Microsoft detuvo un ataque DDoS de 2.4 Tbps dirigido a clientes de Azure

Autor: I. Stepanenko

Fecha: Sunday 24th of October 2021 05:41:05 AM

Microsoft reveló este lunes que su plataforma en la nube Azure mitigó un ataque de denegación de servicio distribuido (DDoS) de 2.4 Tbps en la última semana de agosto dirigido a un cliente anónimo en Europa, superando un ataque de 2.3 Tbps detenido por Amazon Web Services en febrero de 2020.

> «Se trata de un 140 por ciento más alto que el ataque de 2020 de 1 Tbps y más alto que cualquier otro acontecimiento volumétrico de red detectado previamente en Azure», dijo Amir Dahan, director senior del programa de redes Azure.

Los ataques de amplificación reflejada o «Reflexión UDP», son un tipo de ataques de denegación de servicio en los que un actor de amenazas se aprovecha de la naturaleza sin conexión del protocolo UDP con solicitudes falsificadas para abrumar a un servidor o red de destino con una avalancha de paquetes, causando interrupciones o haciendo que el servidor y su infraestructura circundante no esté disponible.

Se dice que el ataque se originó a partir de una botnet de aproximadamente 70 mil dispositivos comprometidos ubicados principalmente en la región de Asia y el Pacífico, como Malasia, Vietnam, Taiwán, Japón y China, así como en Estados Unidos.

Microsoft dijo que observó tres ráfagas de corta duración, cada una de las cuales aumentó en segundos a volúmenes de terabit: la primera a 2.4 Tbps, la segunda a 0.55 Tbps y la tercera a 1.7 Tbps.

La noticia del ataque DDoS llega un mes después de que el gigante ruso de Internet Yandex se convirtiera en el objetivo de un ataque de denegación de servicio distribuido (DDoS) sin precedentes por parte de una nueva botnet llamada Meris, que golpeó la infraestructura web de la compañía con millones de solicitudes HTTP antes de alcanzar un pico de 21.8 millones de solicitudes por segundo (RPS).

> «Los malos actores, ahora más que nunca, buscan continuamente formas de desconectar las aplicaciones. Los ataques de este tamaño demuestran la capacidad de los malos actores para causar estragos al inundar los objetivos con volúmenes de tráfico gigantescos que intentan ahogar la capacidad de la red», dijo Dahan.