RELATÓRIO

Relatório Trimestral sobre DDoS da Lumen

1º trimestre de 2021

LUMEN

Introdução

O último ano foi novamente ativo para o espaço de ataque de DDoS. Os temas comuns dos anos recentes – maior complexidade, frequência e escala – continuaram a impulsionar o espaço, com atores mudando e adotando táticas, técnicas e procedimentos (TTPs), incluindo ataques multivetor e ataques mistos à camada de aplicação, e diversificando seu grupo de vítimas para maximizar o impacto e/ou o lucro.

Como indústria, vimos um dos maiores ataques já registrados, no primeiro trimestre de 2020, com 2.3 Tbps*, seguido por um ataque de DDoS de resgate (RDDoS) durante o verão e outono nos Estados Unidos, direcionado às indústrias de finanças e saúde, entre outras.

Além disso, a contínua evolução das botnets de IoT capazes de realizar ataques de DDoS, em conjunto com os amplamente acessíveis códigos-fonte das botnets e infraestrutura de DDoS por aluguel, reduziram as competências mínimas necessárias exigidas para lançar ataques, expandindo ainda mais o pool de potenciais atores.

Com este pano de fundo, as empresas atuais enfrentam os desafios de uma dependência crescente da receita de aplicações digitais para servir e engajar clientes, de um crescimento sem precedentes no tráfego, estimulado pela confiança amplamente difundida nos serviços digitais, e da pressão para satisfazer as expectativas dos usuários finais por uma entrega de aplicações integrada e desempenho sempre ativo.

Em nosso Relatório Trimestral sobre DDoS da Lumen para o 1º trimestre de 2021, compartilhamos nossa visão do cenário de DDoS, com achados que tanto reforçam quanto expandem essas tendências mais abrangentes, com um olhar nas ameaças de DDoS baseado na inteligência do Black Lotus Labs, assim como em tendências de ataques da plataforma de Serviços de Mitigação de DDoS da Lumen.

LUMEN

Principais achados para o 1º trimestre de 2021

Botnets DDoS de IoT

- Botnets de IoT reconhecidas como Gafgyt e Mirai continuam sendo sérias ameaças, com 700 C2s ativos atacando 28.000 vítimas únicas combinadas.
- Em um total de cerca de 3.000 C2s de DDoS que rastreamos globalmente no primeiro trimestre, o país hospedando o maior número de C2s é a Sérvia, seguido dos Estados Unidos e China.
- Dos mais de 400 C2s globalmente que observamos emitindo comandos de ataque, o país com o maior número foi os Estados Unidos, seguido da Holanda e Alemanha.
- Dos mais de 160.000 hospedeiros de botnets de DDoS globais que rastreamos, o maior número está localizado nos Estados Unidos, com cerca de 42.000 bots.

Tendências de Ataques de DDoS

- O maior ataque medido por largura de banda que depuramos foi de 268 Gbps e o maior ataque medido por taxa de pacote que depuramos foi de 26 Mpps.
- O período de ataque de DDoS mais longo que mitigamos para um cliente individual durou quase duas semanas.
- Cerca de 60% dos períodos de ataques de DDoS duraram menos do que uma hora, mas cerca de 20% dos períodos de ataques de DDoS duraram mais do que 24 horas.
- As mitigações multivetor representaram 41% de todas as mitigações de DDoS, com as mais comuns usando uma inundação de consulta DNS combinada a uma inundação de TCP SYN.
- A filtragem estática, tipicamente feita em itens como porta e protocolo, fornecem uma mitigação inicial contra os ataques e foi o tipo de mitigação de vetor único mais prevalecente, seguida de pacotes inválidos, amplificação UDP e TCP SYN.
- As principais três verticais que foram alvo nos 500 maiores ataques no 1º trimestre de 2021 foram: Finanças, Software & Tecnologia, e Governo.

Botnets DDoS de IoT

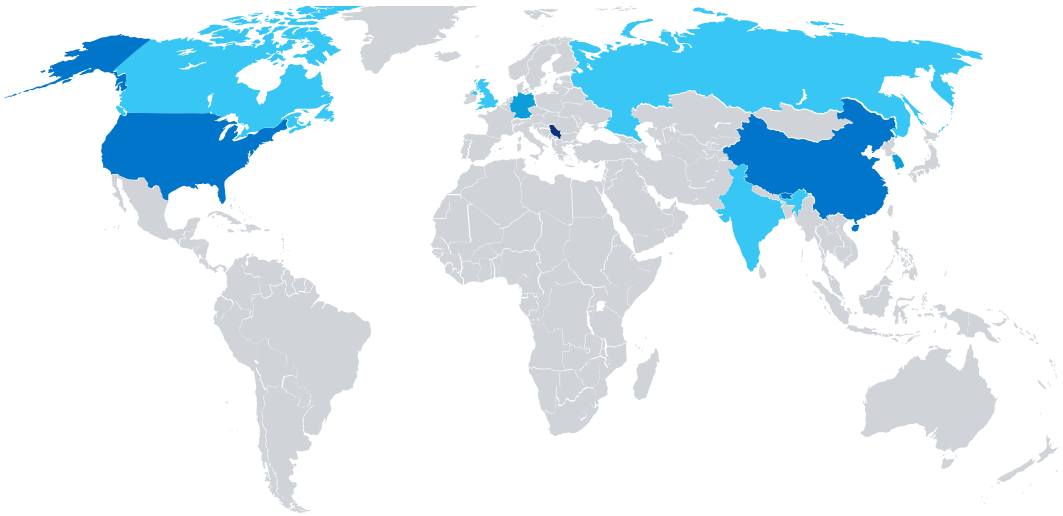
Família	C2s únicos rastreados	Vítimas únicas de ataque por família	Ciclo de vida médio de um C2 (em dias)
Gafgyt	451	2.870	21
Mirai	249	25.240	10

Como em relatórios anteriores, o Black Lotus Labs continua a monitorar duas das famílias de DDoS de IoT mais predominantes, Gafgyt e Mirai. Notavelmente, apesar do número de C2s Mirai totalizando um pouco mais que metade dos Gafgyt no primeiro trimestre, e apesar de ter um ciclo de vida médio muito menor, o Black Lotus Labs identificou aproximadamente 10 vezes mais o número de vítimas únicas de ataques de Mirai do que de Gafgyt.

Ameaças globais de DDoS rastreadas por país

Os seguintes mapas de calor específicos para DDoS representam os principais 10 países por C2s rastreados, C2s emitindo comandos de ataque, e hospedeiros de botnets para o trimestre, baseados na visibilidade do Black Lotus Labs e divididos por tipo de ameaça e país de origem suspeito. A equipe determina o país de origem tomando o endereço IP de cada hospedeiro e comparando-o com um rico conjunto de endereços IP para mapeamentos geográficos.

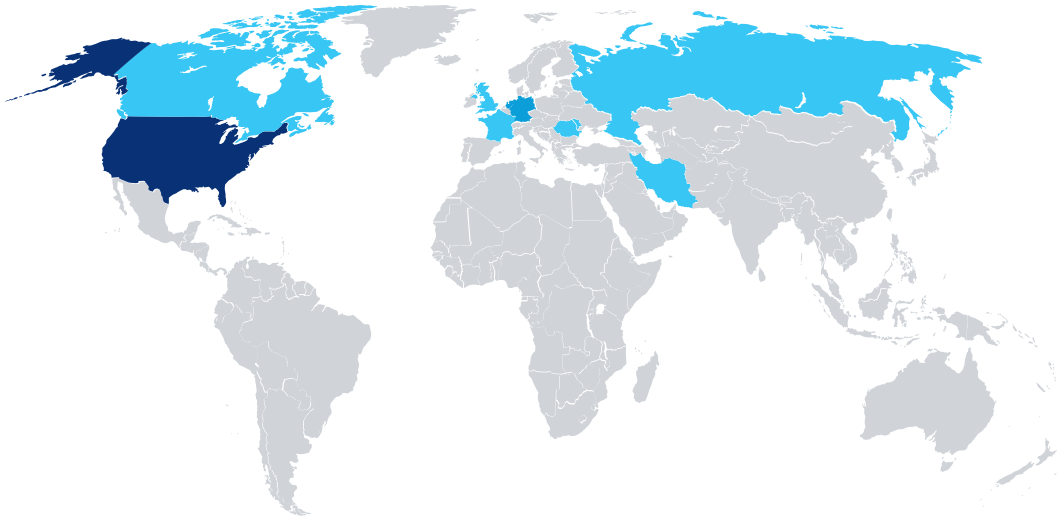
Principais 10 países por C2s



Nome do país	C2s	População**	Per Capita (100.000)
Sérvia	1.260	8.737.371	14.42
Estados Unidos	380	331.002.651	0.11
China	373	1.439.323.776	0.03
Coréia do Sul	166	51.269.185	0.32
Alemanha	138	83.783.942	0.16
Holanda	132	17.134.872	0.77
Canadá	53	37.742.154	0.14
Rússia	41	145.934.462	0.03
Reino Unido	38	67.886.011	0.06
Índia	36	1.380.004.385	0.003

O país hospedando a maioria dos C2s de DDoS é a Sérvia, com um total de 1.260, seguido dos Estados Unidos e da China, com 380 C2s e 373 C2s, respectivamente. A Sérvia também tem o número mais alto de C2s per capita, com mais de 14 C2s por 100.000 pessoas, seguida à distância pela Holanda e Coréia do Sul.

Principais 10 países por C2s emitindo comandos de ataque

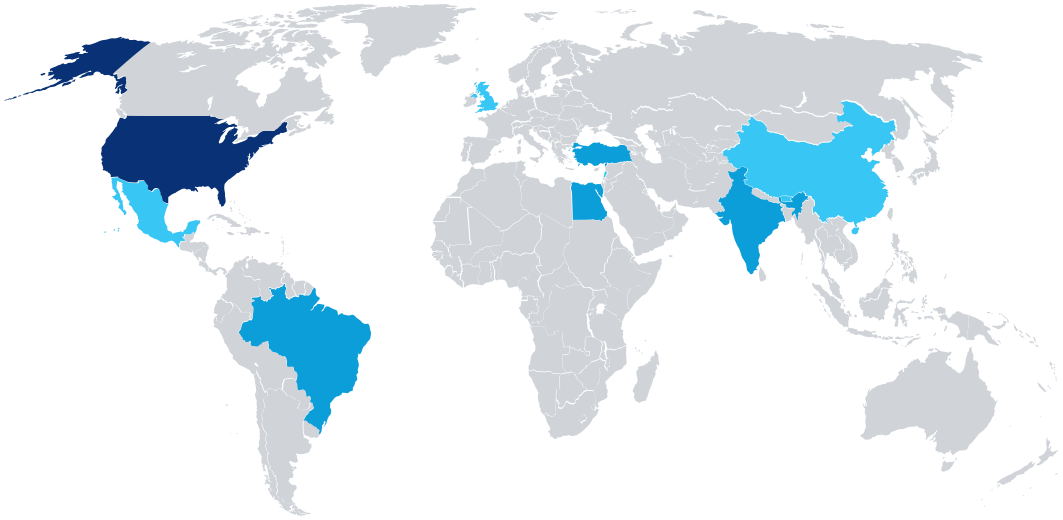


Nome do país	número de C2s	População**	Per Capita (100.00)
Estados Unidos	163	331.002.651	0.05
Holanda	73	17.134.872	0.43
Alemanha	70	83.783.942	0.08
Canadá	15	37.742.154	0.04
Reino Unido	14	67.886.011	0.02
França	13	65.273.511	0.02
Romênia	13	19.237.691	0.07
Rússia	12	145.934.462	0.01
Irã	8	83.992.949	0.01
Moldávia	8	4.033.963	0.20

O país com o maior número de C2s rastreados observados emitindo comandos de ataque neste período é o Estados Unidos, seguido pela Holanda e Alemanha. A Holanda tem o maior número de C2s per capita, seguida pela Moldávia e Alemanha.

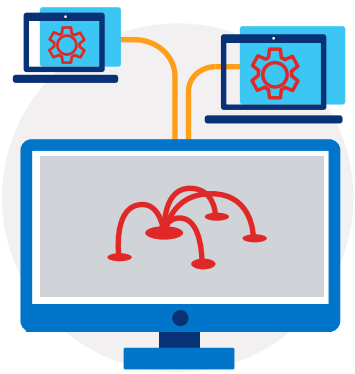
LUMEN

Principais 10 países por hospedeiros de botnets de DDoS



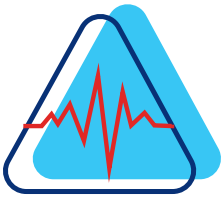
Nome do país	Número de bots	População**	Per Capita (100.000)
Estados Unidos	41.752	331.002.651	13
Iraque	23.647	40.222.493	59
Turquia	12.921	84.339.067	15
Brasil	12.196	212.559.417	6
Egito	11.009	102.334.404	11
Índia	10.939	1.380.004.385	1
China	7.371	1.439.323.776	1
México	5.821	128.932.753	5
Líbano	3.612	6.825.445	53
Reino Unido	3.168	67.886.011	5

Dos mais de 166.000 hospedeiros de botnets de DDoS que rastreamos no primeiro trimestre, o maior número de hospedeiros está localizado nos Estados Unidos, com cerca de 42.000 bots. Em uma base per capita, a maior quantidade de bots de DDoS por 100.000 pessoas está localizada no Iraque e no Líbano, com 59 e 53, respectivamente.



LUMEN

Tamanho e duração do ataque



	Bits/s Perdidos	Pacotes/s Perdidos
Maior ataque depurado	268 Gbps	26 Mpps

A Lumen absorve ataques de DDoS de grande escala em seu backbone global antes sequer do tráfego chegar a seu centro de depuração. Os tamanhos dos ataques neste relatório mostram os maiores ataques depurados pela infraestrutura global de depuração de DDoS da Lumen, ao invés dos maiores ataques observados trafegando pela rede da Lumen

A Lumen analisa e mitiga dois principais tipos de ataque volumétrico de DDoS: aqueles medidos por largura de banda que interrompem o serviço através da inundação de um circuito ou aplicação com tráfego medido em bits por segundo, e aqueles medidos com taxas de pacotes que também podem amarrar os recursos específicos da rede, tais como roteadores ou outros aparelhos na rede, e são medidos em pacotes por segundo. Os tamanhos dos ataques neste relatório mostram os maiores ataques depurados pela infraestrutura global de depuração de DDoS da Lumen, ao invés de os maiores ataques observados entrando na rede da Lumen.

O maior ataque medido por largura de banda que depuramos no primeiro trimestre foi de 268 Gbps. Muitas empresas hoje não têm a capacidade para aguentar um ataque de +250 Gbps, que equivale a mais de 50 milhões de e-mails de texto simples, todos sendo recebidos ao mesmo tempo.

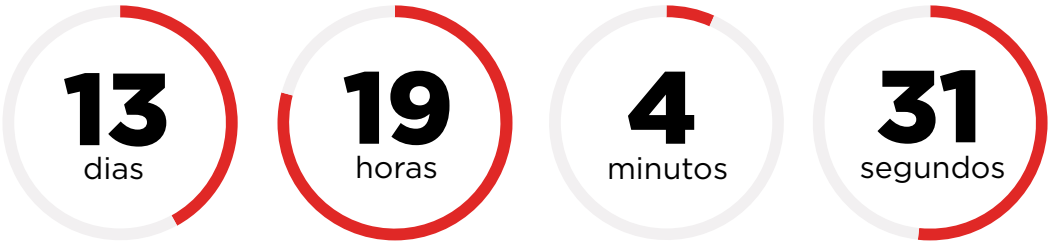
O maior ataque de alta taxa de transferência de pacotes que depuramos no trimestre foi de 26 Mpps, que equivale a 62 portas de 10 GigE baseadas em um tamanho de pacote médio de 300 bytes, que poderia facilmente sobrecarregar os recursos de um roteador, tal como CPU, encaminhamento, memória e outras funções.

LUMEN

Duração mediana do ataque

Duração média do ataque

Ataque de mais longa duração

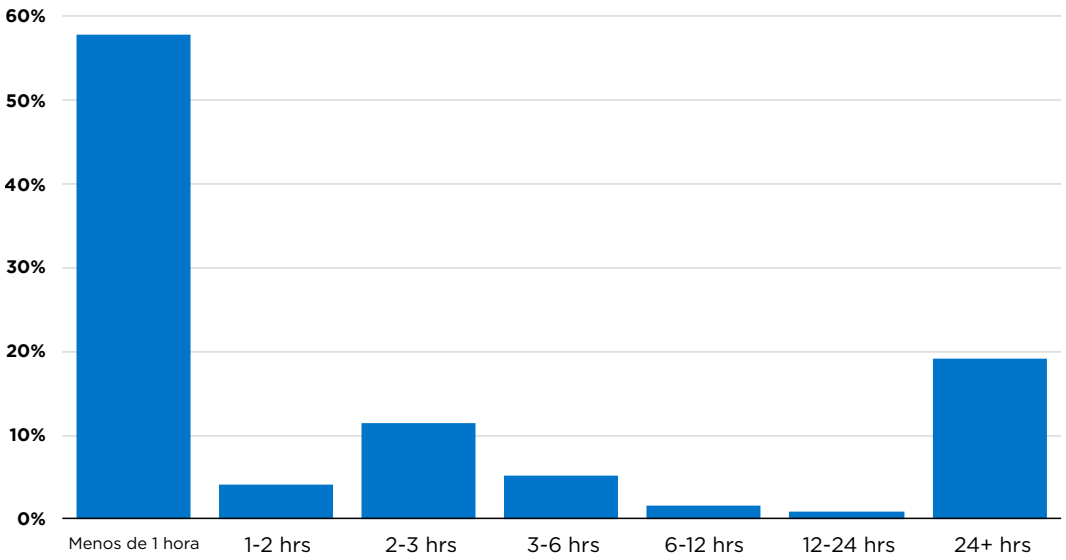


Embora a duração mediana do período de ataque tenha sido um pouco abaixo de 26 minutos, o período de ataque mais longo que observamos durou quase duas semanas. Em média, os períodos de ataques de DDoS no primeiro trimestre duraram cerca de sete horas.

Cerca de 60% dos períodos de ataques de DDoS duraram menos do que uma hora, mas cerca de 20% dos períodos de ataques de DDoS duraram mais do que 24 horas.

LUMEN

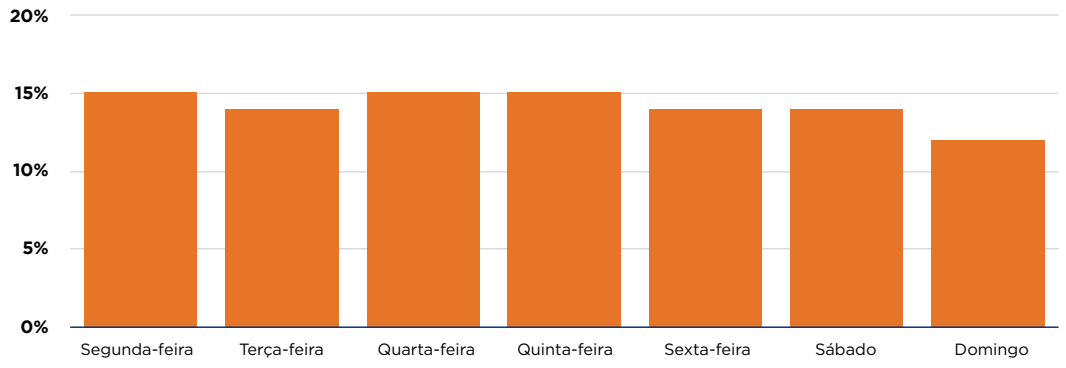
Distribuição por duração



Olhando para a distribuição por duração, vimos que cerca de 60% dos períodos de ataques de DDoS duraram menos do que uma hora, mas cerca de 20% dos períodos de ataques de DDoS duraram mais do que 24 horas. Interessantemente, o próximo maior percentual de duração de período de ataque de DDoS foi no período de 2 a 3 horas, com 11%.

Embora não surpreenda que a maioria dos ataques fosse de menos do que uma hora, dado que os SLAs do provedor de serviços de mitigação de DDoS eram no intervalo de 10 a 15 minutos, é notável ver um percentual de período de ataque tão alto durando mais do que 24 horas. Para compradores que são sensíveis aos SLAs, a mitigação sempre ativa, onde o tráfego é constantemente enviado através de depuradores, pode ser a escolha adequada.

Distribuição por dia



Investigamos também se era mais provável que os ataques de DDoS ocorressem em certos dias, mas percebemos que a distribuição era feita de forma razoavelmente consistente por todos os dias da semana, com 14-15% dos ataques caindo a cada dia de segunda a sábado, com uma leve queda aos domingos, com 12% dos ataques. Parece que até os operadores de DDoS precisam de uma pausa.

Tipos de mitigação de ataques

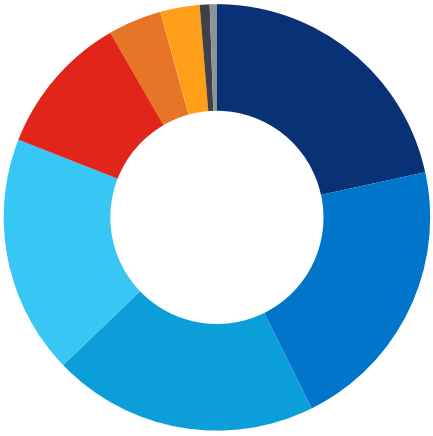
Multivetor	41%
Vetor único	59%

Ataques de vetor único/multivetor

A distribuição entre ataques de vetor único e multivetor é de cerca de 60% a 40%, respectivamente. Nos últimos anos, a mistura de vetores únicos e multivetores flutuou, com alguns na indústria acreditando que os ataques multivetor ultrapassaria em muito os ataques de vetor único. No entanto, dada a ampla disponibilidade de código fonte de redes bots de DDoS e a relativa facilidade com que uma infraestrutura de ataque de DDoS pode ser alugada através da dark web - que pode estender capacidades de ataques de DDoS a atores menos sofisticados - não surpreende ver uma grande parte dos ataques sendo feitos através de um vetor único. Adicionalmente, atores mais sofisticados podem também aproveitar ataques de vetor único para lançar DDoS com o propósito de distrair a vítima de seu real objetivo, que é a extração de dados.

Mitigações de Vetor Único

Divisão por tipo de mitigação de vetor único



Filtragem Estática	21%
Pacotes Inválidos	21%
Amplificação UDP	20%
TCP SYN	18%
DNS	11%
Fragmentação IP	4%
Outros volumétricos	3%
ICMP	1%
Reflexo TCP SYN/ACK	1%

A filtragem estática, tipicamente feita em itens como porta e protocolo, fornece uma mitigação inicial contra os ataques e foi o tipo de mitigação de vetor único mais prevalecente, seguida de pacotes inválidos, amplificação UDP e TCP SYN. Pacotes inválidos incluem tráfego com campos de dados malformados, assim como fragmentos incompletos, duplicados ou muito grandes. Embora possam ser resultado de um bug de rede ou falha de sequenciamento da rede, também são uma característica comum de ataques de DDoS.

Ataques de amplificação baseados em UDP são um vetor comum visando protocolos da camada de aplicação e já provaram ser um vetor poderoso capaz de amplificar muito seu potencial impacto. Nestes ataques, os atores manipulam a natureza sem conexão e sem estado do User Datagram Protocol para imitar o IP de origem de um pacote de solicitação UDP para que uma vítima receba pacotes de resposta UDP indesejados de um servidor intermediário insuspeito. Como as respostas UDP a certas consultas ou serviços podem ser muito maiores do que os tamanhos dos pacotes de solicitações, o IP da vítima pode rapidamente ficar sobrecarregado.

Durante ataques de DDoS de amplificação de UDP, frequentemente as respostas geradas pelos servidores sendo usados para amplificar as mensagens devem responder em fragmentos, devido ao tamanho da resposta. A maior carga de processamento que isto causa nos roteadores lidando com inundações massivas pode levar a fragmentos perdidos ou malformados. Isto faz com que ataques de amplificação de UDP existam tanto na área de amplificação de UDP quanto na área inválida. Adicionalmente, para muitos de nossos clientes, utilizamos

filtragem estática para bloquear completamente uma parte deste tráfego, fazendo com que a amplificação UDP tenha um impacto em muitas mitigações e demonstrando o quanto é comum como um vetor de ataque.

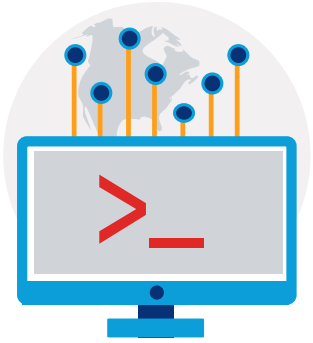
Os ataques TCP SYN exploram o handshake de três vias do TCP ao nunca responder com o pacote de reconhecimento exigido, deixando um servidor segurando dezenas ou centenas de milhares de conexões abertas, fazendo com que leve à exaustão o espaço de soquete, o espaço de porta efêmero, o espaço de memória, ou similar.

Mitigações Multivetor

Principais 10 combinações de tipos de mitigação multivetor

DNS, TCP SYN	12%
Amplificação DNS, fragmentação IP	4%
TCP SYN, UDP	4%
DNS, TCP SYN, filtragem estática	4%
Pacotes inválidos, UDP	3%
DNS, filtragem estática	3%
Fragmentação IP, tráfego total, UDP	3%
Pacotes inválidos, filtragem estática	3%
DNS, TCP SYN, filtragem estática	3%

As mitigações multivetor representaram 41% de todas as mitigações de DDoS, com as mais comuns usando uma inundação de consulta DNS combinada com uma inundação de TCP SYN. Os ataques de DDoS baseados em DNS aqui referem-se a inundações DNS, onde os atacantes buscam interromper os servidores de Sistema de Nome de Domínio para evitar a resolução DNS de um certo domínio. Estes ataques frequentemente fazem perguntas randômicas para que os mecanismos de caching naturais do DNS não protejam o servidor.



Outras combinações repetidas que encontramos, todas ocorrendo aproximadamente na mesma frequência, incluem a amplificação de DNS e fragmentação de IP, TCP SYN e UDP, e pacotes inválidos e UDP. Estas combinações refletem os vetores padrão usados para travar os ataques de DDoS, mas combinadas de várias maneiras para causar um impacto maior.

BLACK LOTUS LABS®

Rastreando Refletores UDP em busca de uma Internet mais segura

Nos últimos anos, os eventos Distribuídos de Negação de Serviço (DDoS) se tornaram uma ameaça sempre presente, com tráfego de ataque chegando a níveis medidos em terabits por segundo (Tbps). Uma das ferramentas-chave nas mãos dos cibercriminosos buscando aumentar a largura de banda de seus ataques é o reflexo baseado em UDP.

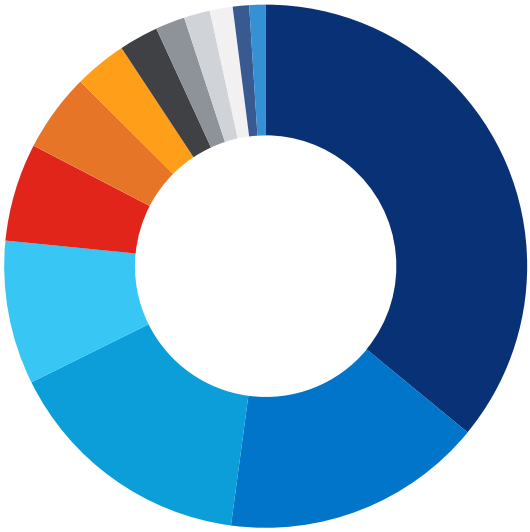
Por exemplo, o ataque de DDoS de 2018 na GitHub usou um serviço na camada de aplicação chamado Memcached para dirigir, no pico, 1.35 Tbps de tráfego UDP refletido nos servidores da GitHub. Em 2020, a indústria ficou sabendo sobre um ataque de DDoS de 2017 que usou um pacote de serviços UDP como refletores (CLDAP, DNS, e SMTP) para obter taxas de fio de até 2.5 Tbps.

No Black Lotus Labs, aproveitamos a visibilidade de nossa rede global para identificar os serviços que estão sendo potencialmente manipulados para lançar ataques, tais como as instâncias de Memcached, CLDAP e DNS, e depois trabalhar para confirmar se estão abertos para serem usados como refletores. Baseados em nossos dados do primeiro trimestre de 2021, vemos cada um destes serviços sendo ativamente usados para lançar significativos ataques de DDoS atualmente.

Leia nosso blog, Rastreando Refletores UDP em busca de uma Internet mais segura, para saber mais.

LUMEN

500 Maiores ataques por indústria



Finanças	36%
Software & Tecnologia	16%
Governo	15%
Telecom	9%
Jogos	6%
Educação	5%
Outras verticais	3%
Serviços públicos	2%
Varejo e Distribuição	2%
Consultoria	2%
Serviços corporativos	1%
Sem fins lucrativos	1%
Saúde	1%

Dos 500 maiores ataques, dois terços foram direcionados a apenas três verticais (em ordem): Finanças, Software & Tecnologia, e Governo. A vertical de finanças experimentou a maior quantidade de ataques volumétricos, com 36% dos 500 maiores ataques. Software & Tecnologia experimentou 16% dos maiores ataques, e o setor de Governo, que inclui estadual, local e federal, experimentou 15%. Finanças há muito vem sendo alvo de ataques de DDoS, mas esta distribuição mostra que nenhuma vertical hoje está livre no ambiente de ameaças atual.

As principais três verticais que foram alvo dos 500 maiores ataques no primeiro trimestre de 2021 foram Finanças, Software & Tecnologia e Governo.

Principais Mensagens

Para aplicações de próxima geração e cargas de trabalho modernas - a força vital da economia digital - as expectativas são altas. Tudo se trata da experiência do usuário, que depende de disponibilidade, desempenho e segurança.

À medida que a dependência das aplicações para gerar receita se aprofunda, muitas organizações estão percebendo que não podem mais arriscar renunciar às defesas essenciais de DDoS. As organizações devem proteger ativos e aplicações críticos voltados para a web contra os ataques cada vez mais complexos - tudo com um talento interno limitado, uma superfície de ataques em expansão e uma necessidade inerente de mitigar grandes ataques na nuvem ou na rede.

Elas precisam de um provedor de serviços com alcance global e uma capacidade de mitigação altamente escalável, que ofereça proteção agnóstica a operadoras contra os ataques multivetor e ataques mistos de camada de aplicação, com recursos avançados, como serviço sempre ativo e detecção e resposta automática de ameaças para ajudar a interromper os ataques antes que cheguem à rede do cliente.

Orientação para os Defensores das Redes

Os defensores das redes devem buscar um provedor de mitigação de DDoS que possa oferecer:

- Escala e capacidade de absorver grandes ataques no backbone como uma primeira camada de defesa
- Pegada global para uma latência reduzida ao rotear o tráfego para depuração
- Flexibilidade e recursos avançados para proteger experiências modernas na web
- 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 híbridos de suporte para proteger os ambientes corporativos atuais, do colaborador remoto ao escritório corporativo, e do data center à nuvem

Com uma das maiores implementações de mitigação de DDoS na indústria, +85 Tbps de capacidade de FlowSpec no backbone global, contramedidas derivadas do Black Lotus Labs e de depurações inteligentes de próxima geração, a Lumen possui a mitigação em escala.
O Serviço de Mitigação de DDoS da Lumen fornece opções de mitigação sob demanda e 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 do tamanho, duração ou frequência dos ataques.

Saiba mais sobre o Serviço de Mitigação de DDoS da Lumen

Metodologia

Os dados neste relatório são do período de 1 de janeiro de 2021 a 31 de março de 2021. 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 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 o 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 sempre ativos são agregados em acréscimos de minutos, horas ou dias, de acordo com a duração dos tempos de mitigação. Se uma mitigação rodar 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 ataque único com período de vários dias.

Notas finais

* Fonte: https://www.tripwire.com/state-of-security/security-data-protection/amazon-web-services-mitigated-a-2-3-tbps-ddos-attack/

** Fonte: Worldometer (www.worldometers.info)

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