LUMEN

BLACK LOTUS LABS®

Tendências dos ataques de DDoS do Q3 2021

O 3º trimestre de 2021 registrou o maior número de hosts de botnet globais este ano

Comando & Controles (C2s)

O cérebro de uma botnet, que emite os comandos para lançar os ataques de DDoS.

Total:

+2.100

Principais 3 países:

- China - 653
- Estados Unidos - 381
- Taiwan - 128
- Holanda - 128

Hosts de botnet de DDoS

Total:

+217.000

Principais 3 países:

- Brasil - 44.837
- México - 42.736
- Egito - 19.546

Estatísticas dos ataques de DDoS do 3º trimestre de 2021

Maior ataque volumétrico depurado pela Lumen

612 Gbps

Maior ataque de transferência de pacotes depurado pela Lumen

252 Mpps

Período médio de ataque de DDoS mitigado pela Lumen

2 horas **42** m **22** s

Período mais longo de ataque de DDoS mitigado pela Lumen

14 dias

46% dos períodos de ataque de DDoS duraram **<10 minutos**

Ataques multivetor representaram 44% de todos os ataques de DDoS

O que é um ataque multivetor?

Um ataque de DDoS multivetor ocorre quando um ator malicioso utiliza diversos métodos de ataque ao mesmo tempo. É um tipo de ataque mais complexo, pois cada vetor pode exigir uma forma de mitigação diferente, dificultando ainda mais a proteção. No 3º trimestre, a Lumen observou quatro combinações de tipos de ataque, que é a combinação mais variada em 2021.

As botnets de DDoS continuaram generalizadas este trimestre, com um aumento na vida útil média dos C2s de Gafgyt

	C2s únicos rastreados	Vítimas de ataque único por família	Vida útil média de um C2 (em dias)
Gafgyt	349	Dados inconclusivos	38
Mirai	284	22.308	21

Principais 5 verticais alvo dos 500 maiores ataques

Telecomunicações 34%

Software & Tecnologia 21%

Varejo & Distribuição 12%

Governo 7%

Jogos 6%

Veja como as ameaças de DDoS evoluíram em comparação a trimestres anteriores, lendo o relatório completo da Lumen e do Black Lotus Labs.

LEIA O RELATÓRIO COMPLETO AGORA