La botnet detrás del mayor ataque de denegación de servicio distribuido (DDoS) de HTTPS en junio de 2022, se ha relacionado con una serie de ataques dirigidos a casi 1000 clientes de Cloudflare.

Llamando a la poderosa botnet Mantis, la compañía de seguridad y rendimiento web la atribuyó a más de 3000 ataques HTTP DDoS contra sus usuarios.

Los sectores verticales de la industria más atacados incluyen Internet y telecomunicaciones, medios, juegos, finanzas, negocios y compras, de los cuales más del 20% de los ataques se dirigieron a empresas con sede en Estados Unidos, seguidas de Rusia, Turquía, Francia, Polonia, Ucrania, Reino Unido, Alemania, Países Bajos y Canadá.

El mes pasado, la compañía dijo que mitigó un ataque DDoS sin precedentes dirigido a un sitio web de un cliente anónimo utilizando su plan gratuito que alcanzó un máximo de 26 millones de solicitudes por segundo (RPS), con cada nodo generando aproximadamente 5200 RPS.

El tsunami de tráfico basura duró menos de 30 segundos y generó más de 212 millones de solicitudes HTTPS de más de 1500 redes en 121 países, encabezados por Indonesia, Estados Unidos, Brasil, Rusia e India.

> *«La red de bots Mantis opera una pequeña flota de aproximadamente 5000 bots, pero con ellos puede generar una fuerza masiva, responsable de los ataques HTTP DDoS más grandes que jamás hayamos observado»,* dijo Omer Yoachimik, de Cloudflare.

Mantis se destaca por varias razones. La primera es su capacidad para llevar a cabo ataques HTTPS DDoS, que son caros por naturaleza debido a los recursos informáticos necesarios para establecer una conexión cifrada TLS segura.

En segundo lugar, a diferencia de otras botnets tradicionales que dependen de dispositivos

IoT como DVR y enrutadores, Mantis aprovecha las máquinas virtuales secuestradas y los servidores potentes, equipándolo con más recursos.

Estos ataques volumétricos tienen como objetivo generar más tráfico del que el objetivo puede procesar, lo que hace que la víctima agote sus recursos. Mientras que los adversarios utilizan tradicionalmente UDP para lanzar ataques de amplificación, ha habido un cambio a vectores de amplificación reflejados de TCP más nuevos que hacen uso de cajas intermedias.

Microsoft, en mayo de 2022, reveló que evitó alrededor de 175,000 ataques de amplificación reflejada de UDP durante el año pasado, que estaban dirigidos a su infraestructura de Azure. También observó un ataque de amplificación reflejada de TCP en un recurso de Azure en Asia, que alcanzó los 30 millones de paquetes por segundo (pps) y duró 15 minutos.

> *«Los ataques de amplificación reflejada llegaron para quedarse y representan un serio desafío para la comunidad de Internet. Continúan evolucionando y explotando nuevas vulnerabilidades en protocolos e implementaciones de software para eludir las contramedidas convencionales»,* dijo el equipo de redes de Azure.