La empresa de infraestructura web y seguridad de sitios web, Cloudflare, reveló este jueves que logró mitigar el mayor ataque volumétrico distribuido de denegación de servicio (DDoS) registrado hasta ahora.

El ataque, lanzado a través de una botnet Mirai, se dirigió a un cliente anónimo en la industria financiera el mes pasado.

> *«En segundos, la botnet bombardeó el borde de Cloudflare con más de 330 millones de solicitudes de ataque»,* dijo la compañía.

También mencionó que en algún momento, alcanzó un récord de 17.2 millones de solicitudes por segundo (rps), lo que la hace tres veces más grande que los ataques DDoS HTTP reportado antes.

Los ataques DDoS volumétricos están diseñados para apuntar a una red específica con la intención de abrumar su capacidad de ancho de banda y, por lo general, utilizan técnicas de amplificación reflectante para escalar su ataque y causar la mayor interrupción operativa posible.

Por lo general, también se originan en una red de sistemas infectados con malware, que consta de computadoras, servidores y dispositivos de IoT, lo que permite a los atacantes tomar el control y cooptar las máquinas en una botnet capaz de generar una afluencia de tráfico basura dirigido contra la víctima.

En este incidente específico, el tráfico se originó en más de 20 mil bots en 125 países de todo el mundo, y casi el 15% del ataque se originó en Indonesia, seguido de India, Brasil, Vietnam y Ucrania. Además, los 17.2 millones de rps por sí solos representaron el 68% de la tasa de rps promedio del tráfico HTTP legítimo procesado por Cloudflare en el segundo trimestre de 2021, que es de 25 millones de rps HTTP.

Esta no es la primera vez que se detectan ataques similares en las últimas semanas.

Cloudflare dijo que la misma botnet Mirai se utilizó para atacar a un proveedor de alojamiento con un ataque HTTP DDoS que alcanzó un máximo de poco menos de 8 millones de rps.

Por otro lado, se observó que una botnet variante de Mirai lanzaba más de una docena de ataques DDoS basados en UDP y TCP, que alcanzaron su punto máximo varias veces por encima de 1 Tbps. La compañía dijo que los ataques fallidos estaban dirigidos a una compañía de juegos y un importante proveedor de servicios de Internet, telecomunicaciones y alojamiento con sede en Asia Pacífico.

> *«Aunque la mayoría de los ataques son pequeños y breves, seguimos viendo que este tipo de ataques volumétricos surgen con mayor frecuencia. Es importante tener en cuenta que estos ataques volumétricos de ráfagas cortas pueden ser especialmente peligrosos para los sistemas de protección DDoS heredados u organizaciones sin protección activa y siempre activa basada en la nube»,* dijo Cloudflare.