RELATÓRIO

Relatório trimestral de DDoS da Lumen

1º trimestre de 2022

LUMEN TECHNOLOGIES

Introdução

Esperamos que tenha tido um excelente início de 2022. O início de um novo ano é sempre emocionante e cheio de possibilidades: você conta com novos orçamentos, novos planos, novas estratégias, etc. Pode se dizer o mesmo dos atores maliciosos. Enquanto os cibercriminosos operam cada vez mais como organizações legítimas, estão atravessando as mesmas coisas que nós, pensando em quais projetos ambiciosos querem adotar este ano, onde reinvestirão sua receita de 2021 e como podem ampliar sua presença. Enquanto você pensa no que precisa conquistar este ano, é importante ter as últimas tendências em segurança a seu alcance, para ajudá-lo a determinar as áreas de foco.

Em nosso Relatório Trimestral de DDoS da Lumen para o primeiro trimestre de 2022 você aprenderá sobre:

- A atividade de DDoS dirigida à Ucrânia e o que você pode fazer para proteger a sua organização
- A magnitude, duração e frequência dos ataques
- Os vetores dos ataques de DDoS
- As indústrias que foram alvo

Para elaborar este relatório, examinamos os dados da plataforma de Mitigação de DDoS da Lumen, que reforçaram e se aprofundaram nas tendências mais abrangentes.

LUMEN
TECHNOLOGIES

Índice:

Principais achados do 1º trimestre de 2022 4

O conflito na Ucrânia afetará sua organização? 5

Ataques de DDoS em números 7

Tipos de mitigação de ataques 13

Os 500 maiores ataques por indústria 16

Principais Conclusões 19

LUMEN TECHNOLOGIES

Principais achados do 1º trimestre de 2022

- A quantidade de ataques que mitigamos aumentou 66% em comparação ao quarto trimestre de 2021 e 32% anualmente.
- O maior ataque de largura de banda que depuramos no primeiro trimestre foi de 775Gbps, o maior ataque já mitigado até hoje.
- O maior ataque baseado em taxa de pacotes depurado no primeiro trimestre foi de 127 Mpps, o que representa mais que o dobro do que mitigamos no quarto trimestre.
- O período de ataque de DDoS mais longo que mitigamos para um cliente individual durou 5 dias.
- 72% das durações dos períodos de ataque foram de menos de 30 minutos, ao analisarmos nossos clientes de DDoS On-Demand.
- O dia mais frequente para os ataques foi quarta-feira.
- As mitigações multivetor representaram 38% de todas as mitigações de DDoS, sendo que as combinações mais comuns utilizaram as contramedidas DNS e TCP SYN.
- A inundação de TCP SYN foi o tipo de mitigação de vetor único mais comum, representando 32% das mitigações de DDoS.
- As três principais verticais que foram alvo dos 500 maiores ataques foram: Telecomunicações, Jogos, e Software e Tecnologia.

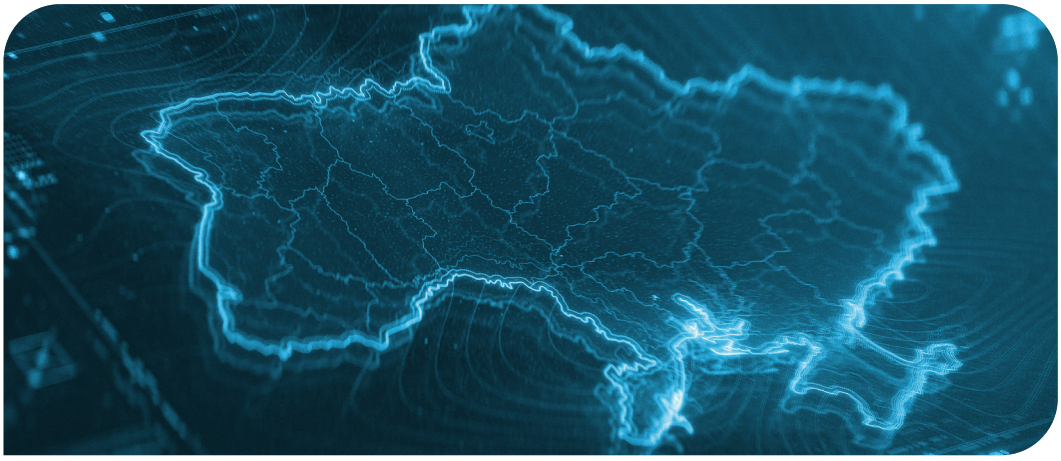
O conflito na Ucrânia afetará sua organização?

Não podíamos compilar este relatório sem focar em um dos maiores eventos ocorrendo no mundo atualmente: a invasão da Ucrânia pela Rússia. Embora este evento trágico tenha causado um enorme impacto no povo da Ucrânia, falaremos especificamente sobre as implicações deste contínuo conflito na segurança cibernética.

De forma coordenada com os ataques na Ucrânia, observamos contínuos ataques cibernéticos provenientes de países vizinhos, de malware wiper a ataques sustentados de DDoS à infraestrutura crítica ucraniana. O Serviço Estadual de Proteção das Comunicações e Informações Especiais da Ucrânia relatou que os "hackers russos continuam atacando ininterruptamente os recursos de informação ucranianos". Esses ataques de DDoS não ficaram sem resposta – de acordo com a Wired, a Rússia está sendo atingida por ataques similares de grupos de "hacktivistas" e, em alguns casos, de hackers contratados pelos ucranianos.

Com tantos desenvolvimentos, a divisão de inteligência sobre ameaças da Lumen, Black Lotus Labs®, está monitorando a atividade de ameaças russas tanto na região quanto ao redor do mundo. O Black Lotus Labs está trabalhando com parceiros da indústria, incluindo a Colaboração Conjunta de Defesa Cibernética (JCDC, na sigla em inglês), enquanto continuamos monitorando a evolução da situação na Ucrânia, seja analisando o tráfego de DDoS visível no backbone da Lumen ou identificando infraestrutura de C2 sendo utilizada para ordenar ataques. Saiba mais sobre o preparo da Lumen para enfrentar eventos globais.

Embora a atividade de DDoS esteja atualmente limitada à região, isto não significa que continuará assim. Se está preocupado com a proteção de sua organização, a Lumen sugere seguir os conselhos fornecidos pela Agência de cibersegurança e segurança da informação (CISA):



LUMEN TECHNOLOGIES

1. Reduza a probabilidade de uma intrusão cibernética prejudicial

a. Certifique-se de que todos os acessos remotos à rede de sua organização e os acessos privilegiados ou administrativos exijam a autenticação multifator.
b. Assegure-se de que o software esteja atualizado.
c. Confirme que o pessoal de TI de sua organização desabilitou todas as portas e protocolos não essenciais.
d. Se sua organização usa serviços na nuvem, assegure-se de que estes tenham sido analisados e implemente controles sólidos.

2. Adote medidas para detectar rapidamente uma intrusão potencial

a. Garanta que sua equipe esteja focada em identificar e avaliar rapidamente qualquer comportamento inesperado ou incomum da rede.
b. Assegure-se que toda a rede de sua organização esteja protegida por software antivirus/anti-malware atualizado.
c. Se você trabalha com organizações ucranianas ou russas, tome muito cuidado para monitorar, inspecionar e isolar o tráfego destas organizações.

3. Assegure-se de que sua organização esteja preparada para responder caso um ataque ocorra

a. Designe uma equipe de resposta a crises com funções e responsabilidades nos departamentos de tecnologia, comunicações, jurídico e continuidade de negócios.
b. Conduza um exercício rápido para garantir que todos conhecem suas funções durante um incidente ativo.

4. Maximize a resiliência de sua organização ao enfrentar um incidente cibernético

a. Teste seus procedimentos de backup para garantir que seus dados críticos possam ser restaurados rapidamente.
b. Se você usa sistemas de controle industrial ou tecnologia operacional, realize um teste dos controles manuais para que as funções críticas permaneçam operacionais.

LUMEN TECHNOLOGIES

Tudo mencionado acima pode parecer incrivelmente assustador. Entretanto, não precisa ser assim. A Lumen pode ajudá-lo a encontrar vulnerabilidades em sua organização, avaliando suas estruturas de segurança e fornecendo à sua equipe recomendações para obter a postura de segurança desejada.

Saiba mais

O que é Black Lotus Labs?

Black Lotus Labs é a equipe de inteligência sobre ameaças da Lumen. É um grupo de profissionais de segurança e cientistas de dados cuja missão consiste em aproveitar a visibilidade global da rede da Lumen tanto para ajudá-lo a proteger seu negócio e a 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 tiver interesse em saber mais sobre a última pesquisa e as capacidades avançadas de rastreamento de atores e crimeware do Black Lotus Labs, leia seu blog.

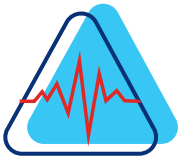
Leia agora

Ataques de DDoS em números

Após um quarto trimestre relativamente tranquilo, 2022 começou com um estouro. A Lumen mitigou 6.162 ataques de DDoS no primeiro trimestre, o que representa um aumento de 66% em relação ao quarto trimestre e de 32% em relação ao primeiro trimestre de 2021. Na média, a Lumen mitigou 70 ataques diariamente, um aumento de 63% de trimestre a trimestre. Os dias com mais ataques registrados foram 30 de março (150 ataques), 24 de janeiro (139 ataques) e empatados em terceiro lugar, 17 de março e 27 de março (125 ataques).

Magnitude e duração de ataques

Maior ataque depurado



	Bits/s perdidos	Pacote/s perdidos
Q1 2022	775 Gbps	127 Mpps
Q4 2021	499 Gbps	60 Mpps
Mudança Q a Q	▲55%	▲112%

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 pacotes:** Estes ataques consomem recursos nos elementos da rede, como roteadores e outros aparelhos, assim como de servidores. Estes são medidos em pacotes por segundo, com taxas normalmente maiores do que as dos ataques de largura de banda.

Ataques de largura de banda

Mitigamos nosso maior ataque de largura de banda desde que iniciamos nosso relatório: 775 Gbps. Isto representa um aumento trimestral de 55% e um aumento anual de 189%.

O tamanho médio de um ataque mitigado foi de 2 Gbps, que é o que observamos nos relatórios anteriores da Lumen.

Ataques por taxa de pacotes

O maior ataque por taxa de pacotes mais do que duplicou em comparação ao 4º trimestre, passando de 60 Mpps para 127 Mpps.

Há um salto monumental na magnitude do maior ataque quando observamos as comparações anuais: no 1º trimestre de 2021, o maior ataque foi de 26 Mpps, mostrando um aumento anual superior a 380%.

A magnitude média de um ataque foi de 477 Kpps, representando uma pequena redução em comparação ao 4º trimestre de 2021, mas ainda assim maior do que o restante dos dados apresentados em 2021.

LUMEN TECHNOLOGIES

Conclusão #1

Por que devo me preocupar com a magnitude dos ataques?

Com a magnitude dos ataques seguindo uma tendência de aumento, é óbvio que os cibercriminosos estão escalando para se igualarem às medidas de defesa e sobrecarregar os alvos com infraestruturas de botnets de enormes proporções.

Certamente, embora seja possível que você não seja atingido pelo maior ataque de DDoS da história, há uma grande chance de que seja atingido por algum ataque de DDoS, se é que ainda não foi. As organizações que não contam com serviços de mitigação de DDoS podem facilmente ficar fora do ar devido a um ataque de 1 Gbps. Ter uma solução de mitigação de DDoS não evitará que você seja atacado; no entanto, ajudará a garantir que sua organização possa continuar com suas operações normais durante um ataque ativo.

Quanto tempo estão durando os ataques?

Os índices de duração dos ataques são afetados pelo modelo de mitigação do cliente. Existem duas opções.

1. 1. Mitigação On- Demand (sob-demanda): O tráfego é sempre monitorado, mas é depurado apenas 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, responsáveis por 69% dos ataques mitigados pela Lumen no quarto trimestre. Saiba mais sobre as diferenças entre mitigações On-Demand e Always-On.

Assista o vídeo

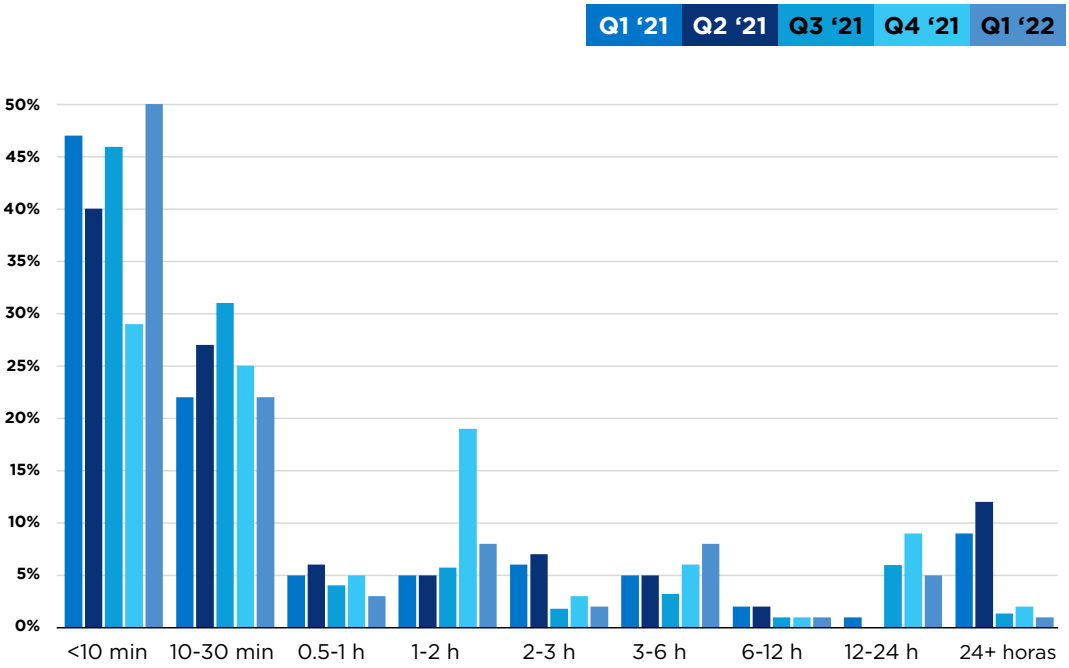
LUMEN TECHNOLOGIES

	Q1	Mudança Q a Q
Duração mediana de ataques	10m 0s	⬇67%
Duração média de ataques	2h 37m 55s	⬇44%
Maior duração de um ataque	5 dias	0%

Houve reduções tanto nas durações médias quanto nas medianas dos períodos de ataque, comparados ao 4º trimestre de 2021; no entanto, durante tal trimestre, experimentamos ataques mais longos do que nos trimestres anteriores. Os dados para o 1º trimestre estão em linha com o que foi mitigado durante o restante de 2021. A duração de um período mediano de ataque foi de 10 minutos, o que representa uma redução trimestral de 67% em relação ao 4º trimestre (duração mediana de ataque de 30 minutos) e uma redução anual de 33% em relação ao 1º trimestre de 2021 (duração mediana de ataque de 15 minutos).

A duração mais longa de um período de ataque foi de 5 dias e se manteve estável de trimestre a trimestre. Representa uma redução do que foi observado no 3º trimestre de 2021, que registrou os períodos mais longos de ataques, com mais de 10 dias. Isto não significa que podemos relaxar; os cibercriminosos não desistirão. Como qualquer negócio, as organizações cibercriminosas têm o objetivo de realizar eficiências e estão executando ataques maiores e mais eficazes, mais rapidamente. À medida que 2022 avança, podemos esperar flutuações nestes dados, baseadas nas novas táticas dos atacantes. É importante notar que a duração de um período de ataque não indica apenas a duração de um ataque único - uma organização pode sofrer uma enxurrada de ataques durante um período de duração.

Distribuição por duração

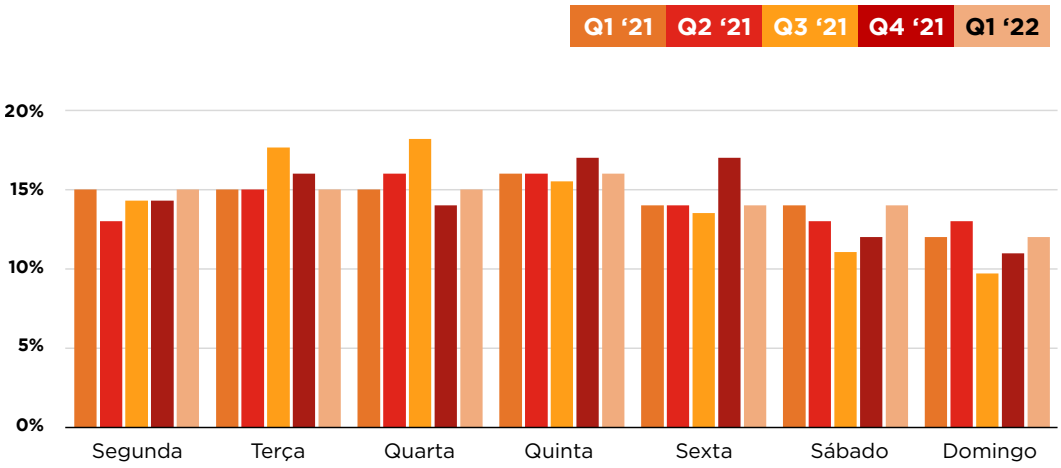


Metade de todos os ataques aos clientes de mitigação On-Demand da Lumen duraram menos do que 10 minutos, que é o percentual mais alto de atividade que observamos, comparado a relatórios anteriores. Isto pode significar que estes atores maliciosos estão focados em ataques rápidos e investigando os ataques para testar as defesas de uma organização antes de implementar ataques de maior escala.

A segunda duração de período de ataque mais popular foi de 10-30 minutos, representando 22% da atividade. Houve também um ligeiro aumento nos ataques com duração de três a seis horas, passando de 6% de atividade no 4º trimestre para 8% de atividade no 1º trimestre de 2022. Observamos uma queda na dependência de períodos de ataque com maior duração. Os ataques de mais de 24 horas perceberam uma redução anual de 85%.

LUMEN TECHNOLOGIES

Distribuição por dia

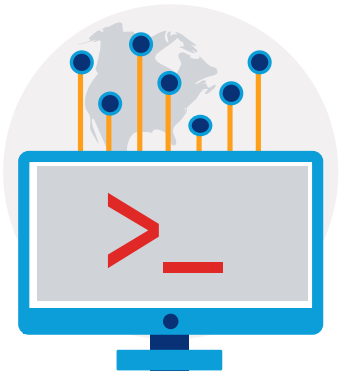


Os ataques ocorreram regularmente durante a semana; no entanto, houve uma probabilidade um pouco maior de ocorrerem de segunda a quinta (~15% dos ataques por dia) do que de sexta a domingo (~13% por dia). Isto está em linha com nossa observação de que os cibercriminosos operam de forma similar às empresas, o que inclui ter semanas de trabalhos dedicadas.

Conclusão #2

Por que devo me importar com a duração dos ataques?

Se atualmente você opera como uma organização digital, você é extremamente dependente de seu website, suas aplicações, ferramentas e sua capacidade de computação, de forma geral. Algum destes elementos é capaz de enfrentar um tempo de inatividade? Seus colaboradores poderão trabalhar? Seus clientes poderão interagir com você? O custo de um ataque não significa apenas que seus ativos de internet não funcionarão; o tempo de inatividade enfrentado pode ter ramificações de longo alcance em sua receita, incluindo multas e golpes à sua reputação. Nos últimos anos, o custo médio de um ataque de DDoS pode estar na casa das centenas de milhares de dólares



LUMEN TECHNOLOGIES

Tipos de mitigação de ataques

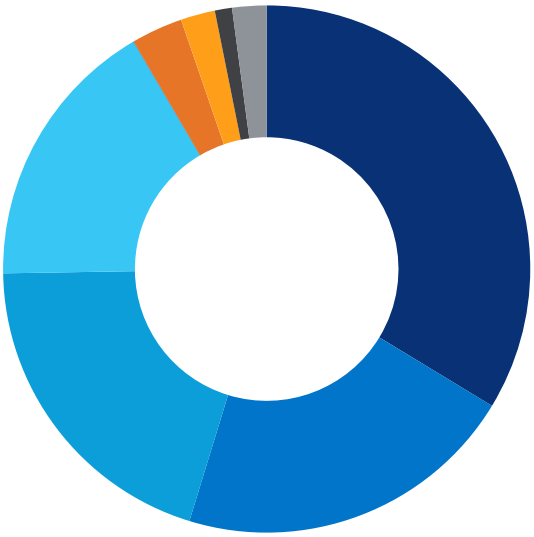
Ataques de vetor único/multivetor

	Q1 2022	Q4 2021	Mudança Q a Q
Vetor único	62%	65%	↓4%
Multivetor	38%	35%	↑8%

No 1º trimestre, os ataques de vetor único continuam sendo o método principal usado pelos atores maliciosos, mesmo com uma redução trimestral de 4%. Os achados continuam em linha com os dados de relatórios anteriores. Os ataques multivetor representaram 38% do total de ataques, ainda que muito mais altos em verticais como a de jogos (80%) e telecomunicações (67%).

Mitigações de Vetor Único

Divisão por tipo de mitigação de vetor único



			Q a Q
TCP SYN	32%	↑148%
UDP	20%	↓33%
Filtrado estática	19%	↓19%
Pacotes inválidos	16%	↓37%
DNS	0%	↑412%
Otros ataques volumétricos	3%	↑7%
HTTP	2%	↑70%
Fragmentação IP	1%	↓6%
Outros	2%	↓29%

LUMEN TECHNOLOGIES

Ao observar a divisão dos tipos de mitigação de vetor único, TCP-SYN se destacou no topo da lista, passando de 13% de atividade no 4º trimestre de 2021 para 32% de atividade no 1º trimestre de 2022, o que representa um aumento trimestral de 148% e um aumento anual de 61%. Isto poderia significar que os atacantes estão confiando em métodos de ataques simples, testados e comprovados, para obter os resultados ideais.

As mitigações de amplificação baseada em UDP passaram da primeira para a segunda posição. Esta foi uma redução de 33% em relação ao 4º trimestre, mas em linha com o que achamos durante o restante de 2021. Os ataques baseados em UDP têm o objetivo de consumir a largura de banda disponível e provaram ser bastante poderosos, com capacidade de gerar ataques de magnitude muito maior do que os bytes enviados inicialmente. Se quiser conhecer mais sobre ataques baseados em UDP, leia nosso relatório Trimestral de DDoS para o 3o trimestre de 2021, que analisa o vetor de ataque em profundidade.

A filtragem estática continua alta entre nossas mitigações de vetor único com 19%, o que representa uma queda de 19% em relação ao 4º trimestre, mas ainda em linha com o restante de nossos achados de 2021. As contramedidas para a filtragem estática são tipicamente feitas em itens como porta e protocolo. Estas estatísticas também incluem bots conhecidas e refletores abusados, conforme descoberto pelo Black Lotus Labs, que fornece a mitigação inicial contra os ataques.

Mitigações Multivetor

Principais combinações de tipos de mitigação multivetor

		Q a Q
DNS, TCP SYN	17%	▲38%
TCP SYN, filtragem estática	7%	▲65%
UDP, filtragem estática	5%	▼3%
Outras volumétricas, TCP SYN, UDP, filtragem estática	4%	N.A.
Pacotes inválidos, UDP	4%	▼41%
Outras volumétricas, UDP, filtragem estática	3%	▼35%
Pacotes inválidos, filtragem estática	3%	▼16%
TCP SYN, UDP	2%	▲20%
Outras volumétricas, TCP SYN, UDP,	2%	N.A.
Outras volumétricas, UDP	2%	▼49%

As mitigações multivetor representaram 38% da atividade, sendo que as mais comuns utilizaram uma inundação de consulta DNS em conjunto com uma inundação de TCP SYN (17% das mitigações multivetor). A Lumen observou um aumento trimestral de 38% e anual de 28% nesta combinação. Este foi o método de ataque mais utilizado durante a maior parte de 2021, especialmente no 4º trimestre, 2º trimestre e 1º trimestre. Aqui, os ataques de DDoS baseados em DNS referem-se a inundações de DNS, onde os atacantes buscam interromper os servidores de Sistema de Nome de Domínio para evitar a resolução de DNS de um determinado domínio. Estes ataques frequentemente formulam perguntas aleatórias para que os mecanismos de caching naturais do DNS não protejam o servidor.
Outras combinações incluem TCP SYN e Filtragem Estática (7% da atividade) e amplificação baseada em UDP e Filtragem Estática (5% da atividade).

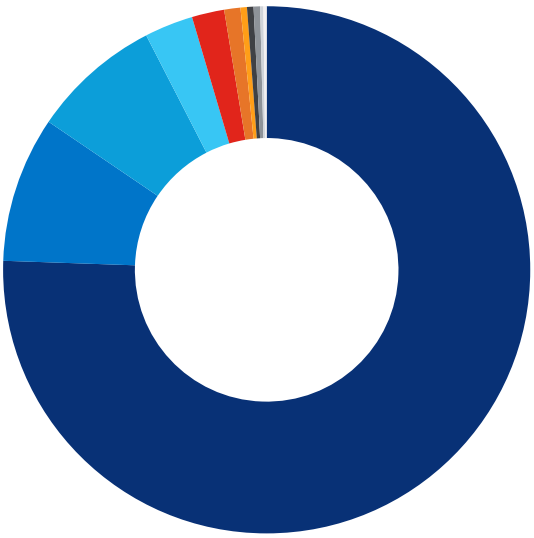
Conclusão #3

Por que devo me preocupar com os vetores de ataque que estão sendo usados?

Os cibercriminosos estão constantemente mudando seus vetores de ataque como resposta às novas estratégias de defesa que encontram. Os atores maliciosos são motivados a continuar modificando seus ataques até conseguir o que querem.
É uma corrida contínua entre atacantes e defensores sendo escalada continuamente. Isto pode sobrecarregar as equipes de segurança que tentam se manter atualizadas em relação às táticas mais recentes. A equipe de inteligência sobre ameaças da Lumen, Black Lotus Labs, trabalha diariamente para defender nossa comunidade global de atividades maliciosas. Sua inteligência sobre ameaças é incorporada a nossas soluções de mitigação de DDoS e outras soluções de segurança gerenciada, através de nossa capacidade de Defesa Rápida contra Ameaças.

Leia a página de dados

Os 500 maiores ataques por indústria



Telecomunicações	76%
Jogos	9%
Software & Tecnologia	8%
Hosting	3%
Governo	2%
Educação	1%
Outros	0.4%
Finanças	0.4%
Serviços corporativos	0.4%
Bancos	0.2%
Mídia & Entretenimento	0.2%

Dos 500 maiores ataques, 97% foram dirigidos a estas cinco principais verticais (em ordem): Telecomunicações, Jogos, Software e Tecnologia, Hosting e Governo.

É importante ressaltar que um único cliente contribuiu com a maioria dos ataques de telecomunicações que mitigamos. Durante o primeiro trimestre, foram atacados mais de 1.300 vezes. Isto não significa que a empresa de telecomunicações era o alvo específico, já que poderia haver vários alvos em sua base de clientes. A seguir poderá encontrar mais detalhes sobre as principais indústrias que são alvo de ataques.

Telecomunicações

76%
dos 500 maiores ataques

1.487
total de ataques contra a vertical

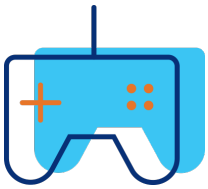
Maior ataque de largura de banda:
775 Gbps

Período mais longo de duração de um ataque:
4 dias

67%
Ataques multivetor

Maior ataque baseado em pacotes:
70 Mpps

LUMEN TECHNOLOGIES



Jogos

9%
dos 500 maiores ataques

167
Maior ataque de largura de banda

Maior ataque de largura de banda:
93 Gbps

Período mais longo de duração de um ataque:
4 dias

80%
Ataques multivetor

Maior ataque baseado em pacotes:
17 Mpps

Software e Tecnologia

8%
dos 500 maiores ataques

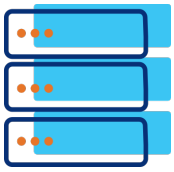
419
total de ataques contra a vertical

Maior ataque de largura de banda:
18 Gbps

Período mais longo de duração de um ataque:
4 dias

68%
Ataques de vetor único

Maior ataque baseado em pacotes:
3 Mpps



Hosting

3%
dos 500 maiores ataques

108
total de ataques contra a vertical

Maior ataque de largura de banda:
111 Gbps

Período mais longo de duração de um ataque:
5 dias

76%
Ataques de vetor único

Maior ataque baseado em pacotes:
11 Mpps

LUMEN TECHNOLOGIES

Governo

2%
dos 500 maiores ataques

2.447
total de ataques contra a vertical

Maior ataque de largura de banda:
110 Gbps

Período mais longo de duração de um ataque:
2 dias

66%
Ataques de vetor único

Maior ataque baseado em pacotes:
11 Mpps

Conclusão #4

Devo me preocupar com ataques de DDoS se não vejo minha vertical na lista acima?

A resposta curta é sim. Os setores listados acima foram alvo de ataques neste trimestre; entretanto, praticamente todas as verticais e tipos de organização podem ser e são atacadas regularmente. Uma pergunta que você deve fazer a si mesmo é: tenho algum tipo de dado que alguém poderia querer atacar? Dados desejáveis incluem informações de clientes, informações de colaboradores ou informação privilegiada. 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 Conclusões

A mensagem mais importante que esperamos que leve após ler nossos Relatórios Trimestrais de DDoS é que a segurança não deveria ser uma reflexão tardia; pelo contrário, ela precisa ser um esforço consciente de cada parte da organização. Com os estados-nação desempenhando um papel maior no panorama de ataques, os espectadores serão atacados ainda que você não seja o alvo pretendido.

Ao pensar sobre sua própria postura de segurança, pergunte a si mesmo: o que eu faria se minha organização você atacada amanhã? Nossos dados mostram que os ataques de DDoS, embora aumentem e diminuam, estão se tornando maiores, mais difundidos, mais complexos, mais distribuídos e com maior duração.

Está na dúvida se está sofrendo um ataque de DDoS?

Aprenda a reconhecer os sinais: Como saber se seu negócio está sofrendo um ataque de DDoS.

O que faço se atualmente não tenho proteção de DDoS?

Se você não conta com um parceiro de mitigação de DDoS ou se estiver procurando um novo, aqui estão algumas perguntas a serem feitas aos potenciais provedores:

- Como vocês enfrentam ataques de grande magnitude?
- Se um de seus outros clientes for atacado, como isto afetará minha organização?
- Como é sua arquitetura de depuração? É global?
- Você faz algo para bloquear as ameaças antes que se tornem ataques?
- De onde recebe sua inteligência sobre ameaças para bloquear novas ameaças? Essa inteligência sobre ameaças está integrada às suas soluções?
- Você conta com colaboradores trabalhando em diversos locais? Pode apoiar modelos de trabalho híbrido?

Como a Lumen pode me ajudar com a mitigação de DDoS?

Com uma das maiores implementações de Mitigação de DDoS da indústria, respaldada por 170 Tbps de capacidade de mitigação baseada em rede aplicada a mais de 500 localidades de depuração de múltiplas camadas, a Lumen possui mitigação de DDoS em escala. Você poderá escolher a mitigação certa para sua organização, com opções de mitigação On-Demand ou Always-On, e recursos avançados como depuração inteligente para ajudar a reduzir a latência e melhorar o desempenho. Você também poderá beneficiar-se de uma taxa de serviço mensal fixa. Você não controla a magnitude, duração ou frequência dos ataques então por que deveria ser cobrado por isto?

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

Saiba mais sobre o serviço de mitigação de DDoS da Lumen

Saiba mais sobre Lumen® DDoS Hyper®

Se estiver interessado, leia nossos relatórios trimestrais de 2021

LUMEN TECHNOLOGIES

Metodologia

Os dados deste relatório abrangem o período de 1 de janeiro de 2022 a 31 de março de 2022. Os ataques depurados são definidos como:

- Incidentes sinalizados por alertas de alto nível mitigados pela plataforma, ou
- Períodos em mitigações ativas onde as contramedidas individuais fazem o tráfego cair, ou
- Eventos onde o tráfego derrubado excedeu o tráfego enviado.

Os vetores de ataque ou tipos de mitigação são identificados por contramedidas que reduzem o tráfego ou tipos de uso indevido 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 sempre ativos são agregados em acréscimos de minutos, horas ou dias, de acordo com a duração do tempo de mitigação. Se uma mitigação levar tempo suficiente para que o tempo de resolução alcance a duração de um dia e se houver diversos dias sequenciais de ataque, então é contabilizada como um único ataque de vários dias.

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

Serviços não disponíveis em todas as localidades. Apenas clientes corporativos. A Lumen pode alterar, cancelar ou substituir produtos e serviços, ou variá-los de acordo com a área de serviço a seu critério exclusivo e sem aviso prévio. ©2022 Lumen Technologies. Todos os direitos reservados.

LUMEN TECHNOLOGIES