2024 registró el DDoS más grande de la historia y un aumento del 53% en incidencia

CIUDAD DE MÉXICO. 30 de enero de 2025.- En el ámbito de la ciberseguridad, el 2024 pasará a la historia como el año en que los ataques de Denegación de Servicio Distribuida (DDoS) alcanzaron niveles sin precedentes. Según la vigésima edición del Informe de Amenazas DDoS de Cloudflare, recién publicado, los sistemas de protección global de la compañía bloquearon 21.3 millones de ataques, lo que representa un aumento del 53% en comparación con 2023. En promedio, en 2024, Cloudflare bloqueó 4,870 ataques DDoS cada hora a nivel mundial.

El informe resalta que el cuarto trimestre del año fue particularmente significativo, con más de 420 ataques hiper volumétricos que superaron los mil millones de paquetes por segundo (pps) y 1 terabit por segundo (Tb/s). Entre estos, destaca el ataque registrado el 29 de octubre: un ataque DDoS de 5.6 Tb/s lanzado por una variante de la botnet Mirai, lo que lo convierte en el ataque más grande del mundo jamás reportado.

En cuanto a México, en el cuarto trimestre de 2024, Cloudflare bloqueó un promedio de 88 millones de amenazas cibernéticas dirigidas al país cada día, un aumento del 137% en comparación con el mismo periodo del año anterior. La empresa gestionó un promedio de 56 mil millones de solicitudes de Internet a México diariamente, de las cuales un promedio de 2.5 mil millones (4%) fueron bloqueadas como ciberataques, principalmente clasificados como ataques DDoS originados en México, lo que representó un incremento del 22% en comparación con el trimestre anterior.

Aunque los ataques se registraron en varios sectores, las industrias más atacadas en el cuarto trimestre incluyeron Telecomunicaciones, Personal y Reclutamiento, Electrónica de Consumo y Empresas Holding.

- El ataque que rompió todos los récords

Este ataque sin precedentes tuvo como objetivo a un proveedor de servicios de Internet en Asia, cliente de Cloudflare Magic Transit. Aunque duró sólo 80 segundos, se originó en más de 13,000 dispositivos IoT, con un promedio de 5,500 direcciones IP y puertos de origen únicos por segundo. La detección y mitigación fueron completamente automatizadas, sin necesidad de intervención humana, gracias a los sistemas de defensa distribuidos de Cloudflare.

A pesar de su intensidad, este ataque es solo un ejemplo de la sofisticación que los ciberdelincuentes han logrado alcanzar. Además, en el cuarto trimestre, el número de ataques que superaron 1 Tb/s aumentó en un 1,885% en comparación con el trimestre anterior, mientras que los ataques que superaron los 100 millones de paquetes por segundo aumentaron un 175%.

- Una perspectiva global alarmante

En total, durante los últimos tres meses de 2024, Cloudflare mitigó 6.9 millones de ataques DDoS, lo que representó un aumento del 16% respecto al trimestre anterior y un incremento del 83% en comparación con el mismo período del año pasado. De estos, el 49% fueron ataques de capa 3 y 4, mientras que el 51% fueron ataques HTTP.

Estas cifras reflejan no solo un aumento en la cantidad, sino también en la complejidad y el tamaño de los ataques. Por ejemplo, el 11% de los ataques HTTP detectados suplantaron navegadores legítimos, mientras que otro 10% contenían atributos HTTP sospechosos o inusuales. Además, aproximadamente el 92% de las solicitudes de ataques DDoS HTTP se realizaron a través de conexiones HTTPS.

- Duración y Volumen: nuevos desafíos

Mientras que la mayoría de los ataques DDoS HTTP (72%) y de capa de red DDoS (91%) finalizan en menos de diez minutos, esta brevedad plantea un desafío significativo. Debido a que la duración de la mayoría de los ataques es tan corta, no es factible, en la mayoría de los casos, que una persona responda a una alerta, analice el tráfico y aplique mitigación. La corta duración de los ataques resalta la necesidad de un servicio de protección DDoS automatizado, en línea y siempre activo.

Otro aspecto clave es el volumen de los ataques. Cloudflare comenzó a observar un aumento en los ataques DDoS hiper volumétricos en la capa de red en el tercer trimestre de 2024. Más recientemente, en el cuarto trimestre, la cantidad de ataques que superaron 1 Tbps aumentó un 1,885% en comparación con el trimestre anterior y los ataques que superaron los 100 millones de paquetes por segundo aumentaron un 175%. El 16% de los ataques que superaron los 100 millones de paquetes por segundo también superaron los mil millones de paquetes por segundo.

Entre sus conclusiones, Cloudflare enfatiza que la proliferación de dispositivos IoT y la creciente sofisticación de las botnets siguen posicionando a los ataques DDoS como una amenaza persistente. Sin embargo, el informe también resalta el papel crucial de las tecnologías avanzadas para contrarrestar estos ataques.

La experiencia de Cloudflare a lo largo de 2024 demuestra que la detección rápida y la mitigación automática son clave para minimizar el impacto de estas amenazas. La preparación e innovación en ciberseguridad serán esenciales en 2025 para proteger tanto a las empresas como a los usuarios de Internet.