CLOUDFLARE

Relatório de tendências de DDoS da Cloudflare

Conteúdo

T4 de 2023

Sumário executivo

Boas-vindas à décima sexta edição do relatório sobre ameaças DDoS da Cloudflare. Os ataques DDoS, ou ataques de negação de serviço distribuída, são um tipo de ataque cibernético que visa interromper sites (e outros tipos de ativos da internet) para torná-los indisponíveis para usuários legítimos, sobrecarregando-os com tráfego excessivo. Pense nisso como causar um engarrafamento em uma estrada crítica, impedindo as pessoas de chegarem ao seu destino

Nossa rede é uma das maiores do mundo, abrangendo mais de 310 cidades em mais de 120 países. Lidamos com uma enorme quantidade de tráfego da internet, atendendo mais de 70 milhões de solicitações da web por segundo no pico e processando 2,6 bilhões de consultas de DNS diariamente. Em média, frustramos 170 bilhões de ameaças cibernéticas todos os dias. Este vasto volume de dados nos fornece uma perspetiva única sobre o cenário de ameaças DDoS, o que nos permite partilhar informações e tendências valiosas com a comunidade de segurança cibernética.

Nas últimas semanas, observamos um aumento nos ataques DDoS e outros ataques cibernéticos, no contexto das eleições gerais recentemente concluídas em Taiwan e das tensões relatadas com a China. À medida que o conflito militar entre Israel e o Hamas continua, os sites palestinos e os sites israelenses, têm enfrentado ataques DDoS significativamente maiores.

Para uma comparação anual, os ataques DDoS na camada de aplicação caíram 20% em 2023 em comparação com 2022. Ironicamente, 2023 também viu as maiores campanhas de ataque DDoS na camada de aplicação, ultrapassando 100 milhões de solicitações por segundo em múltiplas instâncias, incluindo a campanha de ataque HTTP/2 Rapid Reset no início deste ano. Na camada de rede, vimos uma tendência completamente diferente: um aumento de 85% nos ataques DDoS na camada de rede em 2023 em comparação com 2022.

Notavelmente, as organizações de serviços ambientais sofreram o maior volume de tráfego de ataques DDoS por HTTP, que coincidiu com a 28ª Conferência das Nações Unidas sobre Alterações Climáticas (COP 28).

Uma versão interativa deste relatório está disponível no Cloudflare Radar.

Destaques do relatório

Tendências de DDoS para 2023

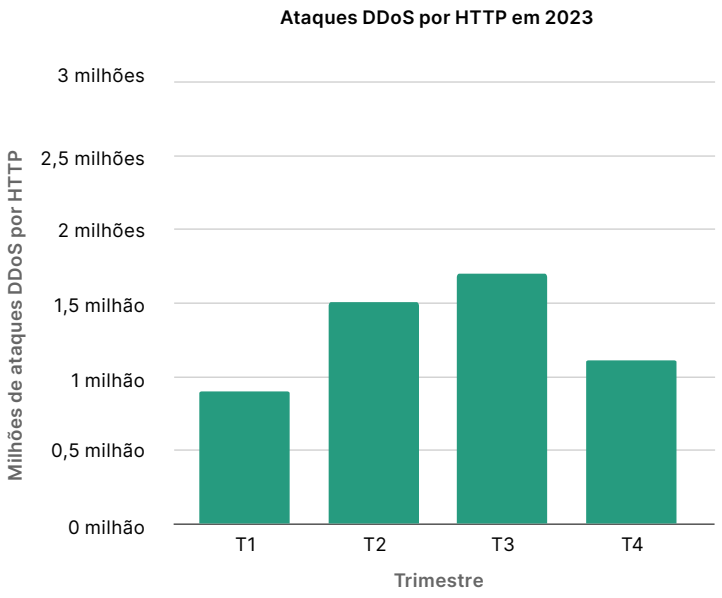
Depois que a campanha hipervolumétrica diminuiu, vimos uma queda inesperada nos ataques DDoS por HTTP de 20% em comparação com 2022. No geral, em 2023, as nossas defesas automatizadas mitigaram mais de 5,2 milhões de ataques DDoS por HTTP, consistindo em mais de 26 trilhões de solicitações. Apesar da queda no número de ataques, a média de ataques interrompidos é muito grande: 594 ataques DDoS por HTTP interrompidos e 3 bilhões de solicitações mitigadas a cada hora de 2023.

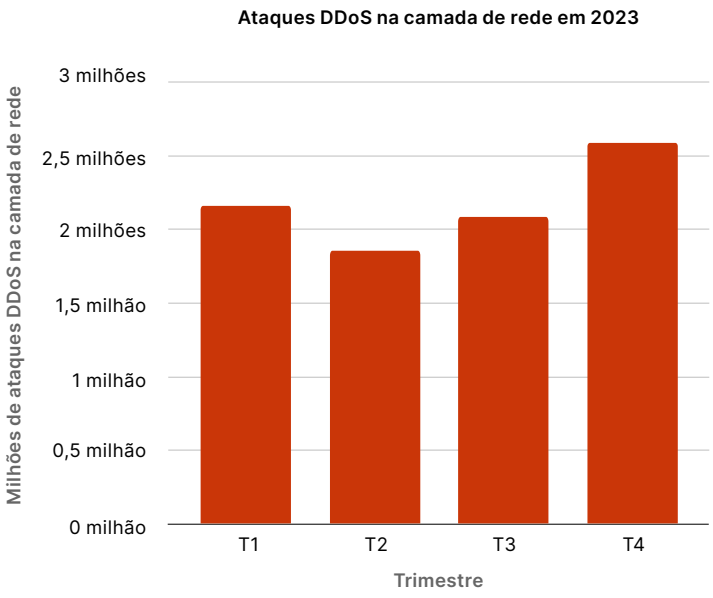
Na camada de rede, vimos uma tendência completamente diferente. Nossas defesas automatizadas mitigaram 8,7 milhões de ataques DDoS na camada de rede em 2023. Isso representa um aumento de 85% em comparação com 2022. Em média, nossos sistemas mitigaram 996 ataques DDoS na camada de rede e 27 terabytes a cada hora.

2023 – Ataques DDoS em números

Ataques DDoS por HTTP
5,2 milhões de ataques mitigados em 2023
-20% A/A

Ataques DDoS na camada de rede
8,7 milhões de ataques mitigados em 2023
+85% A/A





Zonas de conflito específicas e ataques DDoS: eleições gerais em Taiwan e conflito entre Israel e Hamas

O aumento de ataques contra regiões específicas (Taiwan, Israel e territórios palestinos) destaca a utilização de DDoS como ferramenta na guerra cibernética, aproveitando os recursos cibernéticos para exercer pressão política ou perturbar infraestruturas digitais críticas.

Eleições gerais em Taiwan

Vimos um aumento anual de 3.370% nos ataques DDoS por HTTP direcionados a sites em Taiwan. A grande maioria (82%) é originária da China, o que está correlacionado com a acalorada retórica política na China e em Taiwan neste momento. Surpreendentemente, os sites de entretenimento adulto foram mais visados do que setores comuns enraizados na vida cotidiana, como serviços financeiros, saúde e transportes.

Guerra entre Israel e Hamas

Os ataques DDoS são uma ferramenta aceita de guerra e perturbação. Testemunhamos um aumento na atividade de ataques DDoS na guerra entre a Ucrânia e a Rússia, e agora também estamos testemunhando na guerra entre Israel e o Hamas. Relatamos pela primeira vez a atividade cibernética em nosso post do blog Cyber attacks in the Israel-Hamas war e continuamos monitorando a atividade até o momento.

Os territórios palestinos foram a segunda região mais atacada no mundo por ataques HTTP e DDoS na camada de rede no quarto trimestre. Os ataques DDoS representaram mais de 68% de todo o tráfego das camadas 3 e 4 para redes palestinas e mais de 10% de todas as solicitações HTTP para sites palestinos. Nove em cada dez desses ataques DDoS por HTTP tiveram como alvo sites bancários palestinos.

Os sites israelenses também registraram tráfego de DDoS intenso, embora tenham observado um aumento mais modesto, de 27%, no tráfego de DDoS por HTTP em relação ao trimestre anterior. Os setores de jornais, mídia e software de computador receberam quase 65% de todos os ataques DDoS por HTTP em sites israelenses.

Nossos dados sugerem um esforço concertado para prejudicar os setores enraizados na vida quotidiana de ambos os lados.

Tendência crescente de eventos políticos globais que desencadeiam ataques cibernéticos

Observamos uma tendência crescente em que eventos globais podem tornar-se pontos de gatilho para ataques cibernéticos. A 28ª Conferência das Nações Unidas sobre Mudanças Climáticas (popularmente conhecida como COP 28) foi encerrada em 13 de dezembro de 2023. Vimos um aumento impressionante (mais de 61.000%) nos ataques DDoS por HTTP a organizações de serviços ambientais entre outubro e dezembro de 2023 em comparação com o mesmo período em 2022. O padrão não se limitou apenas a este evento.

Analisando os dados históricos, especialmente durante a COP 26 e a COP 27, bem como outras resoluções ou anúncios da ONU relacionados com o ambiente, temos um padrão semelhante. Cada um destes eventos foi acompanhado por um aumento correspondente de ataques cibernéticos dirigidos a sites de serviços ambientais.

Temporada de festas de final de ano do T4: o Grinch do DDoS

Observamos um aumento na atividade de DDoS por HTTP direcionada a sites de varejo, remessas e relações públicas entre a Black Friday, o Natal e o Ano novo. Na camada de aplicação, o setor de embalagens e entrega de cargas foi o segundo mais visado (depois do setor de serviços ambientais) em relação ao tráfego HTTP geral de cada setor. Este setor sustenta o sucesso da Black Friday e da experiência de compras nas festas de final de ano. Os presentes e bens adquiridos devem chegar ao seu destino com precisão e dentro do prazo. Os invasores podem ter tentado interferir nisso. Os ataques DDoS na camada de aplicação contra empresas de varejo também aumentaram 16% em comparação com o ano anterior, 2022.

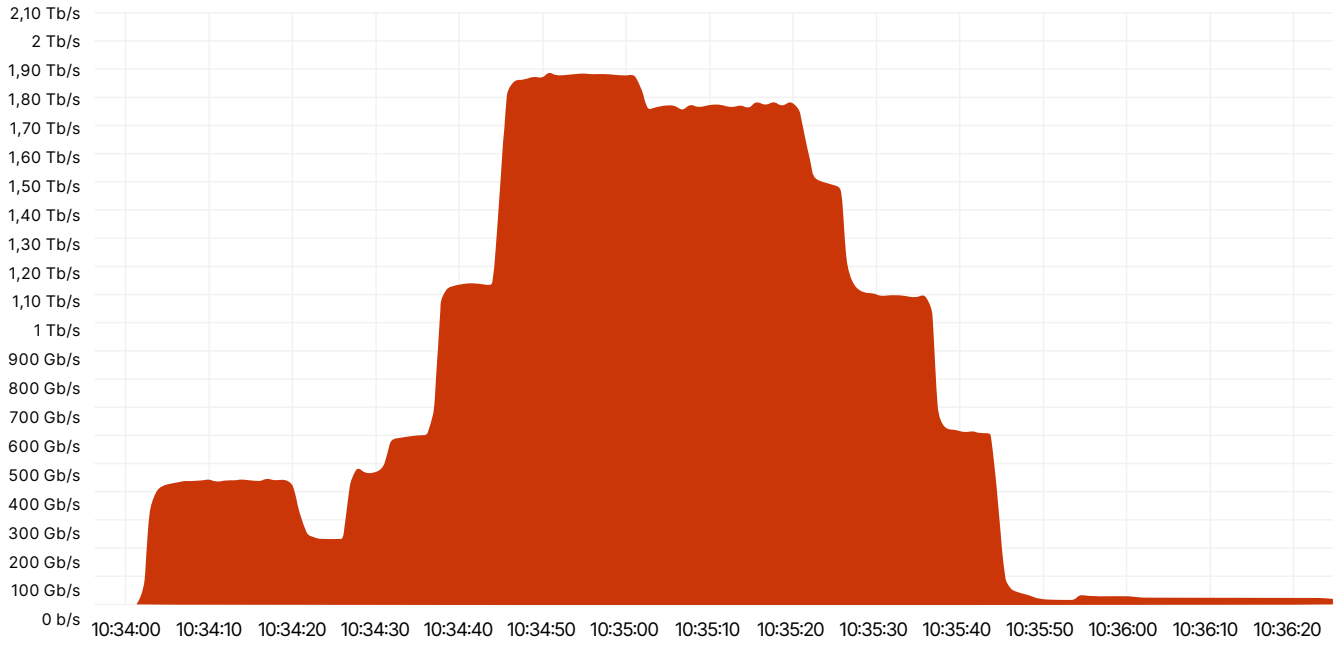
Na camada de rede, o setor de relações públicas (RP) e comunicações foi o setor mais visado, 36% de seu tráfego foi malicioso. A interrupção das operações deste setor pode ter impactos imediatos e generalizados na reputação. Os meses de outubro a dezembro e o final do ano frequentemente apresentam um aumento nas atividades de relações públicas e comunicação devido às festas, resumos de final de ano e preparativos para o novo ano. Resumindo, é um período operacional crítico, que os invasores podem querer interromper.

Vetores de ataque emergentes na camada de rede

Vamos examinar um ataque específico para explorar o cenário em mudança no DDoS na camada de rede.

Um dos grandes ataques entre outubro e dezembro de 2023 foi um ataque da botnet Mirai que teve como alvo um conhecido fornecedor de nuvem europeu, que durou menos de dez minutos e teve origem em mais de 18.000 endereços de IP únicos (supostamente falsificados). Foi automaticamente detectado e mitigado pelas defesas da Cloudflare.

Grande ataque da botnet Mirai ao provedor de nuvem europeu

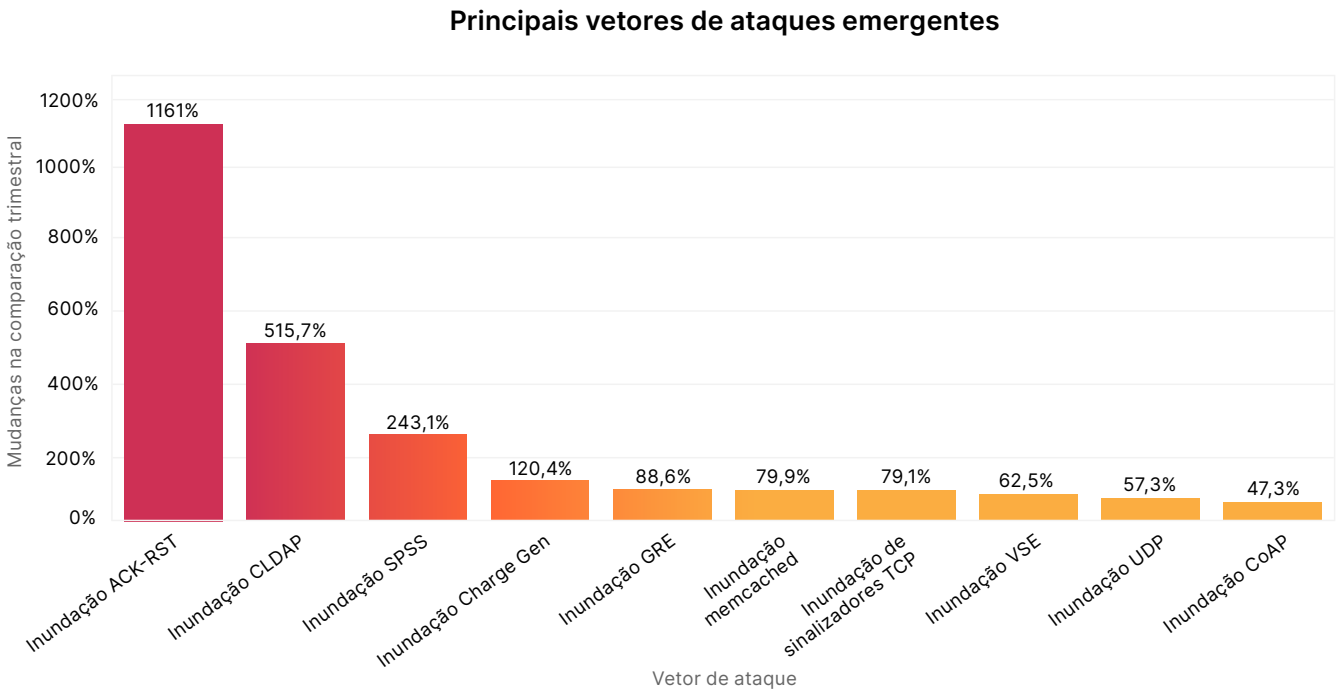


Este ataque foi único em termos da alta taxa de bits por segundo e natureza de ataque multivetorial, mas durou apenas um curto período. Ele atingiu o pico de 1,9 terabits por segundo e combinou vários métodos de ataque, incluindo inundação de fragmentos UDP, inundação UDP/Echo, inundação SYN, inundação ACK e sinalizadores mal formados de TCP. Esses ataques com altas taxas de bits por segundo são raros. Ainda mais sofisticado é que os ataques combinem vários métodos.

A taxa de pacotes por segundo de 160 milhões de pacotes por segundo não foi a maior que já vimos, que foi de 754 milhões de pacotes por segundo em 2020.

Além desse ataque com suas características únicas, as organizações não podem se dar ao luxo de usar centros de depuração manual para suas defesas contra DDoS. Elas precisam de sistemas de defesa automatizados em linha.

Entre as ameaças emergentes que rastreamos, registramos um aumento de 1.161% nas inundações ACK-RST, bem como um aumento de 515% nas inundações CLDAP e um aumento de 243% nas inundações SPSS, em cada caso em comparação com o último trimestre. Vejamos alguns desses ataques e como eles pretendiam causar perturbações.



Inundações ACK-RST

Uma inundação ACK-RST explora o Protocolo de Controle de Transmissão (TCP) enviando vários pacotes ACK e RST para a vítima. Isto sobrecarrega a capacidade da vítima de processar e responder a esses pacotes, levando à interrupção do serviço. O ataque é eficaz porque cada pacote ACK ou RST solicita uma resposta ao sistema da vítima, consumindo seus recursos. As inundações ACK-RST costumam ser difíceis de filtrar, pois imitam o tráfego legítimo, tornando a detecção e a mitigação desafiadoras.

Inundações CLDAP

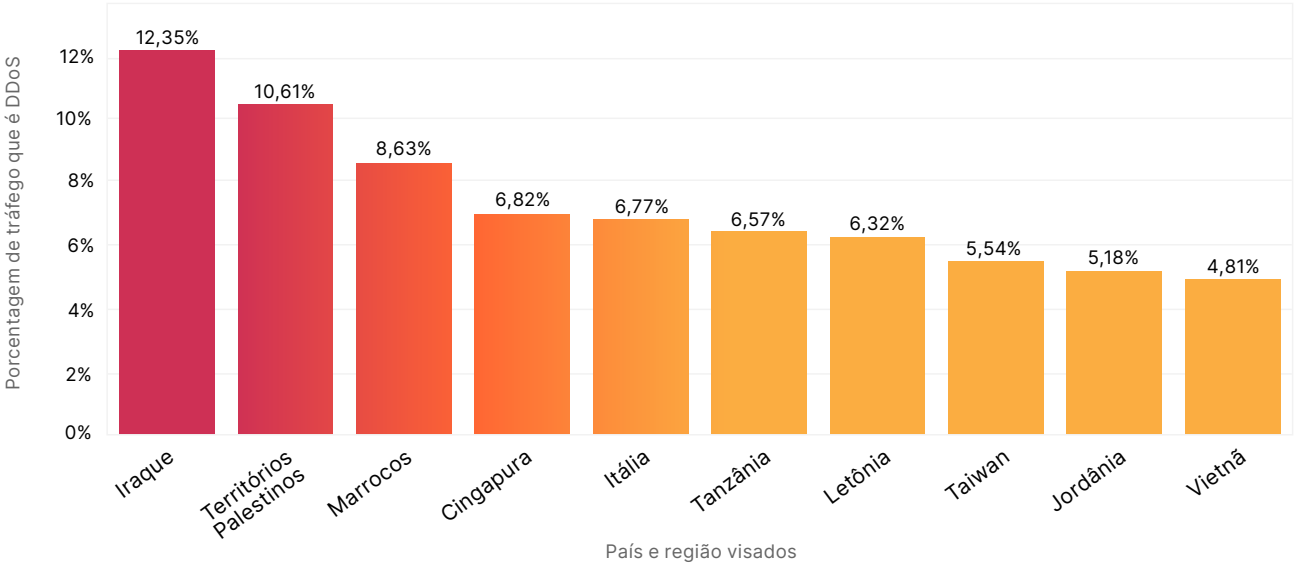
O CLDAP (Connectionless Lightweight Directory Access Protocol) é uma variante do LDAP (Lightweight Directory Access Protocol). É usado para consultar e modificar serviços de diretório executados em redes de IP. O CLDAP não tem conexão, usando UDP em vez de TCP, o que o torna mais rápido, mas menos confiável. Por usar UDP, não há nenhum requisito de handshake o que permite aos invasores falsificar o endereço de IP, permitindo assim que eles o explorem como um vetor de reflexão. Nestes ataques, pequenas consultas são enviadas com um endereço de IP de origem falsificado (o IP da vítima), fazendo com que os servidores enviem grandes respostas à vítima, sobrecarregando-a. A mitigação envolve filtrar e monitorar o tráfego CLDAP incomum.

Inundações SPSS

As inundações que abusam do protocolo SPSS (Source Port Service Sweep) são um método de ataque de rede que envolve o envio de pacotes de várias portas de origem aleatórias ou falsificadas para várias portas de destino em um sistema ou rede visado. Este ataque tem dois objetivos: primeiro, sobrecarregar as capacidades de processamento da vítima, causando interrupções de serviço ou na rede, e segundo, pode ser usado para procurar portas abertas e identificar serviços vulneráveis. A inundação é conseguida através do envio de um grande volume de pacotes, que pode saturar os recursos de rede da vítima e esgotar as capacidades dos seus firewalls e sistemas de detecção de intrusões. Para mitigar esses ataques, é essencial aproveitar os recursos da detecção automatizada em linha.

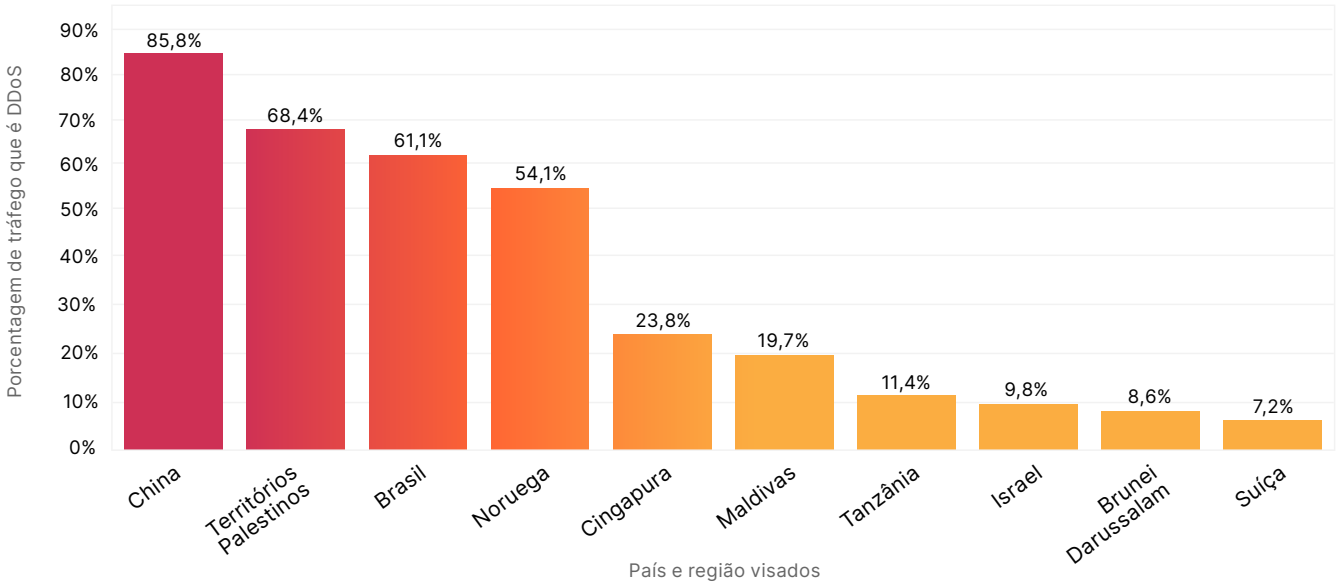
Principais regiões atacadas

Principais países visados por ataques DDoS por HTTP em relação ao tráfego de cada país



O Iraque, os territórios palestinos e o Marrocos assumem a liderança como as regiões mais atacadas no que diz respeito ao seu tráfego total de entrada. O interessante é que Cingapura aparece em quarto lugar. Cingapura não apenas enfrentou a maior quantidade de tráfego de ataques DDoS por HTTP (4% de todo o tráfego de DDoS global), mas esse tráfego malicioso também representou uma quantidade significativa do tráfego HTTP total com destino a Cingapura. Por outro lado, os EUA foram o segundo mais atacado em volume de tráfego de DDoS (3,8% de todo o tráfego de DDoS global), mas ficaram em quinquagésimo lugar quando normalizados pelo tráfego HTTP total com destino aos EUA.

Principais países visados por ataques DDoS na camada de rede em relação ao tráfego de cada país



As tendências da camada de rede por região são ainda mais acentuadas do que na camada de aplicação.

A China continua a ser o país mais visado na camada de rede em 2023. A China é o país mais atacado pelo tráfego de ataques DDoS na camada de rede, e também no que diz respeito a todo o tráfego vinculado da China, o que é ainda mais dramático do que as tendências de DDoS por HTTP em Cingapura. Quase 86% de todo o tráfego com destino à China foi mitigado pela Cloudflare como ataques DDoS na camada de rede. Para três outras regiões, os territórios palestinos, o Brasil e a Noruega, mais de um em cada dois bytes para aquelas regiões transportou um ataque DDoS.

Recomendações e conclusões

Melhores práticas	Otimize seu uso da Cloudflare
Atualizar ou fazer um plano de resposta à negação de serviço	Tem certeza que seu fornecedor de segurança fornece uma linha direta de emergência 24 horas por dia, 7 dias por semana. A linha direta Sob ataque da Cloudflare fornece conhecimento, processos e tecnologia de segurança para lidar com ataques em tempo real. Teste o processo de resposta a incidentes e os acordos de nível de serviço (SLAs) dos seus fornecedores de segurança antes de um ataque DDoS real. Identifique e treine o pessoal sobre seu plano de resposta contra DDoS documentado. Certifique-se de que eles leiam o roteiro de aprendizagem sobre DDoS da Cloudflare para otimizar os controles da Cloudflare.
Implantar inteligência contra ameaças e soluções de mitigação de DDoS automatizadas e em linha. Os centros de depuração manual não são escaláveis para ataques modernos de alto volume e curtos intervalos.	Use diversas técnicas de detecção para otimizar sua postura de segurança diante do cenário de ameaças em constante evolução: 1. Impressão digital dinâmica sem estado. 2. Classificação baseada em aprendizado de máquina. 3. Detecção de tráfego anômalo. 4. Perfil de tráfego e mitigação com estado. 5. Inteligência contra ameaças sobre atividades e tendências atuais de DDoS.
Atualizar sua rede, DNS e infraestrutura de aplicativos para ser mais resiliente ao seu perfil de tráfego.	Garanta que a capacidade das sua solução de mitigação de DDoS seja grande o suficiente para lidar com o dobro dos maiores ataques já registrados e o dobro das taxas máximas do seu tráfego legítimo. Garanta que seu fornecedor de segurança possa mitigar as vulnerabilidades mais recentes dos protocolos de rede e da camada de aplicação. Transfira o tráfego DNS para plataformas em nuvem seguras e compatíveis com o tráfego roteado através de redes de borda mais próximas do usuário.
Melhorar o desempenho da rede e dos aplicativos para evitar gargalos.	Utilize uma sala de espera digital para garantir que usuários e visitantes reais sejam informados sobre o período de espera sem sobrecarregar os servidores de aplicativos. Otimize o armazenamento em cache e gerencie melhor as cargas com uma rede de distribuição de conteúdo (CDN) e soluções de balanceamento de carga baseadas em nuvem.
Usar um modelo de segurança positivo: garantir que o tráfego desejado chegue de maneira confiável.	Mantenha protocolos, IPs, ASNs, portas e agentes de usuários críticos para a empresa abertos para limpar o tráfego. Use validação de esquema e um gateway de API para tráfego de APIs.
Aproveitar a inteligência artificial para ficar à frente das ameaças emergentes.	Pontuações de bots que podem ser usadas dentro de regras de firewall e de limitação de taxa. Descubra automaticamente suas APIs públicas e proteja-as contra ataques DDoS.

Na Cloudflare, queremos tornar ainda mais fácil, e gratuito, para organizações de todos os tamanhos se protegerem até mesmo contra os maiores e mais complexos ataques DDoS. Fornecemos proteção contra DDoS gratuita e ilimitada a todos os nossos clientes desde 2017, quando fomos pioneiros no conceito.

Saiba mais sobre como se defender contra as ameaças DDoS mais recentes com a Cloudflare.

+55 (11) 3230.4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

REV:BDES-5497.2024FEB08