La investigación de Lumen sobre DDoS durante el tercer trimestre revela un aumento en la cantidad, magnitud y complejidad de los ataques

El informe más reciente incluye insights preocupantes, más las estrategias para mitigar los ataques.

DENVER, 16 de noviembre de 2021 – Los datos del **Informe sobre DDoS del tercer trimestre** de Lumen Technologies, publicados hoy, revelan un incremento en tres métricas fundamentales: cantidad, magnitud y complejidad de los ataques de DDoS durante el tercer trimestre de 2021.

Hallazgos clave del informe

Para compilar estos hallazgos, el equipo de seguridad de Lumen analizó los datos de inteligencia de **Black Lotus Labs** – la división de investigación de amenazas de la empresa, y las tendencias de los ataques de la plataforma del **Servicio de Mitigación de DDoS de Lumen**, que integran medidas para contrarrestar directamente dentro de la amplia y profundamente emparejada red global de la empresa.

Para leer el informe completo, visite: tinyurl.com/ykmm2dsz (en inglés)

Tendencias de los ataques de DDoS

- Lumen mitigó un 35% más de ataques en el **tercer trimestre** que en el **segundo trimestre**.
- El mayor ataque de ancho de banda depurado en el tercer trimestre fue de 612 Gbps – un incremento del 49% respecto del segundo trimestre – y el mayor ataque depurado basado en velocidad de paquete fue de 252 Mpps – un aumento del 91%.
- El período más largo de ataques de DDoS mitigado por Lumen para un cliente individual duró 14 días.
- Por primera vez, 28% de las mitigaciones multivector incluyeron una combinación compleja de cuatro tipos de ataques diferentes, que incluyen amplificación DNS, amplificación TCP RST, TCP SYN-ACK y amplificación UDP.
- Al igual que en el segundo trimestre, las dos verticales principales a las que fueron dirigidas los 500 ataques de mayor magnitud durante el tercer trimestre fueron Telecomunicaciones y Software y tecnología; la vertical Minorista, que no figuró dentro de los primeros tres en el segundo trimestre, fue el tercer sector más atacado durante el tercer trimestre.

IoT DDoS Botnets

- Si bien Lumen advirtió una disminución del 26% en los C2 únicos de Gafgyt y Mirai, dos familias de botnets de IoT predominantes que monitorea continuamente, la empresa observó más de 217.000 hosts de botnets de DDoS a nivel global. Esto representa un incremento del 45% respecto del segundo trimestre y el más visto a lo largo del año.
- 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.

Mark Dehus, director de seguridad de la información e inteligencia de amenazas de Lumen, comparte su opinión respecto de qué pueden hacer las empresas para protegerse. “Los ataques de DDoS se dan a un ritmo desenfrenado, y la frecuencia no parece estar ralentizándose,” comentó Dehus. "En todo caso, los ataques están evolucionando para utilizar métodos más complejos y están dirigidos a servicios como el de voz, que normalmente no han sido objeto de ataque en los últimos años".

“En Lumen, nos asociamos con grupos de confianza de la industria para rastrear los ataques hasta sus orígenes y bloquear de manera proactiva el tráfico nefasto, en la medida de lo posible. Deseamos que las empresas se sumen a estar lucha de autodefensa,” agregó Dehus “En primer lugar es necesario contar con una estrategia sólida instalada para abordar todos los problemas potenciales de la seguridad. En segundo lugar, trabajar con un socio de mitigación de DDoS bien establecido, particularmente uno que posea la capacidad de rastrear las botnets de DDoS y de encontrar fuentes nuevas antes de que lancen un ataque. Asimismo, hay que buscar un proveedor que ofrezca servicios de seguridad para las aplicaciones, tales como Web Application Firewall y Botnet Management. Y finalmente, si se encuentra bajo ataque, procure una solución como Lumen DDoS Hyper, que le permite activar el servicio en unos 15 minutos y estar en condiciones de habilitar la mitigación".

La magnitud de los ataques en el informe de DDoS de Lumen para el tercer trimestre reporta los ataques más grandes eliminados por la infraestructura global de depuración de DDoS de Lumen, en lugar de los ataques más grandes observados en tránsito o que son depurados por la red Lumen. Para conocer más acerca de la metodología de Lumen y acceder a la información detallada utilizada para elaborar este informe, por favor consulte el **Informe completo sobre DDoS del tercer trimestre**.

Recursos adicionales:

- Lea el **informe completo de DDoS del tercer trimestre**.
- Para acceder a los resultados de los trimestres anteriores, consulte los informes del

Segundo trimestre de 2021 y del **Primer trimestre de 2021**.

- Lea más acerca de los **Servicios de Mitigación de DDoS y Seguridad de las Aplicaciones** de Lumen
- Conozca cómo pueden las organizaciones actualmente bajo ataque, activar la mitigación de DDoS en minutos con **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, nube, 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.

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

---

https://news.lumen.com/lumen-ddos-report-3q-2021-es