CLOUDFLARE

Relatório sobre ameaças de DDoS da Cloudflare

T2 2023

Conteúdo

Sumário executivo

Boas-vindas ao relatório trimestral de negação de serviço distribuída (DDoS) da Cloudflare dos meses de abril a junho de 2023. Este relatório revela insights e tendências sobre o cenário de ameaças de DDoS observadas em toda a rede global da Cloudflare nesse segundo trimestre de 2023.

O segundo trimestre de 2023 foi caracterizado por ondas de campanhas de ataques DDoS bem planejadas, personalizadas e persistentes.

Na camada HTTP, detectamos os grupos hacktivistas pró-Rússia REvil, Killnet e Anonymous Sudan que estão muito ativos contra sites ocidentais e um aumento nos ataques DDoS altamente randomizados e de baixo volume. No último trimestre, os ataques DDoS baseados em DNS tornaram-se o vetor de ataques DDoS mais comum, com 32% de todos os ataques DDoS direcionados ao protocolo DNS. Na camada UDP, observamos ataques que aproveitam uma vulnerabilidade zero-day (CVE-2022-26143, TP240PhoneHome) que divulgamos em março de 2022.

Além de campanhas de ataque específicas, detalhamos as tendências de ataques à camada de aplicação e de rede juntamente com as variações por setor e região. Por fim, fornecemos orientações sobre como fortalecer proativamente sua segurança para garantir a continuidade dos serviços em um cenário de ameaças de DDoS em constante evolução.

Uma versão interativa deste relatório está disponível no Cloudflare Radar.

Destaques do relatório

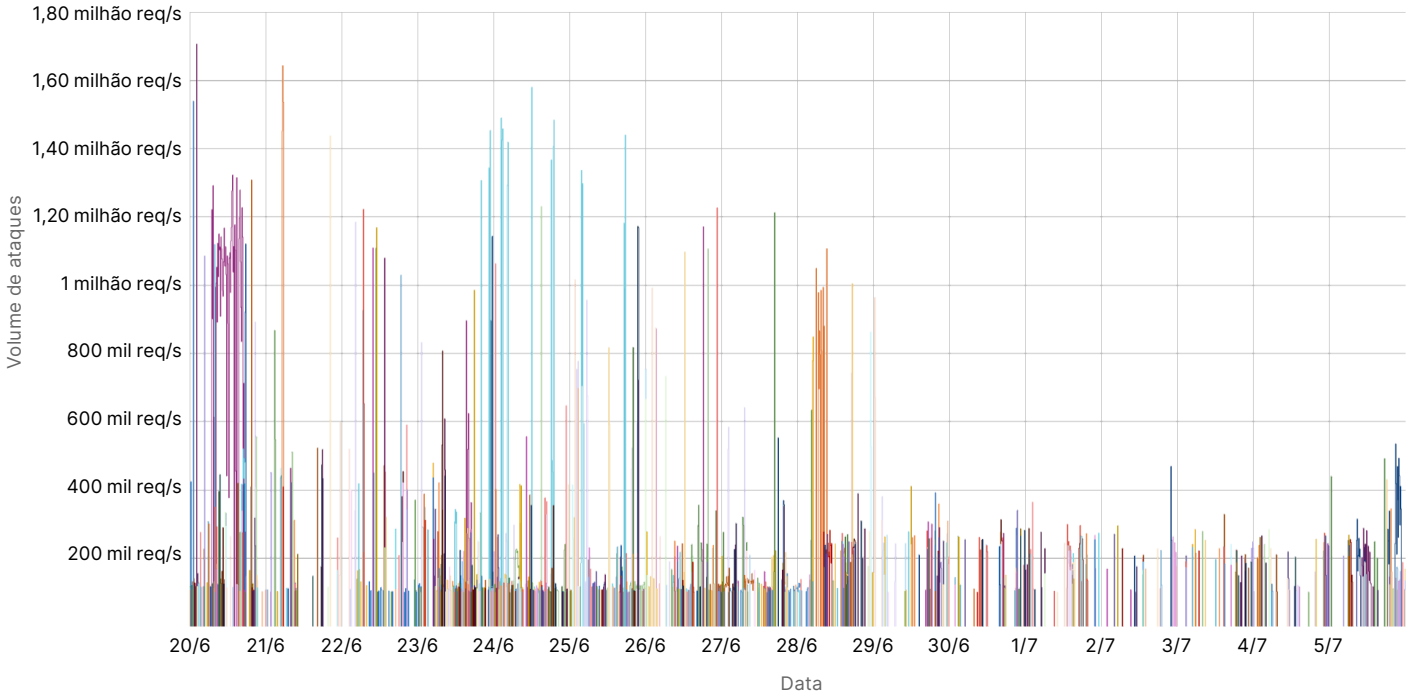
Aliança de hacktivistas apelidada de "Darknet Parliament" em ação

Em 14 de junho, grupos hacktivistas pró-Rússia, incluindo Killnet, um ressurgimento do REvil e Anonymous Sudan, anunciaram que uniram forças e ficaram conhecidos como “Darknet Parliament”.

Os seus objetivos declarados são executar ataques cibernéticos “massivos” ao sistema financeiro ocidental, incluindo os bancos ocidentais, o Sistema da Reserva Federal dos EUA e a rede SWIFT (Sociedade para Telecomunicações Financeiras Interbancárias Mundiais).

Neste trimestre, o Darknet Parliament lançou até 10.000 ataques DDoS contra sites protegidos pela Cloudflare. No entanto, os sites de serviços bancários e financeiros foram apenas o nono setor mais atacado, com base nos ataques que vimos contra os nossos clientes como parte desta campanha. Nossos sistemas detectaram e mitigaram automaticamente os ataques associados a esta campanha.

10.000 ataques do Killnet, REvil e Anonymous Sudan no T2 de 2023 em todos os setores



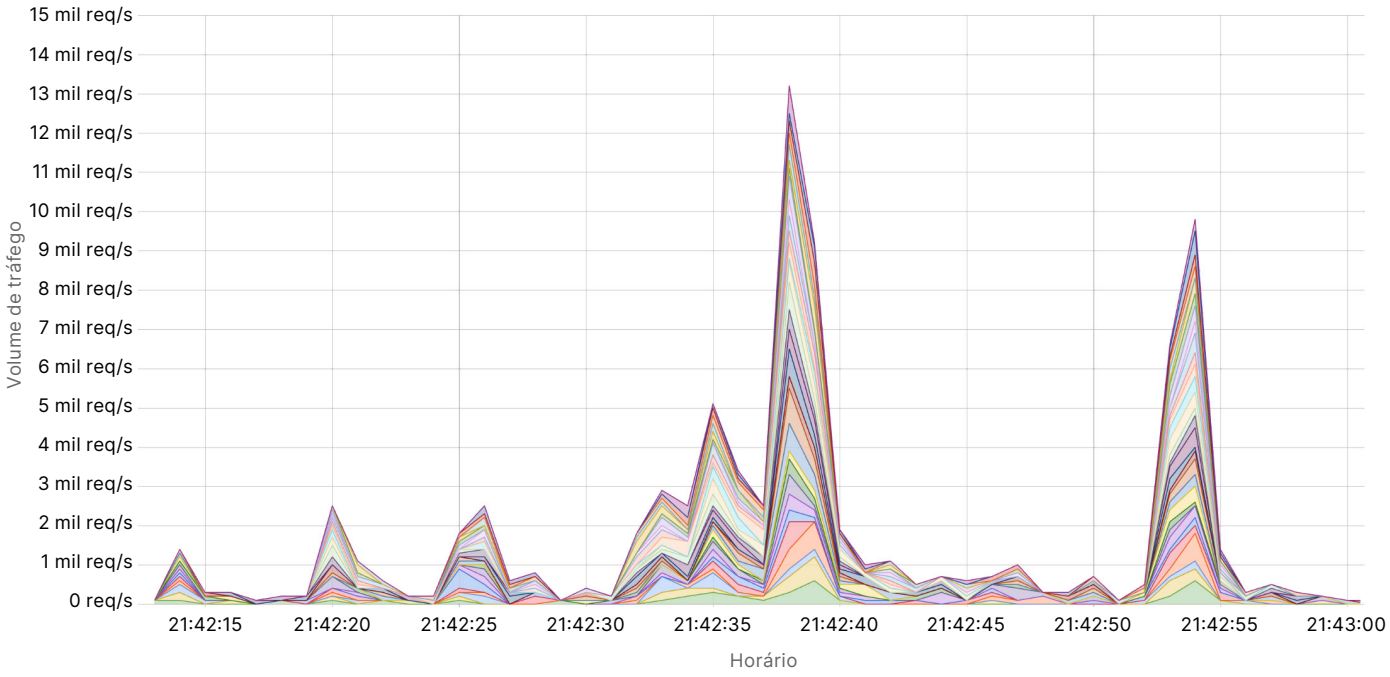
Ataques DDoS por HTTP altamente randomizados e de baixo volume

Um ataque DDoS por HTTP é um ataque DDoS realizado através do Protocolo de Transferência de Hipertexto (HTTP). Ele tem como alvo ativos da internet que utilizam o HTTP, como sites e gateways de APIs. Observamos um aumento nos ataques DDoS por HTTP de baixo volume e altamente randomizados nos últimos meses. Anteriormente, esta era uma tática utilizada principalmente por agentes bem financiados e patrocinados por estados.

Parece que os agentes de ameaças por trás desses ataques os projetaram deliberadamente para superar os sistemas de mitigação, imitando habilmente o comportamento do navegador dos usuários com muita precisão. Em alguns casos, eles introduzem um alto grau de randomização em diversos ativos, como agentes de usuário e impressões digitais JA3.

Fornecemos abaixo um exemplo de tal ataque. Cada cor representa um recurso de randomização diferente.

Volume de tráfego HTTP ao longo do tempo para um ataque DDoS por HTTP de baixo volume e altamente randomizado



Ataques DDoS de lavagem de DNS

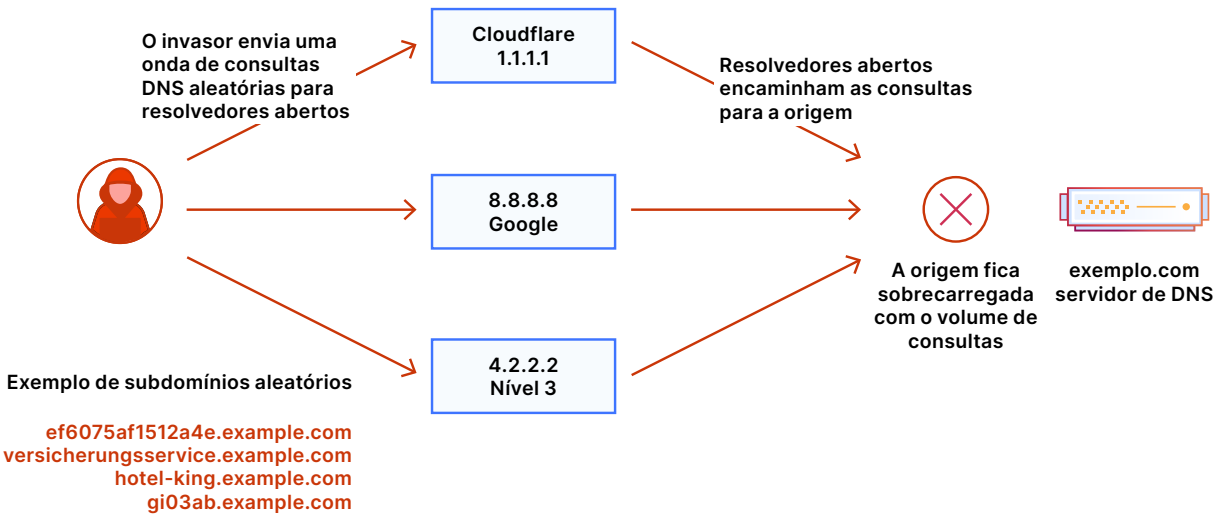
No último trimestre, os ataques DDoS baseados em DNS se tornaram o vetor de ataques DDoS mais comum, com 32% de todos os ataques DDoS direcionados ao protocolo DNS. O Domain Name System, ou DNS, atua como a lista telefônica da internet. O DNS ajuda a traduzir o endereço do site amigável para humanos (por exemplo, www.cloudflare.com) em um endereço de IP amigável para máquinas (por exemplo, 104.16.124.96). Ao interromper os servidores de DNS, os invasores afetam a capacidade das máquinas de se conectarem a um site e, ao fazer isso, tornam os sites indisponíveis para os usuários.

Um tipo preocupante e de rápido crescimento é o ataque de lavagem de DNS. Ele pode representar sérios desafios para organizações que operam seus próprios servidores de DNS autoritativos. Um ataque de lavagem de DNS é o processo de fazer com que o tráfego ruim e malicioso pareça tráfego bom e legítimo, lavando-o por meio de resolvedores de DNS recursivos confiáveis. Isto é semelhante ao processo de fazer com que o “dinheiro sujo” pareça legal, também conhecido como lavagem de dinheiro.

Em um ataque de lavagem de DNS, o agente da ameaça consulta subdomínios de um domínio que é gerenciado pelo servidor de DNS da vítima. O prefixo que define o subdomínio é aleatório e nunca é usado mais do que uma ou duas vezes em tal ataque. Devido ao elemento de aleatoriedade, os servidores de DNS recursivos nunca terão uma resposta armazenada em cache e precisarão encaminhar a consulta para o servidor de DNS autoritativo da vítima. O servidor de DNS autoritativo é então bombardeado com tantas consultas que não consegue atender consultas legítimas ou até mesmo pode falhar completamente.

Uma grande instituição financeira asiática e um provedor de DNS da América do Norte estão entre as vítimas recentes de ataques desse tipo. A origem inclui servidores de DNS recursivos confiáveis, como o 8.8.8.8 do Google e o 1.1.1.1 do Clouflare. O domínio atacado é válido e deve atender a consultas legítimas. Consequentemente, os administradores de DNS não podem bloquear a origem do ataque nem bloquear todas as consultas ao domínio atacado. É um desafio distinguir entre consultas legítimas e maliciosas.

Cadeia de ataque de um ataque DDoS de lavagem de DNS

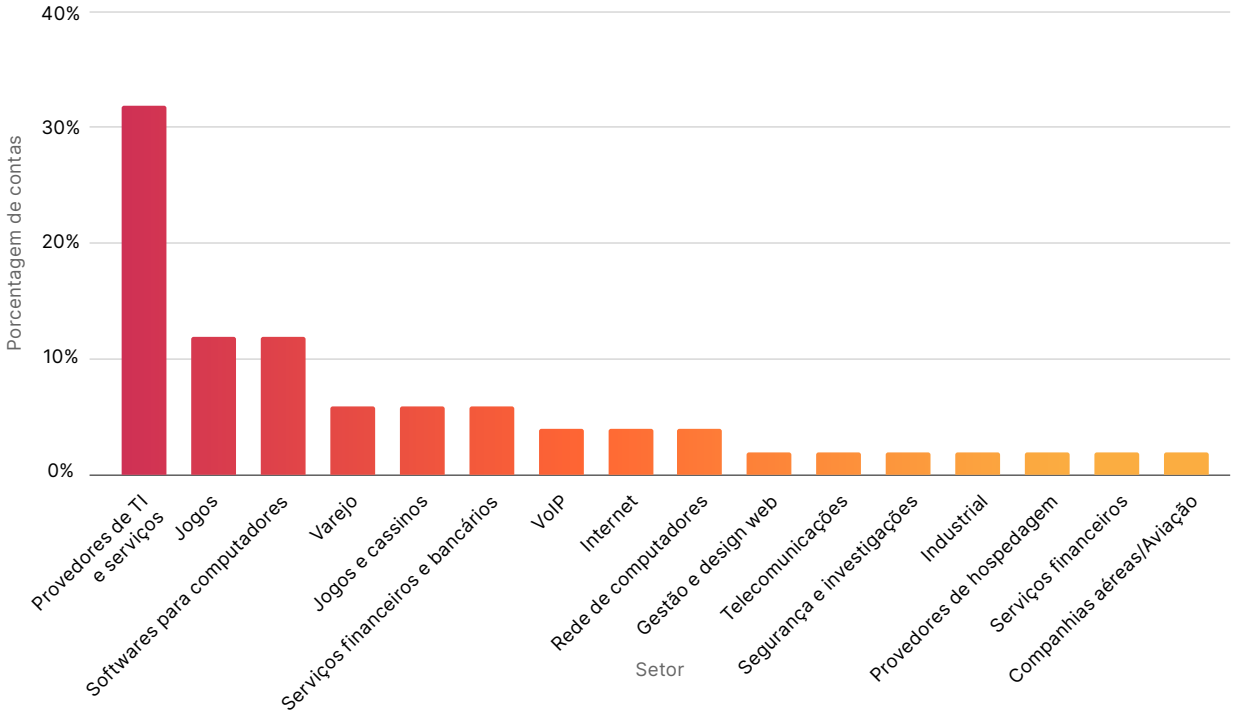


"Startblast": explorando as vulnerabilidades da Mitel para ataques DDoS

Na camada UDP, observamos ataques aproveitando uma vulnerabilidade zero-day (CVE-2022-26143, TP240PhoneHome) que divulgamos em março de 2022. Juntamente com outros membros da comunidade InfoSec, identificamos esta vulnerabilidade no sistema telefônico empresarial Mitel MiCollab, expondo o sistema a ataques DDoS por amplificação de UDP.

O nome da campanha “Startblast” vem do comando de depuração de mesmo nome que é essencial para explorar esta vulnerabilidade. Detectamos a maioria dos ataques direcionados a provedores de serviços e de TI, mais do que ao setor de jogos. Esse tipo de ataque cresceu mais rapidamente entre os ataques DDoS na camada de rede no último trimestre.

Campanhas do ataque Starblast por setor no T2 de 2023



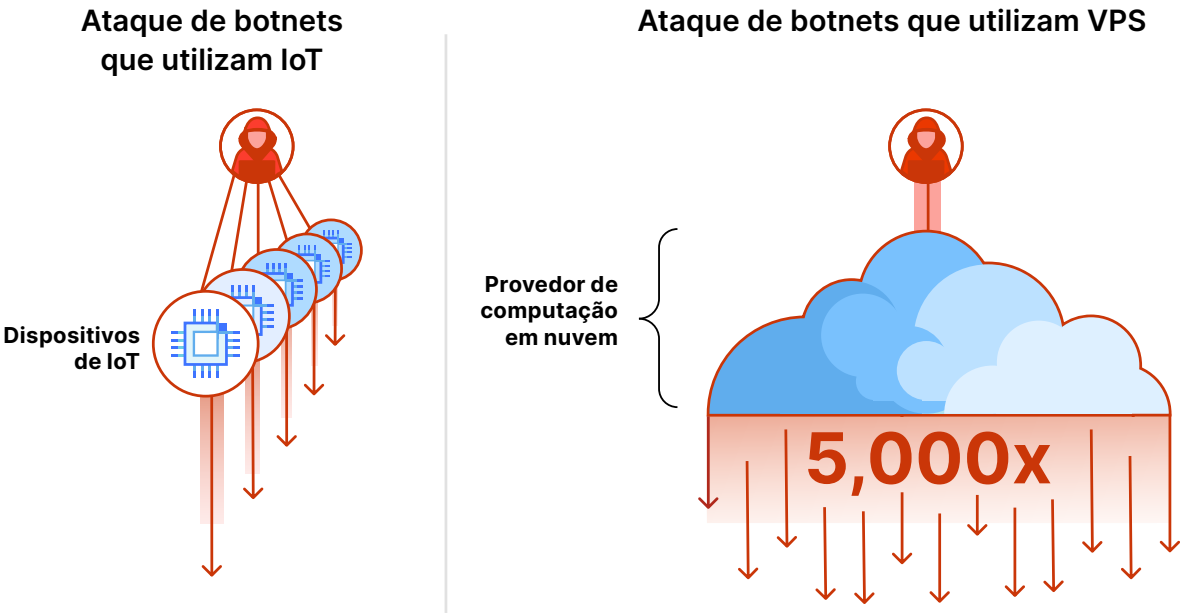
A ascensão contínua das botnets de alto desempenho

Conforme discutido no relatório sobre tendências de DDoS da Cloudflare no T1 de 2023, continuamos testemunhando uma evolução no DNA das botnets. A era das botnets de DDoS baseadas em VM chegou e com ela os ataques DDoS hipervolumétricos. Essas botnets são compostas por máquinas virtuais (VMs), ou servidores virtuais privados, (VPS), em vez de dispositivos da Internet das Coisas (IoT), o que as torna muito mais poderosas, até cinco mil vezes mais fortes.

A Cloudflare está colaborando com importantes provedores de computação em nuvem para combater essas novas botnets. Já notamos resultados iniciais: componentes significativos destas botnets foram neutralizados. Desde então, no T2 de 2023, não observamos mais ataques hipervolumétricos (na escala observada no T1 de 2023 e antes).

Nosso objetivo é automatizar e expandir ainda mais essa colaboração. Solicitamos que provedores de computação em nuvem, provedores de hospedagem e outros provedores de serviços gerais se juntem ao Botnet Threat Feed da Cloudflare.

Ele é gratuito para os provedores e não vendemos nossos dados a terceiros. Ele proporciona visibilidade dos ataques originados nas próprias redes dos prestadores de serviços, contribuindo com nossos esforços coletivos para desmantelar botnets.



Principais tendências de DDoS — T2 2023

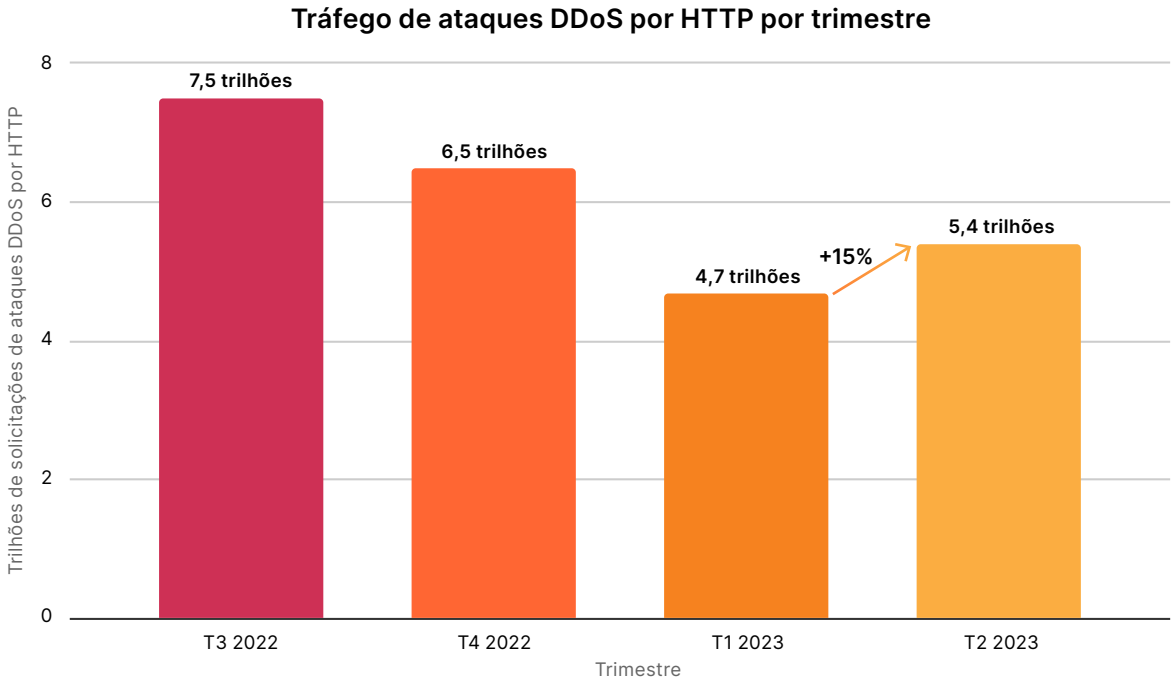
As seções do relatório a seguir vão analisar as principais tendências sobre quem e o que está sendo atacado.

Mudanças gerais no volume de tráfego

Os ataques DDoS nas camadas de aplicação e de rede diminuíram 35% e 14%, respectivamente, nos primeiros seis meses de 2023 em comparação com o mesmo período do ano passado. Na Cloudflare, também esperamos que essa tendência de declínio ano após ano continue, à medida que a Cloudflare e a comunidade de segurança da informação tornam as coisas mais difíceis e complicadas para os cibercriminosos.

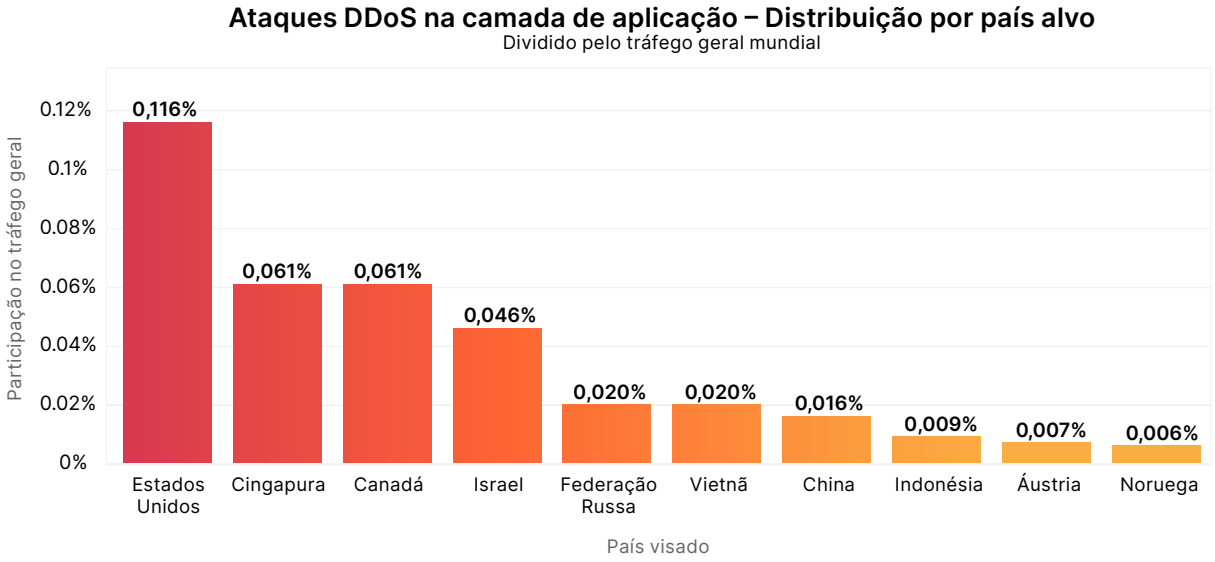
Um aviso de cautela: vimos um aumento de 15% nos ataques DDoS na camada de aplicação entre o T2 de 2023 e o mesmo período do ano passado. Não relaxe suas defesas ainda.

Em geral, os ataques DDoS por HTTP aumentaram em 15% em relação ao trimestre anterior, apesar de uma diminuição de 35% em relação ao ano anterior. Além disso, os ataques DDoS na camada de rede diminuíram neste trimestre em aproximadamente 14% em comparação com o trimestre anterior.



Principais países visados

No último trimestre, informamos que Israel foi o país mais atacado por ataques DDoS na camada de aplicação. Neste trimestre, os sites localizados nos Estados Unidos voltaram a liderar, com os sites de Cingapura e do Canadá em segundo e terceiro lugares, respetivamente. Os ataques direcionados a sites israelenses diminuíram 33%, passando a classificação do país para o quarto lugar.



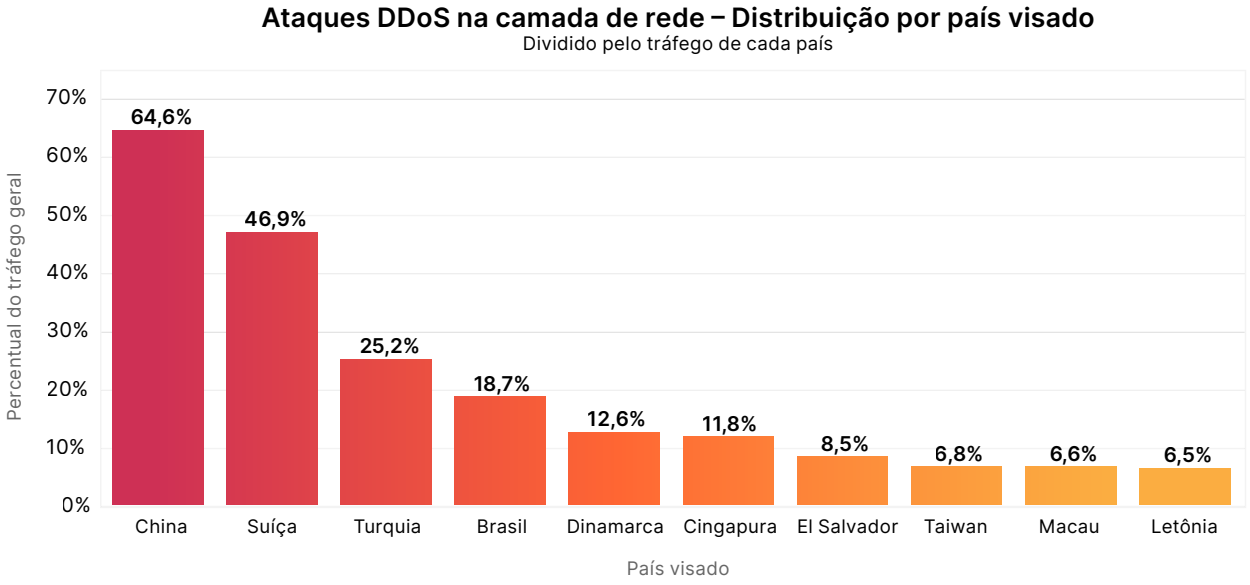
⚠ Duas vezes mais ataques DDoS na camada de aplicação

Os Estados Unidos recebem duas vezes mais ataques DDoS na camada de aplicação do que o próximo país mais atacado

⚠ Mais de 10%

Mais de 10% do tráfego geral da camada de aplicação da Palestina e São Cristóvão e Nevis é ocupado por ataques DDoS.

Na camada de rede, a China está de volta ao primeiro lugar em termos de ter o maior número de ataques DDoS na camada de rede. Dois em cada três bytes das redes chinesas foram ataques DDoS no segundo trimestre de 2023. E observamos uma parcela muito alta de tráfego malicioso para a China em vários trimestres. A situação única no T1 de 2023, onde 83% dos bytes para redes finlandesas transportavam ataques DDoS, retrocedeu. A Finlândia saiu dos dez principais países e regiões que enfrentam ataques DDoS.

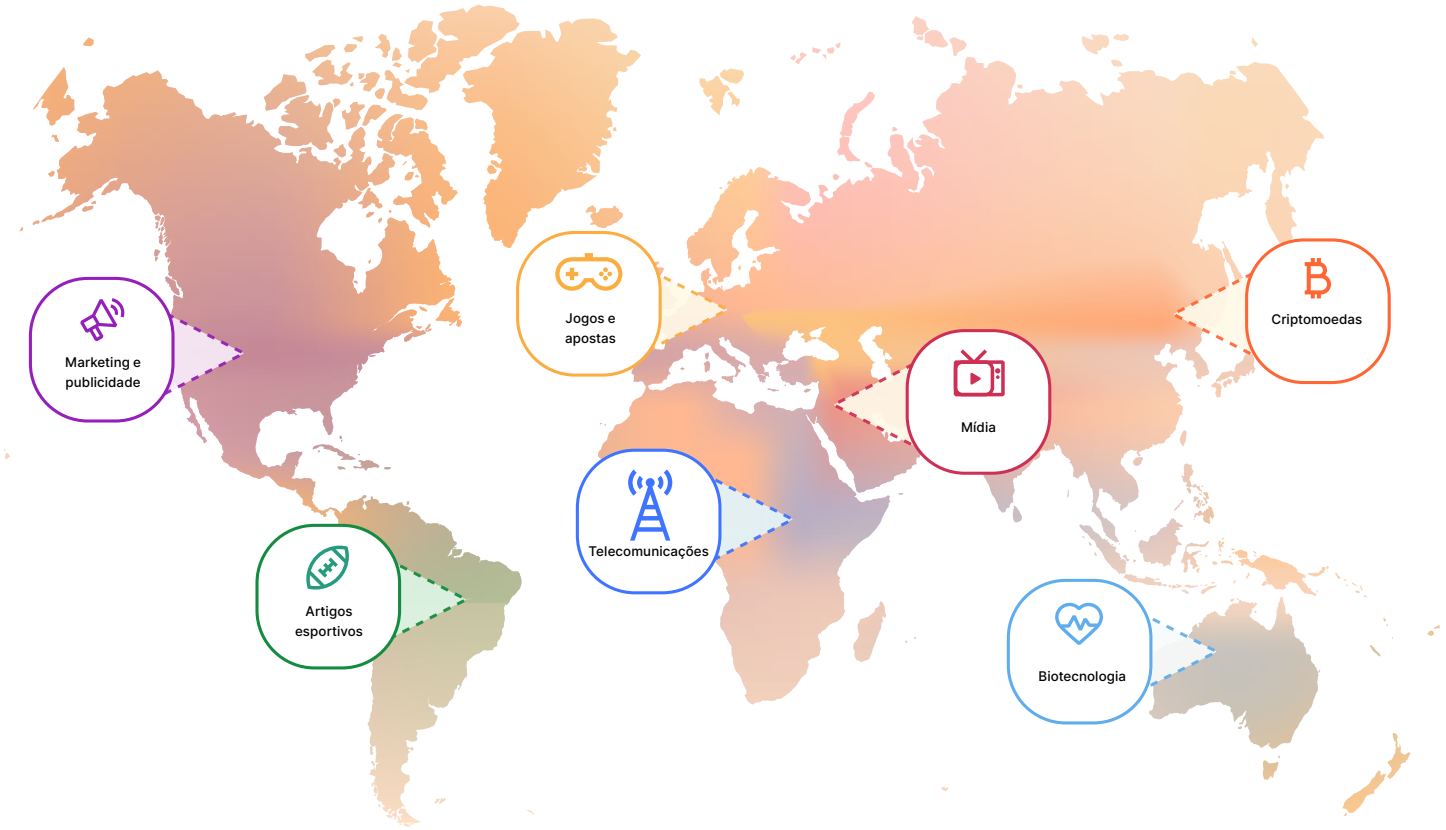


Variações por setor e região nos ataques DDoS

Os sites de criptomoedas foram alvo da maior quantidade de tráfego de ataques DDoS por HTTP no T2 de 2023. Seis em cada dez mil solicitações HTTP para sites de criptomoeda fizeram parte desses ataques. Isso representa um aumento de 600% em comparação com o trimestre anterior.

Os sites de jogos e apostas ficaram em segundo lugar, já que sua parcela de ataques aumentou 19% no T2 de 2023 em comparação com o T1 de 2023. Os sites de marketing e publicidade não ficaram muito atrás, ocupando o terceiro lugar, com pouca mudança em sua participação nos ataques.

Infelizmente, as organizações sem fins lucrativos enfrentam muitos ataques. Na verdade, 12% do tráfego HTTP para organizações sem fins lucrativos foram ataques DDoS, o segundo maior setor em participação de tráfego. A Cloudflare protege mais de 2.271 organizações sem fins lucrativos em 111 países como parte do Projeto Galileo, que celebrou seu nono aniversário este ano. Nos últimos meses, uma média de 67,7 milhões de ataques cibernéticos, diariamente, tiveram como alvo organizações sem fins lucrativos.



Setores mais atacados por região

Recomendações e conclusões

Melhores práticas	Otimize seu uso da Cloudflare
Atualizar ou fazer um plano de resposta à negação de serviço	Você integrou os alertas e a inteligência contra ameaças da Cloudflare às suas operações de segurança? Você sabe como chegar a todos os colaboradores necessários em caso de ataque? Eles são treinados sobre o plano de resposta?
Implantar inteligência contra ameaças e soluções de mitigação de DDoS automatizadas e em linha.	Use diversas técnicas de detecção para lidar com as tendências de ataques listadas neste relatório: 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 infraestrutura para ser mais resiliente ao seu perfil de tráfego. **Melhorar o desempenho da rede e dos aplicativos para evitar gargalos.**	Garanta que a capacidade das suas ferramentas 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. Reduza automaticamente o teto de multiplexação HTTP/2 quando estiver sob ataque, habilitando o WAF. Utilize uma sala de espera digital. 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: garanta que o tráfego desejado chegue de maneira confiável.	Mantenha as portas que são importantes para sua empresa e estão em uso abertas. Use validação de esquema e um Gateway de API para tráfego de APIs.
Aproveitar a inteligência contra ameaças e 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.

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.

Assista o webinar sobre tendências de DDoS para saber mais sobre as ameaças emergentes e como se defender delas.

CLOUDFLARE

+55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

REV:BDES-4839.2023AUG28