INFORME

Informe Trimestral de DDoS de Lumen

3er trimestre 2021 (Q3 2021)

LUMEN TECHNOLOGIES

Introducción

¿Alguien más está cansado? Cuando miramos la magnitud del escenario de la ciberseguridad podemos sentirlo como una corriente de cambios sin fin. Al igual que Sísifo empujando la roca hacia la montaña, justo cuando siente que tiene una idea de lo que está sucediendo, ocurre un nuevo ataque y vuelve a foja cero. Aunque, en nuestra modesta opinión, la seguridad es la parte más vital del trabajo en el espacio de redes y de TI. El presente reporte, fue ensamblado por colaboradores de Lumen apasionados por la ciberseguridad como así también por proteger a las organizaciones y crear una internet más segura. Y comienza poniendo el foco en los tipos y métodos de ataque de manera implacable.

Hoy encontrará tres tendencias principales que afectan a las organizaciones de todas las formas y tamaños.

1. Ataques de DDoS más grandes y generalizados.
2. Las vulnerabilidades de IoT y comando y control (C2) amplían su alcance.
3. Los ciberdelincuentes de distintas especialidades están lanzando ataques con más frecuencia, con volúmenes más grandes y de mayor complejidad.

Si bien puede parecer que cada vez es más difícil empujar la roca hacia la montaña, este informe le ayudará a comprender los ataques de reflexión de spoofing, por qué son importantes las tendencias globales de botnet de IoT, cómo cambian los ataques de un trimestre a otro y a quiénes van dirigidos, para que pueda reforzar sus defensas.

En nuestro Reporte Trimestral de DDoS del tercer trimestre de 2021, examinamos la inteligencia desde Black Lotus Labs y los datos de la Plataforma de mitigación de DDoS de Lumen para desarrollar nuestros hallazgos, algo que ambos refuerzan y amplían sobre estas tendencias más amplias.

Tabla de contenidos

LUMEN TECHNOLOGIES

Hallazgos clave del 3er trimestre de 2021

Botnets de DDoS de IoT

- Los C2s únicos rastreados para botnets de DDoS Gafgyt y Mirai generalizadas, registraron una disminución del 26% en el trimestre.
- La vida útil promedio de un C2 Gafgyt fue de 38 días, mientras que el rango promedio de un C2 de Mirai fue de 21 días.
- Lumen rastreó más de 2.100 C2 a nivel mundial. Los países con la mayor cantidad de C2 resultaron (por orden): China, Estados Unidos y empatados en el tercer puesto Taiwán y los Países Bajos.
- Observamos un incremento trimestral del 45% 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): Brasil, México y Egipto.

Tendencias de los ataques de DDoS

- La cantidad de ataques que mitigamos aumentó un 35% en comparación con el segundo trimestre.
- El mayor ataque de ancho de banda que depuramos en el tercer trimestre fue de 612 Gbps, que significó un aumento del 49% trimestre a trimestre.
- El mayor ataque de ancho de banda que depuramos en el tercer trimestre fue de 252 Gbps, que significó un aumento del 91% trimestre a trimestre.
- El período más largo de un ataque de DDoS que Lumen mitigó para un cliente individual duró 14 días.
- 46% de las duraciones de los períodos de ataque estuvieron por debajo de los 10 minutos, cuando analizamos a los clientes de DDoS on-demand.
- Las mitigaciones multivector representaron 44% de todas las mitigaciones de DDoS, y las combinaciones más comunes fueron: Amplificación de DNS, TCP RST, amplificación de TCP SYN-ACK y amplificación de UDP.
- TCP SYN fue el tipo de mitigación de vector único más común, representando el 25% de las mitigaciones de DDoS.
- Las 3 principales verticales apuntadas en los 500 ataques más grandes durante el tercer trimestres fueron: Telecomunicaciones, Software y tecnología, y Minorista.

Ataques de reflexión de suplantación de identidad (Spoofing): Llamadas telefónicas de broma con impactos enormes

¿Qué son?

Antes de adentrarnos al meollo de este tema, comencemos definiendo qué significa una amplificación o un ataque de reflexión de suplantación de identidad (Spoofing). Un ataque de DDoS de reflexión de suplantación de identidad tiene lugar cuando un actor se hace pasar por otra entidad e inicia una gran cantidad de comunicaciones para provocar una avalancha de tráfico que vuelva a la víctima desprevenida.

Digamos que un atacante quiere apuntar a la empresa X con un ataque de reflexión de DDoS. El atacante envía una solicitud a un servidor de red pidiendo información, proporcionando la dirección IP de la empresa X como el remitente en vez de la propia. El servidor, pensando que está siendo útil, envía la información de regreso a la empresa X. Ahora bien, eso no parece algo tan malo. Pero la intención del atacante es interrumpir las operaciones. Utilizando principalmente servidores UDP que están mal configurados como reflectores abiertos, el atacante puede hacer que la respuesta a la empresa X sea exponencialmente mayor a la solicitud original. Además de eso, el atacante, que aún usa la dirección IP falsificada, ordena a todos los hosts de su botnet que envíen la misma solicitud a varios servidores utilizando la misma IP de origen, lo que hace que la empresa X se vea abrumada muy rápidamente.

Imagínese que alguien se hace pasar por usted, llama a un restaurante y pide una pizza. Además de esa pizza, dice: “envíeme otra pizza cada 15 minutos”. Como si esto fuera poco, consigue que todos sus amigos llamen al restaurante con el mismo pedido. No tiene ni idea de dónde vienen las solicitudes y está abrumado por todas las pizzas que llegan a su casa. ¡Es un gran caos para poner en orden!

¿Cómo se pueden detener los ataques de reflexión de suplantación de identidad (Spoofing)?

El problema es que los ataques de reflexión de suplantación de

identidad son muy difíciles de mitigar por sí solos, y los objetivos por lo general tienen opciones limitadas. Los ciberdelincuentes no buscan únicamente causar el caos; el delito paga. Dada la dificultad de rastrear los ataques de reflexión de suplantación de identidad (Spoofing), son un commodity muy deseado en la dark web. Un hacker puede alquilar su infraestructura, código de ataque, etc., a cualquiera que esté interesado. Entonces, ¿cómo podemos limpiar la internet de los actores maliciosos cuando existe un conjunto enorme de atacantes que están bien escondidos? Lumen se asocia con grupos de confianza del sector para ayudar a rastrear estos ataques hasta saber de dónde provienen. Debido al tamaño de nuestra red y a las capacidades de búsqueda de amenazas, analizamos NetFlow y usamos otras técnicas para encontrar el ingreso del tráfico, ya sea que se trate de un par interconectado con Lumen o de un cliente. Adicionalmente a las asociaciones con pares de la industria, cuando identificamos a un cliente donde el abuso de reflectores abiertos es claramente visible, le recomendamos que cierre el servicio o realice cambios en la configuración para mitigar el abuso potencial.

Hemos rastreado lo imposible de rastrear, ¿y ahora qué? Esta es una pregunta con la que proveedores como Lumen venimos lidiando. No existe una solución única para detectar o filtrar estos ataques, pero utilizamos opciones como listas de control de acceso, filtros de firewall, BGP FlowSpec y reenvío de ruta inversa de unicast (unicast reverse-path-forwarding). En última instancia, el origen o fuente del tráfico falsificado -otros proveedores de red - son responsables de limpiar su propia actividad.

En el amor, en la guerra y en la ciberseguridad, todo vale.

Cuando una organización toma conocimiento de que es la principal fuente de un ataque, uno esperaría que tome alguna medida. Pero hemos visto que no siempre es así. A modo de ejemplo, en el tercer trimestre, un grupo de confianza de la industria denunció que una gran empresa estaba padeciendo un ataque de magnitud. El Centro de Operaciones de Seguridad de Lumen (SOC) utilizó datos de Black Lotus Labs para encontrar la principal red de ingresos, un proveedor de servicios de internet gigante de Rusia. Cuando les informamos del ataque, respondieron que no tenían pruebas del ataque. Después de muchas idas y vueltas, este PSI continuó respondiendo de manera lenta y reticente. La actividad sospechosa nos llevó a pensar que potencialmente estaban haciendo esto de manera intencional para proteger los ingresos de un cliente de sombrero negro, o que estaban siendo complacientes.

El cliente PSI recibió una infracción de la Política de uso aceptable (AUP); sin embargo, no se tomó ninguna medida y los ataques

continuaron. Lumen siguió intentando trabajar con el PSI, pero finalmente tuvo que implementar grandes listas de control de acceso para filtrar el tráfico malicioso.

A pesar de todo esto, los ataques continuaron, aunque en menor escala. Finalmente, llegamos al punto de quiebre. De conformidad con la AUP, teníamos derecho a desconectarlos de la red, a menos que se tomaran medidas, de modo que Lumen en última instancia implementó una lista de control de acceso más prohibitiva para mitigar la situación.

Aprendizaje clave #1

Entonces ¿qué tengo que hacer si considero que mi organización es objeto de ataques de reflexión de suplantación de identidad (Spoofing)?

Dada la naturaleza compleja y la gran escala de estos ataques, será necesario que trabaje con un proveedor de mitigación de DDoS bien establecido. Esto no se trata únicamente de proteger a su organización del acto en sí mismo, sino también de rastrear a las partes cómplices y responsables. Es responsabilidad de cada ISP realizar un barrido de su red en búsqueda de servidores de reflexión no seguros para asegurarse de que cuenten con los parches necesarios para impedir que se usen para DDoS. Limitar el acceso a estos servidores solo a comunicaciones confiables también es una mejor práctica de seguridad sólida. Por último, asociarse con su ISP ascendente si le notifican de una posible infracción de AUP ayudará a limpiar las amenazas que puedan haber sido denunciadas por las víctimas de actividades maliciosas. ¡Estamos todos juntos en esto!

Botnets de DDoS de IoT



Familia	C2 únicos rastreados	Víctimas de ataque único por familia	Ciclo de vida promedio de un C2 (en días)
Gafgyt	349 ▼31% QaQ	Datos inconclusos	38 ▲19% QaQ
Mirai	284 ▼19% QaQ	22,308 ▲43% QaQ	21 ▼25% QaQ

Las dos familias de botnets de IoT de DDoS que rastrea Black Lotus Labs, Gafgyt y Mirai, continúan causando estragos con cientos de C2s dispersos en todo el mundo. Los datos del tercer trimestre estuvieron a la par con los que tuvimos en los trimestres anteriores. Sin embargo, debido a la naturaleza cambiante de la actividad de las botnets, esperamos ver altibajos en estas s cifras. En líneas generales, se registró una disminución del 26% trimestre a trimestre en los C2 únicos rastreados por Lumen. Gafgyt tuvo la mayor disminución, bajando al 31% desde el segundo trimestre.

Definimos a las “víctimas” como el número de direcciones IP únicas contra las que observamos que los C2 lanzan ataques DDoS. Si bien seguimos rastreando a la familia Gafgyt, este trimestre nuestros datos de víctimas no fueron concluyentes.
Sin embargo, las víctimas de Mirai aumentaron un 43% respecto de lo informado en el segundo trimestre y ahora equivalen prácticamente a nuestros hallazgos del primer trimestre.

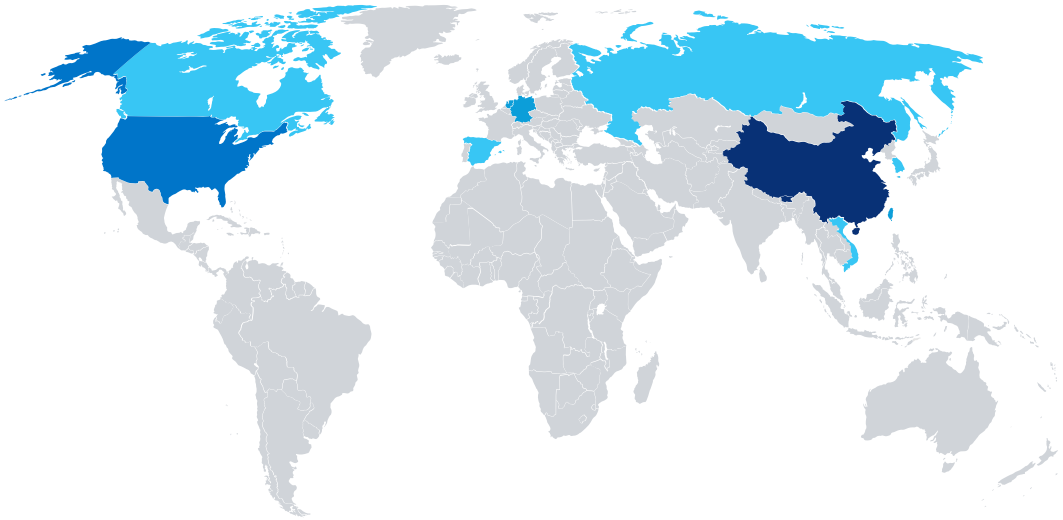
El objetivo de los actores maliciosos consiste en cultivar una infraestructura confiable que puedan usar para sus propios ataques o alquilar como servicio a otros actores para uso temporal. Una vez más, esperamos algunos altibajos en estas cifras conforme evolucionan las botnets. Este trimestre, la expectativa promedio de vida de Gafgyt y Mirai es similar a la que advertimos en el segundo trimestre. La vida útil promedio de Gafgyt aumentó en un 19% y la de Mirai disminuyó en un 25% en el tercer trimestre.

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.

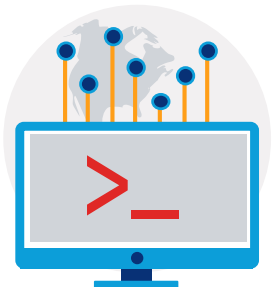
Una nota sobre los mapas de riesgo o de calor: El hecho de que la infraestructura C2 esté ubicada en un país en particular no significa que ese sea el verdadero origen de la infraestructura. Los ciberdelincuentes a menudo ocultan el origen de su actividad aprovechando la infraestructura de otros países.

10 primeros países por C2

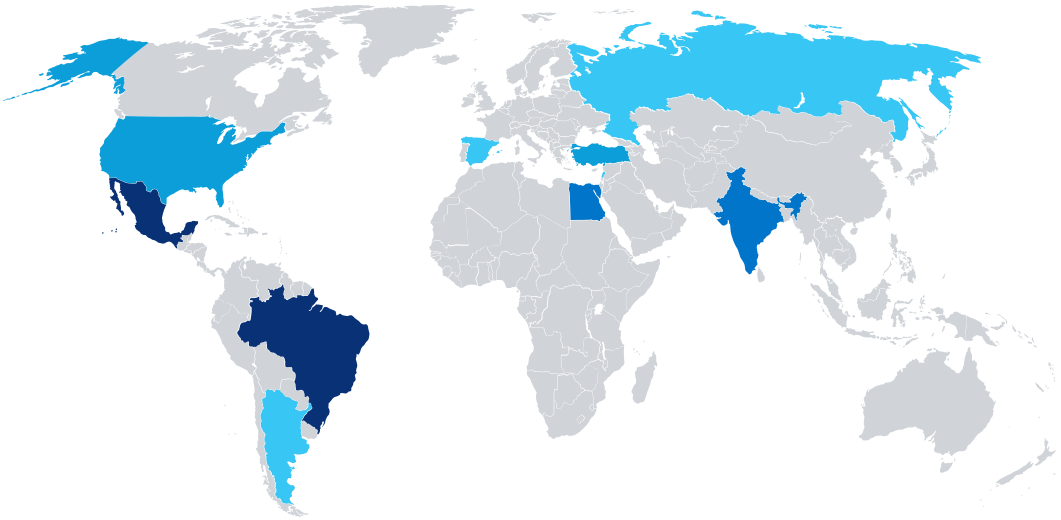


Nombre del país	C2s	Población*	Per Capita (100.000)
China	653	1.439.323.776	0.05
Estados Unidos	381	331.002.651	0.12
Taiwan	128	23.816.775	0.54
Países Bajos	128	17.134.872	0.75
Alemania	115	83.783.942	0.14
Corea del Sur	88	51.269.185	0.17
Vietnam	74	97.338.579	0.08
Canadá	56	37.742.154	0.15
Rusia	51	145.934.462	0.03
España	39	46.754.778	0.08

Lumen rastreó 2.102 C2 a nivel global; el mapa de calor anterior representa los países con la mayor cantidad de C2. La región de APAC tuvo un incremento de C2 este trimestre, representando 4 de los 10 puntos principales, empatando con Europa. El país con más C2 de DDoS fue China, con 653 o el 31% del total de C2 que rastreó Black Lotus Labs en el 3er trimestre. Estados Unidos cayó al puesto número dos después de ser el primero en el segundo trimestre, y Taiwán, nuevo en la lista, compartió el tercer lugar con los Países Bajos. Otros países nuevos que se agregaron a la lista de los 10 primeros incluyen Corea del Sur y Vietnam, mientras que Reino Unido, Italia, Irán y Francia cayeron por debajo de los 10 primeros.

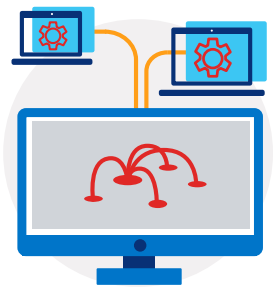


Primeros 10 países por anfitriones de Botnets de DDoS



Nombre del país	Bots	Población*	Per Capita (100.000)
Brasil	44.837	212.559.417	21,09
México	42.736	128.932.753	33,15
Egipto	19.546	102.334.404	19,10
India	15.975	1.380.004.385	1,16
Estados Unidos	10.266	331.002.651	3,10
Turquía	10.171	84.339.067	12,06
Rusia	8.854	145.934.462	6,07
España	8.044	46.754.778	17,20
Argentina	5.976	45.195.774	13,22
Líbano	5.467	6.825.445	80,10

Black Lotus Labs observó un incremento del 45% en los hosts de botnet de DDoS a nivel global trimestre a trimestre, con más de 217.000 — lo más alto que hemos visto todo el año. Nuestros tres primeros países registraron grandes incrementos este trimestre: Brasil: 35%, México: 78% y Egipto: 129%. Líbano, nuevo ingresante a la lista de los primeros 10, posee la mayor cantidad de bots per cápita, alrededor de 80, le siguen México como el segundo número más alto, con 33. España también es nueva en la lista, mientras que China e Irak cayeron por debajo de la línea de los 10.



Aprendizaje clave #2

¿Qué significan estos datos globales?

Probablemente se esté preguntando: "¿Por qué importa lo que está sucediendo en Brasil si solo hago negocios en los Estados Unidos?" Estas dos familias de malware de larga data se han generalizado tanto que existe un alto riesgo de ser atacados. Y también hay más de una forma de verse afectado. Si su red no cuenta con las protecciones adecuadas, podría estar participando involuntariamente en ataques contra otras organizaciones. El simple hecho de ser parte de una botnet puede generar mayores costos de ancho de banda y problemas de rendimiento para sus herramientas y aplicaciones en línea. Y una vez que un hacker tiene acceso a su sistema, ahora está abierto a una gran cantidad de ataques, desde el robo de información a crypto mining y ransomware.

¿Qué es Black Lotus Labs?

Black Lotus Labs es el equipo de inteligencia de amenazas de Lumen. Consta de 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 obtener más información sobre los últimos descubrimientos y eliminaciones de adversarios de Black Lotus Labs, lea sus blogs.

Lea ahora

LUMEN TECHNOLOGIES

Ataques de DDoS en cifras

Aprendizaje clave #3

No se trata de si va a suceder o no, sino cuándo...

Lumen mitigó 7.185 ataques de DDoS en el tercer trimestre. Esto representa un incremento del 35% desde el segundo trimestre y el más alto registrado este año. Estamos protegiendo un promedio de 80 ataques por día, que han estado creciendo a un ritmo constante de 67 por día en el primer trimestre. Los actores maliciosos se están volviendo cada vez más audaces y sofisticados, y buscan causar más disrupción que nunca. Hemos observado niveles crecientes de complejidad en el número de métodos de ataque utilizados contra nuestros clientes.

La mejor defensa es contar con una estrategia. Si está buscando un servicio de mitigación de DDoS que pueda ir de la mano con el cambiante panorama de amenazas, explore nuestros servicios de mitigación de DDoS.

Conozca más

Lumen puede mitigar ataques de DDoS de gran escala en toda su backbone global antes de que el tráfico llegue a un centro de depuración. Las magnitudes de los ataques en el presente informe incluyen los ataques más grandes depurados por la infraestructura de depuración de DDoS de Lumen a nivel global, más que los mayores ataques observados en tránsito o depurados por la red de Lumen.

LUMEN TECHNOLOGIES

Tamaño y duración del ataque

Mayor ataque depurado

	Bits/s perdidos	Paquete/s perdidos
Q3	612 Gbps	252 Mpps
Q2	419 Gbps	132 Mpps
Cambios QaQ	▲46%	▲91%

Existen dos métricas principales para los ataques volumétricos de DDoS:

1. Ataques de ancho de banda: Estos ataques 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. Suelen ser más grandes que los ataques de ancho de banda y se miden en paquetes por segundo.

Lumen observó aumentos significativos en los ataques más grandes que depuramos. Ha habido aumentos casi lineales a lo largo del año en los mayores ataques de ancho de banda. En el tercer trimestre, hubo un aumento del 46% en el ataque más grande, pasando de 419 Gbps a 612 Gbps. No obstante, advertimos que los ataques de velocidad de paquetes más grandes aumentaron exponencialmente en 2021, pasando de 132 Mpps en el segundo trimestre a 252 Mpps este trimestre.

Pero no es necesario que le inflijan el ataque más grande para ver interrumpidas sus operaciones. La magnitud de ataque promedio que vimos (1 Gbps para ancho de banda, 307 Kpps para velocidad de paquetes) podría fácilmente desconectar a las organizaciones desprotegidas.

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 aún más el tiempo de inactividad.

Los datos que siguen solo muestran las tendencias para los clientes on-demand, que representan el 84% de los ataques que Lumen mitigó en el tercer trimestre. Conozca más sobre las diferencias entre mitigación On-Demand y Always-On.

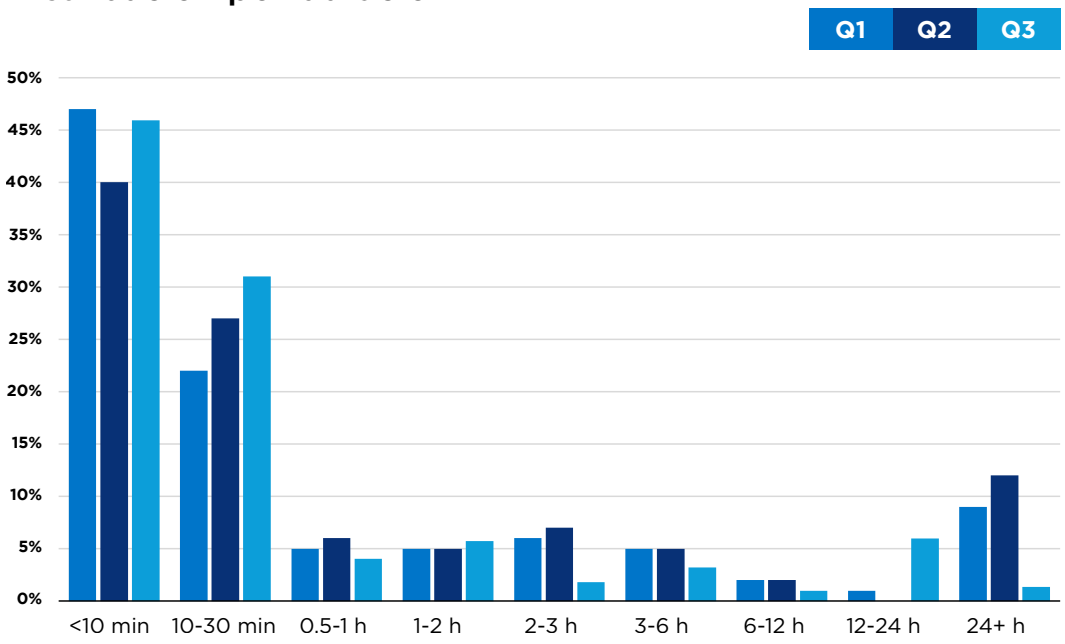
Vea el video

LUMEN TECHNOLOGIES

	Q3	Cambios QaQ
Duración media del ataque	10m 56s	↓30%
Duración promedio del ataque	2h 42m 22s	↓41%
Mayor tiempo de duración de un ataque	14 días	↑40%

Los datos de duración de los ataques sugieren que los ataques más frecuentes tienen una duración breve (<10 minutos). Sí advertimos una ligera disminución en la duración media del ataque, pasando de 15 minutos en el segundo trimestre a apenas menos de 11 minutos en el tercer trimestre. Una de las posibles causas de esta tendencia a la baja podría ser la dependencia de los DDoS de rescate, donde los actores maliciosos despliegan un pequeño ataque para demostrar que son serios en su intención de lanzar ataques más grandes. La duración de nuestro período de ataque más largo volvió a aumentar hasta 14 días, el mismo nivel que informamos en el primer trimestre.

Distribución por duración

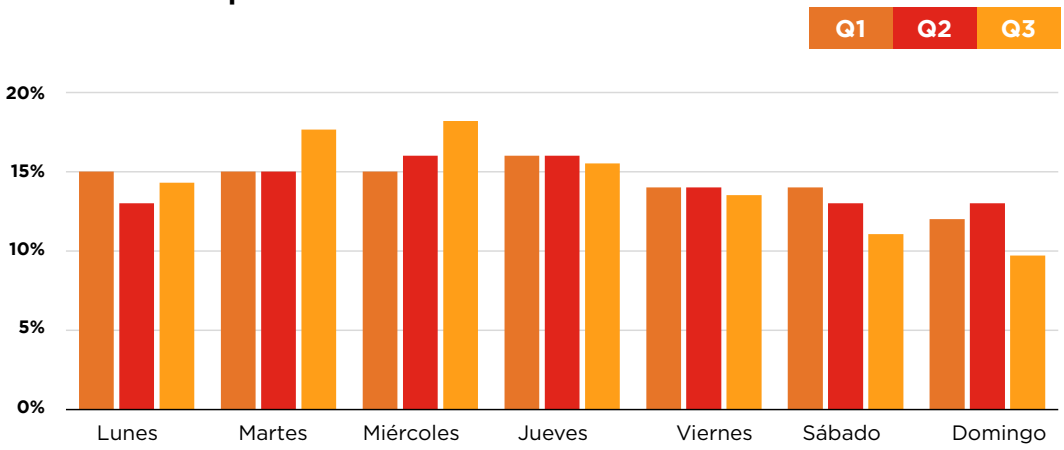


LUMEN TECHNOLOGIES

Cuando analizamos la duración del período de ataque, el 46% de los ataques fueron de menos de 10 minutos, lo que coincide con nuestros hallazgos del primer trimestre. También advertimos ataques en el rango de 10 a 30 minutos en su nivel más alto este año, que representan el 31% de la actividad. Donde registramos la mayor caída fue en los ataques de más de 24 horas, pasando del 12% de los ataques en el segundo trimestre a alrededor del 1% en el tercer trimestre. Una explicación posible es el cambio típico en las tácticas que se produce a lo largo del año, con actores que se focalizan actualmente en ataques más frecuentes y rápidos.

Cuando comparamos la duración y la magnitud de los ataques, advertimos que los ataques más largos tienden a ser mayores en escala también. Por ejemplo, el ataque más grande (612 Gbps en su pico) se extendió durante de 48 horas.

Distribución por día



Los ataques por día de semana estuvieron mayoritariamente alineados con lo que observamos en los dos primeros trimestres de 2021, con excepción del martes, miércoles y domingo. Dispersado por los ataques que vimos en el espacio minorista a principios del trimestre, el martes y el miércoles tuvieron cada uno un 18% de actividad de ataque. Mientras tanto, el domingo se redujo al día menos probable para un ataque, pasando del 13% al 10% de los ataques en dicho día.

Los días que más ataques advertimos en el tercer trimestre fueron el 6 de julio, cuando Lumen mitigó 240 ataques, seguido del 7 de julio con 206 ataques mitigados.

LUMEN TECHNOLOGIES

Aprendizaje clave #4

10 minutos no parecen mal hasta que nos fijamos en el signo pesos

Al mirar estos datos, uno podría pensar: “Bueno, no voy a tener que enfrentarme al ataque más largo, ¿cuáles son las posibilidades de que eso ocurra?” Y si bien eso es cierto, tal vez no tenga que soportar el ataque más largo o grande, los ataques más cortos son igual de efectivos para generar disrupciones en su organización. Supongamos que tiene un cliente que desea acceder a su aplicación y la misma no está disponible porque usted está desprotegido y bajo un ataque DDoS activo. ¿Cuánto tiempo intentará esa persona acceder a su aplicación antes de darse por vencida e ir a otro lugar?

Supongamos ahora que su página lleva más de dos horas caída (nuestro promedio). ¿Cuánto dinero perdió? El costo promedio del tiempo de inactividad se mide en cientos de miles de dólares. Esto sin siquiera considerar el hecho de que los clientes pueden optar por ir a otro lugar para obtener los productos o servicios que ofrece, ni las pérdidas para la reputación de marca que se producirán. Contar con una protección sólida de DDoS instalada le ayudará a prevenir la pérdida de ingresos y de productividad.

Tipos de mitigación de ataques

Ataques de vector único/múltiples

	Q3	Q2	Cambio QaQ
Vector único	56%	62%	▼9%
Multivector	44%	38%	▲40%

LUMEN TECHNOLOGIES

Con el aumento de la cantidad total de ataques este trimestre, vimos un aumento de los ataques multivector y de vector único. Sin embargo, los ataques multivector registraron una suba considerable este trimestre, representando el 44% de todas las mitigaciones de ataques.

Este es el más alto que hemos visto hasta la fecha en 2021, lo que demuestra que los actores maliciosos confían en vectores de ataque cada vez más complejos cuando apuntan a las organizaciones.

Mitigaciones de vector único

División del tipo de mitigaciones de vector único

		QaQ
TCP SYN	25%	↑66%
Filtrado estático	21%	↓26%
UDP	18%	↓17%
Paquetes inválidos	13%	↓21%
DNS	11%	↑34%
Fragmentación de IP	5%	↑28%
Otros volumétricos	3%	↓37%
ICMP	2%	↑56
HTTP	1%	↓43
Amplificación de DNS	0.64%	N.A.
Otros	1.69%	N.A.

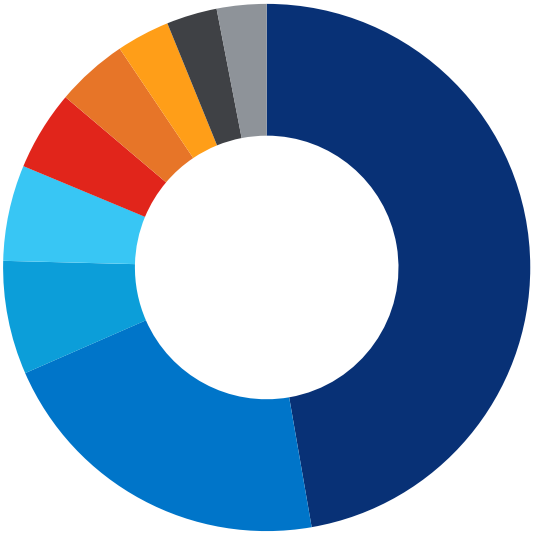
A medida que surgen nuevos métodos de ataque, esperamos una fluctuación de estos resultados. Pero incluso con la llegada y la desaparición de nuevos vectores de ataque, seguimos confiando en los métodos probados y ciertos. Por ejemplo, TCP SYN fue el tipo de mitigación de vector único más común, representando el 25% de las mitigaciones de DDoS. Esto representó un incremento del 66% comparado con los hallazgos de segundo trimestre. Las contramedidas para el filtrado estático y la amplificación UDP cayeron de los puestos número uno y dos al segundo y terceros respectivamente.

Las contramedidas de filtrado estático se realizan generalmente en ítems tales como puerto y protocolo. Esta contramedida también está donde se captan las mitigaciones de alimentación de amenazas de Black Lotus Labs. Provee la mitigación inicial contra los ataques y representó el 21% de los ataques de vector único en el tercer trimestre.

Los ataques de amplificación basados en UDP siguen prevaleciendo, instalándose en nuestro puesto Nro. 3 con un 18% de actividad. Estos ataques apuntan a abusar de los protocolos de capa de aplicación y han demostrado ser muy poderosos con la 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 nuestro blog: Rastreando los reflectores UDP para una internet más segura.

Mitigaciones Multivector

Principales combinaciones de tipo de mitigación multivector



		QaQ
Amplificación de DNS, TCP RST, TCP SYN/ Amplificación de ACK, UDP	28%	N.A.
DNS, TCP SYN	12%	↑23%
DNS, TCP SYN, Filtrado estático	4%	↑35%
DNS, Filtrado estático	3%	↑14%
Filtrado estático, UDP	3%	↓43%
TCIP SYN, Filtrado estático	3%	↓36%
DNS, Filtrado estático	2%	↓62%
Amplificación de DNS, Fragmentación IP	2%	↓10%
Otros ataques volumétricos, UDP	2%	N.A.

Por primera vez este año, los actores maliciosos aprovecharon una variedad mucho mayor de vectores de ataque al lanzar ataques multivector. En trimestres anteriores, Lumen observó un máximo de tres vectores de ataque simultáneos, y este trimestre vimos cuatro: 28% de la mitigaciones Multivector fueron una combinación de amplificación de DNS, TCP RST, TCP SYN-ACK y amplificación de UDP.

La segunda combinación más común fue DNS y TCP SYN, que representaron el 12% de las mitigaciones multivector, subiendo del 10% del segundo trimestre.

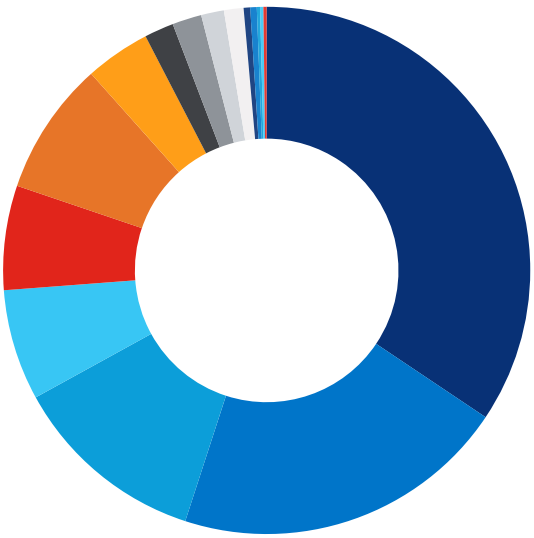
Aprendizaje clave #5

No implemente una protección de DDoS usted mismo

Si calificara sus prácticas de seguridad, ¿se pondría la calificación más alta? Muy pocas organizaciones lo hacen, y muy pocas pueden costear la inversión en una infraestructura de mitigación a gran escala o contratar el talento necesario en la empresa para estar actualizado con el aluvión que presenta el panorama de DDoS. A medida que las organizaciones procuran proteger su infraestructura, los malos actores van perfeccionando sus habilidades. Lo van a atacar con todo lo que puedan para adueñarse de sus activos y aplicaciones que se relacionan con la web. Los ciberdelincuentes pueden cambiar los parámetros y vectores en respuesta a las defensas que pueden encontrar cuando intentan lanzar un ataque. Seguirán modificando el ataque, para que resulte más difícil mitigarlo. Piense en una solución de mitigación de DDoS que tenga automatización incorporada dentro de sus funciones incorporadas. Conozca las soluciones de Lumen sobre Defensa Rápida ante las Amenazas.

Acceda a la ficha técnica

Los 500 mayores ataques por industria



Telecomunicaciones	34%
Software y tecnología	21%
Minorista y distribución	12%
Gobierno	7%
Juegos	6%
Hosting	8%
Medios y Entretenimiento	4%
Finanzas	2%
Transporte	2%
Bancos	1%
Educación	1%
Otros	0.4%
Servicios corporativos	0.4%
Farmacéuticas	0.2%
Consultoría	0.2%
Servicios públicos	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

Tuvimos algunas incorporaciones nuevas a nuestra lista de verticales principales que incluyen: Minorista y distribución; Farmacéutica y Consultoría. Minorista y Distribución tuvo el mayor salto en el tercer trimestre y no representaron a ninguno de nuestros 500 ataques más grandes en el segundo trimestre para ocupar el 12% en este trimestre. A continuación encontrará más información sobre las industrias principales objeto de ataque.

Telecomunicaciones

34%
de los 500 ataques más grandes

956
ataques en total contra la vertical

Mayor ataque de ancho de banda:
612 Gbps

Mayor tiempo de duración de un ataque:
6 días

52%
ataques multivector

Mayor ataque basado en paquete:
252 Mpps

LUMEN TECHNOLOGIES

Software y Tecnología

21%
de los 500 ataques más grandes

515
ataques en total contra la vertical

Mayor ataque de ancho de banda:
405 Gbps

Mayor tiempo de duración de un ataque:
5 días

60%
Ataques de vector único

Mayor ataque basado en paquete:
33 Mpps

Minorista y Distribución

12%
de los 500 ataques más grandes

425
ataques en total contra la vertical

Mayor ataque de ancho de banda:
116 Gbps

Mayor tiempo de duración de un ataque:
3 días

60%
Ataques de vector único

Mayor ataque basado en paquete:
11 Mpps

Gobierno

7%
de los 500 ataques más grandes

2.565
ataques en total contra la vertical

Mayor ataque de ancho de banda:
44 Gbps

Mayor tiempo de duración de un ataque:
4 días

62%
Ataques de vector único

Mayor ataque basado en paquete:
8 Mpps

Juegos

6%
de los 500 ataques más grandes

215
ataques en total contra la vertical

Mayor ataque de ancho de banda:
6 Gbps

Mayor tiempo de duración de un ataque:
3 días

53%
Ataques de vector único

Mayor ataque basado en paquete:
886 Kpps

LUMEN TECHNOLOGIES

Aprendizaje clave #6

Si no veo mi industria en la lista, significa que no me van a atacar, ¿correcto?

El listado anterior incluye los ataques más grandes que hemos experimentado, aunque prácticamente todas las verticales y tipos de empresas son objeto de ataques. Una pregunta que debe formularse: ¿Poseo información que podría interesarle a otra persona? Y la respuesta para cada organización es sí. Usted cuenta con información personal de clientes y de empleados. Cualquier forma de datos puede ser valiosa para los hackers, y los ataques de DDoS por lo general se usan como una distracción para una violación de datos más grande o como una forma de exigir un pago extorsivo. 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

Aprendizajes clave

Los ataques de DDoS se dan a un ritmo desenfrenado, y la frecuencia no parece estar ralentizándose. En todo caso, está evolucionando y cambiando, motivo por el cual los ataques están creciendo en complejidad, envergadura y duración. En este informe incluimos algunas conclusiones para nuestros lectores:

1. Los ataques de reflexión de Spoofing requieren de la ayuda de un proveedor de mitigación de DDoS porque estos pueden crecer de manera exponencial y necesitan tácticas de mitigación extremas.
2. Las tendencias de ataques globales no son “hallazgos lejanos” que no se apliquen a las empresas. De hecho, podría ser fácilmente un objetivo de los C2 o, sin saberlo, podrían ser parte de una botnet que ataca a otras organizaciones.
3. Con un número de ataques que crece día a día, ya no se trata de si sufrirá o no un ataque, sino de cuándo será. Y no importa si no recibe el impacto del ataque más grande o largo; cualquier ataque aún puede interrumpir las operaciones.

4. Incluso 10 minutos de inactividad pueden ser más costosos de lo que cree.

5. Vimos algunos de los ataques más complejos que ocurrieron en el tercer trimestre; implementar su propia estrategia de DDoS es un error.

6. Los datos son la moneda actual y todos son un objetivo, sin importar la industria.

El panorama de las amenazas puede parecernos abrumador. Es tanto lo que tenemos que proteger, y lo que está en juego puede ser increíblemente grande. Las soluciones de mitigación de DDoS pueden liberar parte de la presión de los departamentos de TI. Cuando observamos el balance entre los costos de mitigación de DDoS y el costo del ataque en términos de ingresos, productividad, reputación y experiencia del cliente, es una elección fácil.

Si no tiene un socio de mitigación de DDoS o está buscando uno nuevo, aquí tiene algunos criterios para tener en cuenta:

- Escala y capacidad para absorber grandes ataques 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 bots de DDoS antes de que impacten en la red.
- Modelos de soporte híbridos para proteger los entornos digitales actuales. Desde los colaboradores remotos a las oficinas y desde el data center a la nube.

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 mitigación de DDoS a escala. El servicio de mitigación de DDoS de Lumen provee opciones de mitigación On-Demand y Always-On, con funcionalidades de avanzada como como la depuración inteligente, para ayudarle a reducir la latencia y mejorar el desempeño, y una tarifa de servicio mensual fija independientemente de la magnitud, duración o de la frecuencia de los ataques.

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

LUMEN TECHNOLOGIES

Conozca más acerca de la Mitigación de DDoS de Lumen

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

Metodología

Los datos del presente informe abarcan el período del 1 de julio de 2021 al 30 de septiembre 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 Always-On (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