Nova pesquisa analisa os ataques de DDoS que passaram pelos centros de depuração da Lumen

Relatório inclui um novo blog que rastreia os métodos de ataque usados recentemente contra a rede do governo da Bélgica

DENVER, 19 de maio de 2021 /**PRNewswire**/ -- Os ataques distribuídos de Negação de Serviço (DDoS) continuam a evoluir em complexidade, frequência e escala. A **Lumen Technologies** (NYSE: LUMN) rastreia e mitiga estas ameaças – incluindo as famílias de botnets Gafgyt e Mirai – e hoje a empresa lançou seu relatório trimestral sobre DDoS para o 1º trimestre de 2021. Esta pesquisa fornece uma visão do cenário de DDoS com achados que reforçam e elaboram estas tendências.

Para criar o relatório, a equipe de segurança da Lumen consultou a inteligência do **Black Lotus Labs** – o braço de pesquisas sobre ameaças da empresa – e as tendências de ataques da plataforma de **Serviço de Mitigação de DDoS da Lumen DDoS,** que integra contramedidas diretamente à sua extensa rede global, com profundo peering.

"À medida que as organizações dependem cada vez mais das aplicações para gerar receita, muitas estão percebendo que não podem mais se arriscar a renunciar às defesas essenciais contra DDoS. A informação neste relatório é mais evidência disto", disse Mike Benjamin, vice-presidente de segurança e do Black Lotus Labs, da Lumen. "Enquanto as botnets DDoS de IoT continuam a evoluir, a Lumen está focada em aproveitar nossa visibilidade para identificar e interromper a infraestrutura maliciosa".

Principais Achados:

O tamanho dos ataques no relatório de DDoS relata os maiores ataques depurados pela infraestrutura global de depuração de DDoS da Lumen, ao invés dos maiores ataques observados trafegando pela rede da Lumen.

Botnets de IoT:

- Botnets de IoT reconhecidas, como Gafgyt e Mirai, continuam sendo sérias ameaças, com 700 servidores de Comando e Controle (C2s) ativos atacando 28.000 vítimas únicas combinadas.
- A Lumen rastreou cerca de 3.000 C2s de DDoS globalmente no 1º trimestre. A maioria estava hospedada na Sérvia (1.260), seguida pelos Estados Unidos (380) e China (373).
- Dos C2s globais mais ativos observados pela Lumen emitindo comandos de ataque, os

Estados Unidos tiveram a maioria (163), seguidos pela Holanda (73) e Alemanha (70).
- A Lumen rastreou mais de 160.000 hospedeiros de botnets de DDoS globais. Aproximadamente 42.000 estavam nos Estados Unidos - mais do que em qualquer outro país.

Tendências dos ataques de DDoS

- O maior ataque depurado medido pela Lumen por largura de banda foi de 268 Gbps; o maior ataque depurado medido por taxa de pacote foi de 26 Mpps.
- O período de ataque de DDoS mais longo que a Lumen mitigou para um cliente individual durou quase duas semanas.
- As mitigações multivetor representaram 41% de todas as mitigações de DDoS, com as mais comuns usando uma inundação de consulta DNS combinada com uma inundação de TCP SYN.
- As principais três verticais que foram alvo nos 500 maiores ataques no 1º trimestre de 2021 foram: Finanças, Software e Tecnologia, e Governo.

Rastreando Refletores de Protocolo de Diagrama de Usuário (UDP)

- Uma das principais ferramentas nas mãos dos cibercriminosos buscando aumentar a largura de banda de seus ataques é o reflexo baseado em UDP, aproveitando serviços como Memcached, CLDAP e DNS.
- Através deste processo, um atacante imita um IP de origem, depois usa um servidor intermediário - um refletor - para enviar pacotes de resposta massivos para o IP da vítima, ao invés de enviá-lo de volta ao atacante.
- O Black Lotus Labs aproveita a visibilidade de sua extensa rede global para identificar serviços potencialmente sendo aproveitados para lançar estes tipos de ataques.
- Baseados em dados do 1º trimestre de 2021, o Black Lotus Labs observa que os serviços Memcached, CLDAP e DMS estão sendo ativamente explorados hoje.
- Para um olhar mais detalhado sobre os refletores UDP, leia o blog mais recente do Black Lotus Labs: **Rastreando Refletores UDP em busca de uma Internet mais Segura**.

Recursos Adicionais:

- Leia o **relatório DDoS do 1º trimestre de 2021** completo.
- Veja um resumo dos dados do relatório DDoS **neste infográfico**.
- Aprofunde-se sobre os **refletores baseados em UDP** no mais recente blog do Black Lotus Labs.
- Leia mais sobre o **Serviço de Mitigação de DDoS da Lumen.**
- Aprenda como as organizações atualmente sob ataque podem **ativar a mitigação de DDoS** em minutos através de **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 cerca de 720.000 km de rotas de fibra e atendendo clientes em mais de 60 países, entregamos a plataforma mais rápida e segura para aplicações e dados, para ajudar empresas, governos e comunidades a fornecer experiências surpreendentes. Saiba mais sobre as soluções de rede, edge cloud, 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 da Lumen Technologies, LLC nos Estados Unidos. Lumen Technologies, LLC é uma afiliada de propriedade total da Lumen Technologies Inc.

Infográfico - **https://mma.prnewswire.com/media/1514057/Lumen_Quarterly_DDoS_Report_Q1_2021.jpg**

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

FONTE Lumen Technologies

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

---

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

https://news.lumen.com/2021-05-19-Nova-pesquisa-analisa-os-ataques-de-DDoS-que-passaram-pelos-centros-de-depuracao-da-Lumen