Pesquisa da Lumen sobre DDoS durante o terceiro trimestre revela aumento em quantidade, magnitude e complexidade dos ataques

Último relatório inclui insights preocupantes e estratégias para mitigar os ataques

DENVER, 16 de novembro, 2021 – Os dados do **Relatório DDoS do terceiro trimestre** da Lumen Technologies, divulgados hoje, revelam que três métricas fundamentais – quantidade, magnitude e complexidade dos ataques de DDoS – aumentaram no terceiro trimestre de 2021.

Principais Achados do Relatório

Para compilar esses achados, a equipe de segurança da Lumen analisou a inteligência do **Black Lotus Labs** – o braço de pesquisa sobre ameaças da empresa – e as tendências de ataques da plataforma de **Serviço de Mitigação de DDoS da Lumen,** que integra contramedidas diretamente na rede global extensa e com *peering* profundo da empresa.

Para ler o relatório completo, visite: tinyurl.com/ykmm2dsz (em inglês)

Tendências de Ataques de DDoS

- A Lumen mitigou 35% mais ataques no **terceiro trimestre** do que no **segundo trimestre**.
- O maior ataque de largura de banda depurado no terceiro trimestre foi de 612 Gbps – um aumento de 49% em relação ao segundo trimestre – e o maior ataque depurado baseado em taxa de pacotes foi de 252 Mpps – um aumento de 91%.
- O período mais longo de ataque de DDoS mitigado para um cliente individual durou 14 dias.
- Pela primeira vez, 28% das mitigações multivetor envolveram uma combinação complexa de quatro tipos diferentes de ataque, incluindo amplificação DNS, amplificação TCP RST, TCP SYN-ACK e amplificação de UDP.
- Assim como no segundo trimestre, as duas principais verticais que foram alvo dos 500 maiores ataques no terceiro trimestre foram Telecomunicações e Software/Tecnologia; a vertical de Varejo, que não chegou às principais três no segundo trimestre, foi a terceira indústria mais atacada no terceiro trimestre.

IoT DDoS Botnets

- Embora a Lumen tenha observado uma redução de 26% em C2s únicos para Gafgyt e Mirai, duas famílias de botnet de IoT que monitora continuamente, a empresa observou mais de 217.000 hosts de botnet de DDoS globalmente. Isto representa um aumento de 45% em relação ao segundo trimestre e o maior visto ao longo do ano.
- A Lumen rastreou mais de 2.100 C2s globalmente. Os países com a maioria dos C2s foram (em ordem): China, Estados Unidos e, empatados em terceiro lugar, Taiwan e Holanda.

Mark Dehus, diretor de segurança da informação e inteligência sobre ameaças na Lumen, compartilha o que as empresas podem fazer para se proteger. “Os ataques de DDoS estão ocorrendo em ritmo desenfreado e a frequência não parece estar desacelerando”, disse Dehus. “De fato, os ataques estão evoluindo para usar métodos mais complexos e estão sendo dirigidos a serviços como voz, que tipicamente não vinham sendo alvo nos últimos anos”.

“Na Lumen, nos unimos a grupos de confiança na indústria para rastrear os ataques até suas origens e bloquear proativamente o tráfego nefasto, sempre que possível. Queremos que as empresas se unam à luta para que se protejam", acrescentou Dehus. “Primeiro, é preciso implementar uma estratégia sólida para lidar com todas as questões de segurança. Depois, trabalhar com um parceiro de mitigação de DDoS estabelecido, particularmente um que tenha a capacidade de rastrear botnets de DDoS e encontrar novas fontes antes que lancem um ataque. Além disto, é preciso buscar um provedor que ofereça serviços de segurança das aplicações como Web Application Firewall e Botnet Management. E finalmente, se estiver sob ataque, busque uma solução como Lumen DDoS Hyper, que lhe permite ativar o serviço em cerca de 15 minutos e estar pronto para habilitar a mitigação”.

A magnitude dos ataques no relatório DDoS da Lumen do terceiro trimestre expressam os maiores ataques depurados pela infraestrutura global de depuração de DDoS da Lumen, e não os maiores ataques observados em trânsito ou sendo depurados pela rede da Lumen. Para saber mais sobre a metodologia da Lumen e os dados detalhados usados para criar este relatório, por favor veja o **Relatório DDoS do terceiro trimestre** completo.

Recursos Adicionais:

- Leia o **Relatório DDoS do terceiro trimestre completo**.
- Para resultados de trimestres anteriores, veja os relatórios do **segundo trimestre de 2021** e **primeiro trimestre de 2021**.
- Aprofunde-se em **DDoS de Resgate** e o rastreamento de refletores usados nos ataques de DDoS.
- Leia mais sobre os **Serviços de Mitigação de DDoS e Segurança de Aplicações** da Lumen.
- Aprenda como as organizações atualmente sob ataque podem **ativar a mitigação de**

DDoS em minutos com **Lumen DDoS Hyper.**

Sobre a Lumen Technologies:

A Lumen é guiada por nossa crença de que a humanidade está em sua melhor forma quando a tecnologia promove a maneira como vivemos e trabalhamos. Com aproximadamente 720.000 km de rotas de fibra e atendendo clientes em mais de 60 países, entregamos uma plataforma rápida e segura para aplicações e dados, para ajudar empresas, governos e comunidades a fornecer experiências surpreendentes. Saiba mais sobre as soluções de rede, nuvem, segurança, comunicação e colaboração da Lumen e sobre o nosso propósito de promover o progresso humano através da tecnologia em **news.lumen.com**/home, LinkedIn: /lumentechnologies, Twitter: @lumentechco, Facebook: /lumentechnologies, Instagram: @lumentechnologies e YouTube: /lumentechnologies. Lumen e Lumen Technologies são marcas registradas.

For further information: Contato para a Imprensa: Suzanne K. Dawe Relações Públicas da Lumen Connected Security | Black Lotus Labs 720.217.5476 suzanne.dawe@lumen.com

---

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