RELATÓRIO

Relatório Trimestral de DDoS da Lumen

3º trimestre de 2021 (Q3 2021)

LUMEN TECHNOLOGIES

Introdução

Alguém mais está cansado? Ao olharmos a magnitude do cenário de cibersegurança, pode parecer que há um fluxo interminável de mudanças. Muito similar a Sísifo, empurrando a rocha montanha acima, é justamente quando você sente ter uma compreensão do que está acontecendo que um novo ataque acontece e você está novamente no fundo da colina. No entanto, em nossa humilde opinião, segurança é a parte mais vital de se trabalhar no âmbito de redes e TI. Este relatório foi elaborado por colaboradores da Lumen encantados com a cibersegurança, e com a proteção das organizações e criação de uma internet mais segura. E tudo começa com um foco implacável nos tipos e métodos de ataques.

Atualmente, você encontrará três tendências importantes afetando as organizações de todos os tipos e tamanhos:

1. Ataques de DDoS maiores e mais difundidos.
2. Vulnerabilidades de IoT e comando e controles (C2s) ampliando seu alcance.
3. Cibercriminosos com diversos tipos de expertise estão lançando ataques com mais frequência, em maiores volumes e com maior complexidade.

Embora possa parecer que está cada vez mais difícil empurrar a rocha para o topo da montanha, este relatório o ajudará a entender os ataques de reflexão por spoofing, porque as tendências globais de botnets de IoT são importantes, como os ataques estão mudando a cada trimestre e quem está sendo atingido, para que possa reforçar suas defesas.

Em nosso Relatório Trimestral de DDoS da Lumen para o 3º trimestre de 2021, examinamos a inteligência do Black Lotus Labs e dados da plataforma de Mitigação de DDoS da Lumen para desenvolver nossos achados, que reforçam e analisam essas tendências mais amplas.

Índice

LUMEN TECHNOLOGIES

Principais achados do 3º trimestre de 2021

Botnets de DDoS de IoT

- Houve uma redução de 26% no trimestre dos C2s únicos rastreados em busca de botnets generalizadas de DDoS Gafgyt e Mirai.
- A vida útil média de um C2 de Gafgyt foi de 38 dias, enquanto a vida útil média de um C2 de Mirai foi de 21 dias.
- A Lumen rastreou pouco mais de 2.100 C2s globalmente. Os países com a maior quantidade de C2s foram (em ordem): China, Estados Unidos e, empatados em terceiro lugar, Taiwan e Holanda.
- Observamos um aumento trimestral de 45% na quantidade de hosts de botnet de DDoS globalmente. Os países com a maior quantidade de botnets de DDoS foram (em ordem): Brasil, México e Egito.

Tendências de Ataques de DDoS

- O número de ataques mitigados por nós aumentou 35% em comparação ao segundo trimestre.
- O maior ataque de largura de banda depurado por nós no terceiro trimestre foi de 612 Gbps, o que representa um aumento de 49% trimestre a trimestre.
- O maior ataque baseado em taxa de transferência de pacotes depurado por nós no terceiro trimestre foi de 252 Mpps, o que representa um aumento de 91% trimestre a trimestre.
- O período mais longo de ataque de DDoS mitigado por nós para um cliente individual durou 14 dias.
- 46% das durações dos períodos de ataque foram inferiores a 10 minutos, quando analisamos nossos clientes de DDoS On-Demand.
- As mitigações multivetor representaram 44% de todas as mitigações de DDoS, sendo que a combinação mais comum foi: Amplificação de DNS, amplificação de TCP RST e TCP SYN-ACK e amplificação de UDP.
- TCP SYN foi o tipo de mitigação de vetor único mais comum, representando 25% das mitigações de DDoS.
- As três principais verticais que foram alvo dos 500 maiores ataques no terceiro trimestre foram: Telecomunicações, Software e Tecnologia, e Varejo.

Ataques de reflexão por Spoofing: Chamadas telefônicas de trote com grandes impactos

O que são?

Antes de analisarmos o cerne da questão, comecemos definindo o que é uma amplificação ou ataque de reflexão por falsificação de identidade. Um ataque de DDoS de reflexão por spoofing é aquele onde um ator finge ser outra entidade e inicia diversas comunicações para provocar uma avalanche de tráfego de retorno para a vítima desprevenida.

Digamos que um atacante quer atingir a Empresa X com um ataque de DDoS por reflexão. O atacante envia uma solicitação a um servidor de rede pedindo informações, fornecendo o endereço IP da Empresa X como remetente, ao invés de seu próprio. O servidor, acreditando estar sendo útil, envia a informação de volta à Empresa X. Bem, isto não parece ser tão ruim. Mas, o atacante deseja interromper as operações. Usando principalmente servidores UDP que foram mal configurados como refletores abertos, o atacante pode fazer com que a resposta à Empresa X seja exponencialmente maior do que a solicitação original. Além disto, o atacante, ainda utilizando o endereço IP falsificado, comanda que todos os hosts em sua botnet enviem a mesma solicitação a diversos servidores usando o mesmo IP de origem, levando a Empresa X a ficar rapidamente sobrecarregada.

Imagine que alguém se passe por você e ligue para um restaurante para pedir uma pizza. Além da pizza, diz: “me envie outra pizza a cada 15 minutos”. E para completar, faz com que todos os seus amigos liguem para o restaurante com o mesmo pedido. Você não tem ideia de onde vieram os pedidos e fica sobrecarregado com todas as pizzas chegando em sua casa. É um verdadeiro caos para organizar!

Como você pode impedir ataques de reflexão por spoofing?

O problema é que os ataques de reflexão por falsificação de identidade são muito difíceis de mitigar por conta própria e os alvos normalmente têm opções muito limitadas. Os cibercriminosos não estão buscando apenas causar caos; o crime traz lucro. Dada a dificuldade de rastrear ataques de reflexão por spoofing, eles são uma commodity em alta na dark web. Um hacker pode alugar sua infraestrutura, código de ataque, etc. a qualquer um que tenha interesse.

LUMEN TECHNOLOGIES

Então, como livrar a internet de atores maliciosos quando há um grupo de atacantes tão grande e tão bem escondido? A Lumen está se unindo a grupos de confiança da indústria para ajudar a rastrear esses ataques até suas origens. Devido ao tamanho de nossa rede e suas capacidades de caça às ameaças, analisamos NetFlow e usamos outras técnicas para encontrar a entrada do tráfego, quer seja um par interconectado à Lumen ou um cliente. Além de parcerias com pares da indústria, quando identificamos um cliente que tem refletores sendo visivelmente abusados, recomendamos que encerre o serviço ou realize mudanças de configuração para mitigar o potencial abuso.

Rastreamos o que não era possível rastrear, e agora? Esta é uma pergunta com a qual provedores como a Lumen vêm lidando. Não há uma solução única para detectar ou filtrar esses ataques, mas usamos opções como listas de controle de acesso, filtros de firewall, BGP FlowSpec e reenvio de rota inversa de unicast (unicast reverse-path-forwarding). Em última instância, a origem do tráfego falsificado – os outros provedores de rede – é responsável por depurar sua própria atividade.

Tudo é válido no amor, na guerra e na cibersegurança.

Quando uma organização fica sabendo que é a principal fonte de um ataque, espera-se que tome uma atitude. Mas, descobrimos que este nem sempre é o caso. Como exemplo, no terceiro trimestre, um grupo de confiança da indústria denunciou um ataque significativo que estava afetando uma grande empresa. O Centro de Operações de Segurança (SOC) da Lumen usou dados do Black Lotus Labs para encontrar a principal rede de entrada, um grande provedor de serviços de internet (ISP) da Rússia. Quando lhes informamos sobre o ataque, responderam que não havia qualquer evidência deste. Após muitas idas e vindas, o ISP continuou a postergar uma decisão. A atividade suspeita nos levou a crer que potencialmente estavam fazendo isto intencionalmente para proteger a receita de um cliente “black hat” ou, no mínimo, estavam sendo condescendentes.

Enviamos ao cliente ISP um aviso de violação de Política de Uso Aceitável (AUP); no entanto, nenhuma ação foi tomada e os ataques continuaram. A Lumen continuou tentando trabalhar com o ISP, mas finalmente, precisou implementar grandes listas de controle de acesso para filtrar o tráfego malicioso.

Apesar disto, os ataques continuaram, ainda que em menor escala. Finalmente, chegamos ao ponto de ruptura. De acordo com a AUP, tínhamos o direito de desconectá-los da rede, a menos que atuassem, então a Lumen por fim apresentou uma lista de controle de acesso mais rígida para mitigar a situação.

Ponto relevante #1

Então o que faço caso acredite que minha organização está sob um ataque de reflexão por spoofing?

Dada a natureza complexa e a grande escala desses ataques, você precisará trabalhar com um provedor de mitigação de DDoS bem estabelecido. Não se trata apenas de proteger sua organização do ato em si, mas também de rastrear as partes que são cúmplices e responsáveis. É responsabilidade de todo ISP fazer uma varredura em sua rede em busca de servidores de reflexão desprotegidos para garantir que estejam atualizados, para impedir o uso por DDoS. Limitar o acesso a estes servidores apenas a comunicações confiáveis também é uma melhor prática sólida de segurança. Por último, unir-se a seu ISP de upstream, caso o avisem sobre uma violação potencial de AUP, lhe ajudará a depurar as ameaças que possam ter sido relatadas pelas vítimas das atividades maliciosas. Estamos todos juntos nisto!

Botnets de DDoS de IoT

Família	C2 únicos rastreados	Vítimas de ataque único por família	Vida útil média de um C2 (em dias)
Gafgyt	349 ▼31% QaQ	Dados inconclusivos	38 ▲19% QaQ
Mirai	284 ▼19% QaQ	22,308 ▲43% QaQ	21 ▼25% QaQ

As duas famílias predominantes de IoT de DDoS rastreadas pelo Black Lotus Labs, Gafgyt e Mirai, continuam a causar estragos, com centenas de C2s dispersos ao redor do mundo. Os dados do terceiro trimestre estiveram alinhados aos achados nos trimestres anteriores. Entretanto, devido à natureza transitória da atividade das botnets, esperamos ver altas e baixas nestes números. Em geral, houve uma redução de 26% de trimestre a trimestre nos C2s únicos rastreados pela Lumen, com Gafgyt sendo responsável pela maior redução, caindo 31% desde o segundo trimestre.

Definimos as “vítimas” como o número de endereços IP únicos contra os quais observamos os C2s lançando ataques de DDoS. Embora continuemos a rastrear a família de Gafgyt, neste trimestre nossos dados sobre as vítimas foram inconclusivos. No entanto, as vítimas de Mirai aumentaram 43% em relação ao que informamos no segundo trimestre e agora equivalem praticamente a nossos achados do primeiro trimestre.

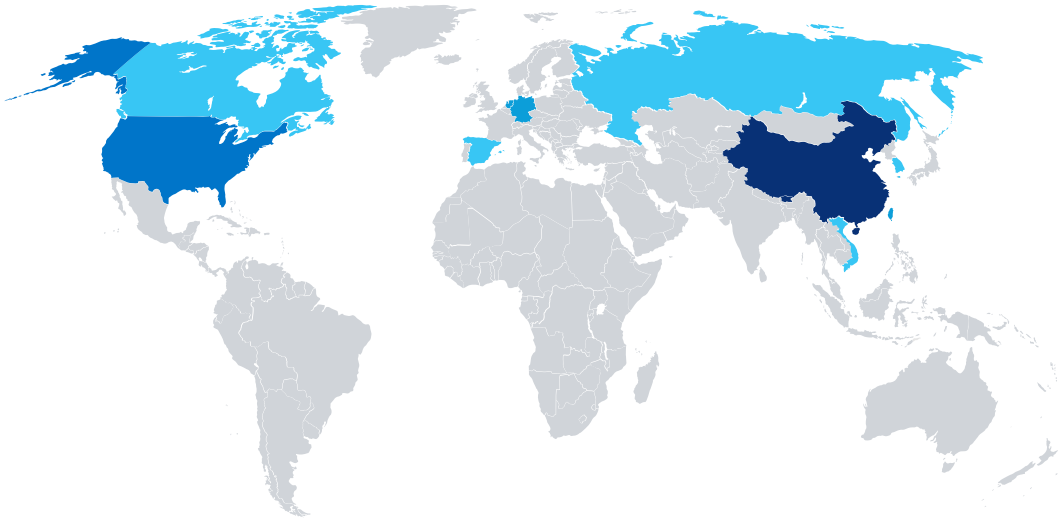
O objetivo dos atores maliciosos é cultivar uma infraestrutura confiável que possam usar para seus próprios ataques ou alugar a outros atores como serviço para uso temporário. Novamente, esperamos altas e baixas nestes números à medida que as botnets evoluam. Neste trimestre, o ciclo de vida médio para Gafgyt e Mirai se parece com o que registramos no segundo trimestre. O ciclo de vida médio de Gafgyt aumentou 19% e o de Mirai caiu 25% no terceiro trimestre.

Ameaças globais de DDoS de IoT rastreadas por país

Os seguintes mapas de calor específicos para DDoS representam os principais 10 países por C2s rastreados e hosts de botnets de DDoS. Os dados se baseiam 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.

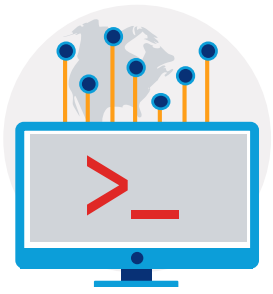
Uma anotação relativa aos mapas de calor: o fato de uma infraestrutura de C2 estar localizada em um país específico não significa que esta seja a verdadeira origem da infraestrutura. Os cibercriminosos frequentemente ocultam a origem de sua atividade ao aproveitar a infraestrutura de outros países.

Principais 10 países por C2

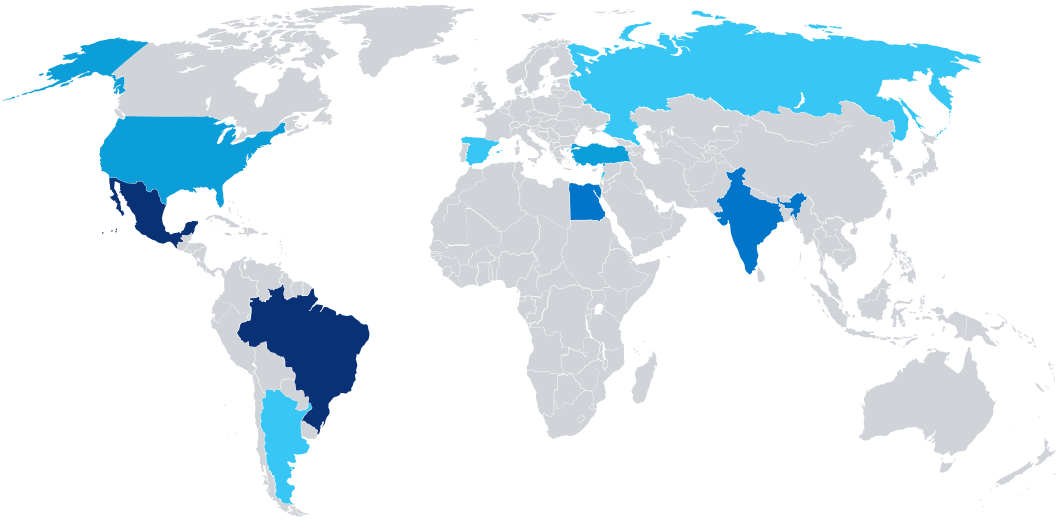


Nome do país	C2s	População*	Per Capita (100.000)
China	653	1.439.323.776	0.05
Estados Unidos	381	331.002.651	0.12
Taiwan	128	23.816.775	0.54
Holanda	128	17.134.872	0.75
Alemanha	115	83.783.942	0.14
Coreia do Sul	88	51.269.185	0.17
Vietnã	74	97.338.579	0.08
Canadá	56	37.742.154	0.15
Rússia	51	145.934.462	0.03
Espanha	39	46.754.778	0.08

A Lumen rastreou 2.102 C2s no mundo todo; o mapa de calor acima representa os países com o maior número de C2s. A região APAC teve um aumento de C2s neste trimestre, representando 4 dos 10 principais locais, empatando com a Europa. O país com mais C2s foi a China, com 653, ou 31% do total de C2s rastreados pelo Black Lotus Labs no terceiro trimestre. Os Estados Unidos caíram para a segunda posição, após estarem em primeiro lugar no segundo trimestre, e Taiwan, nova na lista, empatou em terceiro com a Holanda. Outros países novos que foram acrescentados aos 10 principais incluem a Coreia do Sul e o Vietnã, enquanto Reino Unido, Itália, Irã e França caíram abaixo dos 10 principais.

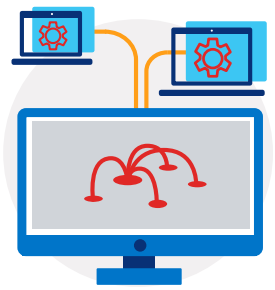


Principais 10 países por hosts de botnets de DDoS



Nome do país	C2s	População*	Per Capita (100.000)
Brasil	44.837	212.559.417	21,09
México	42.736	128.932.753	33,15
Egito	19.546	102.334.404	19,10
Índia	15.975	1.380.004.385	1,16
Estados Unidos	10.266	331.002.651	3,10
Turquia	10.171	84.339.067	12,06
Rússia	8.854	145.934.462	6,07
Espanha	8.044	46.754.778	17,20
Argentina	5.976	45.195.774	13,22
Líbano	5.467	6.825.445	80,10

O Black Lotus Labs observou um aumento de 45% nos hosts de botnet de DDoS de trimestre a trimestre, com mais de 217.000 – o mais alto visto durante o ano. Nossos três principais países registraram aumentos neste trimestre – Brasil: 35%, México: 78% e Egito: 129%. O Líbano, novo na lista dos principais 10, tem o maior número de bots per capita, chegando a cerca de 80, com o México em segundo, com 33. A Espanha também foi acrescentada à lista, enquanto a China e o Iraque caíram abaixo da linha dos principais 10.



Ponto relevante #2

O que estes dados globais significam?

Você pode estar se perguntando: “Por que é importante o que acontece no Brasil se eu só faço negócios nos Estados Unidos?” Estas duas famílias longevas de malware foram tão propagadas que é alto o risco de ser um alvo. Além disto, há mais de uma forma de ser afetado. Se sua rede não conta com as proteções adequadas, você poderia estar participando involuntariamente de ataques contra outras organizações. O simples fato de fazer parte de uma botnet pode gerar custos mais altos de largura de banda e problemas de desempenho em suas ferramentas e aplicações online. E uma vez que um hacker tem acesso a seu sistema, você fica exposto a uma variedade de ataques, desde o roubo de informações até crypto mining e ransomware.

O que é Black Lotus Labs?

Black Lotus Labs é uma equipe de inteligência sobre ameaças da Lumen. Consiste de um grupo de profissionais de segurança e cientistas de dados cuja missão é aproveitar a visibilidade global da rede da Lumen tanto para proteger sua empresa quanto para manter a internet limpa. O Black Lotus Labs utiliza a busca e análise de 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 as últimas descobertas e a derrubada de adversários realizadas pelo Black Lotus Labs, leia seu blog.

Leia agora

LUMEN TECHNOLOGIES

Ataques de DDoS em números

Ponto relevante #3

Não se trata de se, mas de quando...

A Lumen mitigou um total de 7.185 ataques de DDoS no terceiro trimestre. Isto representa um aumento de 35% em relação ao segundo trimestre e o maior registrado este ano. Estamos protegendo uma média de 80 ataques por dia, o que vem aumentando em um ritmo constante de 67 por dia no primeiro trimestre. Os atores maliciosos estão cada vez mais audaciosos e sofisticados e buscam causar mais disrupção do que nunca. Observamos níveis crescentes de complexidade na quantidade de métodos de ataque usados contra nossos clientes.

A melhor defesa é ter uma estratégia. Se você está buscando um serviço de mitigação de DDoS que possa acompanhar o cenário de ameaças em constante evolução, explore nossos serviços de mitigação de DDoS.

Saiba mais

A Lumen pode mitigar ataques de DDoS de grande escala em seu backbone global antes sequer do tráfego alcançar seu centro de depuração. Os tamanhos dos ataques neste relatório expressam os maiores ataques depurados pela infraestrutura global de depuração de DDoS da Lumen, e não os maiores ataques observados em trânsito ou depurados pela rede da Lumen.

LUMEN TECHNOLOGIES

Tamanho e duração do ataque

Maior ataque depurado

	Bits/s Perdido/s	Pacote/s Perdido/s
Q3	612 Gbps	252 Mpps
Q2	419 Gbps	132 Mpps
Mudança de QaQ	▲46%	▲91%

As duas principais métricas para ataques de DDoS volumétricos são:

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 pacotes: Estes ataques consomem recursos nos elementos da rede, como roteadores e outros dispositivos. Estes costumam ser maiores do que os ataques de largura de banda e são medidos em pacotes por segundo.

A Lumen observou aumentos significativos nos maiores ataques que depuramos. Os aumentos foram quase lineares nos maiores ataques de largura de banda durante o ano. No terceiro trimestre, houve um aumento de 46% no maior ataque, passando de 419 Gbps para 612 Gbps. Ao mesmo tempo, enxergamos um aumento exponencial nos maiores ataques de taxa de pacotes em 2021, passando de 132 Mpps no segundo trimestre para 252 Mpps neste trimestre.

Mas não é necessário ser atingido pelo maior ataque para que suas operações sejam interrompidas. O tamanho médio de ataque que vimos (1 Gbps para largura de banda, 307 Kpps para taxa de pacotes) poderia facilmente levar à inatividade empresas desprotegidas.

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

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

2. Mitigação Always-On: 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 84% dos ataques mitigados pela Lumen no terceiro trimestre. Saiba mais sobre as diferenças entre mitigações On-Demand e Always-On.

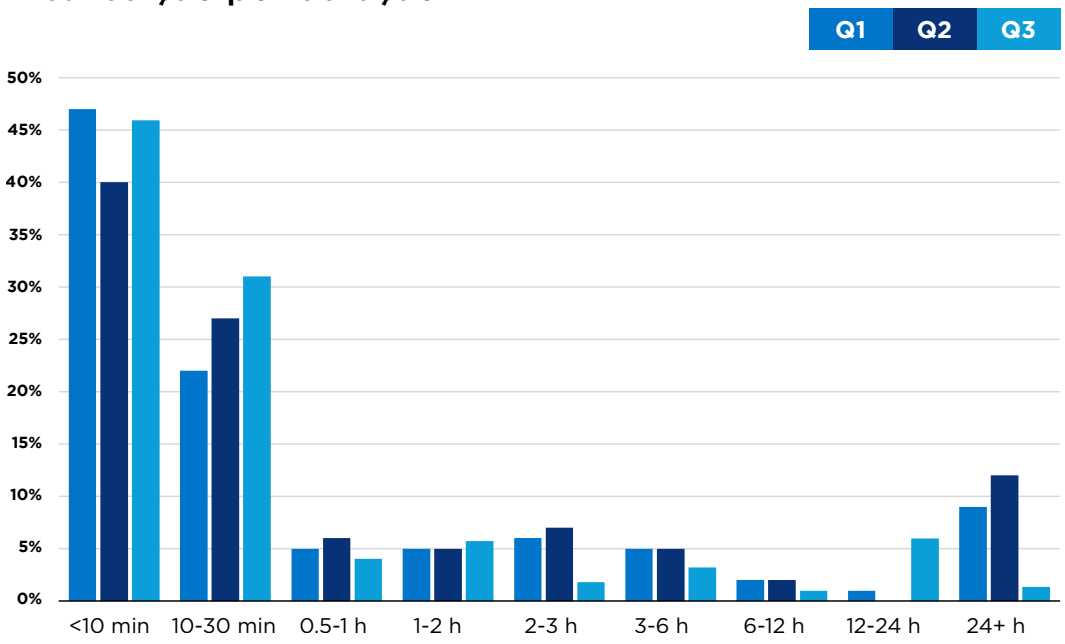
Assista ao vídeo

LUMEN TECHNOLOGIES

	Q3	Mudança QaQ
Duração mediana de um ataque	10m 56s	↓30%
Duração média de um ataque	2h 42m 22s	↓41%
Duração mais longa de um ataque	14 días	↑40%

Os dados de duração dos ataques sugerem que os ataques mais frequentes têm curta duração (<10 minutos). Registramos uma pequena redução na duração mediana de um ataque, de 15 minutos no segundo trimestre para pouco menos de 11 minutos no terceiro trimestre. Uma das possíveis causas desta tendência de queda poderia ser a dependência nos DDoS de resgate, onde os atores maliciosos implementam um ataque menor para provar que estão determinados em sua intenção de lançar ataques maiores. A duração mais longa em nosso período de ataque aumentou para 14 dias, o mesmo nível relatado no primeiro trimestre.

Distribuição por duração

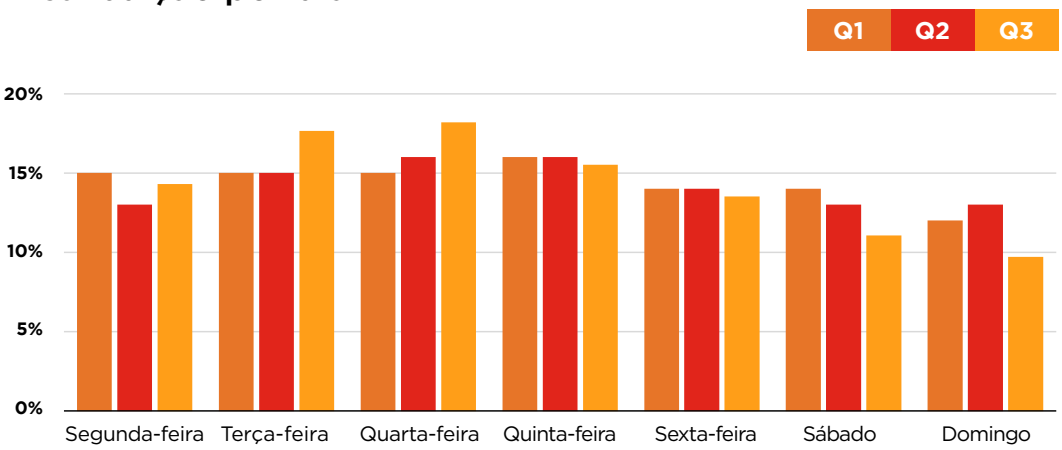


LUMEN TECHNOLOGIES

Ao analisarmos a duração de um período de ataque, 46% dos ataques levaram menos que 10 minutos, o que corresponde a nossos achados do primeiro trimestre. Também vimos ataques na faixa de 10-30 minutos em seu nível mais alto este ano, representando 31% da atividade. A maior queda foi percebida nos ataques com mais de 24 horas, passando de 12% dos ataques no segundo trimestre a cerca de 1% no terceiro trimestre. Uma possível explicação seria a mudança típica de táticas que ocorre durante o ano, com os atores focando atualmente em ataques mais frequentes e rápidos.

Quando comparamos a duração e a magnitude de um ataque, observamos que os ataques mais longos também tendem a ser maiores em escala. Por exemplo, o maior ataque (612 Gbps em seu pico) teve um período de duração de 48 horas.

Distribuição por dia



Os ataques por dia da semana estiveram principalmente alinhados ao que observamos nos primeiros dois trimestres de 2021, exceto às terças, quartas e domingos. Afetadas pelos ataques percebidos no âmbito de varejo no início do trimestre, terças e quartas-feiras tiveram 18% de atividades de ataques, cada uma. Enquanto isto, o domingo caiu para o dia menos provável para um ataque, passando de 13% para 10% dos ataques ocorrendo neste dia.

No terceiro trimestre, os dias em que vimos mais ataques foram 6 de julho, quando a Lumen mitigou 240 ataques, seguido de 7 de julho, com 206 ataques mitigados.

LUMEN TECHNOLOGIES

Ponto relevante #4

10 minutos não parece ser tão ruim, até que você veja o quando isto representa em cifrões

Ao olhar estes dados, você pode pensar: “Bom, não terei que enfrentar o ataque mais longo, quais são as chances disto?” Embora isto possa ser verdade, você pode nem precisar resistir ao ataque maior ou mais longo; ataques curtos são tão efetivos quanto estes para causar disrupção à sua organização. Digamos que você tem um cliente que quer acessar seu aplicativo e ele não está disponível porque você não está protegido e possui um ataque de DDoS ativo. Quanto tempo esta pessoa ficará tentando acessar seu aplicativo antes de desistir e ir para outro lugar?

Agora, digamos que você está inativo por mais de duas horas (nossa média). Quanta receita perdeu? O custo médio de inatividade de TI está por volta de centenas de milhares de dólares. Isto sequer considera que os clientes podem decidir ir para outro lugar para obter os produtos ou serviços que você oferece, ou a perda de reputação da marca que ocorrerá. Implementar uma proteção sólida para DDoS ajudará a evitar a perda de receita e produtividade.

Tipos de mitigação de ataque

Ataques únicos/multivetor

	Q3	Q2	Mudança QaQ
Vetor único	56%	62%	▼9%
Multivetor	44%	38%	▲40%

LUMEN TECHNOLOGIES

Com o número geral de ataques aumentando neste trimestre, vimos um aumento tanto nos ataques multivetor quanto nos de vetor único. No entanto, os ataques multivetor tiveram um aumento neste trimestre, representando 44% de todas as mitigações de ataques. Este é o número mais alto que vimos até o momento em 2021, mostrando que os atores maliciosos estão dependendo cada vez mais de vetores de ataque complexos quando focam as organizações.

Este é o número mais alto que vimos até o momento em 2021, mostrando que os atores maliciosos estão dependendo cada vez mais de vetores de ataque complexos quando focam as organizações.

Mitigações de Vetor Único

Divisão por Tipo de Mitigação de Vetor Único

		QaQ
TCP SYN	25%	↑66%
Filtragem Estática	21%	↓26%
UDP	18%	↓17%
Pacotes Inválidos	13%	↓21%
DNS	11%	↑34%
Fragmentação IP	5%	↑28%
Outros volumétricos	3%	↓37%
ICMP	2%	↑56
HTTP	1%	↓43
Amplificação de DNS	0.64%	N.A.
Outros	1.69%	N.A.

À medida que surgem novos métodos de ataque, esperamos uma flutuação nestes resultados. Mas, ainda que haja uma ida e vinda dos novos vetores de ataque, continua-se a confiar nos métodos antigos e comprovados. Por exemplo, TCP SYN foi o tipo de mitigação de vetor único mais comum que vimos no terceiro trimestre, responsável por 25% da atividade. Isto foi um aumento de 66% em relação aos achados do segundo trimestre. Contramedidas para a filtragem estática e amplificação de UDP caíram das posições um e dois para dois e três, respectivamente.

As contramedidas de filtragem estática são tipicamente feitas em itens como porta e protocolo. Esta contramedida é também onde as mitigações de nosso feed de ameaças do Black Lotus Labs são capturadas. Ela promove uma mitigação inicial contra os ataques e representou 21% dos ataques de vetor único no terceiro trimestre.

Os ataques de amplificação baseada em UDP continuam a prevalecer,

ficando em nossa posição número três, com 18% da atividade. Estes ataques visam abusar dos protocolos da camada de aplicações e têm provado ser bem poderosos, com capacidade de realizar ataques diversas vezes maiores que os bytes enviados inicialmente. Se você está buscando aprender mais sobre ataques baseados em UDP, leia nosso blog: Rastreando Refletores UDP em busca de uma Internet mais Segura.

Mitigações Multivetor

Principais Combinações de Tipos de Mitigação Multivetor

		QaQ
Amplificação de DNS, TCP RST, TCP SYN/ Amplificação de ACK, UDP	28%	N.A.
DNS, TCP SYN	12%	▲23%
DNS, TCP SYN Filtragem Estática	4%	▲35%
DNS, filtragem estática	3%	▲14%
UDP, Filtragem estática	3%	▼43%
TCP SYN, Filtragem estática	3%	▼36%
UDP, Filtragem estática	2%	▼62%
Amplificação de DNS, Fragmentação IP	2%	▼10%
Outros ataques volumétricos, UDP	2%	N.A.

Pela primeira vez este ano, os atores maliciosos aproveitaram uma variedade muito maior de vetores de ataque ao lançar ataques multivetor. Nos trimestres anteriores, a Lumen observou o máximo de três vetores de ataque simultâneos e neste trimestre observou quatro: 28% das mitigações multivetor foram uma combinação de amplificação de DNS, amplificação TCP RST, TCP SYN-ACK e outras amplificações de UDP.

A segunda combinação mais comum foi DNS e TCP SYN, que representou 12% das mitigações multivetor, um aumento de 10% no segundo trimestre.

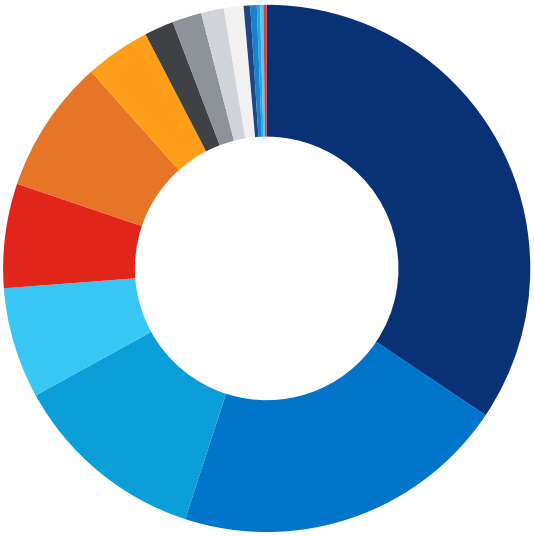
Ponto relevante #5

Não faça você mesmo sua proteção de DDoS

Se você fosse classificar suas práticas de cibersegurança, receberia um A+? Pouquíssimas organizações o receberiam e muito poucas podem bancar investir em uma infraestrutura de mitigação de grande escala ou contratar o talento interno necessário para se manterem atualizadas em relação à barreira que o cenário de DDoS representa. À medida que mais organizações buscam proteger sua infraestrutura, os atores maliciosos estão se tornando mais astutos. Eles farão todo o possível para acessar seus ativos e aplicações voltados à web. Os cibercriminosos podem mudar os parâmetros e vetores de um ataque como resposta às defesas que encontrarem ao tentar lançar um ataque. Eles continuarão a modificar o ataque para que fique cada vez mais difícil mitigá-lo. Considere uma solução de mitigação de DDoS que tenha a automação incorporada à sua funcionalidade central. Aprenda sobre Lumen Rapid Threat Defense.

Veja a folha de dados

500 maiores ataques por indústria



Telecomunicações	34%
Software & Tecnologia	21%
Varejo & Distribuição	12%
Governo	7%
Jogos	6%
Hosting	8%
Mídia & Entretenimento	4%
Finanças	2%
Transportes	2%
Bancária	1%
Educação	1%
Outros	0.4%
Serviços corporativos	0.4%
Farmacêutica	0.2%
Consultoria	0.2%
Serviços públicos	0.2%

LUMEN TECHNOLOGIES

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

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

Tivemos alguns novos participantes em nossa lista das principais verticais, incluindo: Varejo e Distribuição, Farmacêutica e Consultoria. Varejo e Distribuição teve o maior salto no terceiro trimestre, não representando nenhum de nossos 500 maiores ataques no segundo trimestre, e passando para 12% neste trimestre. Abaixo, você poderá encontrar mais detalhes sobre as principais indústrias que são alvo.

Telecomunicações

34%
dos 500 maiores ataques

956
total de ataques contra a vertical

Maior ataque de largura de banda:
612 Gbps

Duração mais longa de período de ataque:
6 dias

52%
ataques multivetor

Maior ataque baseado em pacotes:
252 Mpps

LUMEN TECHNOLOGIES

Software e Tecnologia

21%
dos 500 maiores ataques

515
total de ataques contra a vertical

Maior ataque de largura de banda:
405 Gbps

Duração mais longa de período de ataque:
5 dias

60%
ataques de vetor único

Maior ataque baseado em pacotes:
33 Mpps

Varejo e Distribuição

12%
dos 500 maiores ataques

425
total de ataques contra a vertical

Maior ataque de largura de banda:
116 Gbps

Duração mais longa de período de ataque:
3 dias

60%
ataques de vetor único

Maior ataque baseado em pacotes:
11 Mpps

Governo

7%
dos 500 maiores ataques

2.565
total de ataques contra a vertical

Maior ataque de largura de banda:
44 Gbps

Duração mais longa de período de ataque:
4 dias

62%
ataques de vetor único

Maior ataque baseado em pacotes:
8 Mpps

Jogos

6%
dos 500 maiores ataques

215
total de ataques contra a vertical

Maior ataque de largura de banda:
6 Gbps

Duração mais longa de período de ataque:
3 dias

53%
Ataques de vector único

Maior ataque baseado em pacotes:
886 Kpps

Ponto relevante #6

Se não vejo minha indústria na lista, não serei atacado, certo?

A lista acima inclui os maiores ataques experimentados por nós, mas quase toda vertical e tipo de empresa são atacadas. Faça esta pergunta a você mesmo: tenho informação que alguém poderia querer? E a resposta para todas as organizações é sim. Você tem informações pessoais sobre clientes e colaboradores. Qualquer forma de dados pode ser valiosa para hackers e os ataques de DDoS são normalmente usados como distração para uma violação de dados maior ou como uma forma de extorquir pagamento. 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

Principais pontos relevantes

Atualmente, os ataques de DDoS ocorrem desenfreadamente e não parece haver uma desaceleração na frequência. No mínimo, estão evoluindo e mudando, de forma que estão se tornando mais complexos, maiores e mais longos. Ao longo do relatório, mencionamos alguns pontos relevantes para nossos leitores:

1. Ataques de reflexão por falsificação de identidade (spoofing) requerem a ajuda de um provedor de mitigação de DDoS porque podem crescer exponencialmente e exigir táticas de mitigação extremas.
2. As tendências globais de ataque não são “achados distantes” que não se aplicam às empresas. Na verdade, você pode facilmente ser alvo de C2s ou fazer parte involuntariamente de uma botnet, atacando outras organizações.
3. Com cada vez mais ataques ocorrendo a cada dia, não se trata mais de “se” você será atacado, e sim de quando. E não importa se você não for atingido com o ataque mais longo ou de maior magnitude; qualquer ataque ainda é capaz de interromper as operações.

4. Cada 10 minutos de inatividade pode custar mais do que você pode imaginar.

5. Vimos alguns dos ataques mais complexos ocorrendo no terceiro trimestre; realizar sua estratégia de DDoS por conta própria é um erro.

6. Os dados são a moeda de hoje em dia e todos são alvo, não importa qual a indústria.

O cenário de ameaças pode parecer opressivo. É preciso estar atento a diversas coisas e o preço a pagar pode ser incrivelmente alto. Soluções de mitigação de DDoS podem aliviar um pouco a pressão nos departamentos de TI. Ao observarmos o resultado entre os custos de mitigação de DDoS e os custos de um ataque em termos de receita, produtividade, reputação e experiência do cliente, a escolha é fácil.

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

- Escala e capacidade para absorver grandes ataques no backbone como primeira camada de defesa.
- Infraestrutura global para uma latência reduzida ao rotear 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 de afetar a rede.
- Modelos de suporte híbridos 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, mais de 85 Tbps de capacidade de FlowSpec no backbone global, depurações inteligentes de próxima geração e contramedidas derivadas do 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 e Always-On com características avançadas, como depuração inteligente para ajudar a reduzir a latência e melhorar o desempenho, e uma tarifa de serviço mensal fixa, independentemente 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

Se estiver interessado, leia nosso Relatório trimestral de DDoS do 2º trimestre.

Metodologia

Os dados neste relatório são do período de 1 de julho de 2021 a 30 de setembro 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 superou 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.

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

Os dados de nossos clientes 'Always-On' são agregados em acréscimos de minutos, horas ou dias, de acordo com a duração de tempo de mitigação. Se uma mitigação for executada durante tempo suficiente para que o tempo de resolução alcance a duração de um dia e se houver diversos dias de ataque em sequência, ela é então contabilizada como um ataque único com período de vários dias.

Notas finais

* Fonte: Worldometer (www.worldometers.info)

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

LUMEN TECHNOLOGIES