La compañía francesa de computación en la nube, OVHcloud, anunció que logró mitigar un ataque distribuido de denegación de servicio (DDoS) sin precedentes en abril de 2024, el cual alcanzó una tasa de 840 millones de paquetes por segundo (Mpps).

Este nuevo récord supera al anterior de 809 millones de Mpps, registrado por Akamai en junio de 2020, dirigido a un gran banco europeo.

El ataque DDoS de 840 Mpps consistió en una combinación de una inundación de TCP ACK, que se originó desde 5,000 direcciones IP, y un ataque de reflexión DNS, que utilizó aproximadamente 15,000 servidores DNS para amplificar el tráfico.

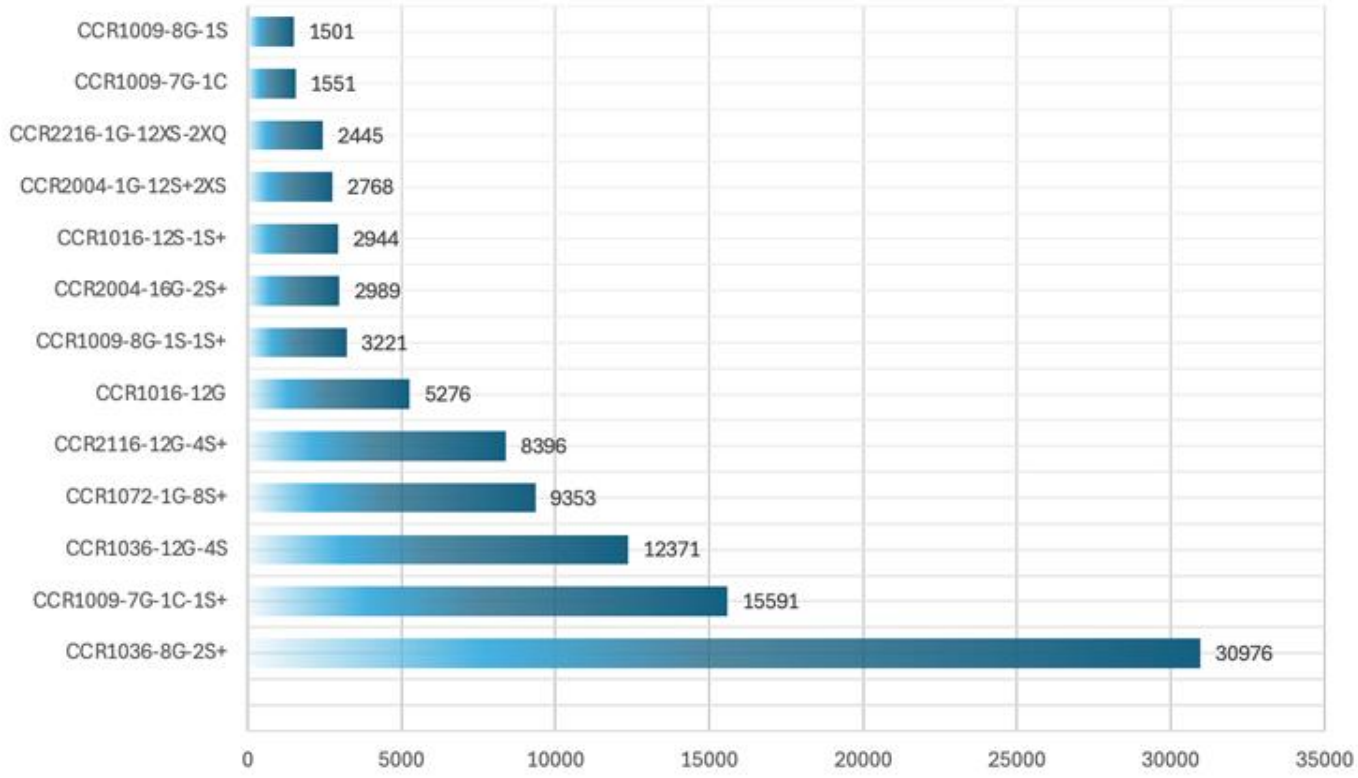
> *«Aunque el ataque estuvo distribuido globalmente, dos tercios del total de paquetes ingresaron desde solo cuatro puntos de presencia, todos ubicados en los EE. UU., tres de ellos en la costa oeste. Esto demuestra la capacidad del adversario para enviar una gran cantidad de paquetes a través de solo unas pocas conexiones, lo que puede resultar muy problemático»*, explicó OVHcloud.

La empresa también mencionó que ha observado un aumento significativo en la frecuencia e intensidad de los ataques DDoS desde 2023, y agregó que aquellos que superan 1 terabit por segundo (Tbps) se han vuelto comunes.

> *«En los últimos 18 meses, pasamos de ver ataques de más de 1 Tbps siendo bastante raros, a ocurrir semanalmente, y ahora casi diariamente (en promedio semanal). La tasa de bits más alta que observamos durante ese período fue de aproximadamente 2.5 Tbps»*, indicó Sebastien Meriot de OVHcloud.

A diferencia de los ataques DDoS típicos que buscan agotar el ancho de banda disponible mediante el envío de una avalancha de tráfico basura, los ataques de tasa de paquetes sobrecargan los motores de procesamiento de paquetes de los dispositivos de red cercanos

al destino, como los balanceadores de carga.



Los datos recopilados por la compañía indican que los ataques DDoS con tasas de paquetes superiores a 100 Mpps han aumentado considerablemente durante el mismo período, y muchos de ellos provienen de dispositivos MikroTik Cloud Core Router (CCR) comprometidos. Hay hasta 99,382 routers MikroTik accesibles a través de internet.

Estos routers, además de tener una interfaz de administración expuesta, operan con versiones desactualizadas del sistema operativo, lo que los hace vulnerables a fallos de seguridad conocidos en RouterOS. Se sospecha que los actores maliciosos están utilizando la función de prueba de ancho de banda del sistema operativo para realizar los ataques.

Se estima que incluso secuestrar el 1% de los dispositivos expuestos en una botnet DDoS

podría proporcionar a los atacantes la capacidad de lanzar ataques de capa 7 que alcancen hasta 2.28 mil millones de paquetes por segundo (Gpps).

Es importante destacar que los routers MikroTik han sido utilizados para construir potentes botnets como Mēris e incluso para lanzar operaciones de botnet como servicio.

> *«Dependiendo de la cantidad de dispositivos comprometidos y sus capacidades reales, esto podría marcar una nueva era para los ataques de tasa de paquetes: con botnets posiblemente capaces de emitir miles de millones de paquetes por segundo, podría desafiar seriamente la manera en que se construyen y escalan las infraestructuras anti-DDoS,»* dijo Meriot.