097»,* añadió Yoachimik.
>
> *«Telefónica Brasil (AS27699) generó la mayor parte del tráfico ofensivo, con un 10.5%. Le siguieron el Grupo Viettel (AS7552) con 9.8%, China Unicom (AS4837) con 3.9%, y Chunghwa Telecom (AS3462) con 2.9%. China Telecom (AS4134) fue responsable del 2.8%».*

La información se publica mientras el equipo XLab de QiAnXin atribuye al botnet RapperBot un ataque contra la firma de inteligencia artificial DeepSeek en febrero de 2025, señalando además que las versiones más recientes del malware buscan extorsionar a sus víctimas solicitando pagos de “protección” para evitar futuros ataques DDoS.

Los países con más dispositivos infectados por RapperBot son China, EE. UU., Israel, México, Reino Unido, Grecia, Irán, Australia, Malasia y Tailandia. Este botnet ha estado activo desde 2022.

Las campañas de RapperBot tienen como blanco enrutadores, dispositivos NAS y grabadores de video, a los que accede mediante contraseñas por defecto débiles o vulnerabilidades del firmware. Luego, instala software malicioso que se conecta con servidores remotos usando registros DNS TXT para recibir instrucciones de ataque.

Además, el malware emplea cifrados personalizados para ocultar los registros TXT y los dominios usados para el control del botnet.

> *«Desde marzo, ha incrementado notablemente su actividad, con más de 100 objetivos diarios y al menos 50,000 bots en funcionamiento»*, explicó la firma china de ciberseguridad.
>
> *«Las víctimas de RapperBot se distribuyen en múltiples sectores: administración pública, servicios sociales, organizaciones civiles, plataformas digitales, industrias manufactureras y financieras»*, concluyó.