INFORME

Informe trimestral de DDoS de Lumen

Q4 2021

LUMEN TECHNOLOGIES

Introducción

Culminamos un año más, y con ello es momento de reflexionar acerca del 2021. Fue un año agitado para todos, especialmente para quienes trabajan incansablemente para mantener una internet limpia. Vimos cómo ataques de magnitud coparon los titulares irrumpiendo en las actividades no solo de las empresas sino de comunidades en escala. Y apenas se detiene una parte de la infraestructura maliciosa, surge otra, como el juego intenso de "golpear un topo" (whack-a-mole).

En nuestro Informe trimestral de DDoS de Lumen, correspondiente al Q4 2021 recibirá información acerca de:

- Predicciones de seguridad para el año que viene
- Magnitud, duración y frecuencia de los ataques
- Vectores de los ataques de DDoS
- Industrias que fueron blanco

Para este informe, examinamos inteligencia de Black Lotus Labs® y datos de la Plataforma de Mitigación de DDoS de Lumen® para desarrollar hallazgos, y ambos fortalecieron y se explayaron sobre las tendencias más amplias. A continuación les brindamos una rápida mirada a las tendencias de los ataques de DDoS de Lumen observados en 2021:

Cantidad total de ataques mitigados:
20.585

C2 promedio de Mirai/Gafgyt rastreados por trimestre:
800

Bots promedio de Mirai/Gafgyt rastreados por trimestre:
200.000

Mayor magnitud de un ataque de ancho de banda:
612 Gbps

Mayor tiempo de duración de un ataque:
14 días

Contramedida más común de ataques de vector único:
Filtrado estático

Las tres verticales más atacadas:

- Telecom
- Software y Tecnología
- Gobierno

LUMEN TECHNOLOGIES

Tabla de Contenidos

LUMEN TECHNOLOGIES

Hallazgos clave del cuarto trimestre de 2021

Botnets de DDoS de IoT

- Hubo un 56% de Incremento trimestral en los C2 únicos rastreados para botnets de DDoS Gafgyt y Mirai generalizadas.
- La vida útil promedio de un C2 Gafgyt fue de 32 días, mientras que el rango promedio de un C2 de Mirai fue de 12 días.
- Lumen rastreó 1.724 C2 a nivel mundial. Los países con la mayor cantidad de C2 resultaron (por orden): Estados Unidos, Países Bajos y Canadá.
- Lumen observó un aumento trimestral del 17% en la cantidad de hosts de botnet de DDoS a nivel global. Los países con la mayor cantidad de botnets de DDoS fueron:(por orden): México, Brasil e India.

Tendencias de los ataques de DDoS

- La cantidad de ataques que mitigamos disminuyó en un 48% en comparación con el tercer trimestre.
- El mayor ataque de ancho de banda que depuramos en el cuarto trimestre fue de 499 Gbps, lo que representa una disminución del 27% trimestre a trimestre.
- El mayor ataque basado en tasa de paquete que depuramos en el cuarto trimestre fue de 60 Mpps, lo que representa una disminución del 76% desde el tercer trimestre.
- El período más largo de un ataque de DDoS que Lumen mitigó para un cliente individual duró 5 días.
- 54% de las duraciones de los períodos de ataque estuvieron por debajo de los 30 minutos cuando analizamos a los clientes de DDoS on-demand.
- Las mitigaciones multivector representaron 35% de todas las mitigaciones de DDoS, y las combinaciones más comunes utilizaron contramedidas DNS y TCP SYN.
- La amplificación de UDP fue el tipo de mitigación de vector único más común, representando el 29% de las mitigaciones de DDoS.
- Las 3 principales verticales apuntadas en los 500 ataques más grandes durante el cuarto trimestres fueron: Telecomunicaciones, Juegos online y Software y tecnología.

¿Qué podemos esperar de 2022?

Antes de adentrarnos en el tema, tomémonos un momento para celebrar que hayamos atravesado otro año con éxito, a pesar de los numerosos desafíos. Analizando lo que ocurrió en todo el mundo, advertimos otro año en el que una enorme porción de la fuerza laboral continuó trabajando de manera remota. Y en 2021, vimos cómo muchos ciberataques de alto perfil ocuparon las primeras planas de las noticias, causando en algunos casos disturbios públicos en los Estados Unidos. Mientras todo hacer parecer de que las cosas están volviendo a un cierto grado de normalidad, tenemos una certeza: los ciberdelincuentes seguirán manteniéndonos en alerta.

Tendencias 2021

1. **Cuidado con los DDoS con pedido de rescate:** A medida que los actores maliciosos buscan beneficios económicos de sus actividades, a menudo se apoyan en los ataques de DDoS con pedido de rescate. Hubo picos a lo largo del año en los que los DDoS con pedido de rescate constituyeron el modo principal de ataque para los actores maliciosos. Específicamente, observamos muchísima actividad entre mayo y julio. Adicionalmente, mientras los pedidos de rescate demandan principalmente Bitcoin para los pagos, hubo varias demandas para que los pagos se realizaran en Monero.

   Para conocer las actividades de DDoS con pedido de rescate, lea nuestro informe del segundo trimestre. Descargar el Informe

2. **Los proveedores de Voz son un blanco principal:** En el tercer trimestre observamos varios proveedores de Voz bajo ataque. Tradicionalmente, los servicios VoIP no habían experimentado el tipo de ataques volumétricos que estaban causando un impacto significativo a algunos proveedores. No obstante, con posterioridad al tercer trimestre, se interrumpió la principal infraestructura de ataque que apuntaba contra ellos.

3. **Los ataques de reflexión continúan siendo un vector de ataque elegido:** En 2021 los atacantes utilizaron ataques del estilo de reflexión porque dichos ataques pueden tornarse muy grandes con poco esfuerzo de parte del atacante. Ya sea que se trate de CLDAP, NTP, DNS, SSDP, u otros protocolos susceptibles a los ataques amplificados de reflexión, los hackers están confiando en esta categoría de vector para causar un daño significativo. Lea nuestro informe del tercer trimestre para acceder a una revisión en profundidad de los ataques de reflexión de suplantación de identidad (Spoofing) . Descargar el Informe

Predicciones 2022

1. **Esperamos momentos muy activos y otros de calma en los DDoS con pedido de rescate:** Lumen espera que comience a aparecer algún tipo de estacionalidad en los ataques de DDoS con pedido de rescate. Probablemente tengamos períodos de muy escasa actividad seguidos de una ráfaga de ataques y con los atacantes optando por una campaña de conmoción y sorpresa. Los atacantes más grandes también inspirarán a otros y predecimos que habrá actividad de imitación.

2. **Habrá un incremento en los ataques multivector, más sofisticados:** Ya vimos un incremento en la complejidad de los ataques a lo largo de 2021 y continuarán en 2022. Para el próximo año se esperan los mayores ataques volumétricos nunca vistos antes ya que las botnets siguen creciendo en magnitud y complejidad año a año. Y de manera similar a lo que ocurre con Hydra (Hiedra), ni bien corte una parte de infraestructura maliciosa, crecerá otra. Asimismo habrá un crecimiento en los ataques de Capa 7, aumentando la necesidad de protección de las aplicaciones web y gestión de bots para defender los ingresos generados por las nuevas aplicaciones.

3. **Aumento de las disrupciones colaborativas en el medio de una mayor actividad de las naciones estado:** Como los ataques de las naciones estado son cada vez más prevalentes (no sólo para los DDoS específicamente), y como la industria y los gobiernos continúan colaborando del mismo modo que lo hicieron con varios intentos de derrocamientos tales como Emotet el año pasado, anticipamos que estos tipos de colaboraciones rendirán mayores frutos.

   Dado el escenario político en Europa del Este, esperamos ver un incremento en los ataques patrocinados por naciones estado en 2022. Adicionalmente, las naciones occidentales deberán estar preparadas para defenderse de las campañas directas o de los daños colaterales. Se espera que las campañas incluyan, sin carácter taxativo, ransomware, DDoS y ataques contra infraestructura crítica.

   Desde Black Lotus Labs y Lumen continuaremos haciendo nuestro aporte para que Internet siga siendo un lugar seguro; lea uno de nuestros blogs recientes para conocer más acerca de las amenazas y tendencias más recientes: Nueva campaña de Konni lanza el Año Nuevo apuntando al Ministerio de Relaciones Exteriores de Rusia.

LUMEN TECHNOLOGIES

Botnets de DDoS de IoT: Lumen continúa en alerta

Familia	C2s únicos rastreados	Víctimas únicas de ataque por familia	Ciclo de vida promedio de un C2 (en días)
Gafgyt	507 ▲45% QaQ	1.117	36 ▼5% QaQ
Mirai	480 ▲69% QaQ	21,140 ▼5% QaQ	12 ▼42% QaQ

Las dos familias de botnet predominantes de DDoS de IoT rastreadas por Black Lotus Labs, Gafgyt y Mirai, siguen generando caos con cientos de C2 dispersos en todo el mundo. Hemos rastreado estas familias durante años porque continúan prevaleciendo, ya sea con ligeros cambios o nuevas estructuras que siguen apareciendo. Los datos del cuarto trimestre estuvieron a tono con nuestros hallazgos de los trimestres anteriores; no obstante debido a la naturaleza cambiante de la actividad de las botnet esperamos ver un flujo y reflujo de dichas cifras.

En líneas generales, hubo un incremento del 56% en el total de C2 únicos rastreados, donde Mirai representa la mayoría durante el cambio de trimestre a trimestre, subiendo a un 69% desde el cuarto trimestre.

Definimos a las “víctimas” como el número de direcciones IP únicas contra las que observamos que los C2 lanzan ataques de DDoS. En conjunto, hubo más de 22.000 víctimas en ambas familias de botnet, cifra similar a nuestro promedio trimestral del año 2021.

Uno de los objetivos de los actores maliciosos consiste en cultivar una infraestructura confiable que puedan usar para sus propios ataques o arrendar como servicio a otros actores para uso temporal. Eso significa que apuntan a mantener dichas infraestructuras vivas el mayor tiempo posible. Durante este trimestre el ciclo de vida de Gafgyt estuvo en línea con lo que vimos en otros trimestres de este año, con un ligero descenso del 5%.

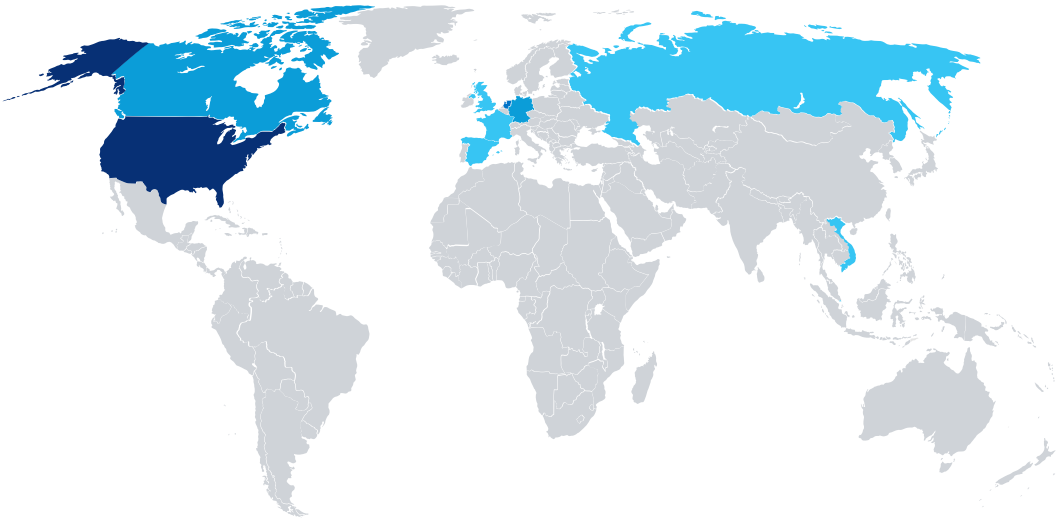
El ciclo de vida de Mirai tuvo una disminución trimestral mayor, del 43%. Si bien ambas familias registraron una caída trimestre a trimestre, sus vidas útiles fueron más altas que nuestro promedio anual.

Amenazas globales de DDoS de IoT rastreadas por país

Los siguientes mapas de riesgo específicos de DDoS representan a los 10 primeros países por C2 rastreados, y hosts de botnet de DDoS. Los datos se basan en la visibilidad de Black Lotus Labs y se dividen por tipo de amenaza y país de origen sospechoso. El país de origen se determina comparando la dirección IP de cada host con un amplio conjunto de direcciones IP mapeadas a nivel mundial.

Una nota respecto de los mapas de calor: el mero hecho de que la infraestructura de C2 esté ubicada en un país en particular no significa que ese sea su verdadero origen. Los ciberdelincuentes a menudo ocultan el origen de su actividad aprovechando la infraestructura de otros países.

10 primeros países por C2

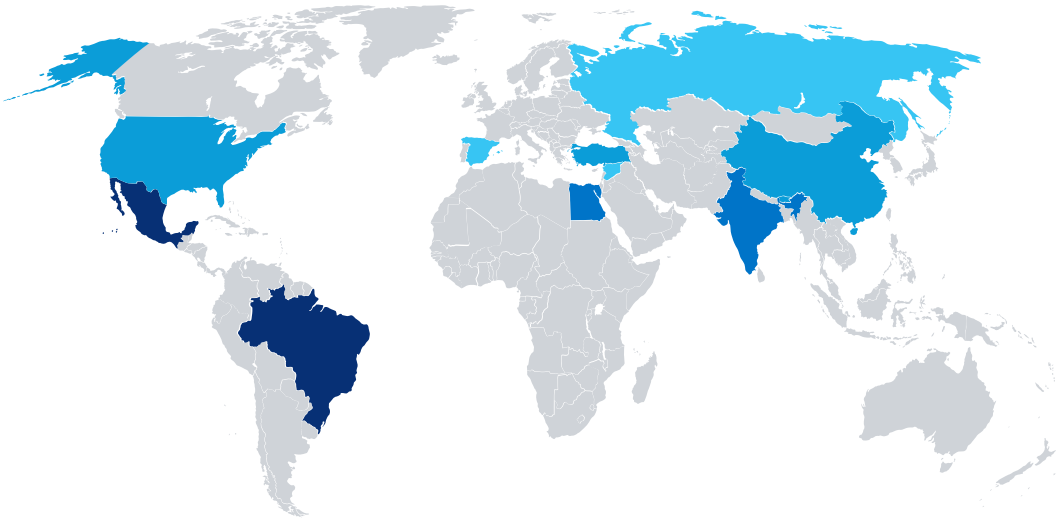


País	C2	Población*	Per Cápita (100.00)
Estados Unidos	554	331.002.651	0,17
Países Bajos	266	17.134.872	1,55
Canadá	197	37.742.154	0,52
Alemania	187	83.783.942	0,22
España	94	46.754.778	0,20
Reino Unido	79	67.886.011	0,12
Francia	36	65.273.511	0,06
Rusia	29	145.934.462	0,02
Singapur	26	5.850.342	0,45
Vietnam	19	97.338.579	0,02

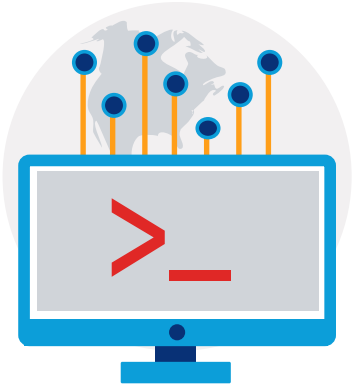
Lumen rastreó 1.724 C2 a nivel global en el cuarto trimestre; el mapa de calor anterior representa los países con la mayor cantidad de C2. Los

Estados Unidos registraron la mayor cantidad de C2 y representaron el 32% del total de C2 rastreados. Canadá, Países Bajos y Alemania también registraron aumentos significativos respecto de los trimestres anteriores. China, que el último trimestre ocupó el primer lugar, salió de nuestro listado de los primeros 10 por completo, junto con Corea del Sur y Taiwán. Los nuevos ingresantes a la lista son: Reino Unido (5% del total), Francia (2% del total) y Singapur (2% del total).

Primeros 10 países por Host de Botnets de DDoS



País	Bots	Población*	Per Cápita (100.000)
México	45.719	128.932.753	35.46
Brasil	41.616	212.559.417	19.58
India	25.304	1.380.004.385	1.83
Egipto	23.631	102.334.404	23.09
Estados Unidos	14.359	331.002.651	4.34
China	10.658	1.439.323.776	0.74
Turquía	10.405	84.339.067	12.34
España	9.857	46.754.778	21.08
Rusia	8.021	145.934.462	5.50
Siria	6.608	17.500.658	37.76



Black Lotus Labs observó un incremento del 17% en los hosts de botnet

de DDoS a nivel global trimestre a trimestre, con más de 250.000 — lo más alto que hemos visto todo el año. Nuestro primer país de la lista, México, registró un incremento del 7% y pasó de la segunda a la primera posición. Brasil pasó a ocupar el puesto número dos con una ligera disminución del 7%. India experimentó el mayor aumento del 58% desde el tercer trimestre, pasando de 15.900 hosts de botnet a 25.300 hosts. China y Siria fueron nuevas incorporaciones al listado, mientras que Argentina y Líbano salieron de los top 10.

Aprendizaje clave #1

¿Por qué debería interesarme por los datos globales?

Si usted tiene una empresa radicada en los Estados Unidos, ¿por qué debería preocuparse si México tiene la mayor cantidad de hosts de botnet? Con Gafgyt y Mirai tan ampliamente esparcidos, siempre hay una chance de pasar a ser víctima, o que su infraestructura se use para apuntar a otras organizaciones. Si su red no cuenta con las protecciones adecuadas, podría estar participando involuntariamente de ataques contra terceros. Formar parte de una infraestructura de botnets puede de hecho, tener impactos negativos en sus propias operaciones, tales como mayor costo del ancho de banda y problemas de desempeño para sus aplicaciones. Y una vez que un hacker tiene acceso a sus sistemas, queda expuesto a un millar de ataques, desde el robo de datos a criptominado o ransomware.

¿Qué es Black Lotus Labs?

Black Lotus Labs es el equipo de inteligencia de amenazas en Lumen. Es un grupo de profesionales de la seguridad y científicos de datos cuya misión es aprovechar la visibilidad de la red global de Lumen, tanto para proteger su empresa como para 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 está interesado en conocer más acerca de las más recientes capacidades de investigación y rastreo de crimeware de Black Lotus Labs, lea sus blogs.

Leer ahora

LUMEN TECHNOLOGIES

Luego de un tercer trimestre muy activo, hubo una desaceleración en el cuarto trimestre

Analizando el 2021, nuestro trimestre más atareado fue el tercero con más de 7.100 ataques mitigados. Y julio en particular, registró el mayor número de ataques en términos de frecuencia, magnitud y duración. En el cuarto trimestre vimos la cantidad más baja de ataques por trimestre en 3.718, una disminución trimestral del 48%. Sin embargo, prácticamente no hubo disminución en la cantidad de sitios atacados (solo una reducción del 3%), lo que significa que a pesar de que hubo menos ataques en el trimestre, los actores maliciosos están esparciendo los ataques a muchos más sitios. Un posible motivo de esta disminución podría ser la estacionalidad. Los ataques de DDoS presentan flujo y reflujo al igual que muchas otras tendencias, y para 2022 esperamos ver una actividad en continuo aumento.

Magnitud y duración del ataque

Mayor ataque depurado

	Bits/s perdidos	Paquete/s perdidos
Q4	499 Gbps	60 Mpps
Q3	612 Gbps	252 Mpps
Cambios QaQ	↓27%	↓76%

LUMEN TECHNOLOGIES

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 por bits por segundo.
2. **Ataques por tasa de paquete:** Estos ataques consumen recursos sobre los elementos de red tales como ruteadores u otros dispositivos. Estos suelen ser más grandes que los ataques de ancho de banda y se miden en paquetes por segundo.

Ataques de ancho de banda

El cuarto trimestre registró una disminución del 27% en los ataques de ancho de banda respecto del tercer trimestre.

El tamaño promedio de casi 500 Gbps, sin embargo, estuvo por encima de nuestro promedio de 2021 que fue de 450 Gbps.

El tamaño de un ataque promedio aumentó de 1 Gbps en Q3 a 2 Gbps en Q4.

Ataques por tasa de paquete

En el cuarto trimestre el mayor ataque disminuyó en un 76% pasando de 252 Mpps a 60 Mpps.

El tamaño de nuestro ataque promedio en el cuarto trimestre fue de 515 Kpps, un 68% menos respecto del trimestre anterior.

Aprendizaje clave #2

¿Por qué importa la magnitud del ataque?

No es necesario que lo golpeen con el ataque más grande de la historia para ver interrumpidas sus operaciones de negocio. Vemos muchísimas organizaciones que no cuentan con una protección de DDoS tomada offline por tamaños tan pequeños como 1 Gbps. Contar con protección de DDoS le ayudará a garantizar que los activos que interactúan con la red sigan funcionando aun cuando esté bajo un ataque activo.

LUMEN TECHNOLOGIES

¿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 el tiempo de inactividad aún más.

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

Ver el video

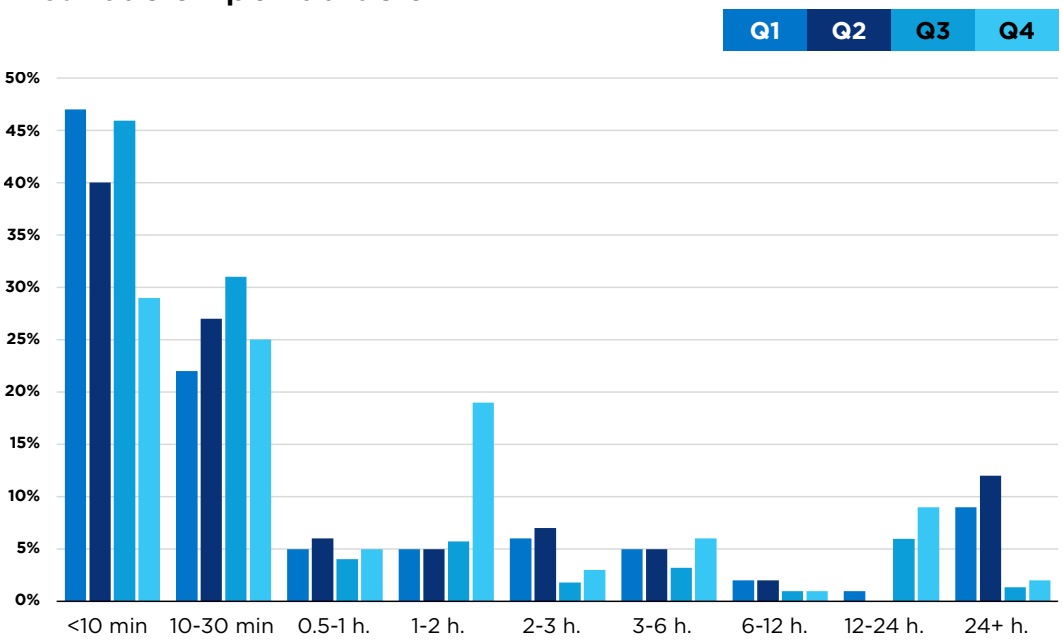
	Q4	Cambios QaQ
Duración media del ataque	30’	▲184%
Duración promedio del ataque	4h 23’50”	▲75%
Mayor tiempo de duración de un ataque	5 días	▼64%

Cuando analizamos la duración de los ataques prolongados, advertimos que el promedio y la media de los períodos de ataques aumentaron 184% y 75% respectivamente. La duración promedio del período de ataque fue la más larga que experimentamos todo el año y tuvo el salto más grande del tercer al cuarto trimestre de apenas 11 a 30 minutos.

LUMEN TECHNOLOGIES

El ataque más largo mitigado por Lumen en el cuarto trimestre fue de 5 días, una disminución significativa respecto de los trimestres anteriores. Esto no significa que podamos relajarnos. Esta disminución puede atribuirse a la estacionalidad donde los actores de DDoS no estuvieron activos. Esperamos encontrar ataques más largos y sofisticados en el futuro próximo.

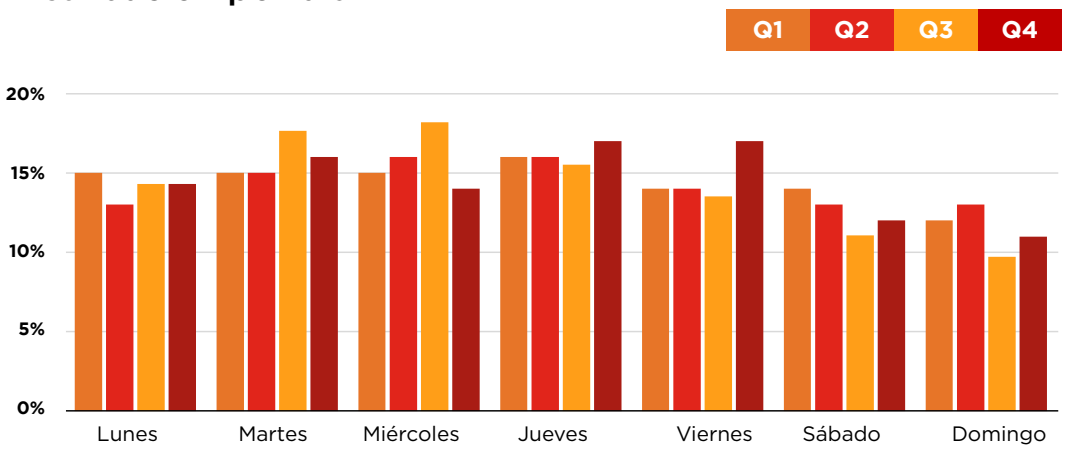
Distribución por duración



Al igual que con el resto de 2021, en el cuarto trimestre 10 minutos sigue siendo la duración más prevalente, representando el 29% de los ataques mitigados. Sin embargo, en el cuarto trimestre, por primera vez en 2021, observamos un enorme salto en las duraciones de los ataques que persistieron de una a dos horas. Por lo general, el porcentaje de ataques menor a 1-2 horas estuvo en torno del 5,5%, y en el cuarto trimestre llegó hasta el 19% de los ataques en total.

Los períodos de ataque tuvieron algunos repuntes extendiéndose 12-24 horas, y los que duraron más de 24 horas (52% y 73% respectivamente). A principios de 2021, los atacantes tuvieron un período de ataque más largo, y entre el 9-12% de los ataques duraron más de 24 horas; no obstante, esta es la primera vez que vemos una dependencia más profunda en la duración de los períodos de ataque de 12-24 horas.

Distribución por día



Los ataques por día de semana estuvieron mayoritariamente alineados con lo observado en los tres primeros trimestres. Durante el tercer trimestre, los martes fueron más activos, mientras que en el cuarto la mayor actividad se registró los viernes. Sábados y domingos continúan siendo los días de menor actividad.

El día que advertimos la mayor cantidad de ataques en el cuarto trimestre fue el 16 de diciembre, en el que Lumen mitigó 83 ataques, seguido del 18 de noviembre cuando mitigamos 79 ataques.

Aprendizaje clave #3

¿Puede afrontar el hecho de estar inactivo incluso durante 30 minutos?

Los atacantes están procurando irrumpir en sus operaciones. ¿Puede afrontar el hecho de estar inactivo incluso durante apenas una media hora? Sus clientes acudirán a su aplicación o sitio, y al ver que no funciona, ¿se irán a otro lugar? La gente, al enterarse del ataque a su organización por las noticias, ¿Dejarán de confiar en usted para que proteja sus datos sensibles como información de pago? ¿Recibirá una multa de parte de alguna organización de compliance? El costo de un ataque no se limita al costo de inactividad que padece sino que puede tener ramificaciones de largo alcance para los resultados financieros de su negocio. En los últimos años, el costo promedio de un ataque de DDoS puede traducirse en cientos o miles de dólares.

LUMEN TECHNOLOGIES

Tipos de mitigación de ataques

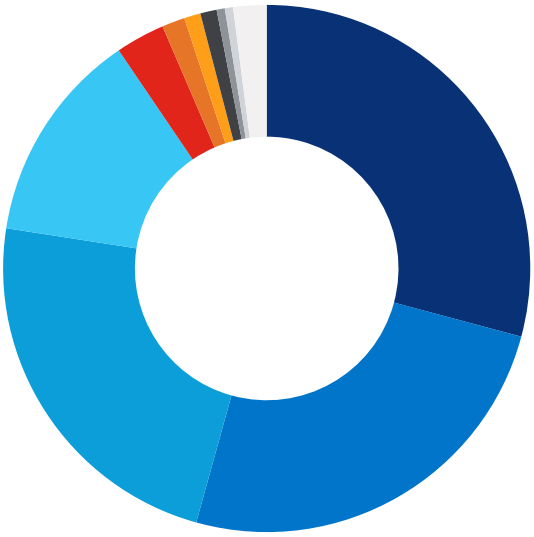
Ataques de vector único/múltiples

	Q4	Q3	Cambios QaQ
Vector único	65%	56%	▲16%
Multivector	35%	44%	▼20%

En el cuarto trimestre, vimos principalmente ataques de vector único, los que registraron un incremento trimestral del 16%, pasando del 56% al 65% de todos los ataques. Este fue el porcentaje más alto de ataques de vector único durante todo el año.

Mitigaciones de vector único

División del tipo de mitigaciones de vector único



		QaQ
UDP	29%	▲60%
Paquetes inválidos	25%	▲89%
Filtrado estático	23%	▲14%
TCP SYN	13%	▼48%
Otros volumétricos	3%	▲6%
Amplificación de DNS	1.40%	▼87%
Fragmentación de IP	1.00%	▼81%
HTTP	1.00%	▲67%
TCP RST	0.50%	▲45%
SIP	0.50%	▲54%
Otros	2.03%	▲20%

Cuando analizamos la división de los tipos de mitigación de vector único, vemos que la amplificación basada en UDP subió abruptamente a la cima, representando el 29% de todos los ataques, con un

incremento del 60% trimestre a trimestre. Mientras que los ataques basados en UDP prevalecen, no representan por lo general nuestro tipo de mitigación más común. Estos ataques apuntan a consumir el ancho de banda disponible y han demostrado ser muy poderosos por su capacidad de manejar ataques que superan con creces la magnitud de los bytes enviados inicialmente. Si desea saber más sobre los ataques basados en UDP, lea el blog de Black Lotus Labs: Rastreando los reflectores UDP para una internet más segura.

Los paquetes inválidos fueron nuestro segundo tipo de mitigación más alta, representando el 25% de la actividad y un aumento del 89% respecto del tercer trimestre. Los datos de paquetes inválidos incluyen el tráfico con campos de datos mal formados, como así también fragmentos incompletos, duplicados, o paquetes demasiado grandes. Si bien pueden ser el resultado de cuestiones relacionadas con la red o una secuenciación defectuosa de la red, los fragmentos de paquete también son una característica común de los ataques de DDoS de amplificación de UDP.

El filtrado estático se mantiene alto entre las mitigaciones de vector único en un 23%, representando un incremento trimestral del 14% y está alineado con lo que observamos a lo largo de 2021. Las contramedidas de filtrado estático por lo general se realizan sobre 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

		QaQ
DNS, TCP SYN	12%	N.A.
Paquetes inválidos, UDP	6%	↓6%
UDP, Filtrado estático	5%	N.A.
Otros ataques volumétricos, UDP	4%	↑183%
Otros ataques volumétricos, UDP, filtrado estático	4%	↑123%
TCP SYN, filtrado estático	4%	N.A.
Paquetes inválidos, filtrado estático	3%	↑50%
Paquetes inválidos, UDP, filtrado estático	2%	N.A.
Amplificación de DNS, Fragmentación IP, Paquetes inválidos, UDP	2%	N.A.
TCP SYN, UDP	2%	N.A.

LUMEN TECHNOLOGIES

En el cuarto trimestre, DNS combinado con TCP SYN representaron la mayor actividad respecto de las mitigaciones de multivector (12%).

Observamos algunas nuevas combinaciones este trimestre. La mayoría incluyó amplificación UDP, que se asemeja a lo que informamos para las mitigaciones de vector único.

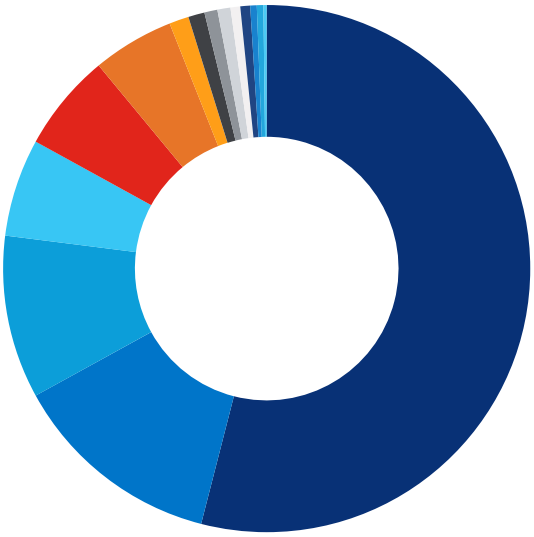
Aprendizaje clave #4

La ciberseguridad es una carrera armamentista.

¿Sabe si está protegido frente a las amenazas más recientes? Los ciberdelincuentes pueden cambiar los parámetros y vectores de los ataques en respuesta a las nuevas defensas que encuentran. Tienen el incentivo financiero para seguir modificando sus ataques hasta derribar las barreras. Esto puede conducir a una carrera continua entre defensa y ataque, para no perderse pisada entre sí. Nuestro equipo de Black Lotus Labs trabaja diariamente para defender a la comunidad global de internet y su inteligencia de amenazas se alimenta de cuatro soluciones de mitigación de DDoS y otras soluciones de seguridad gerenciada. Lumen le ayuda a protegerse de los ataques diarios sobre sus recursos críticos con políticas de respuesta automatizada.

Lea la ficha técnica

Los 500 mayores ataques por industria



Telecomunicaciones	54%
Juegos online (Gaming)	13%
Software y tecnología	10%
Hosting	6%
Gobierno	6%
Finanzas	5%
Medios y entretenimiento	1.2%
Minorista y distribución	1.0%
Manufactura	0.8%
Servicios corporativos	0.8%
Servicios públicos	0.8%
Educación	0.6%
Bancos	0.4%
Otros	0.4%
Salud	0.2%

LUMEN TECHNOLOGIES

De los 500 ataques más grandes, el 80% fue dirigido contra estas cinco verticales principales (por orden):

1. Telecomunicaciones
2. Software y tecnología
3. Minorista y distribución
4. Gobierno
5. Juegos Online

Tuvimos algunas incorporaciones nuevas a nuestra lista de verticales principales que incluyen Manufactura y Salud. La industria de los juegos online registró el mayor salto, duplicando los ataques que vimos durante el resto de 2021. Esto podría deberse a que las empresas de juegos online preparan sus lanzamientos de 2022 a fines del segundo semestre de 2021, de modo que se convierten en blancos de mayor valor durante ese lapso. A continuación encontrará más información sobre las industrias principales objeto de ataque:

Telecomunicaciones

54%
de los 500 ataques más grandes

812
ataques en total contra la vertical

Mayor magnitud de un ataque de ancho de banda:
317 Gbps

Mayor tiempo de duración de un ataque:
4 días

57%
Ataques multi vector

Mayor ataque basado en paquete:
60 Mpps

Juegos online

13%
de los 500 ataques más grandes

129
ataques en total contra la vertical

Mayor magnitud de un ataque de ancho de banda:
59 Gbps

Mayor tiempo de duración de un ataque:
5 días

80%
Ataques multi vector

Mayor ataque basado en paquete:
5 Mpps

LUMEN TECHNOLOGIES

Software y Tecnología

10%
de los 500 ataques más grandes

513
ataques en total contra la vertical

Mayor magnitud de un ataque de ancho de banda:
499 Gbps

Mayor tiempo de duración de un ataque:
3 días

75%
Ataques de vector único

Mayor ataque basado en paquete:
71 Kpps

Hosting

6%
de los 500 ataques más grandes

106
ataques en total contra la vertical

Mayor magnitudde un ataque de ancho de banda:
408 Gbps

Mayor tiempo de duración de un ataque:
5 días

61%
Ataques de vector único

Mayor ataque basado en paquete:
487 Kpps

Gobierno

6%
de los 500 ataques más grandes

754
ataques en total contra la vertical

Mayor magnitudde un ataque de ancho de banda:
26 Gbps

Mayor tiempo de duración de un ataque:
2 días

57%
Ataques de vector único

Mayor ataque basado en paquete:
8 Kpps

Aprendizaje clave #5

¿Estoy a salvo si mi industria no figura en la lista anterior?

El listado anterior incluye los ataques más grandes que hemos experimentado, aunque prácticamente todas las verticales y tipos de empresas son objeto de ataques. Si posee cualquier tipo de datos que alguien podría querer, su organización podría convertirse en blanco. 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.

Contáctenos

LUMEN TECHNOLOGIES

Aprendizajes clave

El mensaje más importante que esperamos se lleve de leer nuestros Informes Trimestrales sobre DDoS es que la seguridad no debería implementarse de forma tardía, requiere de un esfuerzo consciente de cada parte de una organización. Cada vez que se movilicen los datos habrá una vulnerabilidad, pero conocer las tendencias y lo que está pasando en el espacio de la ciberseguridad le ayudará a identificar las vulnerabilidades.

Cuando se trata de los ataques de DDoS es importante que tenga algunas cosas en mente:

1. **Ningún negocio es inmune:** Si posee activos valiosos en internet, los actores maliciosos pondrán a su organización en la mira.
2. **Nadie puede permitirse el lujo de ser una víctima:** Dado que todos son un blanco potencial, sus resultados financieros no deberían ser su resultado financiero. Los costos de un ataque incluyen la pérdida de ingresos, posibles multas, daños a su reputación y posiblemente el rescate para detener el ataque.
3. **Nadie puede hacer esto por sí solo:** Con la continua evolución de las tendencias de DDoS, los equipos de seguridad internos no pueden sostener dicho ritmo ni mitigar por sí solos. El socio adecuado puede ayudarle a reforzar su estrategia de seguridad existente.

¿Tiene dudas si está siendo objeto de un ataques de DDoS? Lea nuestro blog para reconocer los signos: Cómo saber si su empresa está padeciendo un ataque de DDoS

Si no cuenta con un socio de mitigación de DDoS o si está buscando uno nuevo, a continuación le brindamos algunos criterios para su búsqueda:

- Escala y capacidad para absorber ataques de magnitud en la backbone como primera capa de defensa.
- Infraestructura global para latencia reducida al enrutar el tráfico para depuración.
- Flexibilidad y funcionalidades de avanzada para proteger las experiencias de la red moderna.
- Visibilidad del panorama global de las amenazas para reforzar las defensas.
- Automatización basada en inteligencia de amenazas para bloquear el tráfico de las bot de DDoS antes de que impacten en la red.
- Modelos de soporte híbridos para proteger los entornos digitales actuales. Desde los empleados remotos a las oficinas y desde el data center a la nubed.

Cómo puede ayudarle Lumen actualmente

Con una de las implementaciones de mitigación de DDoS más grandes de la industria, más de 85 Tbps de capacidad FlowSpec de backbone global, depuración inteligente de próxima generación y contramedidas derivadas de Black Lotus Labs, Lumen posee la mitigación de DDoS a escala. El servicio de mitigación de DDoS de Lumen ofrece opciones de mitigación a pedido y siempre activas con funciones avanzadas como depuración inteligente para ayudar a reducir la latencia y mejorar el rendimiento y una tarifa de servicio mensual fija independientemente de la magnitud, la duración o la frecuencia de los ataques.

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

Conozca más acerca de la Mitigación DDoS de Lumen

Si está interesado, lea nuestro informe trimestral de DDoS del tercer trimestre

LUMEN TECHNOLOGIES

Metodología

Los datos del presente informe abarcan el período del viernes, 1 de octubre de 2021 al viernes, 31 de diciembre de 2021. 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, o
- 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.

Notas finales

* Fuente: Worldometer (www.worldometers.info)

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

LUMEN TECHNOLOGIES