Informe sobre amenazas DDoS de Cloudflare del 3.er trimestre de 2026: mayor cantidad, menor tamaño

Ciudad de México, 3 de noviembre de 2026.— Cloudflare presentó la 18.° edición de su Informe sobre amenazas DDoS, correspondiente al tercer trimestre de 2026, que comprende los meses de julio, agosto y septiembre y devuelve la serie a su cadencia trimestral tras el volumen combinado del primer semestre de 2026.

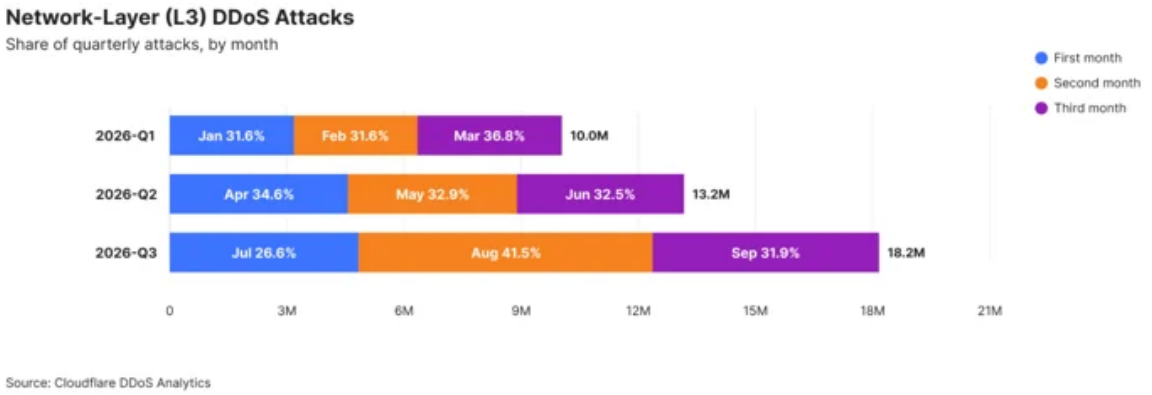
El análisis, realizado por Cloudforce One, la organización de información sobre amenazas de Cloudflare, ofrece una visión integral de la evolución del panorama de amenazas DDoS a partir de los datos de la red de Cloudflare.

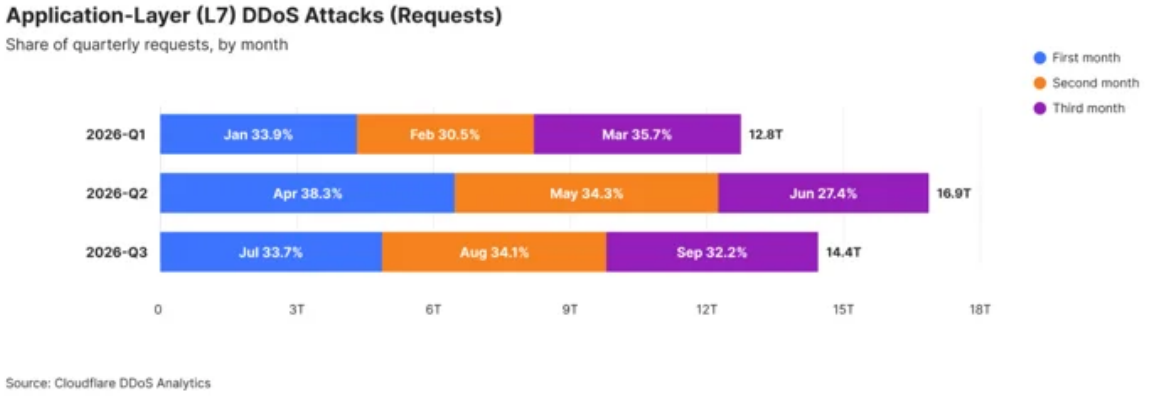
Información clave

1. Los ataques de corta duración y bajo ancho de banda, aquellos que duran menos de 10 minutos y registran una tasa menor de 1 GB/s, aumentaron un 208 %. Por el contrario, los ataques hipervolumétricos que superan 1 Tb/s se desplomaron casi un 69 % respecto al segundo trimestre, lo que posiblemente refleje las medidas adoptadas por los gobiernos a principios de año contra cuatro importantes redes de bots (botnets) de la Internet de las cosas (IoT). Sin embargo, siguen apareciendo variantes, lo que demuestra que las botnets de IoT continúan siendo una amenaza duradera y de gran volumen para la infraestructura de la red.
2. Los atacantes cambiaron drásticamente sus tácticas de reflexión y amplificación y abandonaron de forma repentina las inundaciones de CLDAP, que cayeron un 99,5 % intertrimestral. En su lugar, se centraron en gran medida en otros protocolos sin conexión, lo que provocó un aumento del 215 % en la amplificación de DNS y del 122 % en las inundaciones de UDP en general.
3. Los objetivos de los ataques se ampliaron significativamente tanto en industrias como en geografías, y Estados Unidos reclamó la posición más atacada que antes tenía China. Canadá e Israel experimentaron grandes picos en los ataques específicos, al avanzar 10 y 7 puestos, respectivamente, mientras enfrentaban tensiones geopolíticas, disputas comerciales y eventos nacionales polémicos. Al mismo tiempo, el enfoque operativo se alejó de las organizaciones de medios de comunicación para dirigirse a una mayor variedad de objetivos de la industria, incluidos los servicios al consumidor, la infraestructura de Internet y el entretenimiento para adultos.

El tercer trimestre en cifras: 8.200 ataques DDoS cada hora

En el tercer trimestre de 2026, Cloudflare mitigó de forma autónoma, a través de su red, 18,2 millones de ataques DDoS en la capa de red y 14,4 billones de solicitudes DDoS de HTTP. Esto equivale a aproximadamente 8.226 ataques DDoS de la capa de red por hora, o cerca de 197.400 por día, uno por cada 0,44 segundos. El tráfico mitigado durante el trimestre sumó un total de 272,6 PB en la capa de red y 95,1 PB en la capa de HTTP.



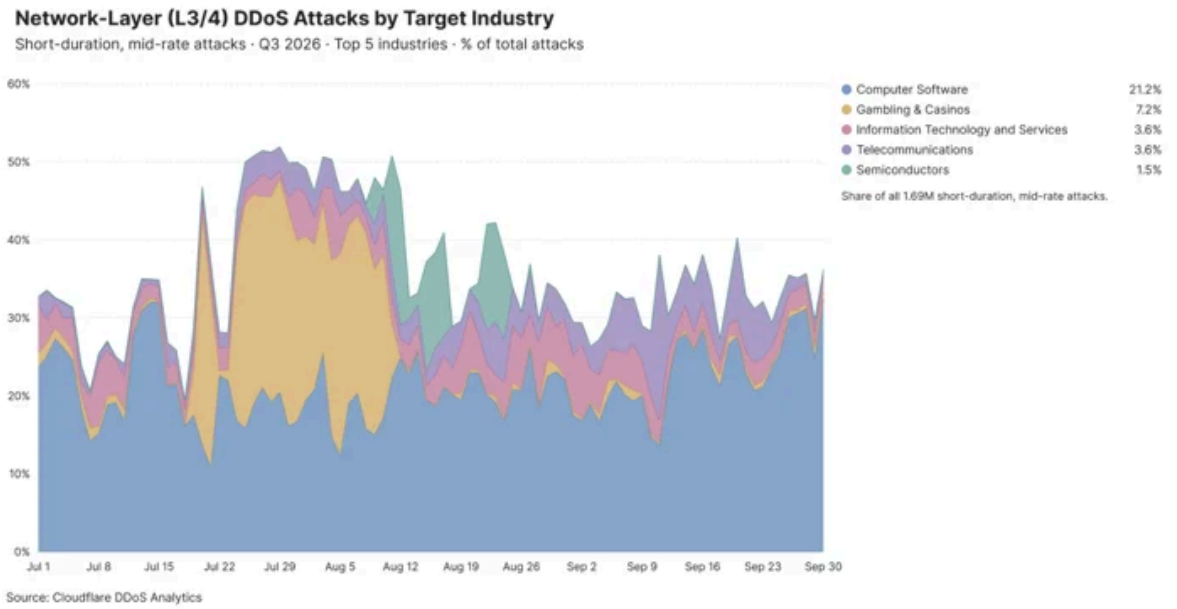


Mayor cantidad, menor tamaño

Durante el trimestre se aceleraron los ataques de corta duración, rango medio y gran cantidad, la firma operativa de los servicios "booter" de DDoS bajo demanda. Estos ataques estuvieron dirigidos principalmente a las industrias de software informático, apuestas y casinos, y tecnología de la información.

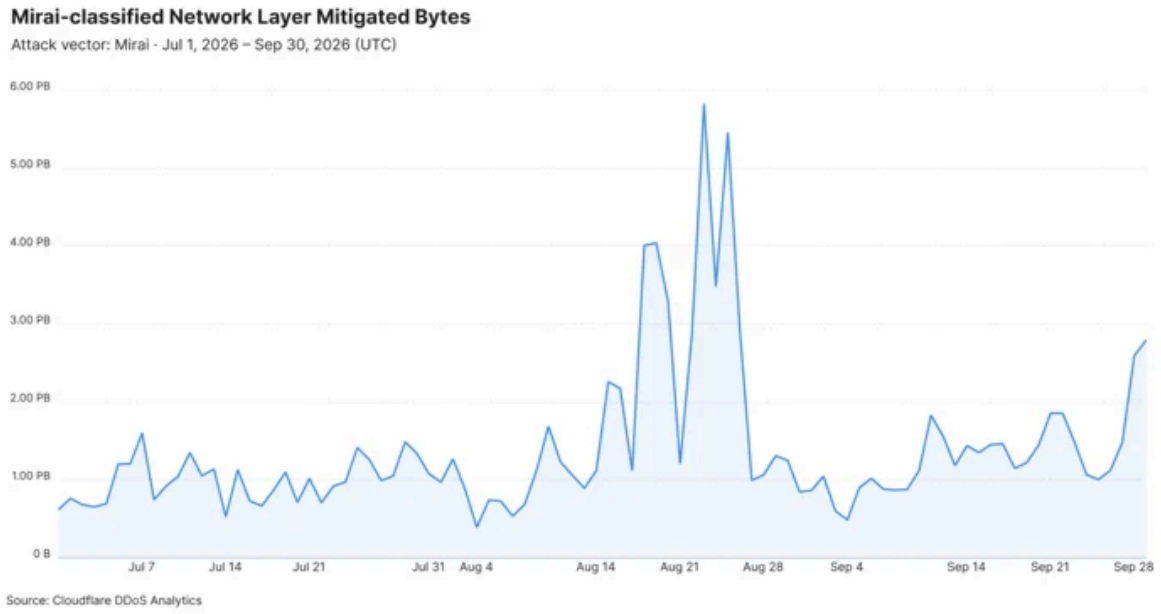
Cloudflare mitigó de manera autónoma 18,2 millones de ataques DDoS de capa de red en el tercer trimestre de 2026, un aumento del 208 % respecto al mismo trimestre de 2025:

- El 96 % terminó en menos de 10 minutos.
- El 98 % se mantuvo por debajo de 1 Gbps, más que suficiente para abrumar a un servidor o sitio web.



Por otro lado, los ataques hipervolumétricos a nivel de red, aquellos superiores a 1 Tb/s, invirtieron la tendencia y se redujeron a 251 ataques en el tercer trimestre, frente a los 805 registrados en el segundo. Esto coincidió con la acción de los gobiernos a principios de 2026, que desmantelaron cuatro de las mayores botnets de DDoS IoT: Aisuru, KimWolf, JackSkid y Mossad.

Sin embargo, las botnets basadas en IoT siguen siendo una amenaza persistente de alto volumen a medida que el ecosistema genera nuevas variantes como Dysphoria y Evooo1Bot. La mitigación clasificada como Mirai alcanzó su punto máximo en agosto con 57,23 PB y representó el 46,5 % de todos los bytes de la capa de red mitigados en el tercer trimestre, incluyendo cuatro días —16, 19, 23 y 25 de agosto— que superaron individualmente los 3 petabytes. El ataque de Mirai más prolongado e ininterrumpido del trimestre duró 49,7 horas entre el 19 y el 21 de agosto.



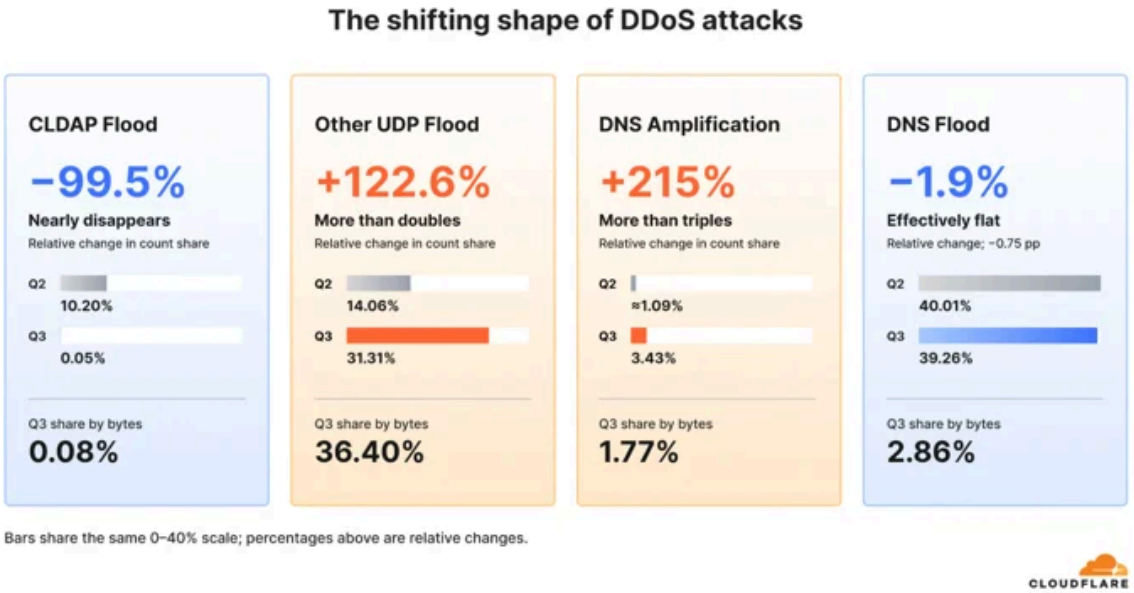
Cambios en los vectores: el colapso del protocolo CLDAP y el aumento de UDP

El cambio de vector más drástico del trimestre fue la disminución de los ataques con CLDAP (Protocolo ligero de acceso a directorios sin conexión), en los que consultas pequeñas con una dirección IP de víctima falsificada engañan a los controladores de dominio público (UDP 389) para reflejar respuestas masivas y amplificadas a la víctima.

Este tipo de ataques había registrado un aumento del 580 % intertrimestral durante el primer semestre del año, antes de desplomarse hasta representar solo el 0,05 % de los ataques en el tercer trimestre.

Mientras tanto, la amplificación de DNS aumentó un 215 % y representó el 3,43 % de todos los ataques a nivel de red, al aprovechar la resolución de DNS abiertos mediante un patrón de reflexión y amplificación similar al de CLDAP: pequeñas consultas falsificadas y grandes respuestas enviadas a la víctima.

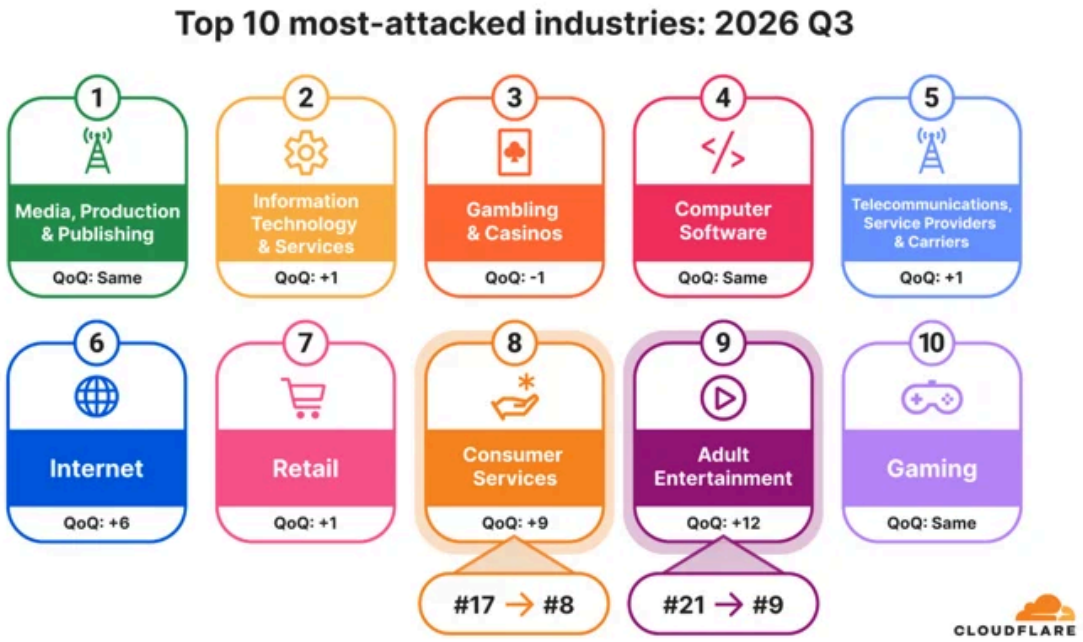
Otros ataques, como las inundaciones UDP, aumentaron del 14,06 % al 31,31 % de los ataques a nivel de red. UDP es un protocolo de transporte no orientado a conexión, lo que lo convierte en un vehículo conveniente para ataques volumétricos directos: los atacantes envían una gran cantidad de paquetes UDP a puertos aleatorios o específicos del objetivo, lo que obliga al objetivo a verificar si existe una aplicación a la escucha y a responder, consumiendo sus recursos de red y de informática.



Los sectores más afectados

Aunque los medios de comunicación, la producción y la edición siguieron siendo el sector más atacado en el tercer trimestre de 2026, su cuota global se redujo de forma marcada hasta la mitad del nivel registrado en el segundo trimestre, mientras que el enfoque se trasladó hacia un abanico más amplio de sectores.

Internet pasó de estar fuera de los 10 primeros puestos a ocupar el n.º 6; los servicios al consumidor y el entretenimiento para adultos también entraron en la clasificación y alcanzaron los puestos n.º 8 y n.º 9, respectivamente.



Las ubicaciones más atacadas

Aumentos geográficos: Canadá e Israel suben en la clasificación

Además de atravesar un periodo ya turbulento de disputas comerciales bilaterales, Canadá pasó del puesto 16 al 6, impulsado por ataques contra sus sectores de venta minorista, telecomunicaciones, proveedores de servicios y operadores, y marketing y publicidad.

Israel avanzó 7 posiciones hasta el puesto n.º 10 como resultado de la actividad DDoS sostenida a mediados de septiembre. Aunque este periodo se caracterizó por decisiones polémicas antes de las elecciones parlamentarias y la festividad de Rosh Hashaná, este año también se registró un aumento masivo y documentado de ciberguerra hostil contra Israel.

Principales 10

Estados Unidos fue la ubicación más atacada en el tercer trimestre de 2026, mientras que China ocupó el puesto n.º 2 e Indonesia se situó entre los tres primeros puestos con un 2,93 % del total de ataques.

La presencia de Estados Unidos y China en los primeros lugares coincide con lo observado durante el primer semestre de 2026, cuando China ocupó el n.º 1 y Estados Unidos el n.º 2. Ambos países han intercambiado posiciones a medida que la atención y las preferencias de los atacantes cambian.



Fortalecer las defensas globales y ayudar a proteger Internet

La red de Cloudflare está diseñada para absorber este tipo de crecimiento en las amenazas DDoS. Cada servicio de su red está protegido por una protección DDoS gratuita y sin medición, que se ejecuta en cada una de sus más de 330 ciudades en todo el mundo, respaldada por 500 Tb/s de capacidad de red.

La autonomía es un elemento clave: los sistemas de Cloudflare detectan y mitigan los ataques sin intervención humana. Esta capacidad resulta especialmente relevante debido a que, como muestran las distribuciones del trimestre, la mayoría de los ataques terminan mucho antes de que un analista humano pueda ver la alerta, mientras que los ataques más grandes siguen superando con regularidad 1 Tb/s, con una cadencia medida en cientos por trimestre.

Para ayudar a los proveedores de alojamiento, las plataformas de informática en la nube y los proveedores de servicios de Internet a identificar y eliminar las direcciones IP y las cuentas abusivas que lanzan estos ataques, Cloudflare aprovecha su punto de observación único sobre los ataques DDoS para proporcionar un feed gratuito de amenazas de botnets DDoS para proveedores de servicios.

Más de 800 redes de todo el mundo se han suscrito a este servicio y Cloudflare ya ha observado una amplia colaboración en toda la comunidad para desmantelar nodos de botnets. Para acceder de forma continua a actualizaciones sobre las tendencias de ataque en Internet, se puede consultar Cloudflare Radar.

Acerca de Cloudforce One

Impulsado por la misión de ayudar a proteger Internet, Cloudforce One aprovecha la telemetría de la red global de Cloudflare, que protege aproximadamente el 20 % de la web,

para impulsar la investigación sobre amenazas y la respuesta operativa, y proteger sistemas críticos para millones de organizaciones en todo el mundo.

xxx

Acerca de Cloudflare

Cloudflare, Inc. (NYSE: NET) es la empresa líder en conectividad cloud. Ayuda a las organizaciones a aumentar la velocidad y mejorar la seguridad de sus empleados, aplicaciones y redes en todas partes, al tiempo que reduce la complejidad y los costos. La conectividad cloud de Cloudflare ofrece la plataforma más completa y unificada de productos nativos en la nube y herramientas para desarrolladores, de manera que cualquier organización pueda obtener el control que necesita para trabajar, desarrollar y acelerar su negocio.

Cloudflare, que utiliza una de las redes más grandes e interconectadas del mundo, bloquea por día miles de millones de amenazas en línea para sus clientes. Millones de organizaciones confían en Cloudflare, desde las marcas más importantes, emprendedores y pequeñas empresas hasta organizaciones sin fines de lucro, grupos humanitarios y gobiernos de todo el mundo.Si deseas obtener más información sobre la conectividad cloud de Cloudflare, visita cloudflare.com/connectivity-cloud. Para conocer las nuevas tendencias y perspectivas de Internet, consulta https://radar.cloudflare.com.

Síguenos en: Blog | X | LinkedIn | Facebook | Instagram