RELATÓRIO

Relatório trimestral de DDoS da Lumen

4º trimestre de 2021

LUMEN TECHNOLOGIES

Introdução

Um outro ano se encerra e, com isto, é momento de refletir sobre 2021. Foi um ano intenso para todos, especialmente para aqueles que trabalham incansavelmente para manter a internet limpa. Observamos ataques importantes ocuparem as manchetes e interromper não só negócios como também comunidades, em grande escala. E, logo que uma parte da infraestrutura maliciosa é interrompida, outra surge, como um intenso jogo de repetição.

Em nosso Relatório Trimestral de DDoS da Lumen do 4º trimestre de 2021 você conhecerá:

- As previsões de segurança para o próximo ano
- Magnitude, duração e frequência dos ataques
- Vetores dos ataques de DDoS
- Indústrias que foram alvo

Para este relatório, examinamos inteligência do Black Lotus Labs® e dados da plataforma de Mitigação de DDoS da Lumen® para desenvolver nossos achados, que reforçaram e se aprofundaram nas tendências mais amplas. Aqui está uma visão rápida das tendências dos ataques de DDoS observados pela Lumen em 2021:

Número total de ataques mitigados:
20.585

Média de C2s Mirai/ Gafgyt rastreados por trimestre:
800

Média de bots Mirai/ Gafgyt rastreados por trimestre:
200.000

Maior ataque de largura de banda:
612 Gbps

Duração mais longa de um ataque:
14 dias

Contramedida mais comum para ataque de vetor único:
Filtragem Estática

As três verticais mais atacadas:

Telecom

Software e Tecnologia

Governo

LUMEN TECHNOLOGIES

Índice:

Principais achados do 4º trimestre de 2021 4

O que podemos esperar de 2022? 5

Botnets de DDoS de IoT 7

Ameaças globais de DDoS de IoT rastreadas por país .. 8

Ataques de DDoS en números 11

Tipos de mitigación de ataques 16

Os 500 maiores ataques por indústria 19

Principais mensagens 21

LUMEN TECHNOLOGIES

Principais achados do quarto trimestre de 2021

Botnets de DDoS de IoT

- Houve um aumento trimestral de 56% em C2s únicos rastreados para as botnets de DDoS generalizadas Gafgyt e Mirai.
- A vida útil média de um C2 de Gafgyt foi de 32 dias, enquanto a vida útil média de um C2 de Mirai foi de 12 dias.
- A Lumen rastreou 1.724 C2s globalmente. Os países com a maioria dos C2s foram (em ordem): Estados Unidos, Países Baixos e Canadá.
- A Lumen observou um aumento trimestral de 17% na quantidade de hosts de botnet de DDoS globalmente. Os países com a maior quantidade de botnets de DDoS foram (em ordem): México, Brasil e Índia.

Tendências dos Ataques de DDoS

- O número de ataques que mitigamos diminuiu 48% em relação ao terceiro trimestre.
- O maior ataque de largura de banda que depuramos no quarto trimestre foi de 499 Gbps, o que representa uma redução de 27% em relação ao trimestre anterior.
- O maior ataque baseado em taxa de transferência de pacotes que depuramos no quarto trimestre foi de 60 Mpps, o que representa uma redução de 76% em relação ao terceiro trimestre.
- O período mais longo de um ataque de DDoS que mitigamos para um cliente individual durou 5 dias.
- 54% das durações dos períodos de ataque foram de mais de 30 minutos, ao observamos nossos clientes de DDoS On-Demand.
- As mitigações multivetor representaram 35% de todas as mitigações de DDoS, sendo que a combinação mais comum utilizando as contramedidas DNS e TCP SYN.
- A amplificação de UDP foi o tipo de mitigação de vetor único mais comum, representando 29% das mitigações de DDoS.
- As três principais verticais que foram alvo dos 500 maiores ataques no quarto trimestre foram: Telecomunicações, Jogos, e Software e Tecnologia.

O que podemos esperar de 2022?

Antes de entrarmos neste tema, aproveitemos um momento para comemorar a passagem de mais um ano, apesar dos inúmeros desafios. Observando o que ocorreu ao redor do mundo, enxergamos um outro ano no qual uma grande parte da força de trabalho continuou a trabalhar remotamente. E em 2021, observamos muitos ataques cibernéticos de grande importância virando notícia e, em alguns casos, causando mal-estar público nos Estados Unidos. Embora pareça que as coisas estejam voltando ligeiramente ao normal, uma coisa é certa: os ciberatacantes continuarão a nos manter em estado de alerta.

Tendências 2021

1. **Cuidado com os DDoS com pedido de resgate:** Como os atores das ameaças buscam lucros financeiros com suas atividades, eles frequentemente se apoiam em ataques de DDoS com resgate. Houve picos ao longo do ano onde DDoS com resgate foi a principal forma de ataque dos atores maliciosos. Especificamente, observamos muita atividade de maio a julho. Adicionalmente, embora os pedidos de resgate exijam principalmente Bitcoin como pagamento, houve várias demandas de pagamento em Monero.

   Para se aprofundar sobre as atividades de DDoS com resgate, leia nosso relatório do segundo trimestre. Baixar o relatório

2. **Os provedores de voz são um alvo principal:** No terceiro trimestre, observamos diversos provedores de voz sendo atacados. Tradicionalmente, os serviços de VoIP não haviam experimentado o tipo de ataque volumétrico que estava causando um impacto significativo a alguns provedores. No entanto, após o terceiro trimestre, a principal infraestrutura de ataque que os tinha como alvo foi interrompida.

3. **Os ataques de reflexão continuam sendo um vetor de ataque preferido:** Em 2021, os atacantes usaram ataques do estilo reflexão porque estes podem se tornar muito grandes com pouco esforço por parte do atacante. Quer seja CLDAP, NTP, DNS, SSDP ou outros protocolos suscetíveis a ataques de reflexão amplificados, os hackers confiam principalmente nesta categoria de vetor para causar danos significativos. Leia nosso relatório do terceiro trimestre para obter uma análise profunda dos ataques de reflexão por imitação de identidade (spoofing). Baixar o relatório

Previsões 2022

1. **Espere picos e quedas nos DDoS de resgate:** A expectativa da Lumen é de que comece a surgir alguma forma de sazonalidade nos ataques de DDoS por resgate. Provavelmente, teremos alguns períodos de seca seguidos de uma enxurrada de atividade, com os hackers optando por uma campanha de comoção e surpresa. Os principais ataques também inspirarão outros e prevemos que ocorrerá atividade de imitação.

2. **Haverá um aumento dos ataques multivetor, mais sofisticados:** Já observamos um aumento na complexidade dos ataques ao longo de 2021 e isto continuará a ocorrer em 2022. Ano que vem, são esperados os maiores ataques volumétricos já vistos, já que as botnets continuam a crescer em magnitude e complexidade a cada ano. E similar a uma Hydra, assim que você remove um pedaço da infraestrutura suspeita, outro surge. Haverá também um crescimento dos ataques de Camada 7, aumentando a necessidade de proteção das aplicações web e gestão de bots para defender a receita impulsionada por novas aplicações.

3. **Aumento das disrupções colaborativas de crimeware em meio ao aumento das atividades dos estados-nação:** À medida que os ataques dos estados-nação se tornam cada vez mais predominantes (não só especificamente para DDoS), e enquanto a indústria e os governos continuam a colaborar, como fizeram nas diversas tentativas de derrubada, tal como a Emotet no ano passado, esperamos que este tipo de colaboração renda mais frutos.

   Dado o cenário político do Leste Europeu, esperamos ver um aumento nos ataques patrocinados por estados-nação em 2022. Além disto, as nações ocidentais devem estar preparadas para se defender contra campanhas diretas ou danos colaterais. As campanhas devem incluir, não exclusivamente, ransomware (malware de resgate), DDoS e ataques contra infraestruturas críticas.

   O Black Lotus Labs e a Lumen continuarão fazendo sua parte para manter a internet um lugar seguro. Leia um de nossos blogs recentes para aprender sobre as ameaças e tendências mais recentes: Nova campanha Konni inaugura o Ano Novo tendo como alvo o Ministro de Relações Exteriores da Rússia.

LUMEN TECHNOLOGIES

Botnets de DDoS de IoT: A Lumen permanece alerta

Família	C2s únicos rastreados	Vítimas de ataque único por família	Vida útil média de um C2 (em dias)
Gafgyt	507 ▲45% QaQ	1.117	36 ▼5% QaQ
Mirai	480 ▲69% QaQ	21,140 ▼5% QaQ	12 ▼42% QaQ

As duas famílias predominantes de DDoS de IoT rastreadas pelo Black Lotus Labs, Gafgyt e Mirai, continuam causando estragos, com centenas de C2s dispersos ao redor do mundo. Rastreamos estas famílias durante anos porque elas continuam prevalecendo, seja com leves modificações ou com novas infraestruturas que continuam surgindo. Os dados do quarto trimestre estavam alinhados ao que encontramos nos trimestres anteriores; no entanto, devido à natureza mutante da atividade das botnets, esperamos ver um fluxo e refluxo destes números.

Em geral, houve um aumento de 56% no total de C2s únicos rastreados, sendo que Mirai foi responsável pela mudança de um trimestre a outro, subindo 69% desde o quarto trimestre.

Definimos as “vítimas” como a quantidade de IPs únicos contra os quais observamos os C2s lançando ataques de DDoS. Juntas, as duas famílias de botnet fizeram mais de 22.000 vítimas, o que se alinha à nossa média trimestral de 2021.

Um dos objetivos dos atores maliciosos é cultivar uma infraestrutura confiável que possam usar para seus próprios ataques ou para alugar como serviço a outros atores, para uso temporário. Isto significa que estão visando manter estas infraestruturas vivas o maior tempo possível. Neste trimestre, a vida útil de Gafgyt se alinhou ao que vimos nos outros trimestres deste ano, com uma ligeira queda de 5%.

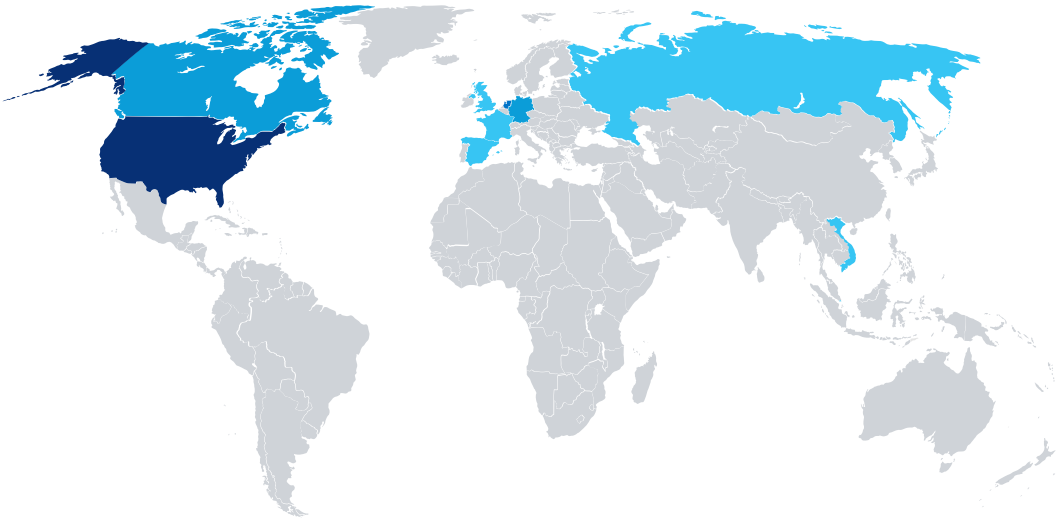
A vida útil de Mirai teve uma queda trimestral maior, de 43%. Embora ambas as famílias tenham registrado queda de um trimestre a outro, suas vidas úteis foram mais altas do que nossa média anual.

Ameaças globais de DDoS de IoT rastreadas por país

Os seguintes mapas de calor específicos de DDoS representam os principais 10 países por C2s rastreados e hosts de botnets de DDoS. Os dados são baseados na visibilidade do Black Lotus Labs e estão divididos por tipo de ameaça e país de origem suspeito. O país de origem é determinado comparando o endereço IP de cada host com um vasto conjunto de endereços IP mapeados globalmente.

Um aviso a respeito dos mapas de calor: o simples fato de uma infraestrutura de C2 estar localizada em um país específico, não significa que esta seja sua verdadeira origem. Os cibercriminosos frequentemente ocultam a origem de sua atividade aproveitando a infraestrutura de outros países.

10 principais países por C2

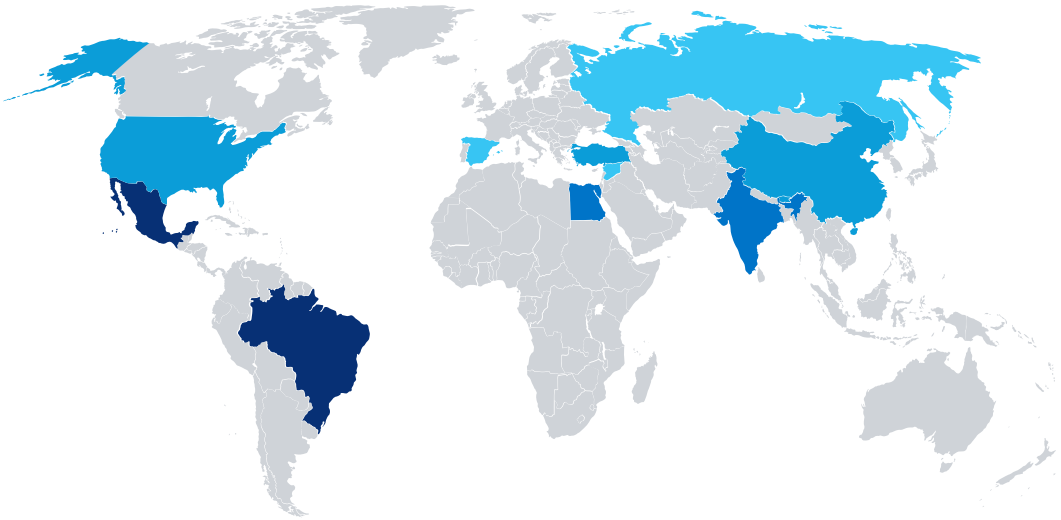


País	C2s	População*	Per Cápita (100.00)
Estados Unidos	554	331.002.651	0,17
Países Baixos	266	17.134.872	1,55
Canadá	197	37.742.154	0,52
Alemanha	187	83.783.942	0,22
Espanha	94	46.754.778	0,20
Reino Unido	79	67.886.011	0,12
França	36	65.273.511	0,06
Rússia	29	145.934.462	0,02
Singapura	26	5.850.342	0,45
Vietnã	19	97.338.579	0,02

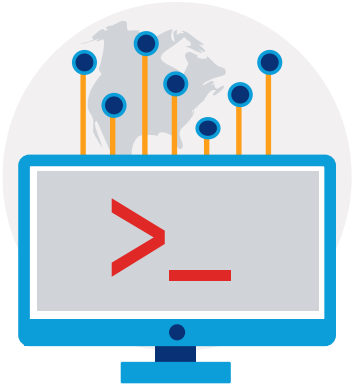
A Lumen rastreou 1.724 C2s no mundo todo no quarto trimestre; o mapa de calor acima representa os países com o maior número de C2s.

Os Estados Unidos tiveram a maior quantidade de C2s e responderam por 32% do total de C2s rastreados. Canadá, Países Baixos e Alemanha também registraram aumentos significativos em relação a trimestres anteriores. A China, que ocupava nosso primeiro lugar no trimestre passado, sumiu completamente de nossa lista dos principais 10, junto com a Coréia do Sul e Taiwan. Os novos integrantes da lista são: Reino Unido (5% do total), França (2% do total) e Singapura (2% do total).

10 principais países por hosts de botnets de DDoS



País	Bots	População*	Per Cápita (100.000)
México	45.719	128.932.753	35.46
Brasil	41.616	212.559.417	19.58
Índia	25.304	1.380.004.385	1.83
Egito	23.631	102.334.404	23.09
Estados Unidos	14.359	331.002.651	4.34
China	10.658	1.439.323.776	0.74
Turquia	10.405	84.339.067	12.34
Espanha	9.857	46.754.778	21.08
Rússia	8.021	145.934.462	5.50
Síria	6.608	17.500.658	37.76



O Black Lotus Labs observou um aumento de 17% nos hosts de botnet de DDoS em todo o mundo, de um trimestre a outro, com mais de 250.000 – o mais alto visto durante todo o ano. Nosso principal país da lista, o México, teve um aumento de 7% e passou do segundo para o primeiro lugar. O Brasil baixou para nossa segunda posição, com uma ligeira queda de 7%. A Índia experimentou o maior aumento, de 58% em relação ao terceiro trimestre, passando de cerca de 15.900 hosts de botnet para 25.300 hosts. A China e a Síria foram os novos acréscimos à lista, enquanto a Argentina e o Líbano saíram de nossa lista dos 10 principais.

Mensagem #1

Por que eu deveria me importar com os dados globais?

Se você é uma empresa nos Estados Unidos, por que deveria se importar se o México tem a maior quantidade de hosts de botnets? Com Gafgyt e Mirai tão amplamente disseminadas, sempre há uma chance de tornar-se vítima ou de ter sua infraestrutura utilizada para atingir outras organizações.
Se sua rede não conta com as proteções adequadas, você poderia estar participando involuntariamente de ataques contra terceiros. Fazer parte de uma infraestrutura de botnet pode, de fato, causar impactos negativos em suas próprias operações, tais como custos mais altos com largura de banda e problemas com o desempenho de suas aplicações. E, uma vez que um hacker tenha acesso a seus sistemas, você estará aberto a uma variedade de ataques, desde roubo de dados até cryptomining ou ransomware.

O que é Black Lotus Labs?

A Black Lotus Labs é uma equipe de inteligência sobre ameaças da Lumen. É um grupo de profissionais de segurança e cientistas de dados cuja missão é aproveitar a visibilidade global da rede da Lumen para ajudar a proteger sua empresa enquanto mantem a internet limpa. O Black Lotus Labs utiliza a busca e análise das ameaças, assim como machine learning e validação automatizada de ameaças, para identificar e interromper o trabalho dos atores maliciosos. Se estiver interessado em aprender mais sobre a última pesquisa e as capacidades avançadas do Black Lotus Labs para o rastreamento dos atores e crimeware, leia seu blog.

Leia agora

Após um terceiro trimestre movimentado, houve uma desaceleração no quarto trimestre

Avaliando 2021, nosso trimestre mais movimentado foi o terceiro, com mais de 7.100 ataques mitigados. E julho, em particular, observou o maior número de ataques, em termos de frequência, magnitude e duração. No quarto trimestre, observamos nosso menor número de ataques por trimestre, com 3.718, o que representa uma queda de 48% de um trimestre a outro. No entanto, quase não houve queda na quantidade de locais atacados (apenas uma redução de 3%), o que significa que apesar de ter havido menos ataques no trimestre, os atores maliciosos estão disseminando os ataques entre muito mais locais. Um possível motivo da queda pode ser a sazonalidade. Assim como muitas outras tendências, os ataques de DDoS apresentam fluxo e refluxo e em 2022, esperamos observar um aumento contínuo da atividade.

Magnitude e duração do ataque

Maior ataque depurado

	Bits/s perdidos	Paquete/s perdidos
Q4	499 Gbps	60 Mpps
Q3	612 Gbps	252 Mpps
Mudança QaQ	⬇27%	⬇76%

LUMEN TECHNOLOGIES

Existem duas métricas principais para os ataques de DDoS volumétricos:

1. **Ataques de largura de banda:** Estes visam interromper o serviço inundando um circuito ou aplicação com tráfego. Este tipo de ataque é medido em bits por segundo.
2. **Ataques por taxa de transferência de pacotes:** Esses ataques consomem recursos nos elementos da rede, como roteadores e outros dispositivos. Estes são normalmente maiores do que os ataques de largura de banda e medidos em pacotes por segundo.

Ataques de largura de banda

No quarto trimestre, houve uma queda de 27% nos ataques de largura de banda em relação ao terceiro trimestre.

O tamanho médio foi de quase 500 Gbps, no entanto, esteve acima de nossa média de 2021, de 450 Gbps.

O tamanho médio dos ataques aumentou de 1Gbps no terceiro trimestre para 2 Gbps no quarto trimestre.

Ataques por taxa de transferência de pacotes

No quarto trimestre, o maior ataque baixou 76%, de 252 Mpps para 60 Mpps.

Nosso tamanho médio de ataque no quarto trimestre foi de 515 Kpps, um aumento de 68% em relação ao trimestre anterior.

Mensagem #2

Por que importa a magnitude do ataque?

Não é preciso que você seja atingido pelo maior ataque da história para que suas operações sejam interrompidas. Vemos muitas organizações que não têm proteção de DDoS ficarem offline por tamanhos tão pequenos quanto 1 Gbps. Contar com uma proteção DDoS ajudará a garantir que os ativos voltados à web continuem funcionando, ainda que você esteja sobre um ataque ativo.

LUMEN TECHNOLOGIES

Quanto tempo estão durando os ataques?

Os números das durações dos ataques são afetados pelo modelo de mitigação do cliente. Há duas opções.

1. Mitigação On- Demand (sob-demanda): O tráfego é sempre monitorado, mas apenas depurado quando uma ameaça é detectada.

2. Mitigação Always-On (sempre ativa): O tráfego é constantemente depurado para minimizar ainda mais o tempo de inatividade.

Os dados abaixo representam apenas as tendências para os clientes On-Demand, que são responsáveis por 69% dos ataques mitigados pela Lumen no quarto trimestre. Saiba mais sobre as diferenças entre mitigações On-Demand e Always-On.

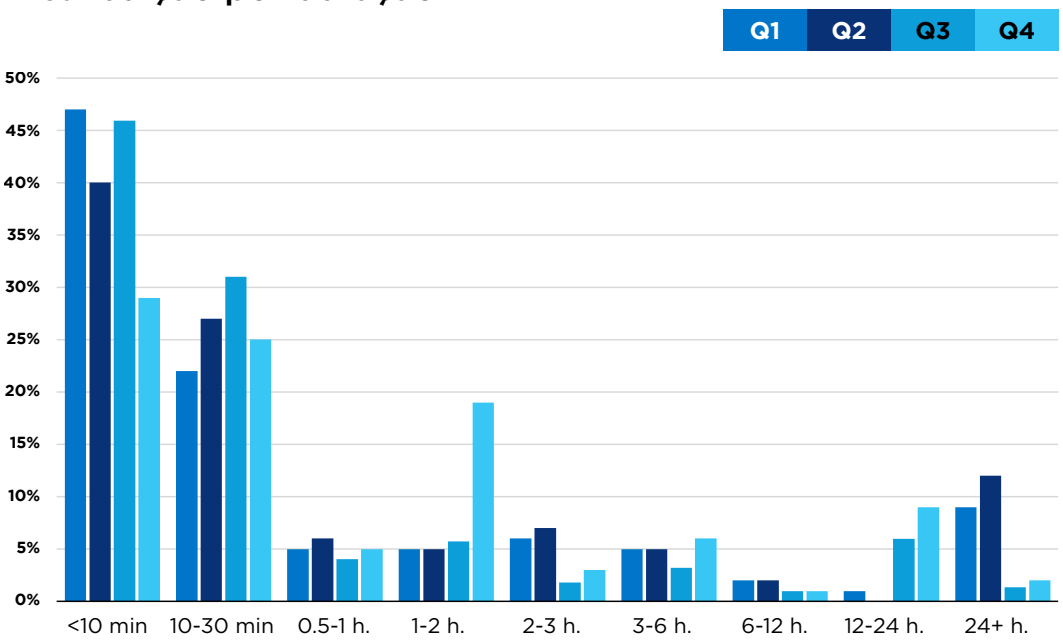
	Q4	Mudança QaQ
Duração mediana dos ataques	30’	▲184%
Duração média dos ataques	4h 23’50”	▲75%
Duração mais longa de um ataque	5 días	▼64%

Ao observarmos a duração dos ataques, vimos que a duração média e mediana de ataques aumentou 184% e 75%, respectivamente. A duração mediana dos ataques foi a mais longa experimentada durante todo o ano e teve o maior salto do terceiro para o quarto trimestre, passando de pouco menos de 11 minutos a 30 minutos.

LUMEN TECHNOLOGIES

O ataque mais longo mitigado pela Lumen no quarto trimestre foi de cinco dias, uma redução significativa em relação aos trimestres anteriores. Isto não significa que podemos ficar aliviados. Esta redução pode ser atribuída à sazonalidade, quando os atores de DDoS estavam menos ativos. Esperamos ver ataques mais longos e sofisticados surjindo no horizonte.

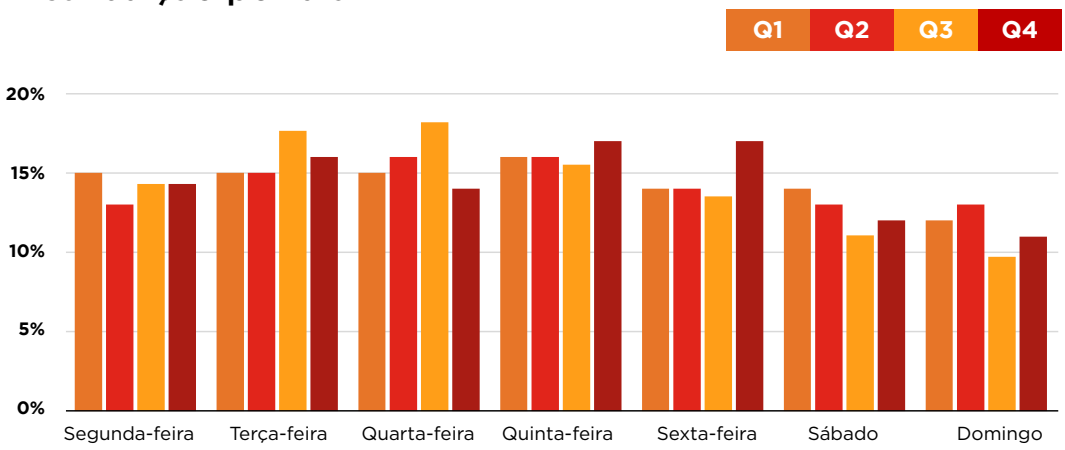
Distribuição por duração



Assim como ocorreu no restante de 2021, a duração de pouco menos de 10 minutos foi a que mais prevaleceu no quarto trimestre, representando 29% dos ataques mitigados. No entanto, pela primeira vez em 2021, no quarto trimestre observamos um enorme salto na duração dos ataques com duração de uma a duas horas. Tipicamente, o percentual dos ataques abaixo de 1-2 horas esteve em torno de 5,5%, saltando no quarto trimestre para 19% do total de ataques.

Houve um aumento nos períodos de ataques com duração de 12-24 horas e nos com duração de mais de 24 horas (52% e 73%, respectivamente). No início de 2021, os atacantes tiveram um período de ataque muito mais longo, com 9-12% dos ataques durando mais do que 24 horas. No entanto, esta é a primeira vez que observamos uma dependência maior nos ataques com períodos de duração de 12-24 horas.

Distribuição por dia



Os ataques por dia da semana estiveram principalmente alinhados ao que observamos nos primeiros três trimestres. No terceiro trimestre, as terças-feiras foram mais ativas, mas no quarto trimestre houve mais atividade nas sextas-feiras. O sábado e o domingo continuam sendo os dias menos ativos.

O dia em que observamos mais ataques no quarto trimestre foi 16 de dezembro, quando a Lumen mitigou 83 ataques, seguido de 18 de novembro, quando mitigamos 79 ataques.

Mensagem #3

Você pode se dar ao luxo de ficar fora do ar, ainda que por 30 minutos?

Os atacantes estão tentando interromper suas operações. Você pode se dar ao luxo de deixar suas operações de internet fora do ar, ainda que por meia-hora? Seus clientes buscarão outra aplicação ou site quando virem que você está fora do ar? Deixarão de confiar em você para

proteger dados sensíveis, tal como informação de pagamento, quando ouvirem notícias sobre o ataque à sua organização? Você será multado por alguma entidade de compliance? O custo de um ataque não se limita ao tempo de inatividade que você enfrenta e pode ter ramificações de longo alcance para seus resultados financeiros. Nos últimos anos, o custo médio de um ataque de DDoS pode estar em torno de centenas de milhares de dólares.

LUMEN TECHNOLOGIES

Tipos de mitigação de ataques

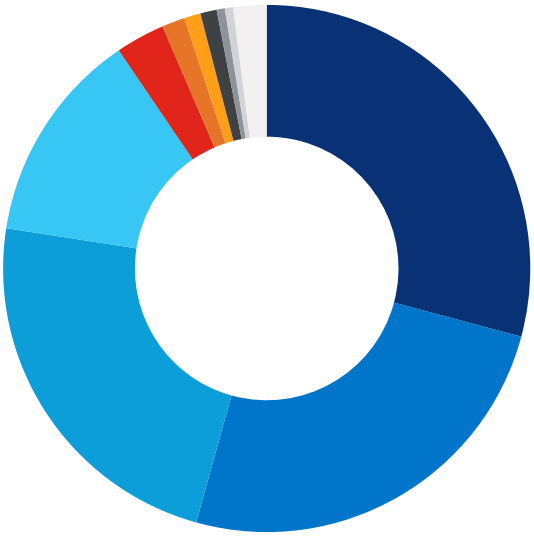
Ataques de vetor único/multivetor

	Q4	Q3	Mudança QaQ
Vetor único	65%	56%	▲16%
Multivetor	35%	44%	▼20%

No quarto trimestre, observamos principalmente os ataques de vetor único, que tiveram um aumento trimestral de 16%, saltando de 56% para 65% de todos os ataques. Este foi o percentual mais alto de ataques de vetor único durante todo o ano.

Mitigações de vetor único

Divisão por tipo de mitigação de vetor único



		QaQ
UDP	29%	▲60%
Pacotes inválidos	25%	▲89%
Filtragem estática	23%	▲14%
TCP SYN	13%	▼48%
Outros volumétricos	3%	▲6%
Amplificação de DNS	1.40%	▼87%
Fragmentação de IP	1.00%	▼81%
HTTP	1.00%	▲67%
TCP RST	0.50%	▲45%
SIP	0.50%	▲54%
Outros	2.03%	▲20%

Quando analisamos a divisão dos tipos de mitigação de vetor único, a amplificação baseada em UDP disparou para o topo, sendo responsável por 29% de todos os ataques e representando um aumento de 60%

de um trimestre a outro. Embora os ataques baseados em UDP sejam predominantes, tipicamente não representam nosso tipo de mitigação mais comum. Esses ataques visam consumir a largura de banda disponível e provaram ser bem poderosos, com capacidade para empunhar ataques que superam muito a magnitude dos bytes enviados inicialmente. Se quiser saber mais sobre ataques baseados em UDP, leia o blog do Black Lotus Labs: Rastreando Refletores UDP em busca de uma internet mais segura.

Os pacotes inválidos foram nossa segunda mais alta mitigação, responsáveis por 25% da atividade e com um aumento de 89% em relação ao terceiro trimestre. Os pacotes inválidos incluem o tráfego com campos de dados com falhas, assim como pacotes com fragmentos incompletos, duplicados ou muito grandes. Embora possam ser resultado de problemas relacionados à rede ou de um sequenciamento defeituoso de rede, os fragmentos de pacotes também são uma característica comum dos ataques de DDoS por amplificação de UDP.

A filtragem estática continua alta entre nossas mitigações de vetor único, em 23%, o que representa um aumento trimestral de 14% e alinha-se ao que observamos ao longo de 2021. As contramedidas de filtragem estática são normalmente realizadas em itens como porta e protocolo. Estas estatísticas também incluem bots conhecidas e refletores abusados, conforme descoberto pelo Black Lotus Labs, o que fornece a mitigação inicial contra os ataques.

Mitigações Multivetor

Principais combinações de tipos de mitigação multivetor

		QaQ
DNS, TCP SYN	12%	N.A.
Pacotes inválidos, UDP	6%	▼6%
UDP, Filtragem estática	5%	N.A.
Other Volumetric, UDP	4%	▲183%
Outros volumétricos, UDP, Filtragem estática	4%	▲123%
TCP SYN, filtragem estática	4%	N.A.
Pacotes inválidos, filtragem estática	3%	▲50%
Pacotes inválidos, UDP, filtragem estática	2%	N.A.
Amplificação de DNS, Fragmentação de IP, Pacotes Inválidos, UDP	2%	N.A.
TCP SYN, UDP	2%	N.A.

No quarto trimestre, DNS e TCP SYN combinados representaram a maioria das atividades relacionadas a mitigações multivetor (12%).

Observamos algumas novas combinações este trimestre. A maioria incluiu amplificação UDP, que repete o que já relatamos para as mitigações de vetor único.

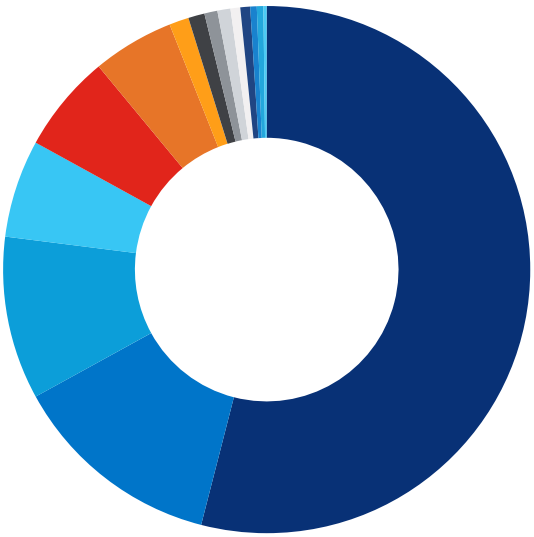
Mensagem #4

A cibersegurança é uma corrida armamentista.

Você sabe se está protegido contra as ameaças mais recentes? Os cibercriminosos podem mudar os parâmetros e vetores de ataques como resposta às novas defesas que enfrentam. Eles têm motivação financeira para continuar modificando seus ataques até derrubar as barreiras. Isto pode levar a uma corrida contínua entre a defesa e o ataque para manter-se em nível de igualdade. Nossa equipe do Black Lotus Labs trabalha todos os dias para defender a comunidade global de internet, e sua inteligência sobre ameaças alimenta quatro soluções de Mitigação DDoS e outras soluções de segurança gerenciada. A Lumen ajuda você a proteger-se contra os ataques diários a seus recursos críticos, com políticas de resposta automatizada.

Leia a ficha técnica

Os 500 maiores ataques por indústria



Telecomunicações	54%
Jogos	13%
Software & Tecnologia	10%
Hosting	6%
Governo	6%
Finanças	5%
Mídia & Entretenimento	1.2%
Varejo & Distribuição	1.0%
Manufatura	0.8%
Serviços corporativos	0.8%
Serviços públicos	0.8%
Educação	0.6%
Bancário	0.4%
Outros	0.4%
Serviços de saúde	0.2%

LUMEN TECHNOLOGIES

Dos 500 maiores ataques, 80% visaram estas cinco principais verticais (em ordem):

1. Telecomunicações
2. Software e Tecnologia
3. Varejo e Distribuição
4. Governo
5. Jogos

Tivemos algumas novas adições à nossa lista das principais verticais, incluindo Manufatura e Serviços de Saúde. A indústria de jogos teve o maior salto, duplicando os ataques que observamos no restante de 2021. Talvez isto se deva ao fato de que as empresas de jogos prepararam seus lançamentos de 2022 no final do segundo semestre de 2021, tornando-se alvos de maior valor durante este período. Abaixo, você pode encontrar mais detalhes sobre as principais indústrias visadas:

Telecomunicações

54%
dos 500 maiores ataques

812
ataques no total contra a vertical

Maior ataque de largura de banda:
317 Gbps

Período mais longo de duração de um ataque:
4 dias

57%
Ataques multivetor

Maior ataque baseado em pacotes:
60 Mpps

Jogos

13%
dos 500 maiores ataques

129
ataques no total contra a vertical

Maior ataque de largura de banda:
59 Gbps

Período mais longo de duração de um ataque:
5 dias

80%
Ataques multivetor

Maior ataque baseado em pacotes:
5 Mpps

Software & Tecnologia

10%
dos 500 maiores ataques

513
ataques no total contra a vertical

Maior ataque de largura de banda:
499 Gbps

Período mais longo de duração de um ataque:
3 dias

75%
Ataques de vetor único

Maior ataque baseado em pacotes:
71 Kpps

Hosting

6%
dos 500 maiores ataques

106
ataques no total contra a vertical

Maior ataque de largura de banda:
408 Gbps

Período mais longo de duração de um ataque:
5 dias

61%
Ataques de vetor único

Maior ataque baseado em pacotes:
487 Kpps

Governo

6%
dos 500 maiores ataques

754
ataques no total contra a vertical

Maior ataque de largura de banda:
26 Gbps

Período mais longo de duração de um ataque:
2 dias

57%
Ataques de vector único

Maior ataque baseado em pacotes:
8 Kpps

Mensagem #5

Estou seguro se minha indústria não estiver na lista acima?

A lista acima inclui os maiores ataques que experimentamos, embora praticamente todas as verticais e tipos de empresa possam ser atacados. Se você possui qualquer tipo de dado que interesse a alguém, sua organização pode ser um alvo. Se quiser aprender mais sobre as tendências de ataque em sua vertical, por favor contate um representante de vendas da Lumen para conversar.

Contate-nos

LUMEN TECHNOLOGIES

Principais mensagens

A mensagem mais importante que esperamos que leve após ler nossos Relatórios Trimestrais sobre DDoS é que a segurança não deve ser encarada como algo a se pensar depois; pelo contrário, ela deve ser um esforço consciente de cada parte da organização. Há vulnerabilidade toda vez que dados são movimentados, mas saber quais são as tendências e o que está acontecendo na esfera de cibersegurança pode ajudá-lo a identificar as vulnerabilidades.

Quando se trata de ataques de DDoS, é importante levar algumas coisas em consideração:

1. **Ninguém está imune:** Se você tem ativos valiosos na internet, os atores maliciosos terão sua organização como alvo.
2. **Ninguém pode se dar ao luxo de ser vítima:** Já que todos são um alvo potencial, seus resultados financeiros não deveriam ser uma dessas vítimas. Os custos de um ataque incluem a perda de receita, potenciais multas, danos à sua reputação e possivelmente, o resgate para impedir o ataque.
3. **Ninguém pode fazer isto sozinho:** Com as tendências de DDoS em constante evolução, as equipes internas de segurança não podem se manter atualizadas ou fazer mitigações por conta própria. O parceiro certo pode ajudar a reforçar sua estratégia de segurança atual.

Não tem certeza se está sofrendo um ataque de DDoS? Leia nosso blog e reconheça os sinais: Como saber se seu negócio está sofrendo um ataque de DDoS.

Se não possui um parceiro de mitigação de DDoS ou se estiver buscando um novo, aqui estão alguns critérios a serem considerados:

- Escala e capacidade para absorver ataques de grande magnitude no backbone como primeira camada de defesa.
- Presença global para uma latência reduzida ao enviar o tráfego para depuração.
- Flexibilidade e recursos avançados para proteger experiências digitais modernas.
- Visibilidade do cenário global de ameaças para reforçar as defesas.
- Automação baseada em inteligência sobre ameaças para bloquear o tráfego bot de DDoS antes que afete a rede.
- Modelos de suporte híbrido para proteger os ambientes digitais atuais. De colaboradores remotos a escritórios, e do data center até a nuvem.

Como a Lumen pode ajudá-lo hoje

Com uma das maiores implementações de mitigação de DDoS na indústria, +85 Tbps de capacidade de FlowSpec no backbone global, depurações inteligentes de próxima geração e contramedidas obtidas no Black Lotus Labs, a Lumen possui mitigação de DDoS em escala. O Serviço de Mitigação de DDoS da Lumen fornece opções de mitigação On-Demand (sob demanda) e Always-On (sempre ativas) com recursos avançados, como depuração inteligente para ajudar a reduzir a latência e melhorar o desempenho e uma taxa de serviço fixa mensal, independente da magnitude, duração ou frequência dos ataques.

Visite nosso website para ver qual solução de mitigação de DDoS melhor se encaixa com seus objetivos.

Saiba mais sobre Mitigação de DDoS da Lumen

Caso tenha interesse, leia nosso Relatório Trimestral de DDoS do terceiro trimestre

LUMEN TECHNOLOGIES

Metodologia

Os dados deste relatório abrangem o período de 1 de outubro de 2021 a 31 de dezembro de 2021. Os ataques depurados são definidos como:

- Incidentes sinalizados por alertas de alto nível mitigados pela plataforma, ou
- Períodos executando mitigações onde contramedidas individuais estão derrubando o tráfego, ou
- Eventos onde o tráfego derrubado excedeu o tráfego enviado.

Os vetores de ataque ou tipos de mitigação são identificados por contramedidas derrubando tráfego ou tipos de utilização inadequada sinalizados em nosso monitoramento baseado em fluxo.

Picos nos dados podem ser atenuados pelas médias das taxas no decorrer de vários acréscimos de tempo.

Os dados de nossos clientes 'sempre ativos' são agregados em acréscimos de minutos, horas ou dias, de acordo com a duração dos tempos de mitigação. Se uma mitigação durar o suficiente para que o tempo de resolução alcance a duração de um dia e se houver diversos dias consecutivos de ataque, então é contabilizada como um único período de ataque de vários dias.

Notas finais

* Fonte: Worldometer (www.worldometers.info)

0800-771-4747 | lumen.com | contato.br@lumen.com

LUMEN TECHNOLOGIES