DOCUMENTO TÉCNICO

CLOUDFLARE

Información sobre seguridad de Cloudflare: Tendencias de ataques DDoS en el 4º trimestre de 2021

+55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/es-la/

INFORMACIÓN SOBRE SEGURIDAD DE CLOUDFLARE: TENDENCIAS DE ATAQUES DDOS EN EL 4º TRIMESTRE DE 2021

En la primera mitad de 2021 se observaron campañas de ataques masivos de ransomware y DDoS de rescate que interrumpieron infraestructura crítica en todo el mundo (incluso uno de los mayores operadores de sistemas de oleoductos en los Estados Unidos) y una vulnerabilidad de software de gestión informática que afectó a centros de enseñanza, el sector público, organizaciones turísticas y uniones de crédito, entre otras industrias.

En la segunda mitad del año se registró una avalancha de una de las botnets más potentes desplegadas (Meris), ataques DDoS HTTP sin precedentes y ataques contra la capa de red de Cloudflare. Además, en diciembre se descubrió la vulnerabilidad en Log4j2 (CVE-2021-44228) que permite a un atacante ejecutar código en un servidor remoto y posiblemente sea una de las vulnerabilidades más graves en Internet desde Heartbleed y Shellshock.

Estos no son más que algunos ejemplos que ponen de manifiesto una mayor tendencia hacia la inseguridad cibernética que afecta a todo el mundo, desde empresas tecnológicas y organizaciones gubernamentales hasta bodegas y plantas de procesamiento de productos cárnicos.

A continuación, se presentan algunas tendencias de ataques DDoS y los aspectos más destacados de 2021, en concreto, del 4º trimestre:

Ataques DDoS de rescate

- En el 4º trimestre, los ataques DDoS de rescate aumentaron un 29 % interanual y un 175 % intertrimestral.
- Solo en diciembre, uno de cada tres participantes en el sondeo reportó haber sido blanco de un ataque DDoS de rescate o haber recibido amenazas de un atacante.

Ataques DDoS a la capa de aplicación

- Los ataques a la industria manufacturera aumentaron un 641 % en comparación con el trimestre anterior, pasando a ser así el objetivo del mayor número de ataques en el último trimestre del año. Las industrias de servicios empresariales y videojuegos/apuestas fueron la segunda y tercera industria más afectadas por los ataques DDoS a la capa de aplicación.
- Por cuarta vez consecutiva en el año, China encabezó las estadísticas con el mayor porcentaje de tráfico de ataque originado en sus redes.
- Una nueva botnet llamada Meris apareció a mediados de 2021 y continuó atacando a organizaciones de todo el mundo con algunos de los mayores ataques HTTP de los que se tiene constancia, incluido un ataque de 17,2 millones de solicitudes por segundo que Cloudflare mitigó automáticamente.

Ataques DDoS a la capa de red

- El cuarto trimestre fue el periodo más atareado de 2021. Solo el mes de diciembre reunió más ataques que en el primer y segundo trimestre por separado.
- Si bien la mayoría de los ataques fueron a pequeña escala, los de varios terabits pasaron a ser la norma en la segunda mitad del año. Cloudflare mitigó de forma automática docenas de ataques con picos de tráfico de más de 1 TB/s, y el más grande alcanzó un pico de casi 2 TB/s, el mayor que hemos visto.
- También en el 4º trimestre de 2021, y concretamente en noviembre, se registró una campaña persistente de ataques DDoS de rescate contra proveedores de VoIP de todo el mundo.
- Los ataques originados en Moldavia se cuadruplicaron en el cuarto trimestre del año pasado, convirtiéndose así en el país con el mayor porcentaje de actividad DDoS a la capa de red.
- Las inundaciones SYN y UDP fueron los vectores de ataque más frecuentes, si bien las amenazas emergentes, como los ataques SNMP, aumentaron prácticamente un 5.800 % con respecto al trimestre anterior.

Este informe se basa en los ataques DDoS que los sistemas de protección contra DDoS de Cloudflare detectaron y mitigaron de manera automática. Para obtener más información sobre su funcionamiento, visita esta publicación detallada del blog.

Nota sobre cómo medimos los ataques DDoS observados en nuestra red

Para analizar las tendencias de los ataques, computamos la tasa de "actividad DDoS", que es el porcentaje de tráfico de ataque sobre el tráfico total (ataque + legítimo) observado en nuestra red global. Medir el número de ataques como porcentaje del tráfico total observado nos permite normalizar los puntos de datos y evitar las desviaciones reflejadas en las cifras absolutas hacia, por ejemplo, un centro de datos de Cloudflare que recibe más tráfico total y, probablemente, también más ataques.

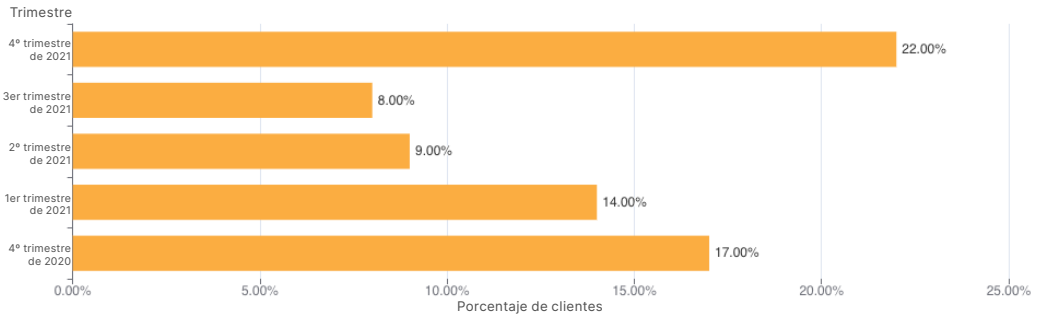
Puedes consultar la versión interactiva de este informe en Cloudflare Radar.

Ataques de rescate

Nuestros sistemas analizan continuamente el tráfico e implementan soluciones de mitigación de forma automática cuando se detectan ataques DDoS. Cada cliente que es blanco de un ataque DDoS recibe un sondeo automatizado que nos ayuda a comprender mejor las carecterísticas del ataque y el éxito de la mitigación.

Desde hace más de dos años, Cloudflare ha sondeado a clientes que han sido víctimas de ataques. Una de las preguntas del sondeo es si han recibido una nota de rescate exigiendo un pago a cambio de detener el ataque DDoS. En el 4º trimestre de 2021, se registró el mayor número de respuestas que indicaban amenazas de rescate. En este periodo, los ataques de rescate se incrementaron un 29 % interanual y un 175 % en términos intertrimestrales. Más concretamente, uno de cada 4,5 participantes (22 %) reportó haber recibido una nota de rescate que exigía un pago.

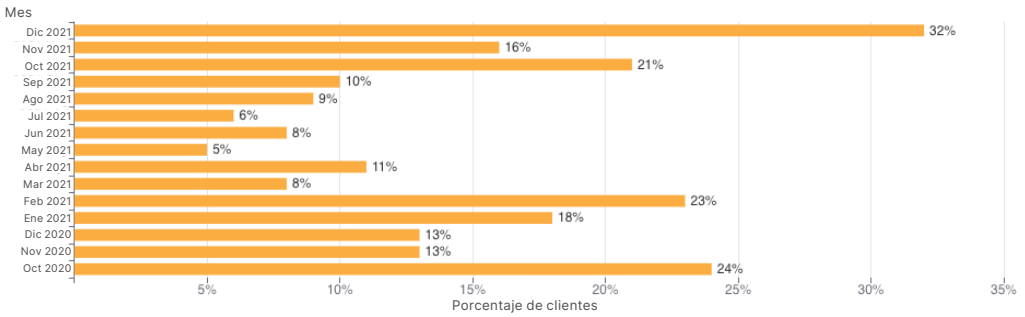
Amenazas y ataques DDoS de rescate



Porcentaje de participantes que reportaron haber sido objeto de un ataque DDoS de rescate o haber recibido amenazas antes del ataque.

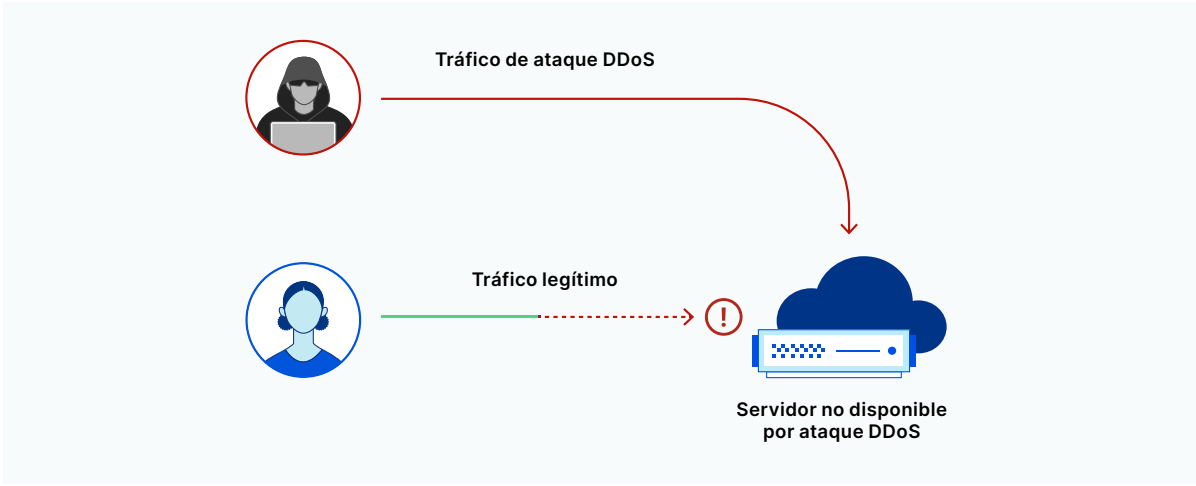
Si lo desglosamos por meses, observamos que diciembre de 2021 encabeza la lista. En ese mes, un 32 % de los participantes declararon haber recibido una nota de rescate, es decir, casi uno de cada tres participantes.

Amenazas y ataques DDoS de rescate



Ataques DDoS a la capa de aplicación

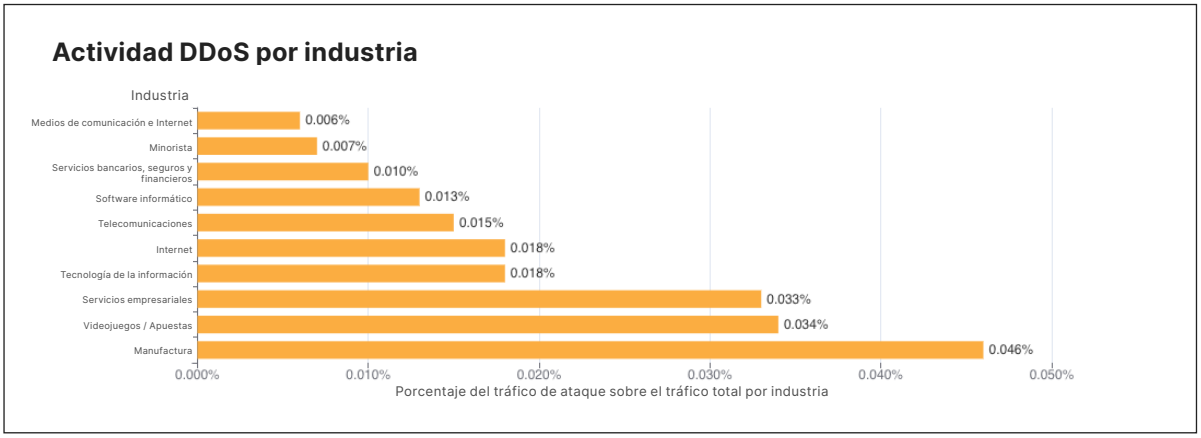
Los ataques DDoS a la capa de aplicación, en concreto los ataques DDoS HTTP, son ataques que suelen tener como objetivo interrumpir un servidor web evitando que pueda procesar las solicitudes legítimas de los usuarios. Si el servidor se satura con más solicitudes de las que puede procesar, descartará las solicitudes legítimas y, en algunos casos, se bloqueará, lo que degradará el rendimiento o interrumpirá los servicios para los usuarios legítimos.



Ataques DDoS a la capa de aplicación por industria

En el 4º trimestre, los ataques DDoS a las empresas de la industria de la manufactura aumentaron un 641 % con respecto al trimestre anterior, y los ataques DDoS a servicios empresariales se incrementaron un 97 %.

Si desglosamos los ataques a la capa de aplicación por industrias,la manufactura, los servicios empresariales y los videojuegos/apuestas fueron las más afectadas en el 4º trimestre de 2021.

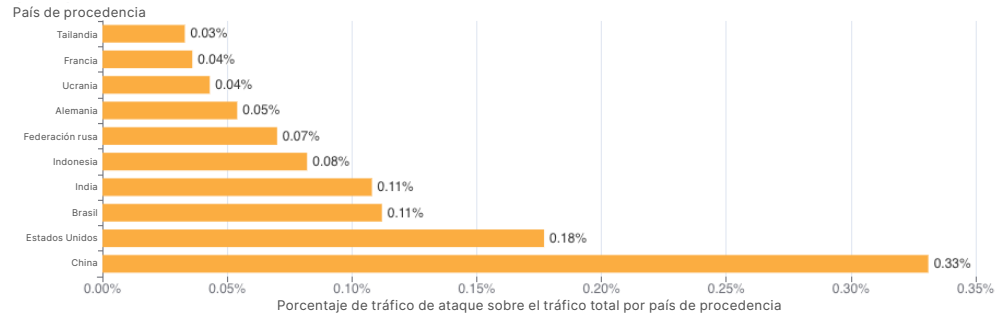


Ataques DDoS a la capa de aplicación por país de procedencia

Para entender la procedencia de los ataques HTTP, analizamos la geolocalización de la dirección IP de origen perteneciente al cliente que generó las solicitudes HTTP de ataque. A diferencia de los ataques a la capa de red, las direcciones IP de origen no se pueden suplantar en los ataques HTTP. Un elevado porcentaje de actividad DDoS en un país determinado suele indicar la presencia de botnets que operan dentro de su propio país.

Por cuarto trimestre consecutivo, China siguió siendo el país con el mayor porcentaje de ataques DDoS originados dentro de sus fronteras. Más de tres de cada mil solicitudes HTTP que se originaron en direcciones IP chinas formaban parte de un ataque DDoS HTTP. Estados Unidos se mantuvo en segundo lugar, por delante de Brasil e India.

Actividad DDoS por país de procedencia.

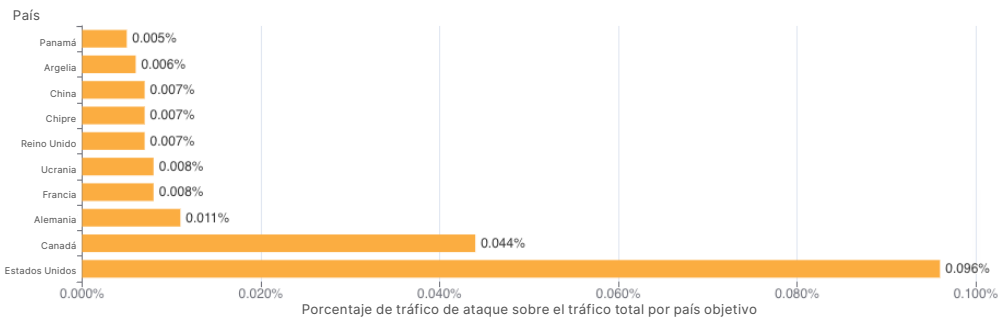


Ataques DDoS a la capa de aplicación por país objetivo

Para identificar qué países son el objetivo de la mayoría de los ataques DDoS HTTP, agrupamos los ataques DDoS por los países de facturación de nuestros clientes y lo representamos como un porcentaje de todos los ataques DDoS.

Por tercera vez consecutiva en 2021, las organizaciones de Estados Unidos fueron blanco de la mayoría de los ataques DDoS HTTP, seguidas por las de Canadá y Alemania.

Actividad DDoS por país objetivo

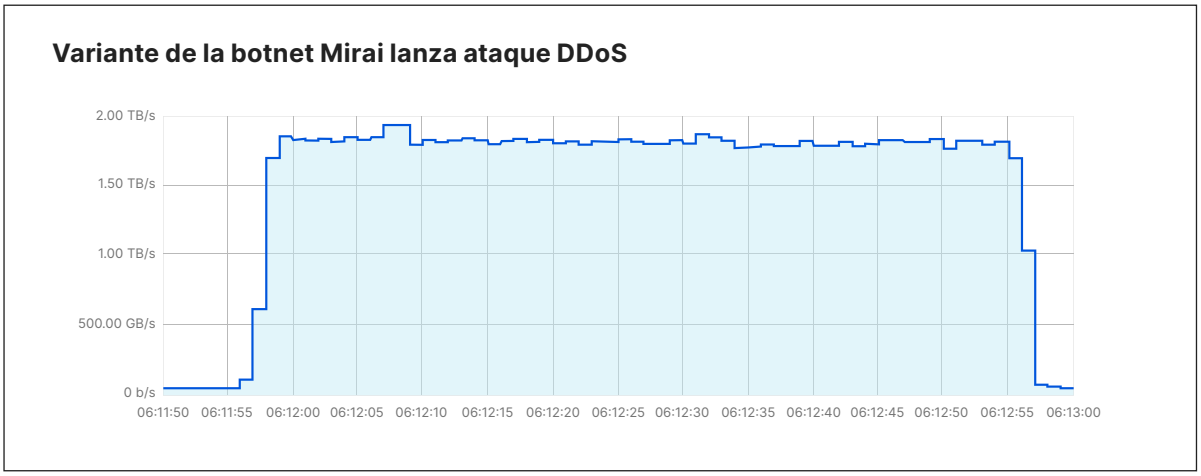


Ataques DDoS a la capa de red

Si bien los ataques a la capa de aplicación (capa 7 del modelo OSI) se dirigen contra la aplicación que ejecuta el servicio al que los usuarios finales intentan acceder, los ataques a la capa de red tratan de saturar la infraestructura de red (como enrutadores y servidores en línea) y la propia conexión de Internet.

Cloudflare impide un ataque de casi 2 TB/s

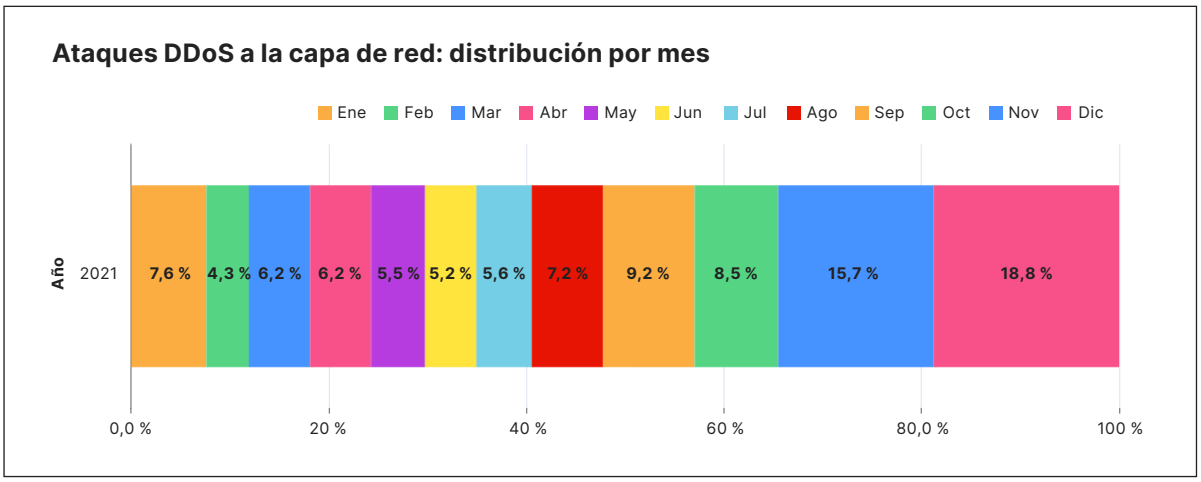
En noviembre, nuestros sistemas detectaron y mitigaron de manera automática un ataque DDoS de casi 2 TB/s. Se trataba de un ataque multivector que combinaba ataques de amplificación de DNS e inundaciones UDP. El ataque completo duró solo un minuto. Se lanzó desde aproximadamente 15.000 bots que ejecutaban una variante del código original de Mirai en dispositivos IoT e instancias de GitLab sin actualizar.



Ataques DDoS a la capa de red por mes

Diciembre fue el mes más activo para los atacantes en 2021.

El 4º trimestre fue el periodo de más actividad del año para los atacantes. Más del 43 % de todos los ataques DDoS a la capa de red ocurrieron en el 4º trimestre de 2021. Si bien octubre fue un mes relativamente más tranquilo, en noviembre, cuando se celebraron el Día del Soltero en China, la festividad estadounidense de Acción de Gracias, el *Black Friday* y el *Cyber Monday*, el número de ataques DDoS a la capa de red se duplicó prácticamente. El número de ataques observados aumentó en los últimos días de diciembre, cuando el mundo se preparaba para despedir el año. De hecho, solo en diciembre, el número total de ataques fue superior a todos los ataques del segundo trimestre de 2021 y casi equivalente a todos los ataques registrados en el primer trimestre.



Ataques DDoS a la capa de red por tasa de ataque

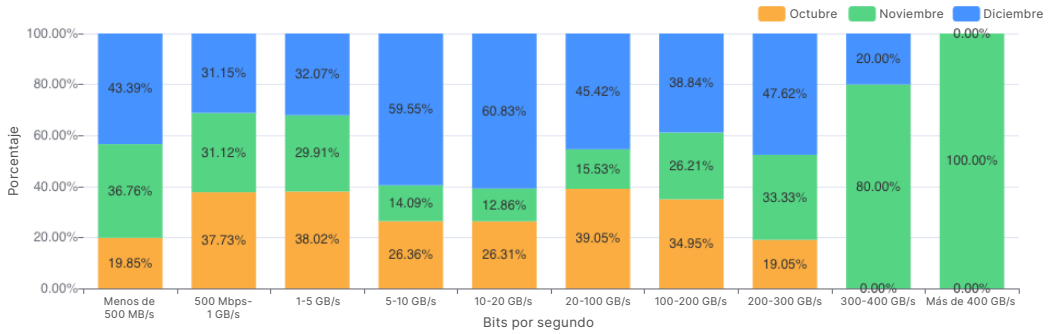
Si bien la mayoría de los ataques siguen siendo relativamente "pequeños" en tamaño, los ataques de varios terabits se están convirtiendo en la norma.

Hay diferentes formas de medir el tamaño de un ataque DDoS a las capas 3 y 4. Una es el volumen de tráfico que entrega, medido como la velocidad de bits (en concreto, terabits por segundo o gigabits por segundo). Otro es el número de paquetes que entrega, medido como la velocidad de paquetes (en concreto, millones de paquetes por segundo).

Los ataques con una velocidad de bits elevada tratan de provocar un evento de denegación de servicio bloqueando la conexión de Internet, mientras que los ataques con alta velocidad de paquetes tratan de saturar los servidores, enrutadores u otros dispositivos de hardware en línea. Estos dispositivos dedican una cierta cantidad de memoria y capacidad de procesamiento para procesar cada paquete. Por lo tanto, si se satura con muchos paquetes, el dispositivo se puede quedar sin recursos de procesamiento. En este caso, los paquetes se "descartan", es decir, el dispositivo no puede procesarlos. Para los usuarios, esto se traduce en interrupciones y denegación del servicio.

A continuación, se muestra la distribución de los ataques por su tamaño (en velocidad de bits) y mes. Como se observa en el gráfico anterior, la mayoría de los ataques sucedieron en diciembre. El gráfico siguiente muestra que los ataques más grandes, de más de 300 GB/s, tuvieron lugar en noviembre. La mayoría de los ataques de entre 5 y 20 GB/s ocurrieron en el último mes del año.

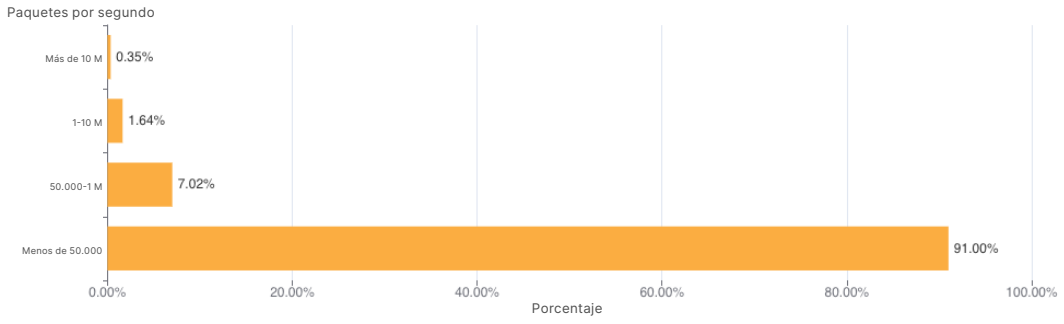
Ataques DDoS a la capa de red: distribución del tamaño por mes



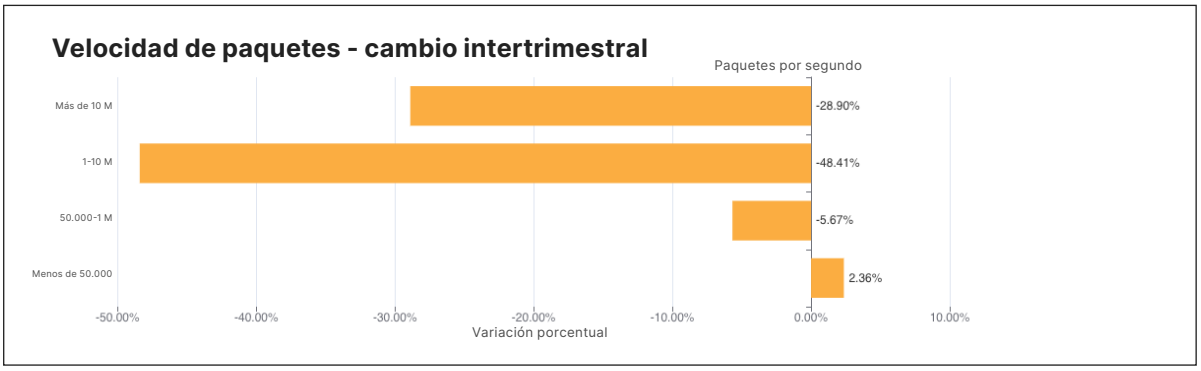
Distribución por velocidad de paquete

Una correlación interesante que Cloudflare ha observado es que cuando el número de ataques aumenta, su tamaño y duración disminuyen. En los ocho primeros meses de 2021, el número de ataques fue relativamente pequeño y, en consecuencia, sus velocidades aumentaron. Por ejemplo, en el tercer trimestre de 2021, los ataques de entre 1 y 10 millones de paquetes por segundo (mpps) se alzaron un 196 %. En el 4º trimestre, el número de ataques aumentó y Cloudflare observó un descenso en el tamaño de los ataques. El 91 % de todos los ataques alcanzaron un pico de tráfico inferior a 50.000 paquetes por segundo (pps), suficiente para interrumpir propiedades de Internet vulnerables.

Ataques DDoS a la capa de red: distribución por tasa de paquetes

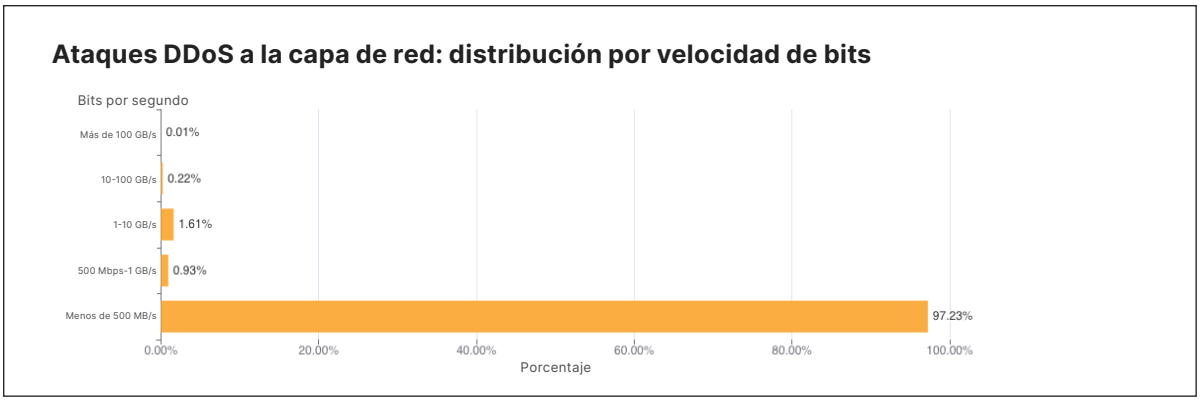


Los ataques más grandes, de más de 1 mpps, se redujeron un 48 % hasta un 28 % intertrimestral, mientras que los ataques con picos inferiores a 50.000 pps aumentaron un 2,36 % respecto al trimestre anterior.

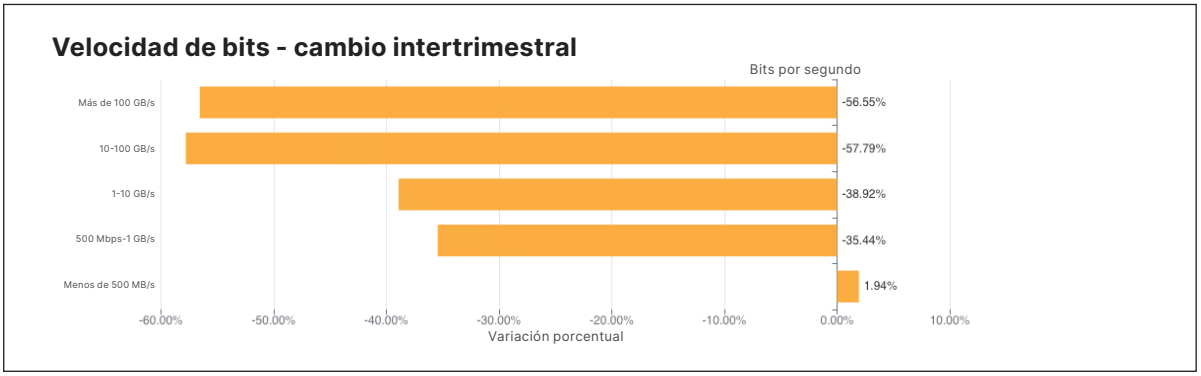


Distribución por velocidad de bits

Al igual que la tendencia observada en los ataques que generan gran cantidad de paquetes, el número de ataques que generan muchos bits también se redujo. Si bien los ataques de más de 1 TB/s se están convirtiendo en la norma, y el mayor que hemos visto alcanzó un pico de tráfico de casi 2 TB/s, la mayoría de los ataques siguen siendo pequeños y alcanzaron un pico inferior a 500 MB/s (97,2 %).



En el 4º trimestre del año pasado, los ataques más grandes de todos los rangos por encima de los 500 MB/s experimentaron descensos masivos que van del 35 % al 57 % en el caso de ataques más grandes de más de 100 GB/s.

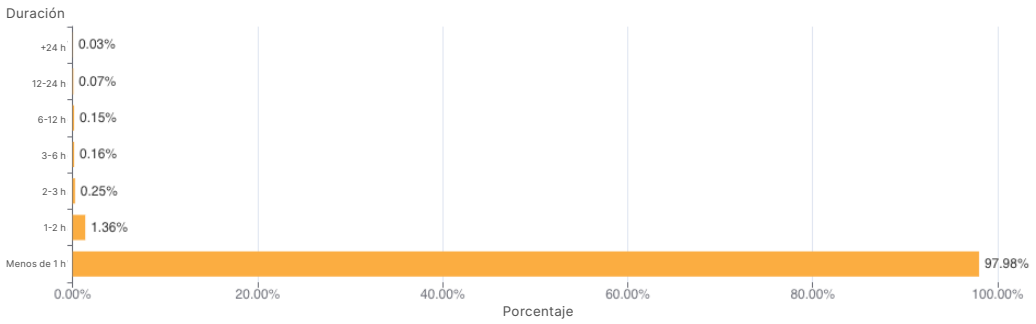


Ataques DDoS a la capa de red por duración

La mayoría de los ataques siguen teniendo una duración inferior a una hora, lo que reitera la necesidad de implementar soluciones automatizadas de mitigación de DDoS siempre activas.

Medimos la duración de un ataque registrando la diferencia entre el momento en que nuestros sistemas lo detectan por primera vez como un ataque y el último paquete que vemos con esa firma de ataque hacia ese objetivo específico. En el último trimestre de 2021, el 98 % de los ataques a la capa de red duraron menos de una hora. Es algo muy común ya que la mayoría de los ataques son de corta duración. Más aún, una tendencia que hemos observado es que cuando el número de ataques aumenta, como en este trimestre, su velocidad y duración disminuyen.

Ataques DDoS a la capa de red: distribución por duración



Los ataques breves pueden pasar fácilmente desapercibidos, sobre todo, los ataques en ráfaga que, en cuestión de segundos, atacan un objetivo con un número significativo de paquetes, bytes o solicitudes. En este caso, los servicios de protección contra DDoS que dependen de la mitigación manual mediante análisis de seguridad no tienen ninguna posibilidad de mitigar el ataque a tiempo. Solo pueden aprender de él en el análisis posterior al ataque, y luego implementar una nueva regla que filtre la huella digital del ataque y esperar a identificarlo la próxima vez. Del mismo modo, el uso de un servicio "a pedido", en el que el equipo responsable de la seguridad redirige el tráfico a un proveedor de DDoS durante el ataque, también es ineficiente porque el ataque ya habrá terminado antes de que el tráfico se dirija al proveedor de soluciones DDoS a pedido.

Se recomienda que las empresas utilicen servicios de protección contra DDoS automatizados y siempre activos que analicen el tráfico y apliquen una huella digital en tiempo real lo suficientemente rápido como para bloquear ataques de corta duración.

Vectores de ataque

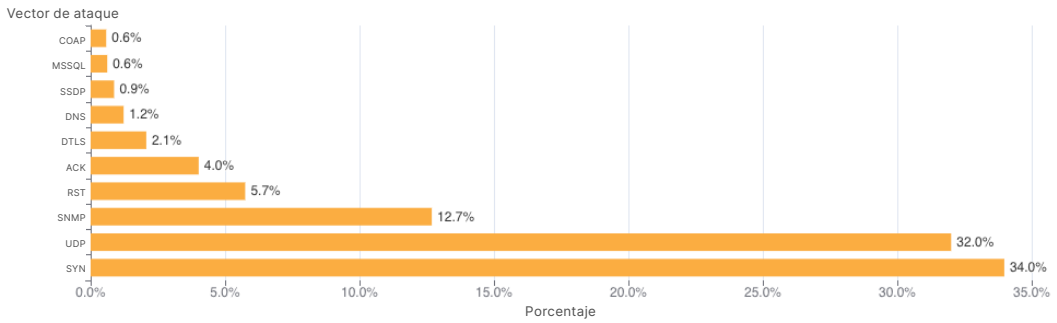
Las inundaciones SYN siguen siendo el método de ataque preferido de los atacantes, si bien los ataques con SNMP se dispararon casi un 5.800 % con respecto al trimestre anterior.

Un vector de ataque es un término utilizado para describir el método que el atacante utiliza para lanzar su ataque DDoS, p. ej., el protocolo IP, los atributos del paquete como las banderas TCP, el método de inundación y otros criterios. Por primera vez en 2021, el porcentaje de ataques de inundación SYN disminuyó significativamente. A lo largo del año, las inundaciones SYN representaron el 54 % de todos los ataques a la capa de red en promedio. Si bien siguen ocupando el primer puesto como vector más frecuente, su porcentaje descendió un 38 % respecto al trimestre anterior, hasta el 34 %.

Sin embargo, los ataques SYN y UDP se disputaron el segundo puesto. Una inundación UDP es un tipo de ataque de denegación de servicio en el que se envía un gran número de paquetes del protocolo de datagramas de usuarios (UDP) a un servidor objetivo con la intención de saturar la capacidad de ese dispositivo para procesar y responder. A menudo, el firewall que protege el servidor objetivo también puede abrumarse como resultado de la inundación UDP, lo que se traduce en una denegación de servicio para el tráfico legítimo. Los ataques a través de UDP pasaron del cuarto lugar en el tercer trimestre al segundo en el 4º trimestre. Representaron una cuota del 32 % de todos los ataques a la capa de red, lo que supone un aumento del 1.198 % en términos intertrimestrales.

En tercer lugar, se situó el ataque con SNMP, hasta ahora el menos favorito. Sin embargo, cobró importancia tras colarse por primera vez en 2021 entre los principales vectores de ataque.

Ataques DDoS a la capa de red: distribución por principales vectores de ataque



Amenazas emergentes

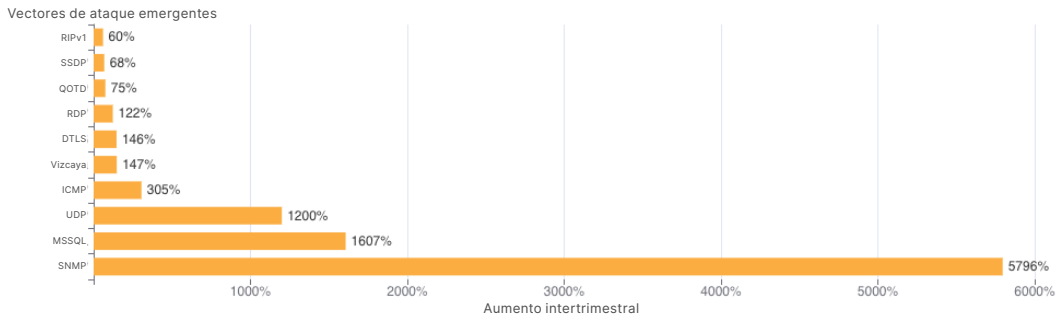
Cuando analizamos los vectores de ataque emergentes, lo que nos ayuda a entender qué nuevos vectores están usando los atacantes para lanzar ataques, observamos un pico masivo de ataques DDoS basados en SNMP, MSSQL y UDP genéricos.

Tanto los ataques SNMP como los MSSQL se utilizan para reflejar y amplificar el tráfico en el objetivo mediante la suplantación de la dirección IP del blanco como la dirección IP de origen en los paquetes utilizados para iniciar el ataque.

El protocolo simple de administración de redes (SNMP) es un protocolo basado en UDP que se suele utilizar para detectar y gestionar dispositivos de red como copiadoras, conmutadores, enrutadores y firewall de una red doméstica o empresarial en el conocido puerto UDP 161. En un ataque de reflexión SNMP, el atacante envía muchas consultas SNMP mientras suplanta la dirección IP de origen en el paquete como los objetivos a los dispositivos en la red que, a su vez, responden a la dirección de ese objetivo. Un gran número de respuestas de los dispositivos de red hace que la red de destino sea blanco de un ataque DDoS.

Al igual que el ataque de amplificación SNMP, el ataque Microsoft SQL (MSSQL) se basa en una técnica que abusa del protocolo de resolución de Microsoft SQL Server con el fin de lanzar un ataque DDoS de reflexión. El ataque se produce cuando un Microsoft SQL Server responde a una consulta o solicitud del cliente, intentando explotar el protocolo de resolución de Microsoft SQL Server (MC-SQLR), que escucha en el puerto UDP 1434.

Ataques DDoS a la capa de red: principales vectores de ataque emergentes



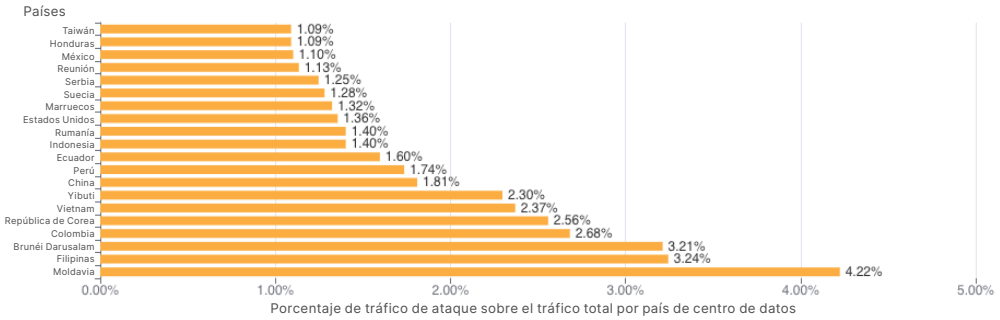
Ataques DDoS a la capa de red por país

Los ataques originados en Moldavia se cuadruplicaron, convirtiéndose así en el país con el mayor porcentaje de actividad DDoS en la capa de red.

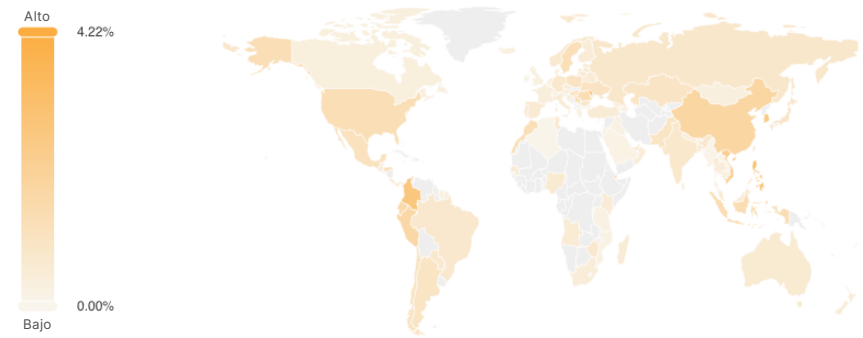
Al analizar los ataques DDoS a la capa de red, agrupamos el tráfico según las ubicaciones de los centros de datos perimetrales de Cloudflare donde se absorbió el tráfico, en lugar de la dirección IP de origen. El motivo es que, cuando los atacantes lanzan ataques a la capa de red, pueden suplantar la dirección IP de origen para ofuscar la procedencia del ataque e introducir aleatoriedad en las propiedades del mismo, lo que puede dificultar el bloqueo del ataque por parte de sistemas de protección DDoS simples. Por lo tanto, si tuviéramos que obtener el país de procedencia basándonos en una dirección IP de origen suplantada, obtendríamos un país falso.

Cloudflare es capaz de superar los desafíos de las direcciones IP falsas mostrando los datos de los ataques por la ubicación del centro de datos de Cloudflare en el que se observó el ataque. Podemos lograr exactitud geográfica en nuestro informe porque tenemos centros de datos en más de 250 ciudades de todo el mundo.

Actividad DDoS por país del centro de datos de Cloudflare



Ataques DDoS a la capa de red - Principales países (a nivel mundial)



Para ver todas las regiones y países, consulta el mapa interactivo.

Resumen

La misión de Cloudflare es ayudar a mejorar Internet. Una red más eficiente es aquella que es más segura, rápida y confiable para todos, incluso frente a los ataques DDoS. Como parte de nuestra misión, desde 2017, hemos estado ofreciendo protección DDoS ilimitada y de uso no medido a todos nuestros clientes, sin cargo. A lo largo de los años, a los atacantes les resulta cada vez más fácil lanzar ataques DDoS. Para contrarrestar su ventaja, queremos asegurarnos de que también sea fácil y gratuito para todo tipo de organizaciones protegerse de ataques DDoS de cualquier índole.

¿Aún no tienes cuenta en Cloudflare? Únete ahora.