INFORMACIÓN DE SEGURIDAD DE CLOUDFLARE

CLOUDFLARE

Tendencias de ataques DDoS durante el segundo trimestre de 2021

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

En las últimas semanas se han producido campañas masivas de ataques de ransomware y DDoS (denegación de servicio distribuido) de rescate que han interrumpido partes importantes de la infraestructura de todo el mundo, entre ellas, uno de los mayores operadores de sistemas de oleoductos y una de las principales empresas cárnicas del mundo. A principios de este trimestre, más de 200 organismos en toda Bélgica, como los sitios web del Gobierno y del parlamento y otros servicios, también se vieron afectados por ataques DDoS.

Cuando la mayor parte de Estados Unidos celebraba el Día de la Independencia el 4 de julio, cientos de empresas estadounidenses se vieron afectadas por un ataque de ransomware que exigía 70 millones de dólares en bitcoin. Los atacantes en ruta conocidos por estar afiliados a REvil, un grupo de ransomware ruso, explotaron múltiples vulnerabilidades previamente desconocidas en el software de administración de TI. Los objetivos incluían escuelas, pequeños organismos del sector público, agencias de viajes y ocio, y cooperativas de crédito, por mencionar algunos. Si bien la amenaza de ransomware y DDoS de rescate no es nueva (lee nuestras publicaciones sobre ransomware y DDoS de rescate del primer trimestre de 2021), los últimos ataques a propiedades de Internet que van desde bodegas, equipos deportivos profesionales, servicios de ferry y hospitales los han llevado de ser ruido de fondo a grandes titulares que afectan nuestra vida cotidiana. De hecho, los ataques recientes han hecho que el ransomware y los ataques DDoS sean prioridad en la agenda de seguridad nacional del presidente Biden de EE. UU.

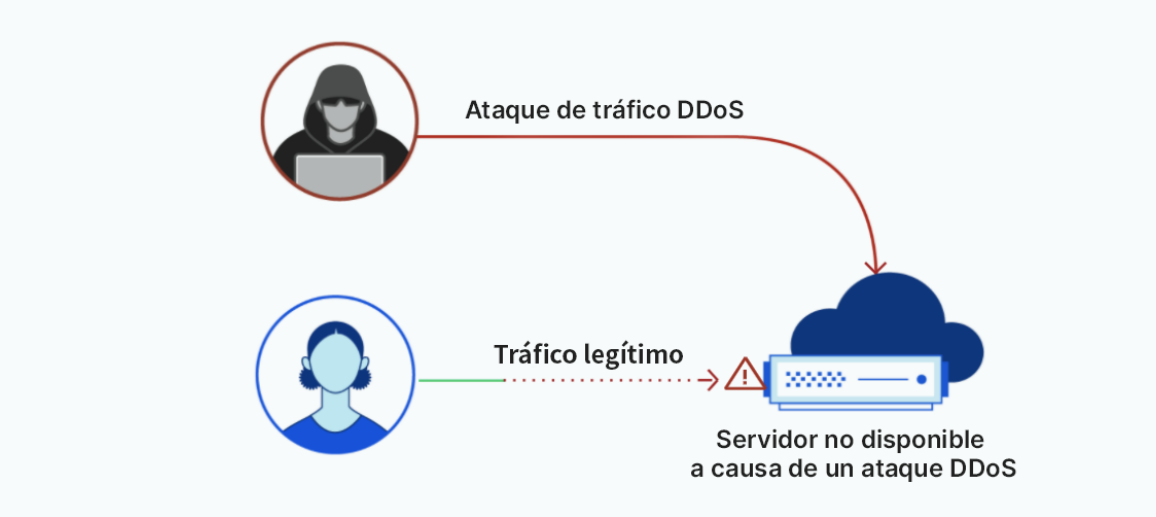
Las tendencias de ataque DDoS observadas en la red de Cloudflare en el segundo trimestre de 2021 presentan una imagen que describe el panorama global de amenazas cibernéticas. Aquí se muestran algunos aspectos destacados de las tendencias de ataques DDoS observadas en el segundo trimestre de 2021.

- Más del 11 % de nuestros clientes encuestados que fueron blanco de un ataque DDoS informaron que recibieron previamente una amenaza o una solicitud de rescate con amenazas, en los primeros seis meses de este año. Las incorporaciones urgentes de clientes víctimas de un ataque DDoS activo aumentaron un 41,8 % en el primer semestre de 2021 en comparación con el segundo semestre de 2020.
- Los ataques DDoS de HTTP dirigidos a los sitios web de la administración/sector público aumentaron un 491 %, lo que los convierte en la segunda industria más atacada después de servicios al consumidor, cuya actividad DDoS creció un 684 % respecto al trimestre anterior.
- China sigue siendo el país con la mayor cantidad de actividad DDoS que se origina dentro de sus fronteras: 7 de cada 1000 solicitudes HTTP que se originan en China fueron parte de un ataque DDoS de HTTP dirigido a sitios web, y más de 3 de cada 100 bytes procesados en nuestros centros de datos en China fueron parte de un ataque DDoS a la capa de red.
- Las amenazas emergentes incluyeron ataques DDoS de amplificación que abusaron del protocolo Quote of the Day (QOTD), que aumentaron un 123 % respecto al trimestre anterior. Además, a medida que la adopción del protocolo QUIC continúa aumentando, también lo hacen los ataques sobre QUIC, que se dispararon un 109 % en el segundo trimestre respecto al primer trimestre de 2021.
- El número de ataques DDoS a la capa de red en el rango de 10-100 Gbps aumentó un 21,4 % entre un trimestre y otro. Un cliente que fue atacado es Hypixel, una empresa estadounidense de videojuegos. Hypixel se mantuvo conectado sin tiempo de inactividad y sin que el rendimiento para sus usuarios se viera afectado, incluso cuando se encontraba bajo una campaña activa de ataque DDoS de más de 620 Gbps. Lee su historia aquí.

Para ver todas las perspectivas de ataques DDoS en todas las regiones y sectores del mundo, visita el panel de control interactivo Radar DDoS de Cloudflare.

Ataques DDoS a la capa de aplicación

Los ataques DDoS en la capa de aplicación, específicamente los ataques DDoS de HTTP, son ataques que generalmente tienen como objetivo interrumpir un servidor HTTP al hacer que no pueda procesar solicitudes de usuarios legítimos. Si un servidor es bombardeado con más solicitudes de las que puede procesar, el servidor descartará las solicitudes legítimas o incluso se bloqueará, lo que afectará al rendimiento u originará un evento de denegación de servicio para los usuarios legítimos.

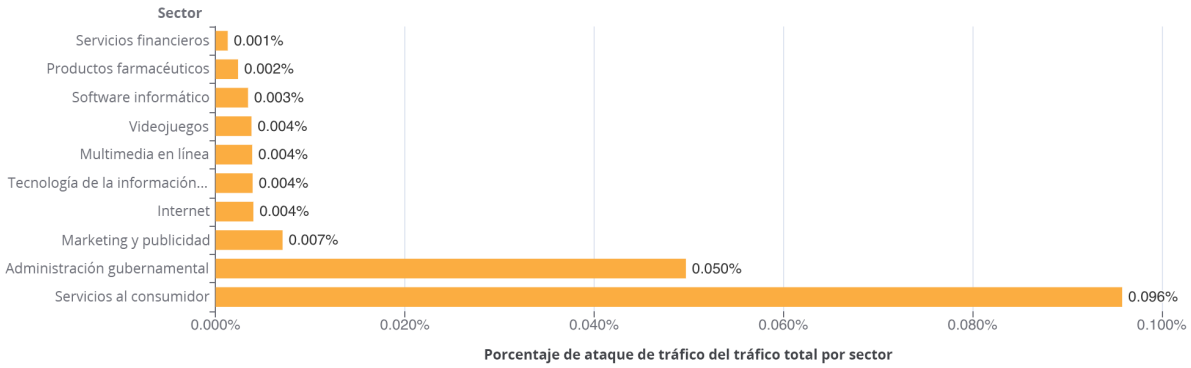


Actividad DDoS por sector

Cuando analizamos los ataques, calculamos la tasa de "actividad DDoS", que es el porcentaje de ataques de tráfico del tráfico total (ataque + legítimo). Esto nos permite normalizar los puntos de datos y evitar sesgos, por ejemplo, hacia un centro de datos más grande que maneja naturalmente más tráfico y, por lo tanto, también más ataques.

En el segundo trimestre de 2021, el sector de los servicios al consumidor fue objeto principal de los ataques, seguido por la administración pública y el sector del marketing y la publicidad.

Ataques DDoS a la capa de aplicación (7): distribución por industria

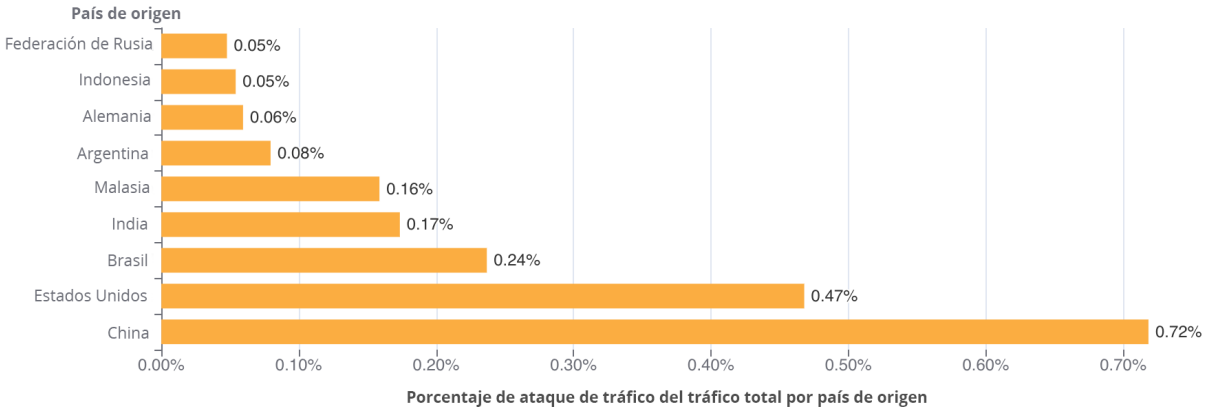


Actividad de DDoS por país de origen

Para comprender el origen de los ataques HTTP que observamos en la red de Cloudflare, observamos la dirección IP de origen del cliente que genera las solicitudes HTTP de ataque. A diferencia de los ataques de capa de red, las direcciones IP de origen no se pueden falsificar en los ataques HTTP. Una alta tasa de actividad DDoS en un país determinado indica grandes botnets que operan desde dentro.

China y EE. UU. permanecen en el primer y segundo lugar, respectivamente, con respecto al porcentaje de actividad DDoS que se origina dentro de sus territorios. En China, más de 7 de cada 1000 solicitudes HTTP fueron parte de un ataque HTTP DDoS, mientras que en EE. UU. casi 5 de cada 1000 solicitudes HTTP fueron parte de un ataque.

Ataques DDoS a la capa de aplicación (7): distribución por país (a nivel mundial)

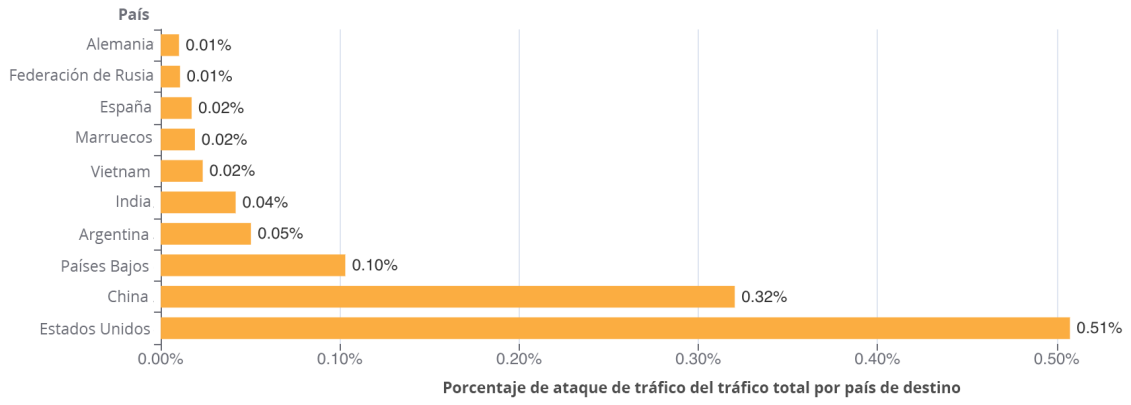


Actividad DDoS por país de destino

Con el fin de identificar en qué países residieron los objetivos de los ataques DDoS, desglosamos la actividad DDoS por parte de los países de facturación de nuestros clientes. Ten en cuenta que Cloudflare no cobra por el tráfico de ataque y ha sido pionero en proporcionar protección DDoS ilimitada y gratuita desde 2017. Mediante la comparación de los datos de ataque y el país de facturación de nuestros clientes, podemos identificar qué países recibieron más ataques.

Los datos observados en el segundo trimestre de 2021 sugieren que las organizaciones de EE. UU. y China fueron las más afectadas por los ataques DDoS de HTTP. De hecho, una de cada 200 solicitudes HTTP destinadas a organizaciones con sede en EE. UU. fue parte de un ataque DDoS.

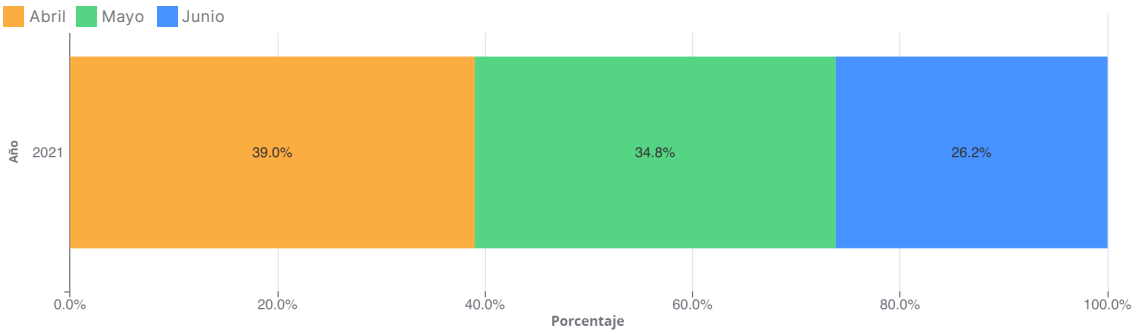
Ataques DDoS a la capa de aplicación (7): distribución por país de destino



Ataques DDoS en la capa de red

Si bien los ataques a la capa de aplicación (capa 7 del modelo OSI) atacan la aplicación que ejecuta el servicio al que los usuarios finales intentan acceder, los ataques a la capa de red se dirigen a la infraestructura de red expuesta (como enrutadores en línea y otros servidores de red) y al propio enlace de Internet.

Ataques DDoS a la capa de red: distribución por mes



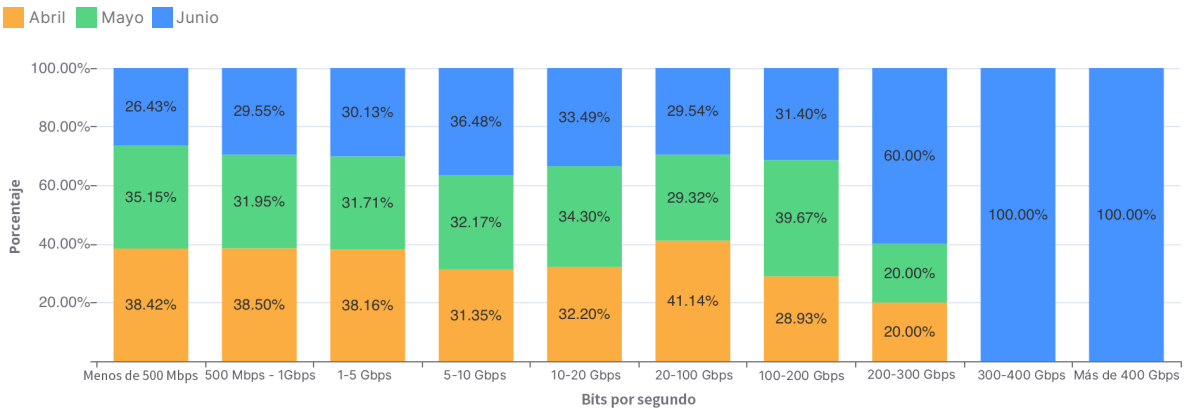
El gráfico anterior muestra la distribución de los ataques DDoS en la capa de red en el segundo trimestre de 2021.

Distribución de ataques por tamaño (tasa de paquetes y tasa de bits)

Hay diferentes formas de medir el tamaño de un ataque DDoS de capa 3/4. Uno es el volumen de tráfico que entrega, que se mide como la tasa de bits (en concreto, gigabits por segundo). Otro es el número de paquetes que entrega, que se mide como la tasa de paquetes (en concreto, paquetes por segundo). Los ataques con una tasa elevada de bits intentan saturar el enlace de Internet, mientras que los ataques con una alta tasa de paquetes buscan sobrecargar los servidores, enrutadores u otros dispositivos de hardware en línea.

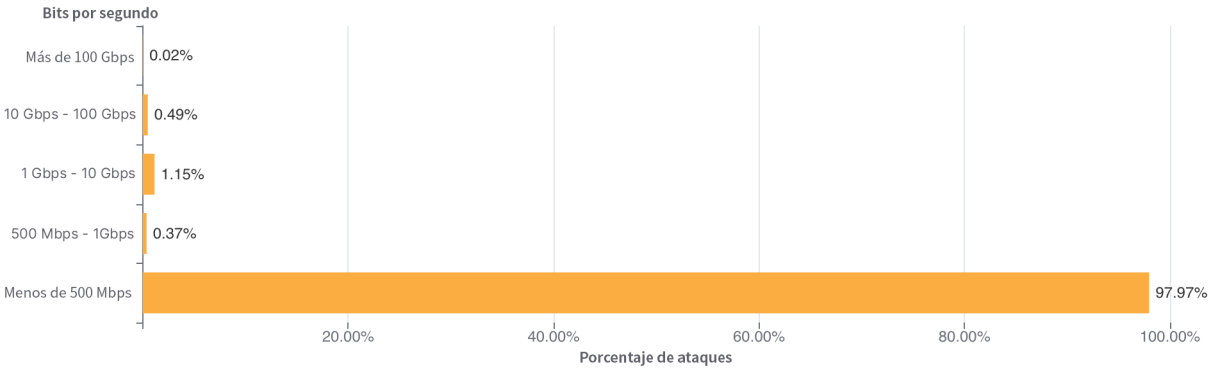
La distribución de los ataques por tamaño (en tasa de bits) y mes se muestra a continuación. Como se observa en el gráfico, todos los ataques superiores a 300 Gbps se observaron en el mes de junio.

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



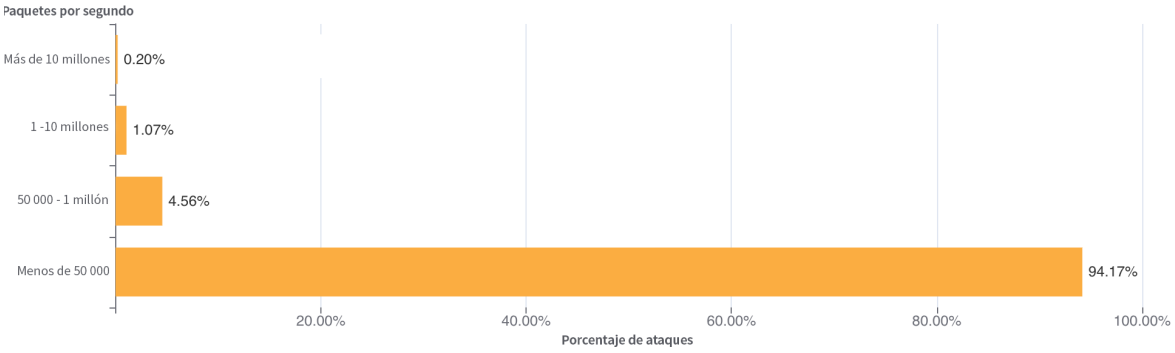
En términos de velocidad de bits, los ataques por debajo de 500 Mbps representaron la mayoría de todos los ataques DDoS observados en el segundo trimestre de 2021.

Ataques DDoS a la capa de red: distribución por velocidad de bits



De manera similar, desde la perspectiva de la tasa de paquetes, casi el 94 % de los ataques fueron por debajo de 50 K pps. Aunque los ataques de 1 a 10 millones de pps constituyeron solo el 1 % de todos los ataques DDoS observados, este número es un 27,5 % más alto que el observado en el trimestre anterior, lo que sugiere que los ataques más grandes lejos de disminuir, están aumentando.

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



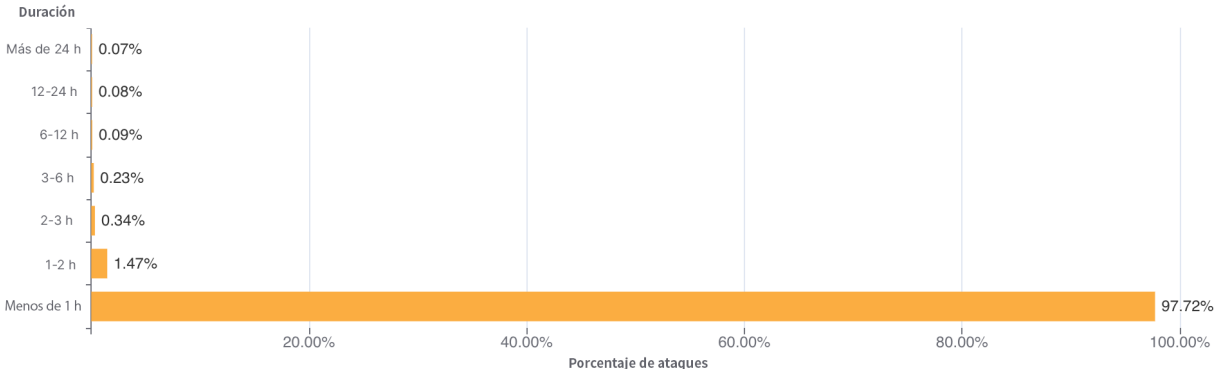
Toma en cuenta que, si bien los ataques de menos de 500 Mbps y 50 K pps pueden parecer "pequeños" en comparación con otros grandes ataques que acaparan titulares, a menudo son suficientes para crear interrupciones importantes en las propiedades de Internet que no están protegidas por un servicio de protección DDoS automatizado y siempre activo basado en la nube. Además, muchas organizaciones tienen enlaces ascendentes proporcionados por sus proveedores de servicios con una capacidad de ancho de banda inferior a 1 Gbps. Suponiendo que su interfaz de red orientada al público también sirva tráfico legítimo, los ataques DDoS de menos de 500 Mbps a menudo son capaces de acabar con las propiedades de Internet expuestas.

Distribución por duración de ataque

Cloudflare sigue viendo un gran porcentaje de ataques DDoS que duran menos de una hora. En el segundo trimestre, más del 97% de todos los ataques DDoS duraron menos de una hora.

Los ataques breves pero intensos pueden tratar de causar daños sin ser detectados por los sistemas de detección de DDoS. Los servicios DDoS que dependen del análisis y la mitigación manuales pueden resultar inútiles contra este tipo de ataques, que terminan incluso antes de que el analista identifique el tráfico de ataque.

Duración del ataque



Los ataques cortos también se utilizan a menudo para sondear las ciberdefensas del objetivo. Las herramientas de prueba de carga y las herramientas DDoS automatizadas, ampliamente disponibles en la web oscura, pueden generar, por ejemplo, una inundación SYN intensa y breve y luego seguir con otro ataque corto mediante un vector de ataque alternativo. Esto permite a los atacantes comprender la postura de seguridad de sus objetivos antes de que decidan lanzar ataques más grandes, con una tasa más elevada y con duraciones más largas, lo cual conlleva un costo.

En otros casos, los atacantes generan pequeños ataques DDoS como prueba y advertencia para la organización objetivo de la capacidad del atacante para causar daños reales más adelante. A menudo, a estas advertencias les sigue un correo electrónico de ransomware exigiendo a la organización el pago de un rescate para evitar un ataque que podría paralizar totalmente la infraestructura de red.

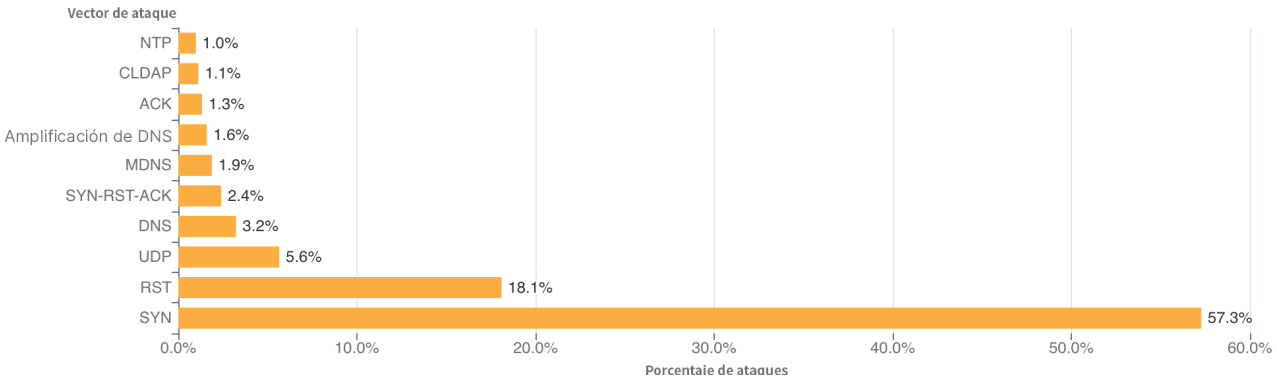
Esto destaca la necesidad de contar con un enfoque de protección DDoS automatizado y siempre activo. Los servicios de protección DDoS que dependen del reenrutamiento, el análisis y la mitigación de forma manual pueden resultar inútiles contra este tipo de ataques, que terminan incluso antes de que el analista identifique el ataque de tráfico.

Distribución de los ataques por vectores de ataque

Un vector de ataque es el término utilizado para describir el método que utiliza el atacante en su intento por causar un evento de denegación de servicio.

Como se observó en trimestres anteriores, los ataques que utilizan inundaciones SYN y protocolos basados en UDP siguen siendo los métodos más populares por los atacantes.

Ataques DDoS en la capa de red: vectores de ataque principales



¿Qué es un ataque de inundación SYN? Es un ataque DDoS que aprovecha la base misma de un protocolo TCP. Una conexión TCP con estado (stateful) entre un cliente y un servidor comienza con un protocolo de enlace TCP de 3 vías. El cliente envía un paquete de solicitud de conexión inicial con una marca de sincronización (SYN). El servidor responde con un paquete que contiene una marca de reconocimiento de sincronización (SYN-ACK). Por último, el cliente responde con un paquete de reconocimiento (ACK). En este punto, se establece una conexión y se pueden intercambiar datos hasta que se cierra la conexión. Los atacantes pueden abusar de este proceso con estado para causar eventos de denegación de servicio.

Al enviar repetidamente paquetes SYN, el atacante intenta sobrecargar un servidor o la tabla de conexión del enrutador que rastrea el estado de las conexiones de TCP. El enrutador responde con un paquete SYN-ACK, asigna una cierta cantidad de memoria para cada conexión dada y espera, de manera falsa, a que el cliente responda con el ACK final. Dada la cantidad suficiente de conexiones que ocupan la memoria del enrutador, el enrutador no puede asignar más memoria para clientes legítimos, lo que hace que el enrutador se bloquee o evita que maneje conexiones legítimas del cliente, esto es, un evento de denegación de servicio.

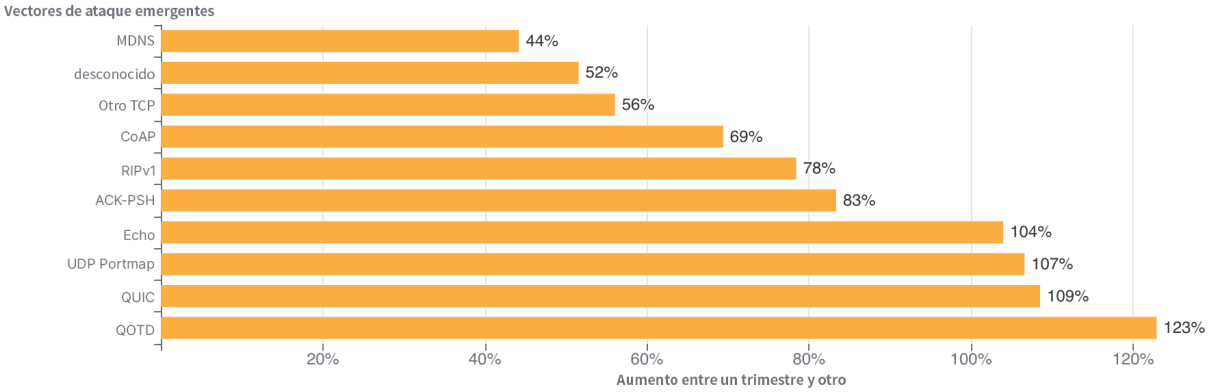
Amenazas emergentes

Las amenazas emergentes incluyeron ataques DDoS de amplificación que abusan del servicio Quote of the Day (QOTD), que aumentaron un 123 % entre un trimestre y otro. QOTD se definió en RFC-865 (1983) y se puede enviar a través de los protocolos UDP o TCP. Se diseñó originalmente para depurar y como una herramienta de medición, sin sintaxis específica para la cotización. Sin embargo, RFC recomienda usar caracteres ASCII y limitar la longitud a 512 caracteres.

Además, se ha observado un aumento del 107 % en los ataques UDP Portmap y Echo, que son vectores de ataque muy antiguos. Por lo tanto, parece ser que los atacantes están recurriendo a métodos y herramientas de ataque antiguos para intentar neutralizar los sistemas de protección.

Como hemos visto en trimestres anteriores, la adopción del protocolo QUIC sigue aumentando. En consecuencia, también lo hacen los ataques a través de QUIC, o más específicamente las inundaciones y los ataques de amplificación de tráfico sin el protocolo QUIC en lugares donde cabría esperar tráfico QUIC. En el segundo trimestre de 2021, este tipo de ataques aumentaron un 109 % en comparación con el trimestre anterior. Esta tendencia incesante puede indicar que los atacantes intentan abusar de los puertos y puertas de enlace designados para QUIC en las redes de las organizaciones, en busca de vulnerabilidades y carencias de seguridad.

Ataques DDoS en la capa de red: principales vectores de amenazas emergentes

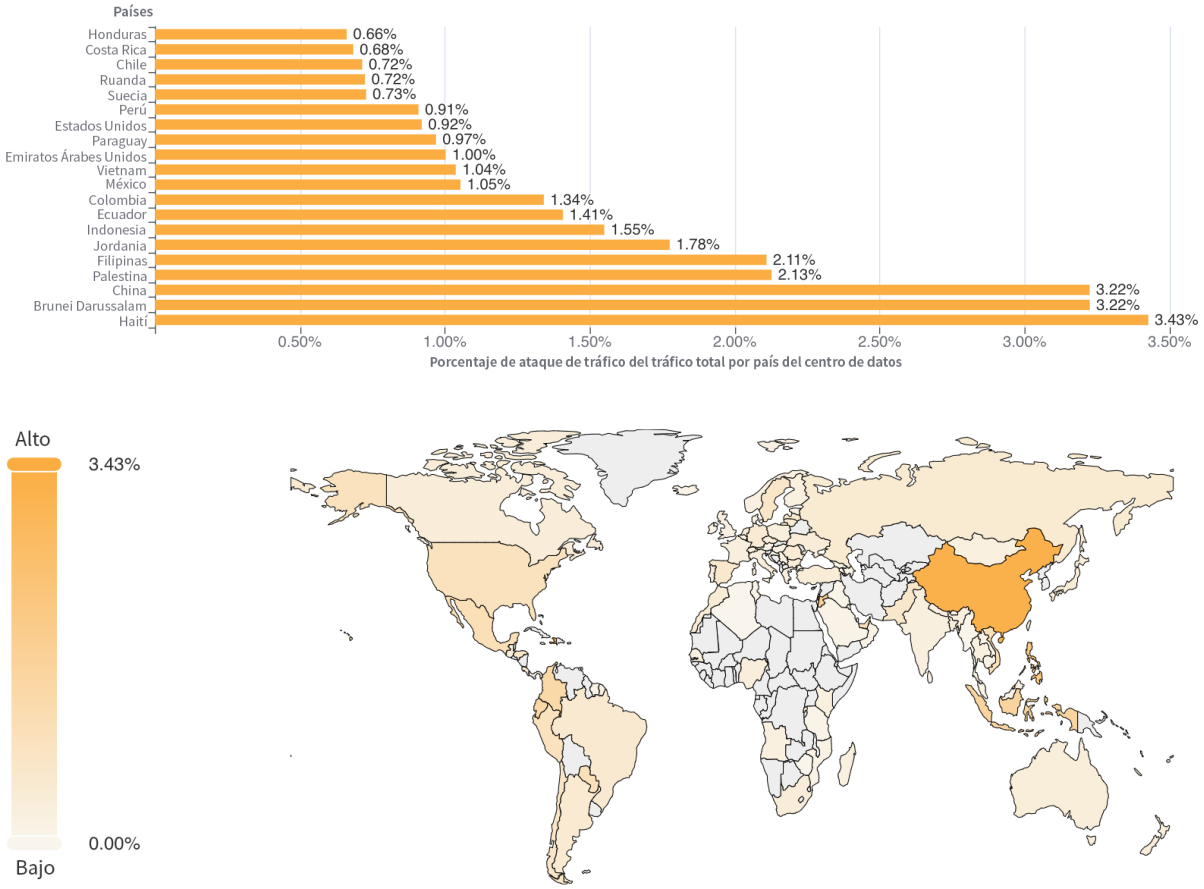


Actividad DDoS por país del centro de datos de Cloudflare

En el segundo trimestre de 2021, nuestro centro de datos en Haití observó el mayor porcentaje de ataques de tráfico DDoS en la capa de red, seguido por Brunei (casi 3 de cada 100 paquetes fueron parte de un ataque) y China.

Toma en cuenta que al analizar los ataques DDoS en la capa de red, agrupamos el tráfico por las ubicaciones del centro de datos del perímetro de Cloudflare donde se procesa el tráfico y no por la IP de origen. Esto se debe a que cuando los atacantes lanzan ataques a la capa de red pueden falsificar la dirección IP de origen para ofuscar la fuente del ataque e introducir aleatoriedad en las propiedades del ataque, lo que puede dificultar que los sistemas de protección DDoS simples bloqueen el ataque. Por lo tanto, si tuviéramos que derivar el país de origen en función de una IP de origen falsificada, obtendríamos un país falsificado. Cloudflare puede superar los desafíos de las IP falsificadas al mostrar los datos del ataque por ubicación del centro de datos de Cloudflare en el que se observó el ataque. Podemos lograr una precisión geográfica en nuestro informe porque tenemos centros de datos en más de 200 ciudades en todo el mundo.

Ataques DDoS en la capa de red: principales países (a nivel mundial)



Para ver todas las regiones y todos los países, consulta el [mapa interactivo del panel de control de Radar DDoS Report](#).

Ransomware y ataques DDoS de rescate: una amenaza global creciente

En las últimas semanas se ha producido un aumento de las amenazas cibernéticas basadas en el pago de un rescate: ransomware y ataques DDoS de rescate (RDDoS).

Entonces, ¿qué es el ransomware y el DDoS de rescate, y en qué se diferencian?

El ransomware es un software malicioso que cifra los sistemas y las bases de datos de una organización, haciéndolos inaccesibles e inutilizables. El malware generalmente se introduce en los sistemas de una organización a través de correos electrónicos de phishing, engañando a los empleados para que hagan clic en un enlace o descarguen un archivo. Una vez que el malware está instalado en el dispositivo del empleado, cifra el dispositivo y puede propagarse a toda la red de los servidores de la organización y los dispositivos de los empleados. El atacante exigirá dinero, generalmente en forma de bitcoin, a cambio de descifrar los sistemas de la organización y otorgarles acceso a sus sistemas.

A diferencia de un ataque de ransomware, un ataque DDoS de rescate no cifra los sistemas de una empresa. Su objetivo es dejarlos fuera de línea si no se paga el rescate. Lo que hace que los ataques DDoS de rescate sean aún más peligrosos es que no requieren que el atacante obtenga acceso a los sistemas internos de un negocio para ejecutar el ataque. Sin embargo, con una sólida estrategia de protección DDoS implementada, un ataque DDoS de rescate tiene poco o ningún efecto en los negocios.

Las amenazas de ransomware y DDoS de rescate están afectando a la mayoría de los sectores en todo el mundo: financiero, transporte, petróleo y gas, bienes de consumidor e incluso educación y atención médica.

Las entidades que dicen ser "Fancy Lazarus", "Fancy Bear", "Lazarus Group" y "REvil" están lanzando una vez más ataques de ransomware y DDoS de rescate contra los sitios web y la infraestructura de red de las organizaciones, a menos que se pague un rescate antes de una fecha límite determinada. En el caso de las amenazas DDoS, antes de solicitar un rescate, se suele lanzar un pequeño ataque DDoS como prueba. El ataque de demostración por lo general es superior al UDP, que dura aproximadamente 30-120 minutos.

La exigencia de rescate suele enviarse a los alias de correo electrónico comunes de la empresa que están disponibles públicamente en línea, como noc@, support@, help@, legal@, abuse@, etc. En varios casos, ha terminado en la carpeta de spam. En otros casos, hemos visto que los empleados ignoran la solicitud de rescate como spam, lo que aumenta el tiempo de respuesta de la organización y resulta en un daño mayor a sus propiedades en línea.

Recomendaciones de Cloudflare para las organizaciones que reciban una amenaza o se les exija el pago de un rescate:

1. **No entres en pánico y no pagues el rescate:** hacerlo solo fomenta y financia a los actores malintencionados. Tampoco existe garantía de que no vuelvas a ser atacado de ninguna manera.
2. **Ponte en contacto con las autoridades locales:** prepara una copia de la solicitud de rescate que has recibido y cualquier otro registro o captura de paquetes.
3. **Activa una estrategia de protección DDoS eficaz:** la protección DDoS basada en la nube se puede incorporar rápidamente en caso de una amenaza activa y, con un equipo de expertos en seguridad a tu lado, los riesgos se pueden mitigar de forma rápida y eficaz.

Aquí encontrarás un breve video del director técnico de Cloudflare, John Graham-Cumming, que aborda la amenaza de los ataques DDoS de rescate.

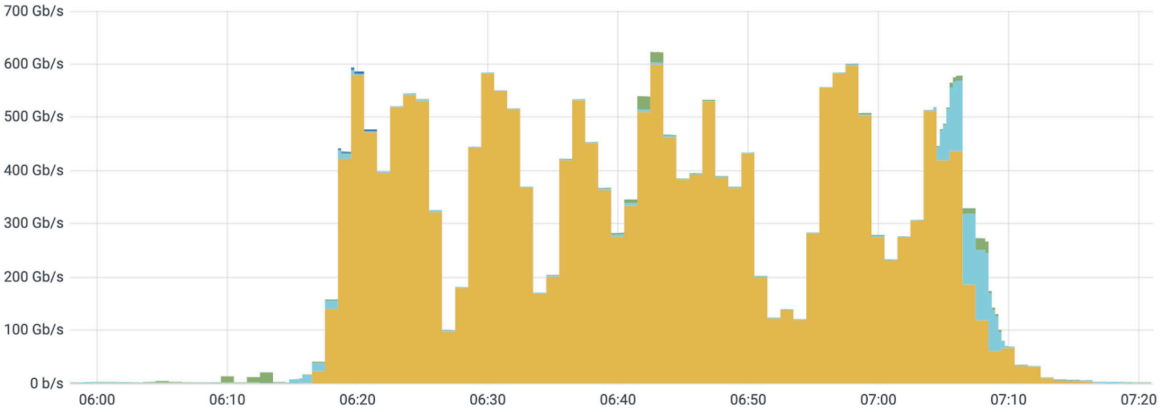
Cloudflare protege a Hypixel contra una campaña masiva de DDoS

Los equipos de Cloudflare han tenido más trabajo de lo habitual en el último trimestre integrando nuestro servicio Magic Transit en los sistemas de varios clientes nuevos y otros ya establecidos, a quienes les estaban exigiendo el pago de un rescate o estaban siendo objetivo de un ataque DDoS activo.

Uno de esos clientes es Hypixel Inc, el estudio de desarrollo detrás del servidor de minijuegos Minecraft más grande del mundo. Con más de 24 millones de inicios de sesión únicos en total hasta la fecha y un récord mundial de más de 216 000 jugadores simultáneos en PC, el equipo de Hypixel trabaja arduamente para agregar valor a la experiencia de millones de jugadores en todo el mundo.

La industria de videojuegos suele ser objetivo de algunos de los ataques DDoS volumétricos más grandes y, como marca reconocida, Hypixel ha sufrido más ataques de lo normal. El tiempo activo y el alto rendimiento son fundamentales para el funcionamiento de los servidores de Hypixel. Cualquier percepción de tiempo de inactividad o retraso detectable podría tener como consecuencia un éxodo de jugadores.

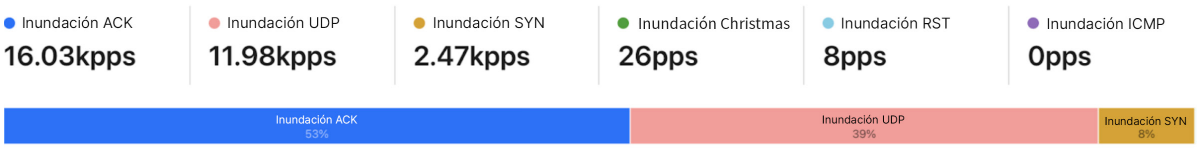
Cuando Hypixel estaba siendo objetivo de una campaña masiva de ataques DDoS, recurrieron a Cloudflare para extender sus servicios con Cloudflare e incluir Magic Transit, el servicio de protección DDoS basado en BGP de Cloudflare para infraestructura de red. Después de incorporarlos rápidamente durante la noche, Cloudflare pudo detectar y mitigar automáticamente los ataques DDoS dirigidos a su red, muchos de los cuales superaron los 620 Gbps. El ataque DDoS constó principalmente de inundaciones de TCP y ataques de amplificación de UDP. En el gráfico, los distintos colores representan los múltiples sistemas de Cloudflare que contribuyen a detectar y mitigar el ataque multivector, al enfatizar el valor de nuestro enfoque DDoS de múltiples capas.



Incluso cuando los patrones de ataque cambiaron en tiempo real, Magic Transit protegió la red de Hypixel. De hecho, debido a que todo su tráfico legítimo se enrutaba a través de la red de baja latencia y alto rendimiento de Cloudflare, los usuarios de Hypixel no observaron ningún cambio en la experiencia del jugador, incluso durante un ataque DDoS volumétrico activo.

Durante la campaña de ataques, Cloudflare detectó y mitigó automáticamente más de 5000 ataques DDoS: el 53 % eran inundaciones ACK, el 39 % eran ataques basados en UDP y el 8 % inundaciones SYN.

Distribución de tipo de ataques



> "Sufrimos varios ataques de más de 620 Gbps sin ningún impacto en nuestros jugadores, cuya experiencia de videojuego siguió siendo rápida y sin interrupciones, gracias a Cloudflare Magic Transit".
>
> Simon Collins-Laflamme
> **Director general, Hypixel Inc.**

El recorrido de Hypixel con Cloudflare comenzó con el uso de Cloudflare Spectrum para ayudar a proteger su infraestructura de videojuegos contra ataques DDoS. A medida que su base de usuarios crecía, adoptaron productos adicionales de Cloudflare para reforzar la solidez y resiliencia de toda su infraestructura crítica. Hoy en día, utilizan múltiples productos de Cloudflare, incluidos CDN, Limitación de velocidad, Spectrum, Argo Smart Routing y Load Balancing para desarrollar y proteger una infraestructura que ofrezca a los jugadores de todo el mundo las experiencias de videojuego en tiempo real que necesitan.

Obtener protección integral contra ciberataques de cualquier tipo

Los ataques DDoS constituyen solo una faceta de las muchas amenazas cibernéticas que las organizaciones están enfrentando hoy en día. A medida que las empresas cambian a un enfoque Zero Trust, los compradores de red y seguridad se enfrentarán a amenazas más grandes relacionadas con el acceso a la red, y un aumento continuo en la frecuencia y sofisticación de los ataques relacionados con bots y ransomware.

Un principio de diseño clave al crear productos en Cloudflare es la integración. Cloudflare One es una solución que utiliza un modelo de seguridad Zero Trust para proporcionar a las empresas una mejor manera de proteger dispositivos, datos y aplicaciones, y está profundamente integrado con nuestra plataforma existente de seguridad y soluciones DDoS.

De hecho, Cloudflare ofrece una solución integrada con productos estrella tales como:

- **DDoS:** Líder en el informe de "The Forrester Wave™: DDoS Mitigation Solutions" del primer trimestre de 2021[1].
- **WAF:** Cloudflare fue reconocido como Aspirante en el informe de Gartner: Magic Quadrant for Web Application Firewall de 2020 (con la mejor clasificación en "Capacidad de ejecución")[2].
- **Zero Trust:** Cloudflare fue nombrado líder en el informe Omdia Market Radar: Zero Trust Access de 2020[3].
- **Protección web:** Líder en innovación en el informe Global Holistic Web Protection Market de 2020 de Frost & Sullivan[4].

La red global (y en crecimiento) de Cloudflare se encuentra en una posición inmejorable para ofrecer protección DDoS y otros servicios de seguridad, rendimiento y fiabilidad con una escala, velocidad e inteligencia incomparables.

Para más información acerca de la solución DDoS de Cloudflare contáctanos o empieza ahora.

REFERENCIAS

[1] Forrester Wave™: DDoS Mitigation Solutions, T1 de 2021, Forrester Research, Inc., 3 de marzo de 2021. Accede al informe en https://www.cloudflare.com/es-la/forrester-wave-ddos-mitigation-2021/

[2] Gartner, “Magic Quadrant for Web Application Firewalls", analistas: Jeremy D'Hoinne, Adam Hils, John Watts, Rajpreet Kaur, 19 de octubre de 2020. https://www.cloudflare.com/es-la/gartner-mq-waf-2020/

[3] https://www.cloudflare.com/es-la/lp/omdia-zero-trust

[4] https://www.cloudflare.com/es-la/lp/frost-radar-holistic-web/