INFORME

# Informe trimestral de DDoS de Lumen

Q1 2022

LUMEN TECHNOLOGIES

# Introducción

Esperamos que haya tenido un excelente inicio de 2022. El comienzo de un nuevo año siempre es emocionante y lleno de posibilidades: cuenta con nuevos presupuestos, nuevos planes, nuevas estrategias, etc. Lo mismo puede decirse para los actores maliciosos. A medida que los ciberdelincuentes operan más como organizaciones legítimas, atraviesan por los mismos procesos que todos nosotros, pensando en qué proyectos ambiciosos quieren emprender este año, dónde van a reinvertir sus ingresos de 2021 y cómo pueden expandir su infraestructura. Mientras piensa en qué objetivos necesita alcanzar este año, es importante contar con las últimas tendencias de seguridad al alcance de la mano para ayudar a determinar las áreas de enfoque

En nuestro informe trimestral de DDoS de Lumen, correspondiente al primer trimestre de 2022 conocerá sobre:

- La actividad de DDoS dirigida contra Ucrania y qué puede hacer para proteger a su organización
- Magnitud, duración y frecuencia de los ataques
- Vectores de los ataques de DDoS
- Industrias que fueron blanco

Para este informe examinamos datos de la plataforma de mitigación de DDoS de Lumen para desarrollar nuestros hallazgos, y ambos fortalecieron y se explayaron sobre las tendencias más amplias.

LUMEN
TECHNOLOGIES

# Tabla de Contenidos





LUMEN TECHNOLOGIES

# Hallazgos clave del Q1 2022

- La cantidad de ataques que mitigamos aumentó un 66% en comparación con el Q4 de 2021 y 32% anualmente.
- El mayor ataque de ancho de banda que depuramos en el primer trimestre fue de 775 Gbps, siendo el ataque más grande mitigado hasta la fecha.
- El mayor ataque basado en tasa de paquete depurado en el Q1 fue de 127 Mpps, representando más del doble de lo mitigado en el Q4.
- El período más largo de un ataque de DDoS que Lumen mitigó para un cliente individual duró 5 días.
- 72% de las duraciones de los períodos de ataque estuvo por debajo de los 30 minutos, analizando a los clientes de DDoS On-Demand.
- Los miércoles fueron los días de mayor frecuencia de ataques.
- Las mitigaciones multivector representaron 38% de todas las mitigaciones de DDoS, y las combinaciones más comunes utilizaron contramedidas DNS y TCP SYN.
- Los ataques de inundación TCP SYN constituyeron el tipo más común de mitigación de vector único, representando el 32% de las mitigaciones de DDoS.
- Las tres verticales principales apuntadas en los 500 ataques más grandes fueron: Telecomunicaciones, Juegos online y Software y tecnología.

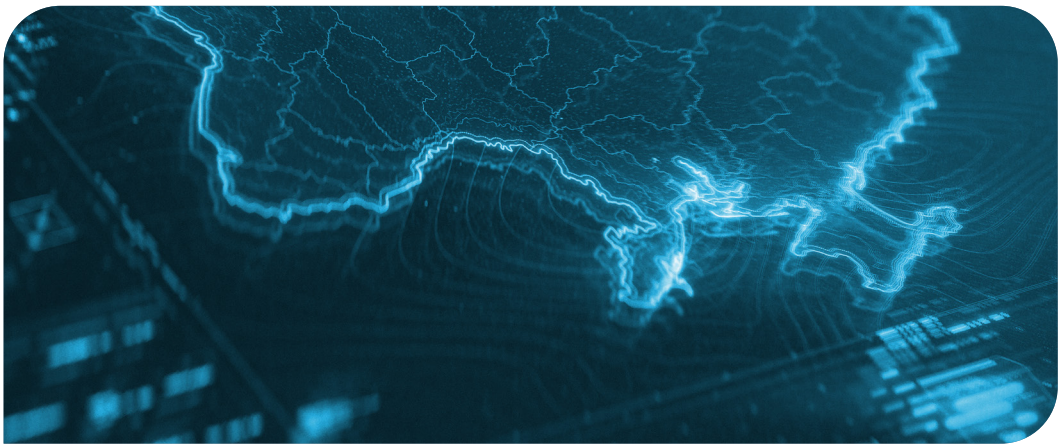
## ¿El conflicto en Ucrania afectará a su organización?

No podíamos compilar este reporte sin focalizarnos en uno de los mayores hechos que está teniendo lugar en el mundo actualmente: la invasión rusa a Ucrania. Si bien este trágico evento ha tenido un enorme impacto en el pueblo de Ucrania, vamos a hablar específicamente sobre las implicancias en la ciberseguridad de este conflicto que sigue desarrollándose.

Junto con los ataques físicos en Ucrania, hemos advertido ataques cibernéticos continuos que van desde malware wiper (limpiador) hasta ataques de DDoS continuos y sostenidos a la infraestructura crítica de Ucrania, provenientes de países vecinos. El Servicio Estatal de Ucrania para la Protección de las Comunicaciones y de la Información manifestó que los "hackers rusos continúan atacando los recursos de la información de Ucrania de manera ininterrumpida." Aunque estos ataques de DDoS han tenido su respuesta — según Wired, Rusia es apuntada con ataques similares por parte de grupos de hacktivistas y en algunos casos de hackers enrolados a favor de Ucrania.

Con tantos acontecimientos, la división de inteligencia sobre amenazas de Lumen, Black Lotus Labs®, se encuentra monitoreando las actividades de amenazas de Rusia, tanto en la región como a nivel mundial.  Black Lotus Labs está trabajando con socios de la industria, entre los que se encuentran el Programa de Colaboración Conjunta de Ciberdefensa  (JCDC, por sus siglas en inglés), mientras seguimos monitoreando cómo evoluciona la situación en Ucrania, ya sea analizando el tráfico de DDoS visible en la backbone de Lumen o identificando la infraestructura de C2 que se usa para lanzar los ataques. Conozca más sobre la preparación de Lumen para enfrentar eventos globales.

Si bien la actividad de DDoS actualmente se encuentra limitada a la región, eso no significa que vaya a continuar así.  Si le preocupa proteger a su organización, Lumen le sugiere seguir las recomendaciones de la Agencia de Seguridad de Infraestructura y Ciberseguridad  (CISA):





LUMEN TECHNOLOGIES

## 1. Reducir la probabilidad de una intrusión cibernética perjudicial

a. Valide que todos los accesos remotos a la red de su organización y los accesos privilegiados o administrativos requieran autenticación multifactor.
b. Asegúrese de que el software esté actualizado.
c. Confirme que el personal de TI de su organización tenga deshabilitados todos los puertos y protocolos que no sean esenciales.
d. Si su organización utiliza servicios en la nube, asegúrese de que hayan sido revisados e implemente controles sólidos.

## 2. Tomar las medidas necesarias para una rápida detección de una intrusión potencial

a. Asegúrese de que su personal se concentre en identificar y evaluar rápidamente cualquier comportamiento de red inesperado o inusual.
b. Confirme que toda la red de su organización esté protegida por un software antivirus/antimalware actualizado.
c. Si trabaja con organizaciones ucranianas o rusas, tenga mucho cuidado de monitorear, inspeccionar y aislar el tráfico de dichas organizaciones.

## 3. Asegurarse de que su organización esté preparada para responder ante la ocurrencia de un ataque

a. Designe un equipo de respuesta ante una crisis junto con roles y responsabilidades en los departamentos de tecnología, comunicaciones, legales y continuidad del negocio.
b. Realice un ejercicio de simulación para asegurarse de que todos conozcan sus roles durante un incidente activo.

## 4. Maximizar la resiliencia de su organización ante un incidente cibernético destructivo

a. Ponga a prueba sus procedimientos de backup para asegurarse de que sus datos críticos puedan restablecerse rápidamente.
b. Si utiliza sistemas de control industrial o tecnología operativa, realice una prueba de los controles manuales para que las funciones críticas permanezcan operativas.



LUMEN TECHNOLOGIES

Todo lo mencionado anteriormente puede parecer increíblemente abrumador. Aunque no tiene que ser así. Lumen puede ayudarle a encontrar vulnerabilidades dentro de su organización, evaluar sus marcos de seguridad y proporcionar recomendaciones a su equipo para lograr la postura de seguridad deseada.

Conozca más

**¿Qué es Black Lotus Labs?**

Black Lotus Labs es el equipo de inteligencia de amenazas de Lumen. Es un grupo de profesionales de la seguridad y de científicos de datos cuya misión consiste en aprovechar la visibilidad de la red global de Lumen para ayudarle a proteger su negocio y a mantener una internet limpia. Black Lotus Labs utiliza la búsqueda y el análisis de amenazas, así como machine learning y validación automatizada de amenazas, para identificar e interrumpir el trabajo de los actores maliciosos. Si le interesa conocer más sobre las investigaciones más recientes y las capacidades de avanzada para la investigación y rastreo de actores y crimeware de Black Lotus Labs, lea sus blogs.

Lea ahora

## Ataques de DDoS en cifras

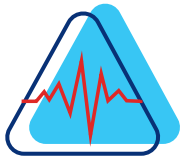
Luego de un cuarto trimestre relativamente tranquilo, 2022 comenzó con una explosión. Lumen mitigó 6.162 ataques de DDoS en el primer trimestre, lo que representa un aumento del 66% respecto del Q4 y un incremento del 32% respecto de lo que vimos en el Q1 2021. En promedio Lumen mitigó 70 ataques por día, un aumento del 63% trimestre a trimestre. Los días donde se registraron la mayor cantidad de ataques fueron: 30 de marzo (150 ataques); 24 de enero (139 ataques); y empatando en el tercer lugar estuvieron el 17 de marzo y el 27 de marzo (125 ataques).



LUMEN TECHNOLOGIES

## Magnitud y duración del ataque

### Mayor ataque depurado



| | Bits/s perdidos | Paquete/s perdidos |
|---|---|---|
| **Q1 2022** | 775 Gbps | 127 Mpps |
| **Q4 2021** | 499 Gbps | 60 Mpps |
| **Cambios Q a Q** | ▲55% | ▲112% |

Existen dos métricas principales para los ataques volumétricos de DDoS:

1. **Ataques de ancho de banda:** Estos apuntan a interrumpir el servicio mediante la inundación de un circuito o aplicación con tráfico. Este tipo de ataque se mide en bits por segundo.
2. **Ataques por tasa de paquete:** Estos ataques consumen recursos en los elementos de red tales como ruteadores u otros dispositivos, como así también de servidores. Estos se miden en paquetes por segundo con tasas por lo general más grandes que los ataques de ancho de banda.

#### Ataques de ancho de banda

Mitigamos nuestro mayor ataque de ancho de banda desde que comenzamos con nuestro reporte: 775 Gbps. Esto representa un incremento trimestral del 55% y un aumento anual del 189%.

El tamaño promedio de los ataques mitigados fue de 2 Gbps, que es lo que observamos en los informes anteriores de Lumen.

#### Ataques por tasa de paquete

El mayor ataque por tasa de paquete registró más del doble comparado con el Q4, pasando de 60 Mpps a 127 Mpps.

Existe un salto monumental en la magnitud del mayor ataque cuando analizamos las comparaciones anuales: en Q1 2021, el mayor ataque fue de 26 Mpps, mostrando un incremento anual superior al 380%.

La magnitud del ataque promedio fue de 477 Kpps, una ligera disminución comparado con Q4 2021, pero aun así más alto que el resto de los datos presentados en 2021.



LUMEN TECHNOLOGIES

Aprendizaje clave #1

## ¿Por qué debería preocuparme por la magnitud de los ataques?

Dado que las magnitudes de los ataques continúan con esta tendencia de aumentar en tamaño, es obvio que los ciberdelincuentes están escalando para igualar a las nuevas medidas defensivas y abrumar a sus blancos con infraestructuras de botnets de enormes proporciones. Si bien es cierto que probablemente no sufra el ataque de DDoS más grande de la historia, existe una buena posibilidad de que el mismo se concrete, si es que aún no ha ocurrido. Las organizaciones que no cuentan con servicios de mitigación de DDoS pueden quedar fácilmente desconectadas por un ataque de 1 Gbps. Contar con una solución de mitigación de DDoS no evitará que el ataque se produzca; sin embargo, le ayudará a garantizar que su organización pueda continuar con las operaciones normales durante un ataque activo.

## ¿Cuánto tiempo están durando los ataques?

Las cifras de duración de los ataques se ven afectadas por el modelo de mitigación del cliente. Existen dos opciones..

1. Mitigación on-demand: El tráfico se monitorea siempre, pero solo se depura una vez detectada la amenaza.
2. Mitigación always-on (siempre activa): El tráfico se depura constantemente para minimizar aun más el tiempo de inactividad.

Los datos a continuación solo muestran las tendencias para los clientes on-demand, que representan el 69% de los ataques que Lumen mitigó en el cuarto trimestre. Conozca más sobre las diferencias entre mitigación On-Demand y Always-On.

Vea el video



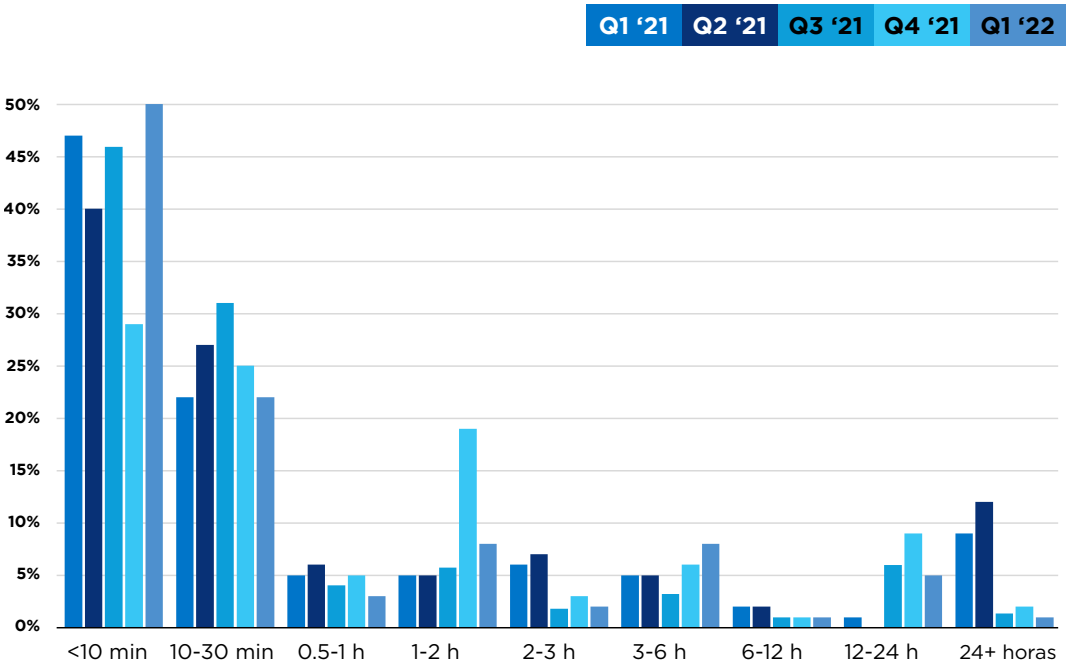
LUMEN TECHNOLOGIES

| | Q1 | Cambios Q a Q |
|---|---|---|
| **Duración media del ataque** | 10m 0s | ↓67% |
| **Duración promedio del ataque** | 2h 37m 55s | ↓44% |
| **Mayor tiempo de duración de un ataque** | 5 días | 0% |

Se registraron disminuciones tanto en las duraciones media y promedio de los períodos de ataque comparados con el Q4 2021; sin embargo, durante dicho trimestre experimentamos ataques más largos que en los trimestres anteriores. Los datos del Q1 están a la par con los mitigados durante el resto de 2021. La duración del período medio de ataque fue de 10 minutos, lo que representa una disminución trimestral del 67% respecto del Q4 (duración promedio del ataque de 30 minutos), y una disminución anual del 33% comparado con el Q1 2021 (duración promedio del ataque de 15 minutos).

La duración más larga de un período de ataque fue de cinco días, y se mantuvo estable trimestre a trimestre. Representa una merma respecto de lo que advertimos en los Q1-3 de 2021, donde registramos los períodos de ataque más largos durante 10 días. Esto no significa que todos podamos relajarnos; los ciberdelincuentes no se van a rendir. Como en cualquier negocio, las organizaciones de ciberdelincuentes apuntan a realizar eficiencias y están ejecutando ataques más largos, más eficientes, con mayor velocidad. A medida que avanza el 2022, podemos esperar ver la fluctuación de estos datos basados en las nuevas tácticas de los atacantes. Es importante advertir que la duración del período de ataque no indica simplemente la extensión de un solo ataque; una organización puede experimentar una ráfaga de ataques durante un período de duración.

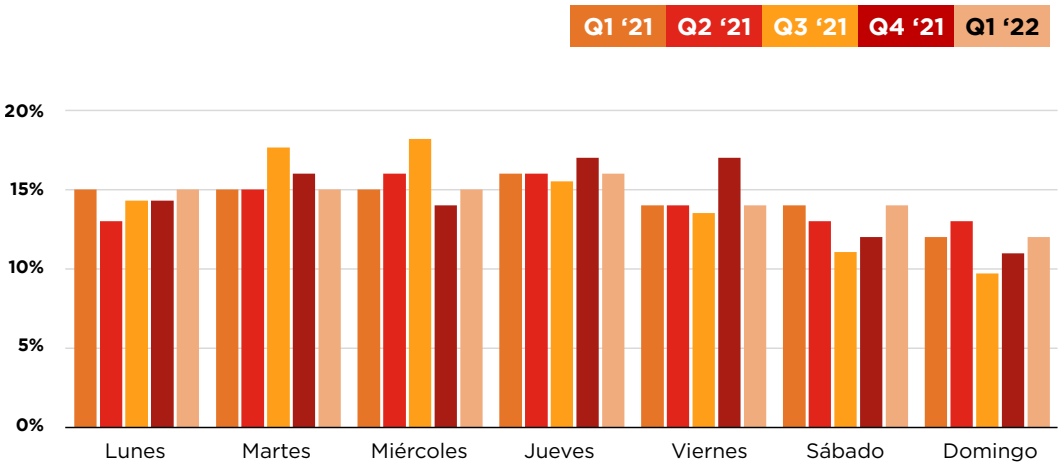
## Distribución por duración




La mitad de todos los ataques a los clientes de mitigación on-demand de Lumen, duró menos de 10 minutos, que es el mayor porcentaje de actividad que hemos visto comparado con informes anteriores. Esto podría significar que dichos actores maliciosos se focalizan en ataques rápidos, y están sondeando los ataques para probar las defensas de una organización antes de implementar ataques en mayor escala.

La segunda duración de período de ataque más popular fue de 10-30 minutos, representando el 22% de la actividad. Asimismo hubo una ligera suba en los ataques que duraron de tres a seis horas, pasando del 6% de la actividad en el Q4 al 8% de la actividad en el primer trimestre de 2022. Advertimos una caída en la dependencia de períodos de ataque de mayor duración. Los ataques de más de 24 horas han experimentado un descenso anual del 85%.

## Distribución por día

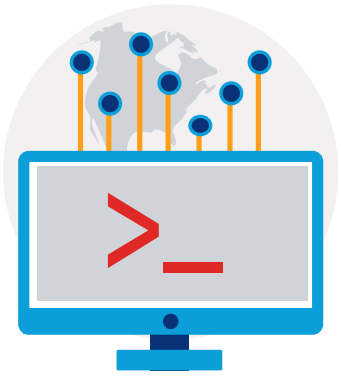



Los ataques ocurrieron uniformemente a lo largo de la semana; sin embargo, era ligeramente más probable que ocurrieran de lunes a jueves (~15% de los ataques por día) que de viernes a domingo (~13% por día). Esto se alinea con nuestra observación de que los ciberdelincuentes operan de manera similar a las empresas, lo que incluye tener semanas de trabajo dedicadas.

**Aprendizaje clave #2**

### ¿Por qué debería preocuparme por el tiempo de duración de los ataques?

Si actualmente está funcionando como una organización digital, depende en gran medida de su sitio web, de sus aplicaciones, herramientas y de su potencia de computación en general. ¿Alguno de estos elementos puede experimentar algún tiempo de inactividad? ¿Funcionarán sus colaboradores? ¿Sus clientes podrán interactuar con usted? El costo de un ataque no significa simplemente que sus activos de interacción con la web no funcionen, sino que el tiempo de inactividad que padezca puede tener ramificaciones de largo alcance para sus ingresos, incluidas las multas o las repercusiones negativas en su reputación. En los últimos años, el costo promedio de un ataques de DDoS puede traducirse en cientos o miles de dólares.





LUMEN TECHNOLOGIES

## Tipos de mitigación de ataques

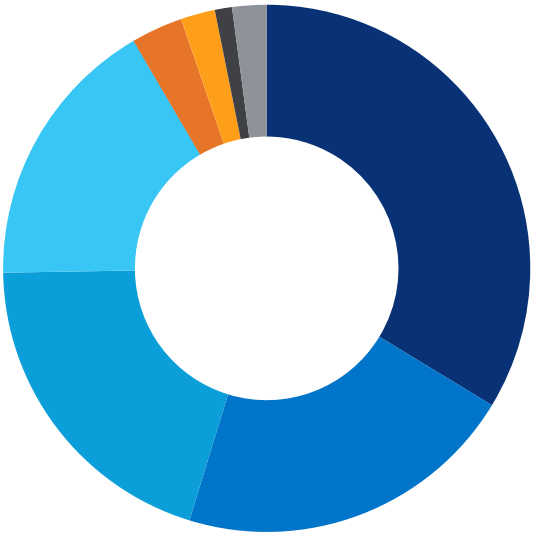
### Ataques de vector único/múltiples

| | Q1 2022 | Q4 2021 | Cambios Q a Q |
|---|---|---|---|
| **Vector único** | 62% | 65% | ↓4% |
| **Multivector** | 38% | 35% | ↑8% |

En el Q1, los ataques de vector único continúan siendo el principal método utilizado por los actores maliciosos, aún con una caída trimestral del 4%. Los hallazgos siguen estando a la par con los datos de informes anteriores.  Los ataques multivector representaron el 38% del total de los ataques, aunque mucho más altos en verticales como juegos (80%) y telecomunicaciones (67%).

### Mitigaciones de vector único

#### División del tipo de mitigaciones de vector único



| | | Q a Q |
|---|---|---|
| **TCP SYN** | 32% | ↑148% |
| **UDP** | 20% | ↓33% |
| **Filtrado estático** | 19% | ↓19% |
| **Paquetes inválidos** | 16% | ↓37% |
| **DNS** | 0% | ↑412% |
| **Otros ataques volumétricos** | 3% | ↑7% |
| **HTTP** | 2% | ↑70% |
| **Fragmentación de IP** | 1% | ↓6% |
| **Otros** | 2% | ↓29% |



LUMEN TECHNOLOGIES

Cuando analizamos el desglose de los tipos de mitigación de un vector único, TCP-SYN saltó directamente a la parte superior de la lista, pasando del 13% de la actividad en el Q4 2021 al 32% de la actividad en el Q1 2022, lo que representa un aumento trimestral del 148% y 61% de aumento anual.

Esto podría significar que los atacantes confían en métodos de ataque más simples y probados para obtener resultados óptimos.

Las mitigaciones de amplificación basadas en UDP pasaron de la primera a la segunda posición. Esto significó una disminución del 33% en comparación con el Q4, pero en línea con nuestros hallazgos a lo largo de todo el 2021. Los ataques basados en UDP apuntan a consumir el ancho de banda disponible y han demostrado ser sumamente potentes con la capacidad de generar ataques que superan con creces la magnitud de los bytes enviados inicialmente. Si desea conocer más acerca de los ataques basados en UDP, puede leer nuestro informe de DDoS trimestral correspondiente al Q3 2021, que analiza el vector de ataque en profundidad.

El filtrado estático sigue manteniéndose alto entre nuestras mitigaciones de vector único en un 19%, lo que significó un declive del 19% comparado con el Q4, pero sigue a la par con el resto de nuestros hallazgos de 2021.  Las contramedidas ante el filtrado estático por lo general se realizan en ítems tales como puerto y protocolo. Estas estadísticas también incluyen bots conocidas y reflectores abusados conforme lo descubierto por Black Lotus Labs, lo que provee una mitigación inicial contra los ataques.

## Mitigaciones Multivector

### Principales combinaciones de tipo de mitigación multivector

| | | Q a Q |
|---|---|---|
| **DNS, TCP SYN** | 17% | ▲38% |
| **TCP SYN, filtrado estático** | 7% | ▲65% |
| **UDP, filtrado estático** | 5% | ▼3% |
| **Otros ataques volumétricos, TCP SYN, UDP, Filtrado estático** | 4% | N.A. |
| **Paquetes inválidos, UDP** | 4% | ▼41% |
| **Otros ataques volumétricos, UDP, filtrado estático** | 3% | ▼35% |
| **Paquetes inválidos, filtrado estático** | 3% | ▼16% |
| **TCP SYN, UDP** | 2% | ▲20% |
| **Otros ataques volumétricos, TCP SYN, UDP** | 2% | N.A. |
| **Otros volumétricos, UDP** | 2% | ▼49% |

Las mitigaciones multivector representaron un 38% de la actividad, las más comunes utilizaron una inundación de consultas DNS combinada con una inundación TCP SYN (17% de las mitigaciones multivector). Lumen observó un incremento trimestral del 38% en esta combinación y un aumento anual del 28%. Este fue el método de ataque más aprovechado a lo largo de 2021, específicamente en los Q4, Q2 y Q1. Los ataques de DDoS basados en DNS aquí se refieren a inundaciones DNS, donde los atacantes procuran interrumpir los servidores del Sistema de Nombre de Dominio para evitar la resolución de DNS de un dominio determinado. Estos ataques a menudo formulan preguntas aleatorias para que los mecanismos naturales de caché de DNS no protejan al servidor.
Otras combinaciones incluyen TCP SYN y Filtrado estático (7% de la actividad) y amplificación basada en UDP y Filtrado estático (5% de la actividad).

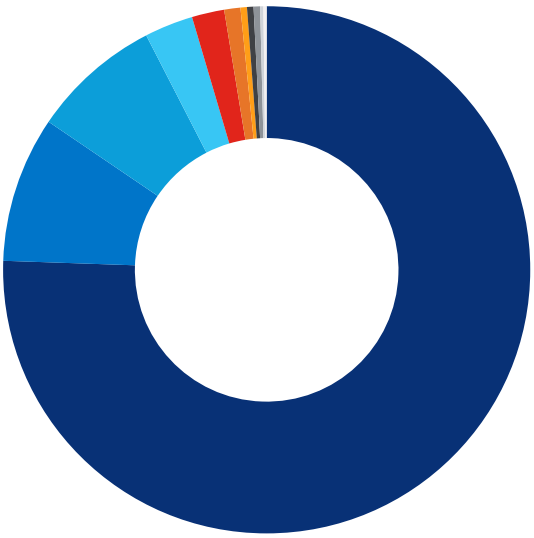
**Aprendizaje clave #3**

## ¿Por qué debería importarme qué vectores de ataque se están usando?

Los ciberdelincuentes están cambiando sus vectores de ataque constantemente como respuesta a las nuevas estrategias de defensa que se les presentan. Los actores maliciosos están motivados para seguir modificando sus ataques hasta derribar las defensas. Es una carrera entre atacantes y defensores y que va escalando continuamente. Esto puede dar como resultado equipos de seguridad sobrecargados tratando de mantenerse actualizados con las tácticas más recientes. El equipo de inteligencia sobre amenazas de Black Lotus Labs de Lumen trabaja diariamente para defender a nuestra comunidad global de la actividad maliciosa. Su inteligencia de amenazas es incorporada a nuestras soluciones de mitigación de DDoS y otras soluciones gerenciadas de seguridad a través de nuestra capacidad de Defensa rápida contra las amenazas.

Lea la ficha técnica

## Los 500 mayores ataques por industria



| | |
|---|---|
| **Telecomunicaciones** | 76% |
| **Juegos** | 9% |
| **Software y tecnología** | 8% |
| **Hosting** | 3% |
| **Gobierno** | 2% |
| **Educación** | 1% |
| **Otros** | 0.4% |
| **Finanzas** | 0.4% |
| **Servicios corporativos** | 0.4% |
| **Bancos** | 0.2% |
| **Medios y Entretenimiento** | 0.2% |

De los 500 ataques más grandes, el 97% apuntó contra estas cinco verticales principales (por orden): Telecomunicaciones, Juegos, Software y Tecnología; Hosting y Gobierno.

Es importante mencionar que un solo cliente contribuyó a la mayoría de los ataques de telecomunicaciones que mitigamos. Durante el primer trimestre, fueron atacados más de 1300 veces. Esto no significa que el blanco fuera específicamente la empresa de telecomunicaciones, ya que podría haber varios blancos dentro de su base de clientes. A continuación encontrará más información sobre las industrias principales objeto de ataque.

### Telecomunicaciones

**76%**
de los 500 ataques más grandes

**1.487**
ataques en total contra la vertica

Mayor magnitud de ataque de ancho de banda:
**775 Gbps**

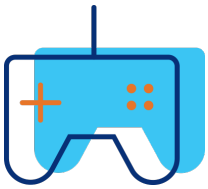
Mayor tiempo de duración de un ataque:
**4 días**

**67%**
Ataques multivector

Mayor ataque basado en paquete:
**70 Mpps**



LUMEN TECHNOLOGIES



## Juegos Online

**9%**
de los 500 ataques más grandes

**167**
Ataques totales contra la vertical

Mayor magnitud de un ataque de ancho de banda:
**93 Gbps**

Mayor tiempo de duración de un ataque:
**4 días**

**80%**
Ataques multivector

Mayor ataque basado en paquete:
**17 Mpps**

## Software y Tecnología

**8%**
de los 500 ataques más grandes

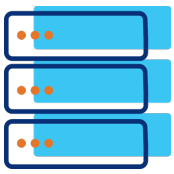
**419**
Ataques totales contra la vertical

Mayor ataque de ancho de banda:
**18 Gbps**

Mayor duración de un a ataque:
**4 días**

**68%**
Ataques de vector único

Mayor ataque basado en paquete:
**3 Mpps**



## Hosting

**3%**
de los 500 ataques más grandes

**108**
Ataques totales contra la vertical

Mayor magnitud de un ataque de ancho de banda:
**111 Gbps**

Mayor tiempo de duración de un ataque:
**5 días**

**76%**
Ataques de vector único

Mayor ataque basado en paquete:
**11 Mpps**



LUMEN TECHNOLOGIES

## Gobierno

**2%**
de los 500 ataques más grandes

**2.447**
Ataques totales contra la vertical

Ataques totales contra la vertical:
**110 Gbps**

Mayor tiempo de duración de un ataque:
**2 días**

**66%**
Ataques de vector único

Ataques de vector único:
**11 Mpps**

**Aprendizaje clave #4**

### ¿Debería preocuparme por los ataques de DDoS si no veo mi vertical en el listado anterior?

La respuesta corta es Sí. Los sectores listados arriba fueron blanco de ataque este trimestre; sin embargo, prácticamente todas las verticales y tipos de organizaciones pueden y son atacados regularmente. La pregunta que debo formularme es: ¿tengo algún tipo de datos que alguien podría querer atacar? Los datos deseables incluyen información de clientes, de empleados o conocimiento privilegiado. Si desea conocer más acerca de las tendencias de los ataques en su vertical, por favor contáctese con un representante de Lumen para conversar al respecto.

Contáctanos



LUMEN TECHNOLOGIES

# Aprendizajes clave

El aprendizaje más importante que esperamos se lleve de leer nuestros Informes Trimestrales sobre DDoS es que la seguridad no debería implementarse de forma tardía; en su lugar debe ser un esfuerzo consciente de cada parte de una organización. Con las naciones estado teniendo un rol cada vez mayor en el escenario de los ataques, habrá algunos en el medio que serán atacados a pesar de no ser el blanco apuntado.

Mientras piensa en su propia postura de seguridad, pregúntese: ¿qué haría si su organización fuera atacada mañana? Nuestros datos muestran que los ataques de DDoS, en su flujo y reflujo, se tornan cada vez más grandes, generalizados, complejos, extendidos y duran más tiempo.

## ¿Tiene dudas si está siendo objeto de un ataque de DDoS?

Aprenda a reconocer las señales: Cómo saber si su empresa está padeciendo un ataque de DDoS.

## ¿Qué hago si actualmente no tengo protección de DDoS?

Si no cuenta con su socio de mitigación de DDoS o si está buscando uno nuevo, a continuación le dejamos algunas preguntas para los proveedores potenciales:

- ¿Cómo maneja los ataques de grandes dimensiones?
- Si uno de sus otros clientes es atacado, ¿cómo afectará a mi organización?
- ¿Cómo es su arquitectura de depuración?  ¿Es global?
- ¿Hace algo para bloquear las amenazas antes de que se conviertan en ataques?
- ¿De dónde recibe su inteligencia de amenazas para bloquear nuevas amenazas? Dicha inteligencia de amenazas ¿está integrada en sus soluciones?
- ¿Cuenta con colaboradores que estén trabajando en una variedad de lugares y puede dar soporte a modelos de trabajo híbridos?

## ¿Cómo puede ayudarme Lumen con la mitigación de DDoS?

Con una de las mayores implementaciones de la industria para la mitigación de DDoS, respaldada por 170 Tbps de capacidad de mitigación basada en la red aplicada en más de 500 sitios de depuración de capas múltiples, Lumen posee mitigación de DDoS en escala.  Podrá elegir la mitigación adecuada para su organización con opciones como mitigación On-Demand o Always-on (bajo demanda y siempre activa) y funcionalidades de avanzada como depuración inteligente para ayudar a reducir la latencia y mejorar el desempeño. Asimismo podrá beneficiarse de una tarifa de servicio mensual plana. Usted no controla la magnitud, longitud o frecuencia de los ataques, así que ¿por qué debería cobrársele por ello?

Visite nuestro sitio web para conocer qué solución de mitigación de DDoS se adecua mejor a sus objetivos.

## Conozca más acerca del servicio de mitigación de DDoS de Lumen

## Conozca más acerca de Lumen® DDoS Hyper®

### Si está interesado, lea nuestros informes trimestrales 2021



LUMEN TECHNOLOGIES

**Metodología**

Los datos del presente informe abarcan el período comprendido entre el 1 de enero de 2022 al 31 de marzo de 2022. Los ataques depurados se definen ya sea como:

- Incidentes señalados por alertas de alto nivel mitigados por la plataforma, o
- Períodos en mitigaciones activas donde las medidas individuales hacen caer el tráfico,
- Eventos donde el tráfico derribado excede al tráfico enviado..

Los vectores de ataque o los tipos de mitigación se identifican mediante contramedidas que reducen el tráfico o los tipos de uso indebido marcados en nuestro monitoreo basado en el flujo.

Los picos en los datos pueden atenuarse por cómo se promedian las tasas a lo largo de varios incrementos de tiempo.

Los datos de nuestros clientes siempre activos se agregan en incrementos de minutos, horas o días según la duración de los tiempos de mitigación. Si una mitigación dura lo suficiente como para que el tiempo de resolución alcance una duración de un día, y si hay varios días consecutivos de ataque, se cuenta como un único período de ataque de varios días..

+5411 5170-1444 | lumen.com | contacto.latam@lumen.com



LUMEN TECHNOLOGIES