Una nueva investigación analiza los ataques de DDoS que pasaron por los centros de depuración de Lumen

El informe incluye un nuevo blog que rastrea los métodos de ataque utilizados recientemente contra la red del gobierno belga

DENVER, 19 de mayo de 2021 /**PRNewswire**/ -- Los ataques distribuidos de Denegación de Servicio (DDoS) continúan evolucionando en complejidad, frecuencia y escala. **Lumen Technologies** (NYSE: LUMN) rastrea y mitiga estas amenazas – incluidas las familias de las botnet Gafgyt y Mirai – y en el día de la fecha la empresa publicó su informe trimestral de DDoS correspondiente al primer trimestre de 2021. La presente investigación provee un panorama del escenario de los DDoS con hallazgos que a la vez refuerzan y amplían estas tendencias.

Para redactar el informe, el equipo de seguridad de Lumen se nutrió de la inteligencia provista por **Black Lotus Labs** – la división de investigación de amenazas de la empresa, y de las tendencias de ataques de la plataforma del **Servicio de mitigación de DDoS de Lumen**, que integra las medidas de contraataque directamente en su amplia red global, profundamente emparejada.

"A medida que las organizaciones dependen cada vez más de las aplicaciones para generar ingresos, muchas se están dando cuenta de que ya no pueden arriesgarse a prescindir de las defensas esenciales contra los DDoS. La información de este informe agrega más evidencia a lo dicho," comentó Mike Benjamin, vicepresidente de seguridad y de Black Lotus Labs de Lumen. "A medida que las botnets de DDoS de IoT continúan evolucionando, en Lumen nos focalizamos en aprovechar nuestra visibilidad para identificar e interrumpir la infraestructura maliciosa".

Hallazgos clave:

La magnitud de los ataques en el informe de DDoS transmiten los ataques más grandes depurados por la infraestructura de depuración de DDoS global de Lumen, en lugar de los ataques más grandes observados que transitan por la red de Lumen.

Botnets de IoT:

- Las 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.
- Lumen rastreó cerca de 3.000 C2 de DDoS a nivel global durante el primer trimestre. La mayoría de ellos estaba alojado en Serbia (1.260), seguida por los Estados Unidos (380) y

China (373).
- De los C2 globales más activos que Lumen observó emitiendo comandos de ataque, los Estados Unidos tuvieron la cantidad mayor (163), seguidos por los Países Bajos (73) y Alemania (70).
- Lumen rastreó más de 160.000 hosts de botnet de DDoS a nivel global. Casi 42.000 estaban en los Estados Unido, el número más alto que en cualquier otro país.

Tendencias de los ataques de DDoS

- El ataque más grande que Lumen midió por ancho de banda depurado fue de 268 Gbps; el ataque más grande medido por la 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.
- 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.
- Las tres principales industrias que fueron blanco de los 500 mayores ataques en el primer trimestre de 2021 fueron: Finanzas, Software y tecnología, y Gobierno.

Rastreo de los reflectores de Protocolo de diagrama de usuario (UDP)

- Una de las herramientas clave en manos de los delincuentes cibernéticos que buscan aumentar el ancho de banda de sus ataques son los servicios de aprovechamiento de reflexión basados en UDP, como Memcached, CLDAP y DNS.
- A través de este proceso, un atacante falsifica una IP de origen, luego utiliza un servidor intermediario, un reflector, para enviar paquetes de respuesta masivos a la IP de la víctima en lugar de devolverlos al atacante.
- Black Lotus Labs aprovecha la visibilidad de su amplia red global para identificar los servicios que potencialmente se aprovechan para lanzar este tipo de ataques.
- Basándose en los datos del primer trimestre de 2021, Black Lotus Labs observa que los servicios de Memcached, CLDAP y DNS se explotan activamente en la actualidad.
- Para un análisis más detallado de los reflectores UDP, lea el blog más reciente de Black Lotus Labs: **Rastreando los reflectores UDP para una internet más segura**.

Recursos adicionales:

- Lea el **informe completo de DDoS del primer trimestre 2021**.
- Vea un resumen de los datos del informe de DDoS en **esta infografía**.
- Profundice su conocimiento de los **reflectores basados en UPD** en el blog más reciente de Black Lotus Labs.
- Más información sobre el **Servicio de mitigación de DDoS de Lumen.**

- Conozca cómo las organizaciones actualmente atacadas pueden **activar la mitigación de DDoS** en minutos a través de **Lumen DDoS Hyper**.

Acerca de Lumen Technologies:

Lumen se guía por la convicción de que la humanidad está en su mejor estado cuando la tecnología mejora nuestra forma de vivir y trabajar. Con aproximadamente 720.000 km de rutas de fibra y prestando servicios a clientes en más de 60 países, entregamos la plataforma más rápida y segura para aplicaciones y datos, para ayudar a empresas, gobiernos y comunidades a entregar experiencias increíbles. Conozca más sobre las soluciones de red, seguridad, comunicación y colaboración de Lumen y nuestro propósito de promover el progreso humano a través de la tecnología en **news.lumen.com**/home, LinkedIn: /lumentechnologies, Twitter: @lumentechco, Facebook: /lumentechnologies, Instagram: @lumentechnologies y YouTube: /lumentechnologies. Lumen y Lumen Technologies son marcas registradas de Lumen Technologies LLC en los Estados Unidos. Lumen Technologies LLC es una filial de propiedad absoluta de Lumen Technologies, Inc.

Contacto de prensa:
Suzanne K. Dawe
Lumen Public Relations
Connected Security | Black Lotus Labs
720.217.5476
suzanne.dawe@lumen.com

infografia - **https://mma.prnewswire.com/media/1514055/Lumen_Quarterly_DDoS_Report_Q1_2021.jpg**
Logo - **https://mma.prnewswire.com/media/1387693/Lumen_Logo.jpg**

FUENTE Lumen Technologies

Additional assets available online: **Photos (1**

https://news.lumen.com/2021-05-19-Una-nueva-investigacion-analiza-los-ataques-de-DDoS-que-pasaron-por-los-centros-de-depuracion-de-Lumen