INFORME

Informe trimestral sobre DDoS de Lumen

Primer trimestre de 2021

LUMEN

Introducción

El año pasado registró nuevamente mucha actividad en el espacio de los ataques de DDoS. Los temas comunes de años recientes como mayor complejidad, frecuencia y escala siguieron impulsando el espacio con actores que fueron cambiando y adoptando sus tácticas, técnicas y procedimientos (TTP), incluidos los ataques de capas de aplicaciones mixtas y multivector, y diversificando los grupos de sus víctimas para maximizar el impacto y/o la rentabilidad.

Como industria, presenciamos uno de los ataques más grandes registrados en el primer trimestre de 2020 con 2,3 Tbps*, seguidos por un ataque de DDoS de Rescate (RDDoS) durante el verano y otoño del hemisferio Norte, dirigido entre otras a las industrias de las finanzas y de la salud.

Adicionalmente, la evolución continua de las botnets de IoT capaces de librar ataques de DDoS, junto con los códigos fuente ampliamente accesibles de las botnet y la infraestructura de botnets de arrendamiento han reducido las competencias mínimas requeridas para lanzar ataques, expandiendo aún más el pool de actores potenciales.

En este contexto, las empresas de hoy se enfrentan al desafío de una creciente dependencia de los ingresos de las aplicaciones digitales para atender y atraer a los clientes, un aumento sin precedentes en el tráfico impulsado por la dependencia generalizada de los servicios digitales y la presión por satisfacer las expectativas del usuario final para la entrega de aplicaciones ininterrumpidas y siempre en funcionamiento.

En nuestro informe trimestral sobre DDoS de Lumen para el primer trimestre de 2021, compartimos nuestra visión del panorama de los DDoS, con hallazgos que refuerzan y a la vez amplían la información sobre esta tendencia creciente, con una mirada en las amenazas de DDoS basadas en inteligencia de Black Lotus Labs, como así también de las tendencias de ataques de la plataforma de servicios de mitigación de DDoS de Lumen.

LUMEN

Principales hallazgos del primer trimestre de 2021

Botnets DDoS de IoT

- Botnets de IoT muy conocidas como Gafgyt y Mirai continúan siendo serias amenazas de DDoS, con 700 servidores activos de Comando y Control (C2s) que atacan de forma combinada a 28.000 víctimas exclusivas.

- De un total de cerca de 3.000 C2 de DDoS rastreados a nivel global en el 1er trimestre, el país que más cantidad alojó fue Serbia, seguida por los Estados Unidos y China.

- De los más de 400 C2 globales que observamos emitiendo comandos de ataque, los Estados Unidos registraron la mayor cantidad, seguidos por los Países Bajos y Alemania.

- De los más de 160.000 hosts de botnet de DDoS rastreados a nivel global, el número mayor corresponde a los Estados Unidos, con casi 42.000 bots.

Tendencias de los ataques de DDoS

- El ataque más grande medido por ancho de banda que depuramos fue de 268 Gbps y el mayor ataque medido por tasa de paquetes depurados fue de 26 Mpps.
- El período más largo de un ataque de DDoS que Lumen mitigó para un cliente individual duró casi dos semanas.
- Cerca del 60% de los períodos de ataques de DDoS duraron menos de una hora, pero casi el 20% de los períodos de ataques de DDoS duraron más de 24 horas.
- Las mitigaciones multivector representaron 41% de todas las mitigaciones de DDoS, y las más comunes utilizaron una inundación de consultas DNS combinada con una inundación SYN TCP.
- El filtrado estático que por lo general se realiza sobre ítems tales como puerto y protocolo, provee una mitigación inicial contra los ataques y fue el tipo de mitigación de vector único más predominante, seguido de paquetes inválidos, amplificación de UDP y TCP SYN.
- Las tres principales verticales que fueron blanco de los 500 mayores ataques en el primer trimestre de 2021 fueron: Finanzas, Software& Tecnología y Gobierno.

Botnets de DDoS de IoT

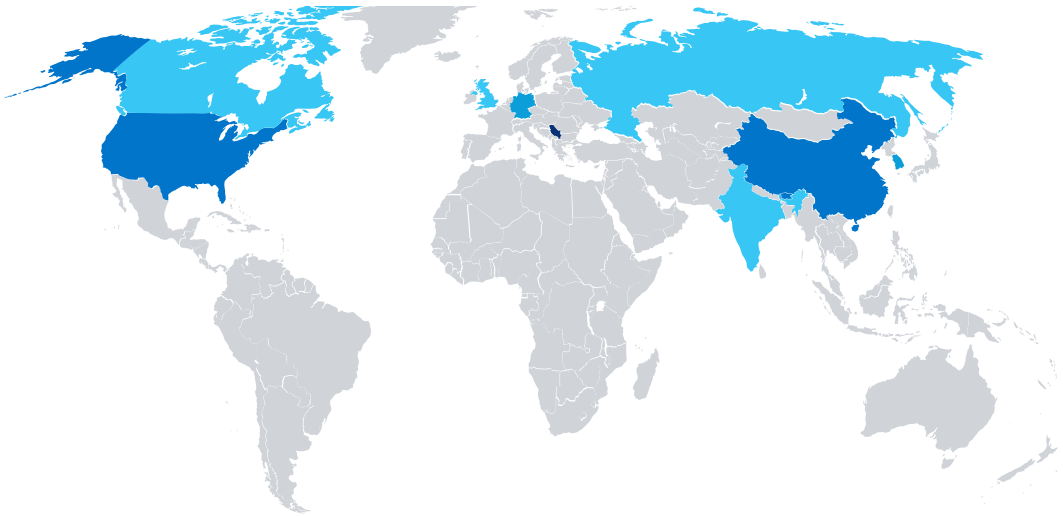
Família	C2s únicos rastreados	Víctimas únicas de ataque por familia	Ciclo de vida promedio de un C2 (en días)
Gafgyt	451	2.870	21
Mirai	249	25.240	10

Al igual que en los informes previos, Black Lotus Labs sigue monitoreando dos de las familias de DDoS de IoT más predominantes: Gafgyt y Mirai. Notablemente, a pesar de que el número de C2s de Mirai -que totalizan un poco más que la mitad de los de Gafgyt en el primer trimestre, y no obstante tener un ciclo de vida promedio mucho menor, Black Lotus Labs identificó aproximadamente 10 veces más de víctimas únicas de ataques de Mirai que de Gafgyt.

Amenazas de DDoS globales rastreadas por país

Los siguientes mapas de calor específicos de DDoS representan a los 10 primeros países por C2 rastreados, C2 que emiten comandos de ataques y anfitriones de botnet para el trimestre basados en la visibilidad de Black Lotus Labs y divididos por tipo de amenazas y país de origen sospechoso. El equipo determina el país de origen tomando la dirección IP de cada host y comparándola contra un conjunto nutrido de direcciones IP para mapeos geográficos.

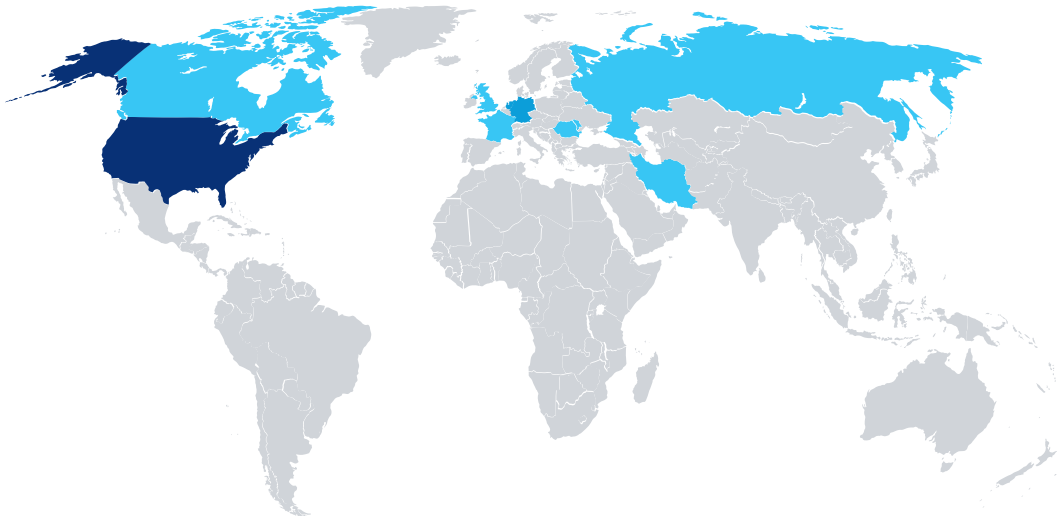
10 primeros países por C2



Nome do país	C2s	Población**	Per Capita (100.000)
Serbia	1.260	8.737.371	14,42
Estados Unidos	380	331.002.651	0,11
China	373	1.439.323.776	0,03
Corea del Sur	166	51.269.185	0,32
Alemania	138	83.783.942	0,16
Países Bajos	132	17.134.872	0,77
Canadá	53	37.742.154	0,14
Rusia	41	145.934.462	0,03
Reino Unido	38	67.886.011	0,06
India	36	1.380.004.385	0,003

El país que aloja la mayor cantidad de C2 de DDoS es Serbia, con un total de 1260, seguida por los Estados Unidos y China con 380 C2 y 373 C2 respectivamente. Serbia también posee el mayor número de C2 per cápita con más de 14 C2 cada 100.000 habitantes, seguida de lejos por los Países Bajos y Corea del Sur.

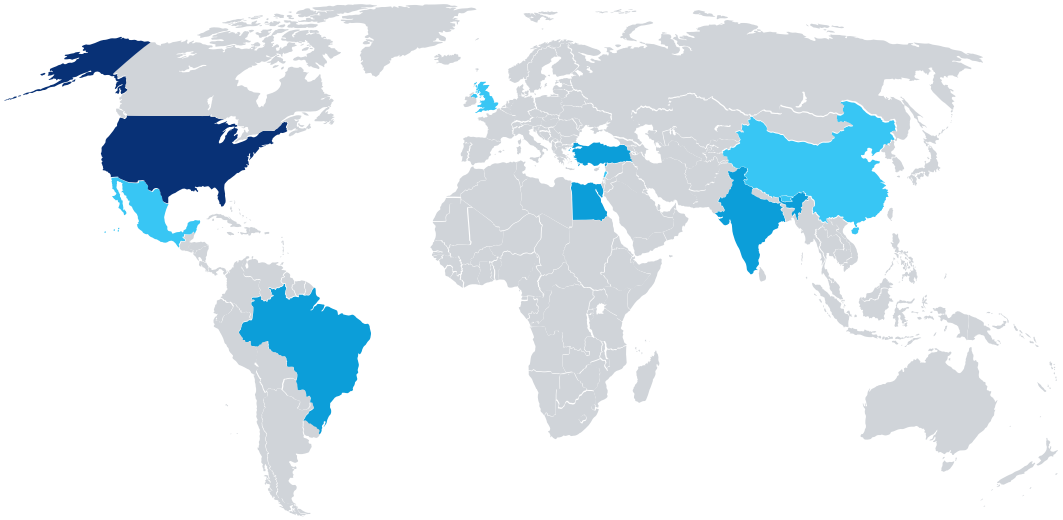
Principales 10 países por C2 que emiten comandos de ataques



Nombre del país	Número de C2s	Población**	Per Cápita (100.00)
Estados Unidos	163	331.002.651	0.05
Países Bajos	73	17.134.872	0.43
Alemania	70	83.783.942	0.08
Canadá	15	37.742.154	0.04
Reino Unido	14	67.886.011	0.02
Francia	13	65.273.511	0.02
Rumania	13	19.237.691	0.07
Rusia	12	145.934.462	0.01
Irán	8	83.992.949	0.01
Moldavia	8	4.033.963	0.20

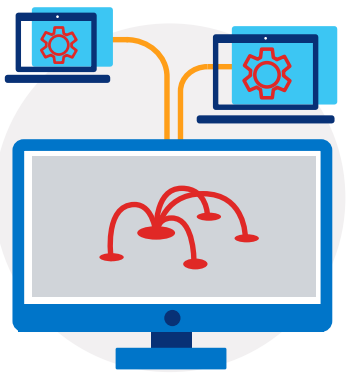
El país con la mayor cantidad de C2 rastreados, observados que emitieran comandos de ataque en este lapso son los Estados Unidos, seguidos por los Países Bajos y Alemania. Los Países Bajos registraron la mayor cantidad de C2 per cápita, seguidos por Moldavia y Alemania.

Primeros 10 países por anfitriones de Botnets de DDoS



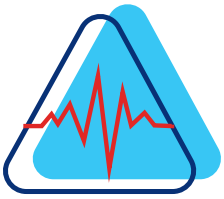
Nombre del país	Número de Bots	Población**	Per Cápita (100.000)
Estados Unidos	41.752	331.002.651	13
Irak	23.647	40.222.493	59
Turquía	12.921	84.339.067	15
Brasil	12.196	212.559.417	6
Egipto	11.009	102.334.404	11
India	10.939	1.380.004.385	1
China	7.371	1.439.323.776	1
México	5.821	128.932.753	5
Líbano	3.612	6.825.445	53
Reino Unido	3.168	67.886.011	5

De los más de 166.000 hosts de botnet de DDoS rastreados en el primer trimestre, el número mayor de hosts está ubicado en los Estados Unidos, con casi 42.000 bots. Sobre una base per cápita, la mayor cantidad de bots de DDoS cada 100.000 habitantes, está ubicada en Irak y Líbano con 59 y 63 respectivamente.



LUMEN

Magnitud y duración del ataque



	Bits/s Perdidos	Paquete/s Perdidos
Mayor ataque depurado	268 Gbps	26 Mpps

Lumen absorbe ataques de DDoS de gran escala en toda su backbone global antes de que el tráfico llegue a un centro de depuración. Los tamaños de los ataques en este informe muestran los mayores ataques depurados por la infraestructura global de depuración de DDoS de Lumen, en lugar de los mayores ataques observados en tránsito en la red de Lumen.

Lumen analiza y mitiga dos tipos principales de ataques volumétricos de DDoS: los medidos por ancho de banda que interrumpen el servicio mediante la inundación de un circuito o aplicación con tráfico medido en bits por segundo, y aquellos medidos por tasa de paquete que también pueden amarrar los recursos específicos de la red tales como ruteadores u otros dispositivos en la red y se miden en paquetes por segundo. Los tamaños de los ataques del presente informe muestran los mayores ataques depurados por la infraestructura global de depuración de DDoS de Lumen, en lugar de los mayores ataques observados en tránsito en la red de Lumen.

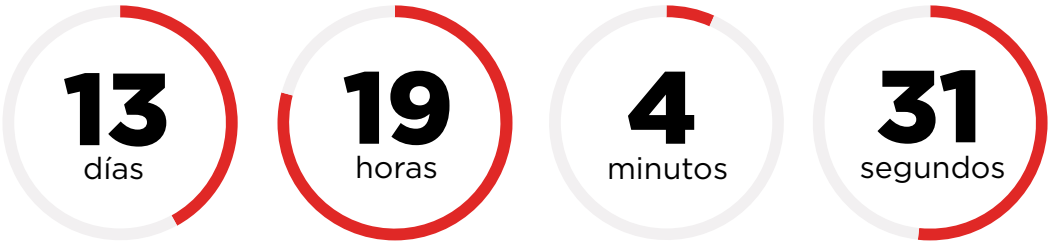
El mayor ataque medido por ancho de banda y depurado en el 1er trimestre fue de 268 Gbps. Muchas empresas actualmente no cuentan con la capacidad de soportar un ataque de +250 Gbps, equivalente a más de 50 millones de emails de texto plano recibidos simultáneamente.

El mayor ataque de alta tasa de transferencia de paquetes que depuramos en el trimestre fue de 26 Mpps, que equivale a 62 puertos de 10 GigE basados en un tamaño promedio de paquete de 300 bytes, que podría fácilmente abrumar los recursos de ruteadores tales como CPU, direccionamiento, memoria u otras funciones.

Duración promedio del ataque

Duración promedio del ataque

Ataque de mayor tiempo de duración

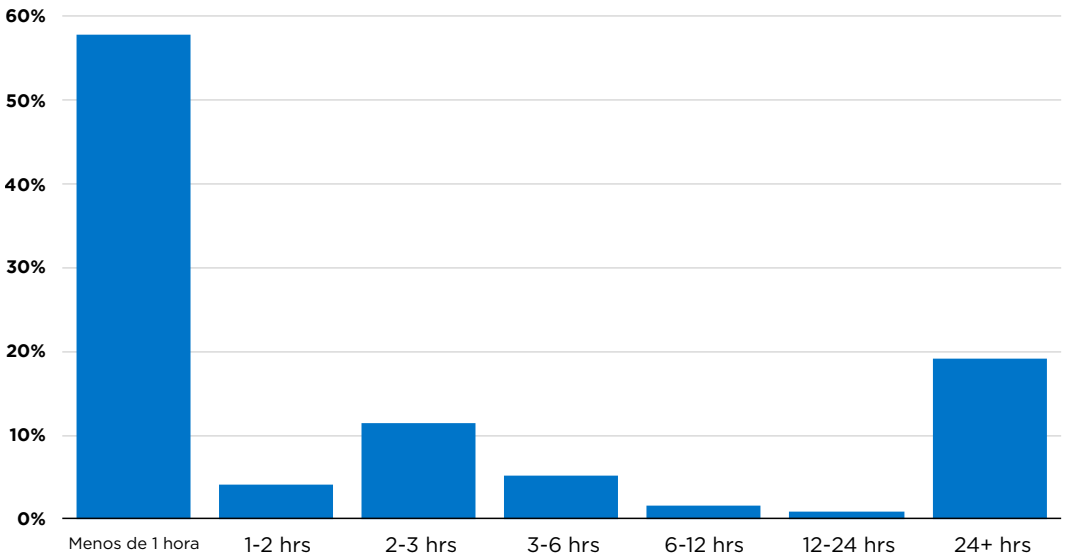


Mientras que la duración promedio del período de ataque fue apenas inferior a 26 minutos, el período de ataque más largo que observáramos duró casi dos semanas. En promedio, los períodos de ataque de DDoS en el primer trimestre duraron casi siete horas.

Cerca del 60% de los períodos de ataques de DDoS duraron menos de una hora, pero casi el 20% de los períodos de ataques de DDoS duraron más de 24 horas.

LUMEN

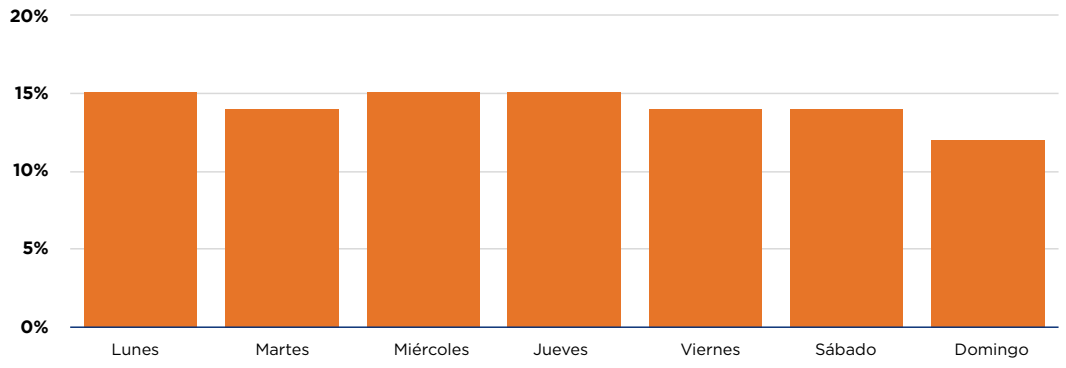
Distribución por duración



Al analizar la distribución por duración, descubrimos que cerca del 60% de los períodos de ataques de DDoS duraron menos de una hora, pero casi el 20% de los períodos de ataques de DDoS duraron más de 24 horas. Y como dato Interesante, el siguiente porcentual mayor de duración de período de ataque de DDoS fue de 2 a 3 horas, con un 11%.

Si bien a nadie le sorprende que la mayoría de los ataques sean inferiores a una hora, dado que los SLA de los proveedores de servicio de mitigación de DDoS oscilan entre 10 y 15 minutos, llama la atención ver un porcentaje de períodos de ataques tan alto que se extiende por más de 24 horas. Para los clientes sensibles a los SLA, la mitigación siempre activa, donde el tráfico se envía a través de depuradores todo el tiempo, puede resultar la elección adecuada.

Distribución por día



También investigamos si los ataques de DDoS se daban con mayor probabilidad en ciertos días por encima de otros, aunque descubrimos que la distribución a lo largo de los días de la semana era bastante consistente, con un 14-15% de ataques fracasando diariamente de lunes a sábado y luego una leve caída los domingos con 12% de ataques. Aparentemente hasta los operadores de DDoS necesitan una pausa.

Tipos de mitigación de ataques

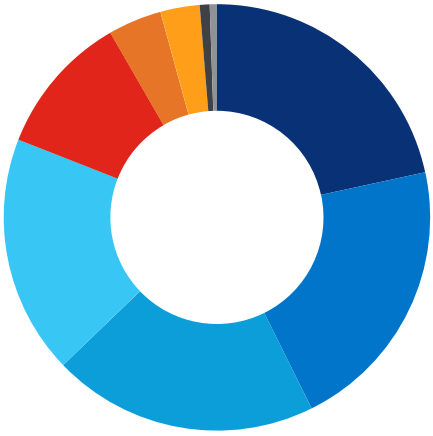
Ataques de vector único/múltiples

Multivetor	41%
Vetor único	59%

La división de los ataques únicos a los de multivector es de aproximadamente 60% a 40% respectivamente. En años recientes, la combinación de único a multivector ha fluctuado, algunos en la industria consideran que los ataques multivector sobrepasan considerablemente a los ataques de vector único. No obstante, dada la amplia disponibilidad de códigos de fuente botnet de DDoS y la relativa facilidad con la que puede arrendarse la infraestructura de ataques de DDoS a través de la darknet, capaz de extender la capacidad de los ataques de DDoS a actores menos sofisticados, no sorprende ver una porción considerable de ataques dirigidos a través de un vector único. Además, los actores más sofisticados también pueden aprovechar los ataques de vector único para lanzar DDoS con el fin de distraer a la víctima de su meta real, como por ejemplo la exfiltración de datos.

Mitigaciones de vector único

División del tipo de mitigaciones de vector único



Filtrado estático	21%
Paquetes inválidos	21%
Amplificación UDP	20%
TCP SYN	18%
DNS	11%
Fragmentación de IP	4%
Otros volumétricos	3%
ICMP	1%
Reflejo TCP SYN/ACK	1%

El filtrado estático que por lo general se realiza sobre ítems tales como puerto y protocolo, provee una mitigación inicial contra los ataques y fue el tipo de mitigación de vector único más predominante, seguido de paquetes inválidos, amplificación de UDP y TCP SYN. Los paquetes inválidos incluyen el tráfico con campos de datos mal formados, como así también fragmentos incompletos, duplicados o demasiado grandes. Si bien pueden ser el resultado de un error de programación de la red o una secuenciación defectuosa de la red, también son características comunes de los ataques de DDoS.

Los ataques de amplificación basados en UDP constituyen un vector común que apunta a los protocolos de capas de aplicaciones y demostraron ser un vector poderoso capaz de amplificar enormemente su impacto potencial. En estos ataques, los actores manipulan la naturaleza sin conexión y sin estado del User Datagram Protocol para falsificar la IP de origen de un paquete de solicitud UDP, para que de ese modo, la víctima reciba paquetes de respuesta UDP no deseados de un servidor intermediario desprevenido. Debido a que las respuestas de UDP a determinadas consultas o servicios pueden ser mucho mayores que los tamaños de los paquetes de solicitud, la IP de la víctima puede sobrecargarse rápidamente.

Durante los ataques de DDoS de amplificación de UDP, a menudo las respuestas generadas por los servidores que se usan para amplificar los mensajes deben responder en fragmentos debido al tamaño de las respuestas. La mayor carga de procesamiento causada por esto en los ruteadores que están manejando inundaciones masivas puede llevar a la pérdida o malformación de fragmentos. Esto genera que los ataques de amplificación de UDP existan tanto dentro del área de amplificación UDP como en el área inválida. Adicionalmente, con muchos de nuestros

clientes, utilizamos filtrado estático para bloquear completamente parte de este tráfico, lo que hace que la amplificación UDP tenga un impacto en muchas mitigaciones y demuestra lo común que es como vector de ataque.

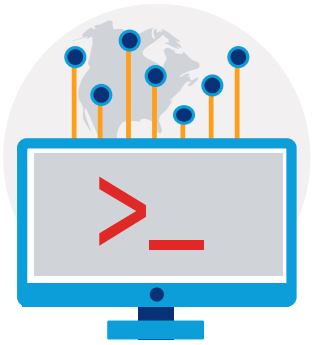
Los ataques TCP SYN exploran el handshake de tres vías de TCP al no responder jamás al paquete de reconocimiento requerido, dejando que un servidor contenga potencialmente decenas o cientos de miles de conexiones abiertas, haciendo que se agote el espacio de socket, el espacio de puerto efímero, el espacio de memoria y similares.

Mitigaciones Multivector

Las 10 principales combinaciones de tipo de mitigación multivector

DNS, TCP SYN	12%
Amplificación DNS, fragmentación IP	4%
TCP SYN, UDP	4%
DNS, TCP SYN, filtrado estático	4%
Paquetes inválidos, UDP	3%
DNS, Filtrado estático	3%
Fragmentación IP, tráfico total, UDP	3%
Paquetes inválidos, filtrado estático	3%
TCP SYN, filtrado estático	3%

Las mitigaciones multivector representaron el 41% de todas las mitigaciones de DDoS; las más comunes utilizaron una inundación de consultas DNS combinada con una inundación TCP SYN. Los ataques de DDoS basados en DNS aquí se refieren a Inundaciones de 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 repetidas encontradas, todas teniendo lugar casi en la misma frecuencia, incluyen amplificación de DNS y fragmentación de IP, TCP SYN y UDP, y paquetes inválidos y UDP. Estas combinaciones reflejan los vectores estándar usados para lanzar ataques de DDoS, aunque combinados de diversas maneras para generar un impacto mayor.

.

BLACK LOTUS LABS®

Rastreando los reflectores UDP para una internet más segura

En años recientes, los eventos Distribuidos de Denegación de Servicio (DDoS) se han convertido en una amenaza siempre presente, con el tráfico de ataque llegando a niveles medidos en terabits por segundo (Tbps). Una de las herramientas clave en manos de los delincuentes cibernéticos que buscan aumentar el ancho de banda de sus ataques, es la reflexión basada en UDP.

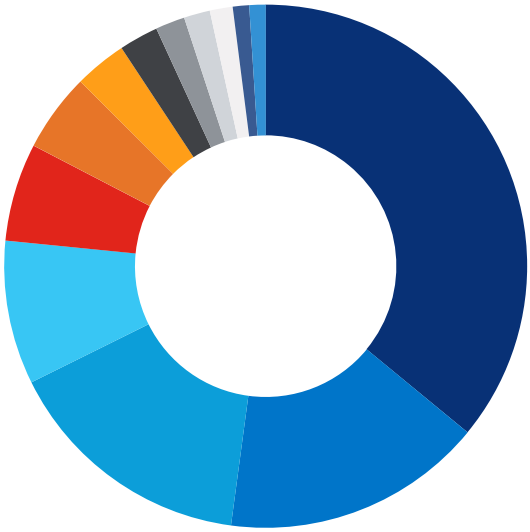
Por ejemplo, el ataque de DDoS de 2018 a GitHub utilizó un servicio de capa de aplicación llamado Memcached para dirigir durante el momento de máxima actividad, 1,35 Tbps de tráfico UDP reflejado en los servidores de GitHub. En 2020, la industria tomó conocimiento de un ataque de DDoS en 2017 que usó paquetes de servicios de UDP como reflectores (CLDAP, DNS y SMTP) para alcanzar tasas de cable de hasta 2.5 Tbps.

En Black Lotus Labs, aprovechamos la visibilidad de nuestra red para identificar servicios que están siendo potencialmente manipulados para lanzar ataques, tales como instancias Memcached, CLDAP y DNS, y luego trabajamos para confirmar si están abiertos para ser utilizados como reflectores. Según nuestros datos del primer trimestre de 2021, vemos que cada uno de estos servicios se utilizan activamente para lanzar ataques de DDoS significativos actualmente.

Lea nuestro blog, Rastreando Reflectores UDP para una Internet más segura, para más información.

LUMEN

500 ataques mayores por industria



Finanzas	36%
Software y Tecnología	16%
Gobierno	15%
Telecomunicaciones	9%
Juegos	6%
Educación	5%
Otras verticales	3%
Servicios públicos	2%
Minorista y distribución	2%
Consultoría	2%
Servicios corporativos	1%
Sin fines de lucro	1%
Salud	1%

De los 500 ataques más grandes, dos tercios apuntaron a solo tres verticales (por orden): Finanzas, Software& Tecnología, y Gobierno. La vertical de finanzas experimentó la mayor cantidad de ataques volumétricos, con el 36% de los 500 ataques más grandes. Software y Tecnología experimentaron 16% de los mayores ataques y el sector de Gobierno, que incluye estatal, local y federal, experimentó 15%. Finanzas siempre ha sido blanco de los ataques de DDoS, pero esta distribución muestra que ninguna vertical está a salvo en el escenario actual de las amenazas.

As principais três verticais que foram alvo dos 500 maiores ataques no primeiro trimestre de 2021 foram Finanças, Software & Tecnologia e Governo.

Aprendizajes clave

Para las aplicaciones de próxima generación y cargas de trabajo modernas, el impulso vital de la economía digital, las expectativas son altas. Todo se trata de la experiencia del usuario, que depende de la disponibilidad, desempeño y seguridad.

A medida que se profundiza la dependencia de las aplicaciones para generar ingresos, muchas organizaciones están dándose cuenta de que ya no pueden arriesgarse a prescindir de las defensas esenciales de DDoS. Las organizaciones deben proteger los activos y aplicaciones críticos de interacción con la web de los ataques cada vez más complejos, y todo con talento interno limitado, una superficie de ataque en expansión y una necesidad inherente de mitigar grandes ataques en la nube o en la red.

Necesitan un proveedor de servicio con alcance global y capacidad de mitigación altamente escalable que les ofrezca protección agnóstica de operador contra los ataques de capas de aplicación mixta y multivector, con características avanzadas como servicio siempre activo y detección y respuesta de amenazas automáticas que los ayude a frenar los ataques antes de que lleguen a la red del cliente.

Guía para los defensores de la red

Los defensores de la red deben buscar un proveedor de mitigación de DDoS capaz de ofrecerles:

- 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 bot de DDoS antes de que impacten en la red.
- Modelos de soporte híbridos para proteger los entornos corporativos actuales, dese el colaborador remoto a la oficina remota, y el data center a la nube.

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 del tamaño, la duración o la frecuencia de los ataques.

Conozca más acerca del Servicio de mitigación de DDoS de Lumen

Metodología

Los datos del presente informe abarcan el período del 1 de enero de 2021 al 31 de marzo 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: https://www.tripwire.com/state-of-security/security-data-protection/amazon-web-services-mitigated-a-2-3-tbps-ddos-attack/

** Fuente: Worldometer (www.worldometers.info)

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