CLOUDFLARE

Informe de Cloudflare sobre amenazas DDoS

2º trimestre de 2023

Contenido

Resumen ejecutivo

Te damos la bienvenida al informe trimestral de Cloudflare sobre los ataques de denegación de servicio distribuido (DDoS) del segundo trimestre de 2023. Este documento revela información y tendencias importantes sobre las amenazas de los ataques DDoS que se observaron en la red global de Cloudflare entre abril y junio de 2023.

Estos meses se caracterizaron por oleadas de campañas de ataques DDoS bien planificadas, especializadas y persistentes en distintos frentes.

En la capa HTTP, detectamos que los grupos hacktivistas prorrusos REvil, Killnet y Anonymous Sudan estuvieron muy activos contra sitios web de países occidentales, y observamos un repunte de los ataques DDoS de bajo volumen y un grado de aleatoriedad elevado. En el último trimestre, los ataques DDoS contra los DNS se convirtieron en el vector de ataque DDoS más común, de hecho, un 32 % de todos los ataques DDoS se dirigieron contra el protocolo DNS. En la capa UDP, observamos ataques que aprovecharon la vulnerabilidad de día cero (CVE-2022-26143, TP240PhoneHome) que revelamos en marzo de 2022.

Además de las campañas de ataque específicas, desglosaremos las tendencias de los ataques a la capa de aplicación y a la capa de red, junto con las variaciones sectoriales y regionales. Por último, te ofreceremos algunos consejos para que aprendas a reforzar tu seguridad de forma proactiva y garantizar así la continuidad de tus servicios en un panorama de amenazas DDoS en constante transformación.

También está disponible una versión interactiva de este informe en Cloudflare Radar.

Aspectos destacados

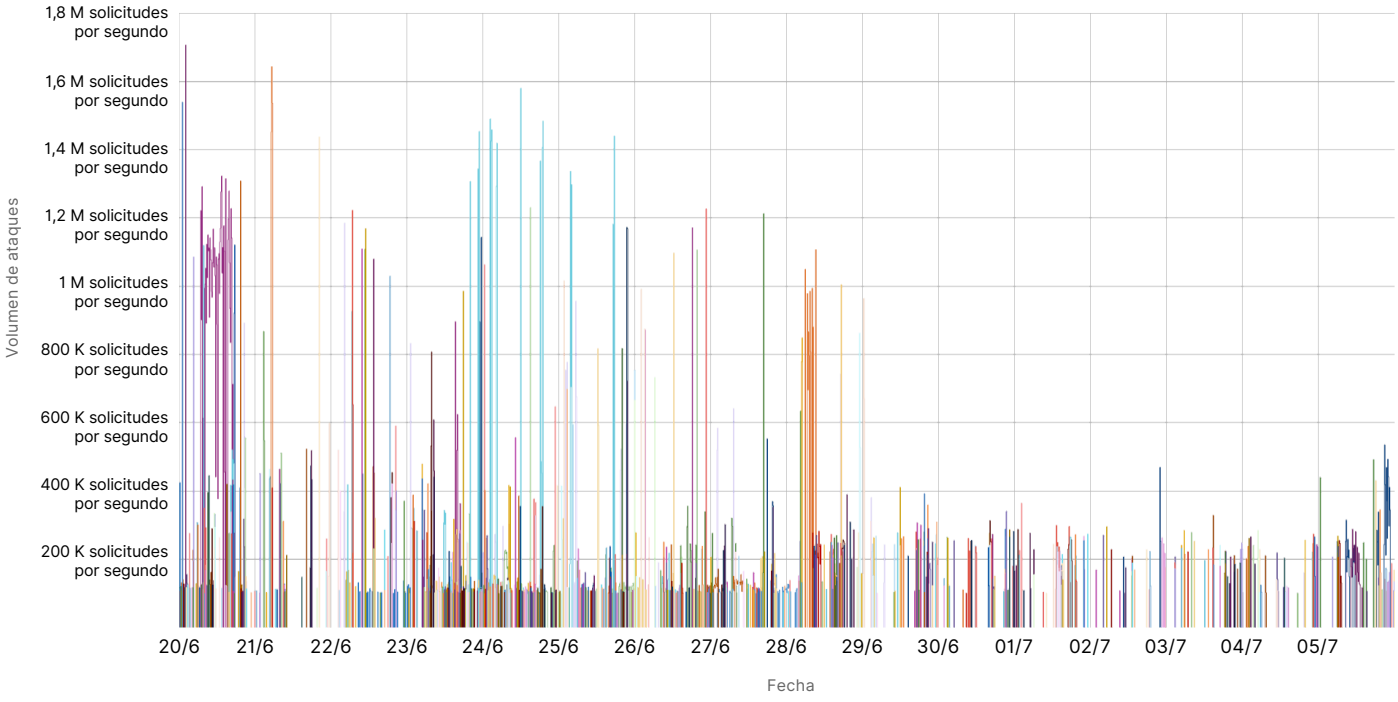
La alianza hacktivista "Darknet Parliament", en acción

El 14 de junio, grupos hacktivistas prorrusos, entre ellos Killnet, el resurgimiento del grupo REvil y Anonymous Sudan, anunciaron su unión con el nombre "Darknet Parliament".

Su propósito, según afirmaron, es lanzar ciberataques "masivos" contra el sistema financiero occidental, incluidos bancos occidentales, el Sistema de Reserva Federal de Estados Unidos y la red SWIFT (Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales).

Durante el trimestre objeto de estudio, Dark Parliament lanzó hasta 10 000 ataques DDoS contra sitios web protegidos por Cloudflare. Sin embargo, los sitios web de servicios bancarios y financieros solo fueron el noveno sector más afectado, según los ataques que hemos observado contra nuestros clientes en el marco de esta campaña, y que nuestros sistemas detectaron y mitigaron de forma automática.

Ataques (10 000) que Killnet, REvil y Anonymous Sudan lanzaron contra todos los sectores en el segundo trimestre de 2023



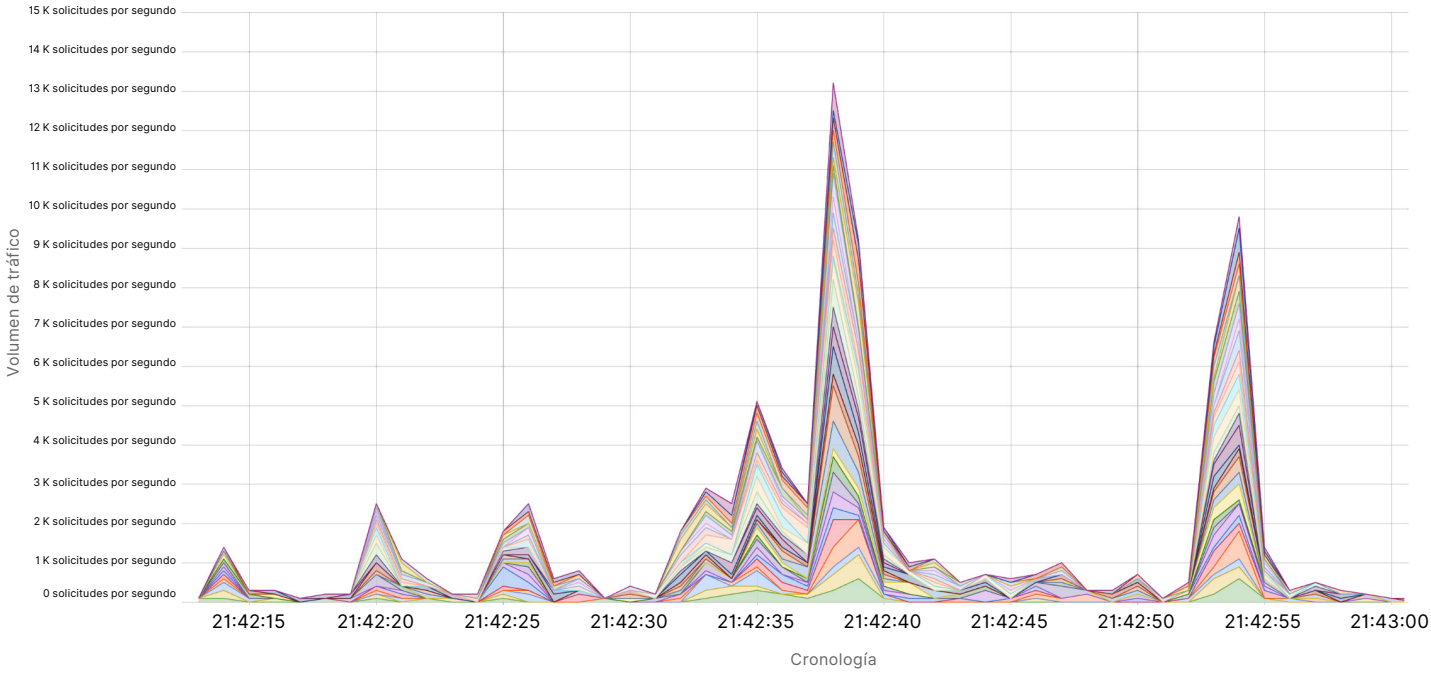
Ataques DDoS HTTP de bajo volumen y un grado de aleatoriedad elevado

Un ataque DDoS HTTP es un ataque DDoS a través del protocolo de transferencia de hipertexto (HTTP). Se dirige a propiedades de Internet HTTP, como sitios web y puertas de enlace de API. En los últimos meses, hemos observado un repunte de los ataques DDoS HTTP de bajo volumen y un grado de aleatoriedad elevado. Anteriormente, era una táctica empleada sobre todo por atacantes financiados por estados.

Parece que los atacantes han diseñado sus estrategias intencionadamente para lograr eludir los sistemas de mitigación, imitando hábilmente y con gran precisión el comportamiento del navegador de usuarios reales. En algunos casos, presentan un alto grado de aleatoriedad en distintas propiedades, tales como los agentes de usuario y las huellas digitales JA3.

A continuación, te mostramos un ejemplo de un ataque de este tipo. Cada color diferente representa una función de aleatoriedad distinta.

Evolución del volumen de tráfico HTTP de un ataque DDoS HTTP de bajo volumen y alto grado de aleatoriedad



Ataque DDoS: blanqueo de DNS

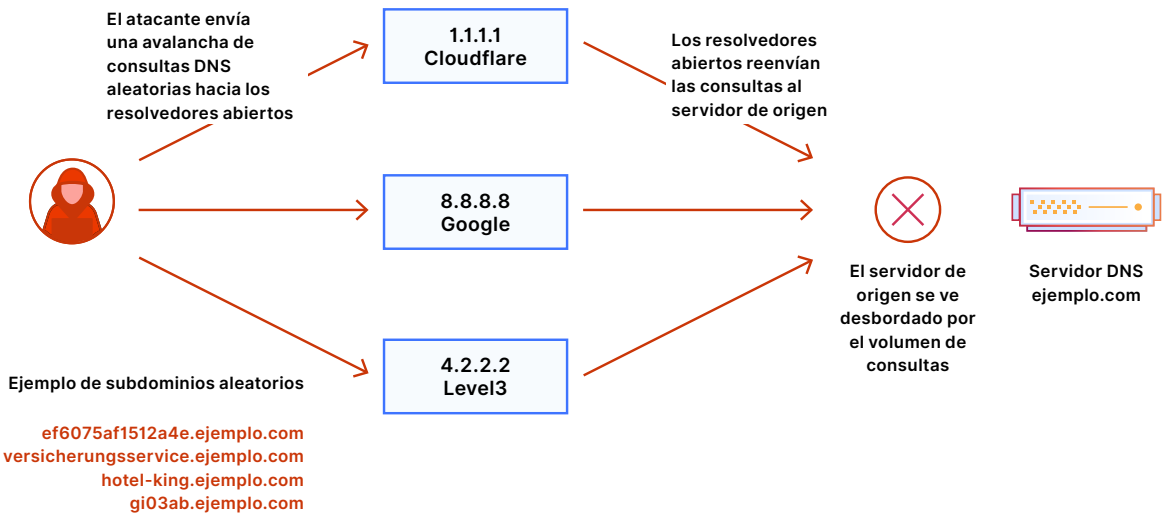
En el último trimestre, los ataques DDoS a los DNS se convirtieron en el vector de ataque DDoS más común, de hecho, el 32 % de todos los ataques DDoS se dirigieron contra el protocolo DNS. El sistema de nombres de dominio, o DNS, funciona como la guía telefónica de Internet. El DNS ayuda a traducir la dirección de un sitio web legible por humanos (p. ej., www.cloudflare.com) a una dirección IP legible por máquinas (p. ej., 104.16.124.96). Cuando los atacantes interrumpen los servidores DNS, afectan a la capacidad de las máquinas para conectarse a un sitio web, y al hacerlo impiden que los usuarios accedan a los sitios web.

El ataque de blanqueo de DNS es un tipo de ofensiva preocupante y de rápido crecimiento. Es un ataque que puede plantear graves problemas a las organizaciones que gestionan sus propios servidores DNS autorizados. Un ataque de blanqueo de DNS es el proceso de hacer que el tráfico malicioso parezca tráfico legítimo, blanqueándolo a través de resolvedores de DNS recursivos de confianza. Es similar al proceso de hacer que el "dinero negro" parezca legal, también conocido como blanqueo de dinero.

En un ataque de blanqueo de DNS, el ciberdelincuente consultará subdominios de un dominio gestionado por el servidor DNS de la víctima. El prefijo que define el subdominio es aleatorio y nunca se utiliza más de una o dos veces en un ataque de este tipo. Debido al componente de aleatoriedad, los servidores DNS recursivos nunca tendrán una respuesta en caché y tendrán que reenviar la consulta al servidor DNS autoritativo de la víctima. Entonces, el servidor DNS autoritativo recibe tal bombardeo de consultas que no puede atender consultas legítimas, e incluso se bloquea por completo.

Una gran institución financiera asiática y un proveedor de DNS norteamericano son dos de las últimas víctimas de este tipo de ataques. El origen del ataque incluye servidores DNS recursivos de confianza, como el 8.8.8.8 de Google y el 1.1.1.1 de Clouflare. El dominio afectado es válido y debe dar respuesta a consultas legítimas. Por lo tanto, los administradores de los DNS no pueden bloquear el origen del ataque ni todas las consultas al dominio afectado. La capacidad de distinguir las consultas legítimas de las maliciosas supone todo un desafío.

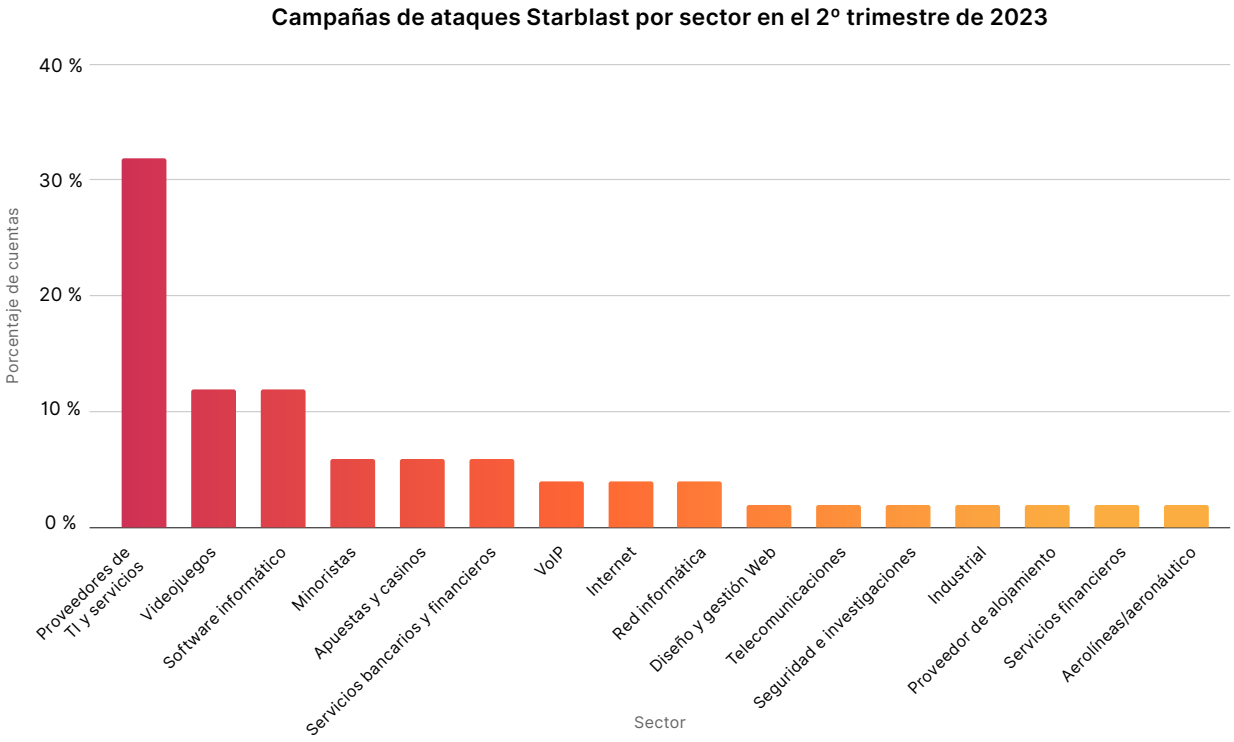
Cadena de un ataque DDoS de blanqueo de DNS



"Startblast": abuso de las vulnerabilidades de Mitel para lanzar ataques DDoS

En la capa UDP, observamos ataques que aprovecharon la vulnerabilidad de día cero (CVE-2022-26143, TP240PhoneHome) que revelamos en marzo de 2022. Junto con otros miembros de la comunidad InfoSec, identificamos esta vulnerabilidad en el sistema telefónico empresarial Mitel MiCollab, que expuso al sistema a un ataque de amplificación UDP.

El nombre de la campaña "Startblast" procede del comando de depuración homónimo que es decisivo para explotar esta vulnerabilidad. Hemos detectado que la mayoría de los ataques se dirigieron contra proveedores de TI y servicios, más que al sector de los videojuegos. Este tipo de ofensiva es la que más ha crecido entre los ataques DDoS a la capa de red en el último trimestre.



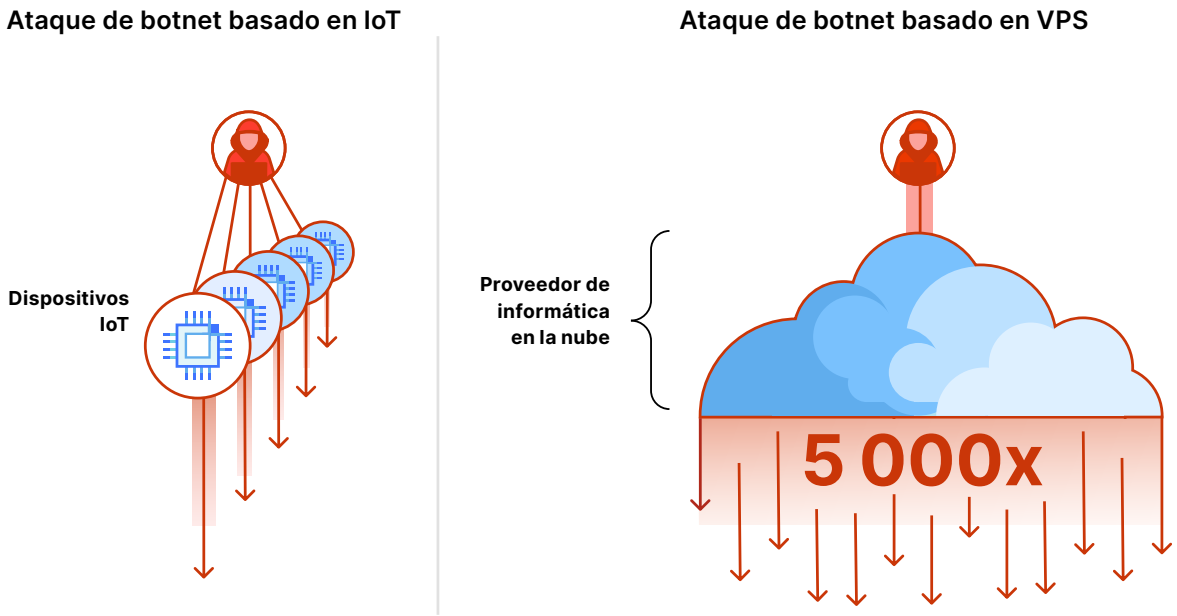
El continuo aumento de botnets eficaces

Tal y como se explica en nuestro informe sobre las tendencias de las amenazas DDoS en el 1.er trimestre de 2023, seguimos siendo testigos de una evolución en el ADN de las botnets. Ha llegado la era de las botnets DDoS en máquinas virtuales y, con ella, los ataques DDoS hipervolumétricos. Estas botnets se componen de máquinas virtuales (VM) o servidores privados virtuales (VPS), en lugar de dispositivos de Internet de las cosas (IoT), lo que multiplica por 5 000 su eficacia.

Cloudflare ha colaborado con destacados proveedores de informática en la nube para hacer frente a estas nuevas botnets. Los primeros resultados no se han hecho esperar, como la neutralización de sus componentes más importantes. Desde entonces, en el 2º trimestre de 2023, no hemos observado más ataques hipervolumétricos (al nivel de la escala observada en el 1.er trimestre de 2023 y con anterioridad).

Nuestro objetivo es automatizar y ampliar aún más esta colaboración. Solicitamos a los proveedores de informática en la nube, proveedores de alojamiento y otros proveedores de servicios generales que se unan a Botnet Threat Feed de Cloudflare.

Es un servicio gratuito para proveedores y no vendemos nuestros datos a terceros. Ofrece visibilidad de los ataques que se originan en las propias redes de los proveedores de servicios, y contribuye a nuestra iniciativa común para desmantelar las botnets.



Principales tendencias de los ataques DDoS — 2º trimestre de 2023

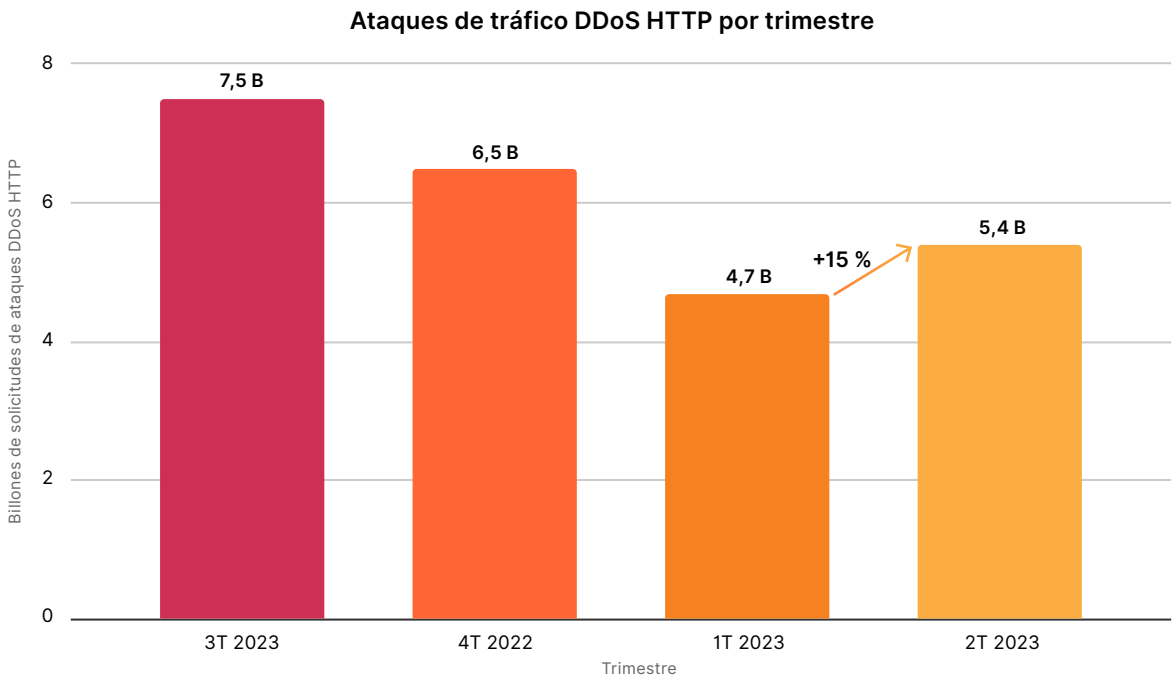
En las siguiente secciones del informe, analizaremos las principales tendencias en torno a los blancos de ataques.

Cambios generales en el volumen de tráfico

Los ataques DDoS a la capa de aplicación y a la capa de red disminuyeron un 35 % y un 14 %, respectivamente, en los seis primeros meses de 2023, en comparación con el mismo periodo del año pasado. En Cloudflare, esperamos que se mantenga esta tendencia de descensos interanuales, ya que Cloudflare y la comunidad de seguridad de la información se lo están poniendo cada vez más difícil a los ciberdelincuentes.

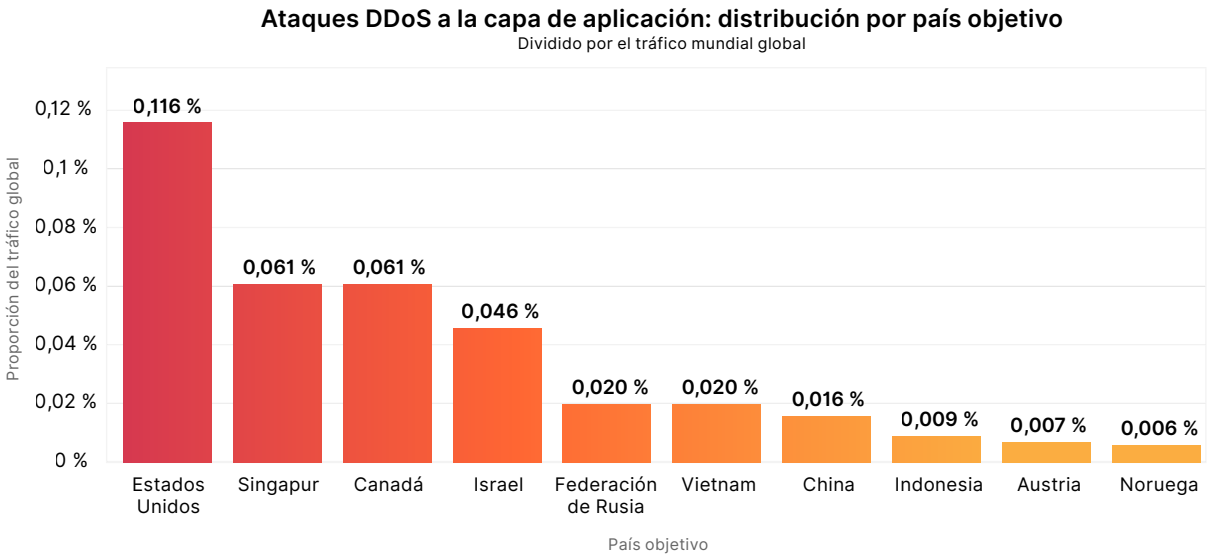
Sin embargo, debemos hacer un llamamiento a la prudencia, ya que hemos observado un aumento interanual del 15 % en los ataques DDoS a la capa de aplicación en el 2º trimestre. ¡No bajes la guardia aún!

En general, los ataques DDoS HTTP se alzaron un 15 % en términos intertrimestrales, pese a que disminuyeron un 35 % respecto al mismo periodo del año pasado. Además, los ataques DDoS a la capa de red descendieron aproximadamente un 14 % en el 2º trimestre, en comparación con el trimestre anterior.



Principales países objetivo

El trimestre pasado, informamos de que Israel fue el país más afectado por los ataques DDoS a la capa de aplicación. Este trimestre, los sitios web de Estados Unidos vuelven a ocupar el primer puesto, y los sitios web de Singapur y Canadá se posicionan en el segundo y el tercer lugar de la lista, respectivamente. Los ataques contra sitios web israelíes disminuyeron un 33 %, lo que llevó al país a ocupar la cuarta posición.



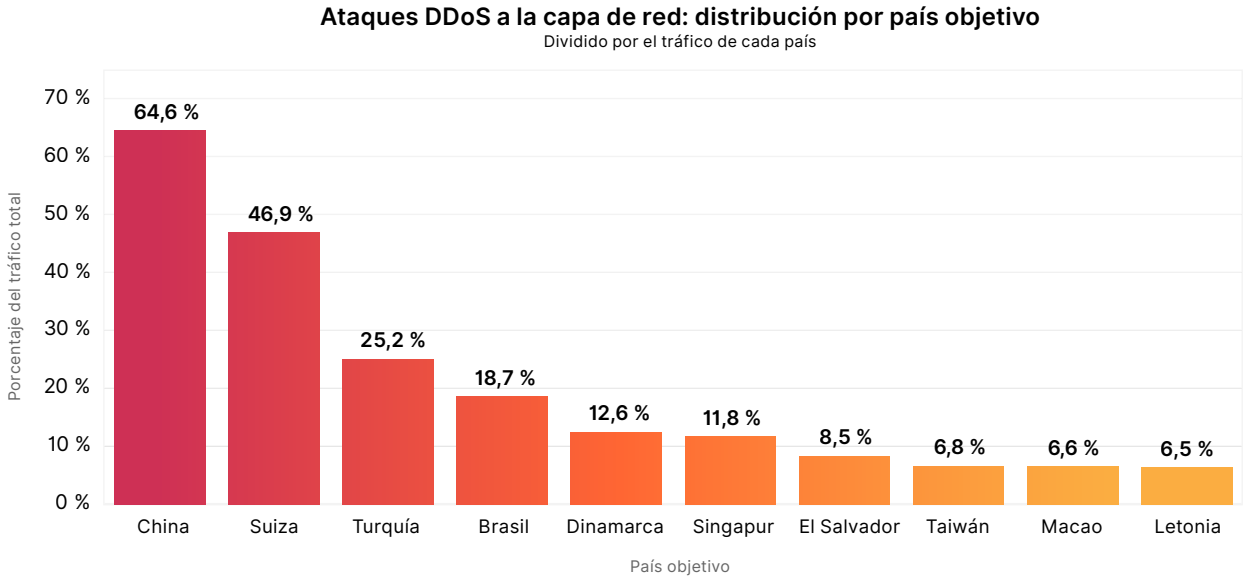
⚠ El doble de ataques DDoS a la capa de aplicación

Estados Unidos recibe el doble de ataques DDoS a la capa de aplicación que el siguiente país más afectado.

⚠ Más del 10 %

Más del 10 % del tráfico global a la capa de aplicación de Palestina y San Cristóbal y Nieves formó parte de ataques DDoS.

En la capa de red, China vuelve a ocupar el primer puesto en cuanto al mayor número de ataques DDoS a la capa de red. 2 de cada 3 bytes a redes chinas formaron parte de ataques DDoS en el 2º trimestre de 2023. Hemos observado este porcentaje tan alto de tráfico malicioso hacia China a lo largo de varios trimestres. La situación excepcional del 1.er trimestre de 2023, en la que el 83 % de los bytes dirigidos a redes finlandesas formaban parte de ataques DDoS, ha remitido. Finlandia ha salido de los diez primeros puestos de regiones y países afectados por ataques DDoS.



Variaciones sectoriales y regionales en los ataques DDoS

Los sitios web de criptomonedas fueron el blanco del mayor número de ataques de tráfico DDoS HTTP en el 2º trimestre de 2023. 6 de cada 10 000 solicitudes HTTP dirigidas a sitios web de criptomonedas formaron parte de estos ataques. Esta cifra se ha disparado un 600 % en comparación con el trimestre anterior.

Los sitios web de videojuegos y apuestas ocuparon el segundo lugar, de hecho, el porcentaje de ataques contra estos sectores se alzó un 19 %, en comparación con el trimestre anterior. Los sitios web de marketing y publicidad les siguieron de cerca en tercer lugar, si bien apenas hubo cambios en su porcentaje de ataques.

Por desgracia, las organizaciones sin ánimo de lucro continúan siendo uno de los principales objetivos de los ataques DDoS. El 12 % del tráfico HTTP contra organizaciones sin ánimo de lucro fueron ataques DDoS, el segundo sector con mayor porcentaje de tráfico. Cloudflare protege a más de 2 271 organizaciones sin ánimo de lucro de 111 países como parte del proyecto Galileo, que ha celebrado su noveno aniversario este año. En los últimos meses, una media de 67,7 millones de ciberataques se dirigieron diariamente a este tipo de organizaciones.

Sectores más afectados por región

Recomendaciones y conclusiones

Prácticas recomendadas	Optimiza el uso de Cloudflare
Actualiza o elabora un plan de respuesta a ataques DDoS.	¿Has integrado las alertas y la información sobre amenazas de Cloudflare en tus operaciones de seguridad? ¿Sabes cómo contactar a todos los colaboradores necesarios en caso de ataque? ¿Han recibido formación sobre el plan de respuesta?
Implementa soluciones de información sobre amenazas y de mitigación de DDoS automatizadas y en línea.	Utiliza diferentes técnicas de detección para hacer frente a las tendencias de ataque enumeradas en este informe: 1. Creación de huellas digitales dinámicas sin estado 2. Clasificación basada en aprendizaje automático 3. Detección de tráfico anómalo 4. Creación de perfiles de tráfico y mitigación con estado 5. Información sobre amenazas relativa a la actividad y tendencias DDoS actuales
Actualiza tu infraestructura para que sea más resistente a tu perfil de tráfico. **Mejora el rendimiento de la red y las aplicaciones para evitar cuellos de botella.**	Asegúrate de que la capacidad de tus herramientas de mitigación de DDoS es lo suficientemente grande como para gestionar el doble del tamaño de los mayores ataques jamás registrados y el doble de la velocidad máxima de tu tráfico legítimo. Reduce automáticamente el límite de multiplexación HTTP/2 cuando seas víctima de un ataque, habilitando WAF. Usa una sala de espera digital. Optimiza el almacenamiento en caché, gestiona mejor las cargas con una red de entrega de contenido (CDN) y soluciones de equilibrio de carga basadas en la nube.
Utiliza un modelo de seguridad positiva. Asegúrate de que el tráfico que quieres, llega de forma fiable.	Mantén abiertos los puertos en uso que son importantes para tu negocio. Utiliza la validación de esquemas y una puerta de enlace de API para el tráfico API.
Usa la información sobre amenazas y la inteligencia artificial para adelantarte a las amenazas emergentes.	Puntuaciones de bots que se pueden utilizar en reglas de firewall y de limitación de velocidad.

En Cloudflare, queremos que sea aún más fácil, y gratuito, para las organizaciones de todos los tamaños protegerse incluso de los ataques DDoS más grandes y complejos. Llevamos ofreciendo protección DDoS gratuita e ilimitada a todos nuestros clientes desde 2017, cuando fuimos pioneros en este concepto.

No te pierdas el seminario web de las tendencias DDoS para saber más sobre estas amenazas DDoS emergentes y aprender a defenderte contra ellas.

CLOUDFLARE

+34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

REV:BDES-4839.23AGO2023