# DDoS em Camada 7

## O que é e como se proteger

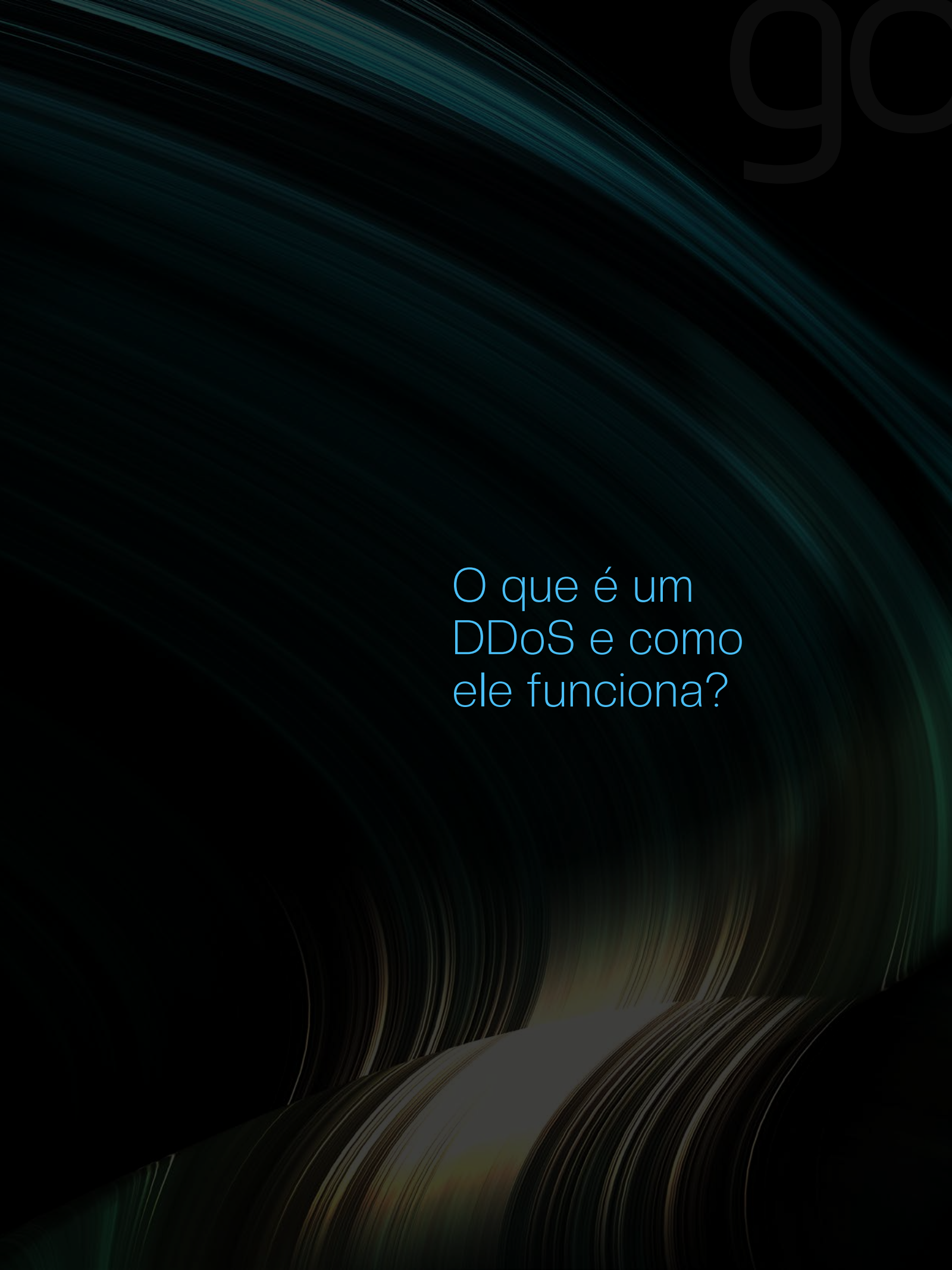
UM GUIA PARA INICIANTES

gocache

your apps safe.
your audience happy.

# Sumário

# SUMÁRIO


O que é um
DDoS e como
ele funciona?

# Um estudo recente mostrou que cerca de 75% dos tomadores de decisão de TI sofreram pelo menos um DDoS nos últimos 12 meses e 31% relataram interrupção do serviço como resultado desses ataques.

A cada dia mais e mais organizações comerciais e governamentais estão descobrindo da maneira mais difícil que o DDoS é uma ameaça que não pode ser ignorada.

E qual o segredo do "sucesso" do DDoS? Muitos ataques DDoS são bem-sucedidos não devido à habilidade ou recursos de quem faz o ataque, mas devido à falta de preparação do lado de quem precisa se defender.

Os gerentes de segurança, acostumados a lidar com ameaças como intrusões, explorações de aplicativos da web e worms, podem ainda não estar totalmente cientes de que lidar com DDoS requer uma gama de ferramentas de proteção web exclusiva e dedicada a isso.

Os ataques de negação de serviço distribuído (DDoS - Distributed denial of service) são uma subclasse de ataques de negação de serviço (DoS - denial of service). Um ataque DDoS envolve vários dispositivos online conectados, coletivamente conhecidos como botnets, que são usados para sobrecarregar um site de destino ou aplicação com tráfego falso.

O DDoS também pode ser usado como cortina de fumaça para outras atividades maliciosas e para derrubar dispositivos de segurança, violando o perímetro de segurança do alvo.

Um ataque de negação de serviço bem-sucedido é um evento altamente perceptível que afeta toda uma base de usuários online. Isso o torna uma arma popular de escolha para hacktivistas, extorsionistas e qualquer outra pessoa que queira defender uma causa ou um ponto de vista.

Os ataques DDoS podem ocorrer em explosões curtas ou ataques repetidos, mas de qualquer forma o impacto em um site ou empresa pode durar dias, semanas e até meses, à medida que a organização tenta se recuperar. Isso pode tornar o DDoS extremamente destrutivo para qualquer organização online. Entre outras coisas, os ataques DDoS podem levar à perda de receita, corroer a confiança do consumidor, forçar as empresas a gastar fortunas em compensações e causar danos à reputação a longo prazo.

Se você administra um projeto online e ainda não sabe por onde começar a proteger sua aplicação, as perguntas básicas abaixo podem ajudar a dar os primeiros passos. Perguntas básicas importantes incluem:

1# Quais ativos de infraestrutura precisam de proteção?

2# Quais são os pontos fracos ou pontos únicos de falha?

3# O que é necessário para derrubá-los?

4# Como e quando você saberá que é o alvo? Será tarde demais?

5# Quais são os impactos (financeiros e outros) de uma interrupção prolongada?

De posse dessas informações, é possível priorizar suas preocupações, examinando várias opções de mitigação de DDoS dentro da estrutura do seu orçamento de segurança.

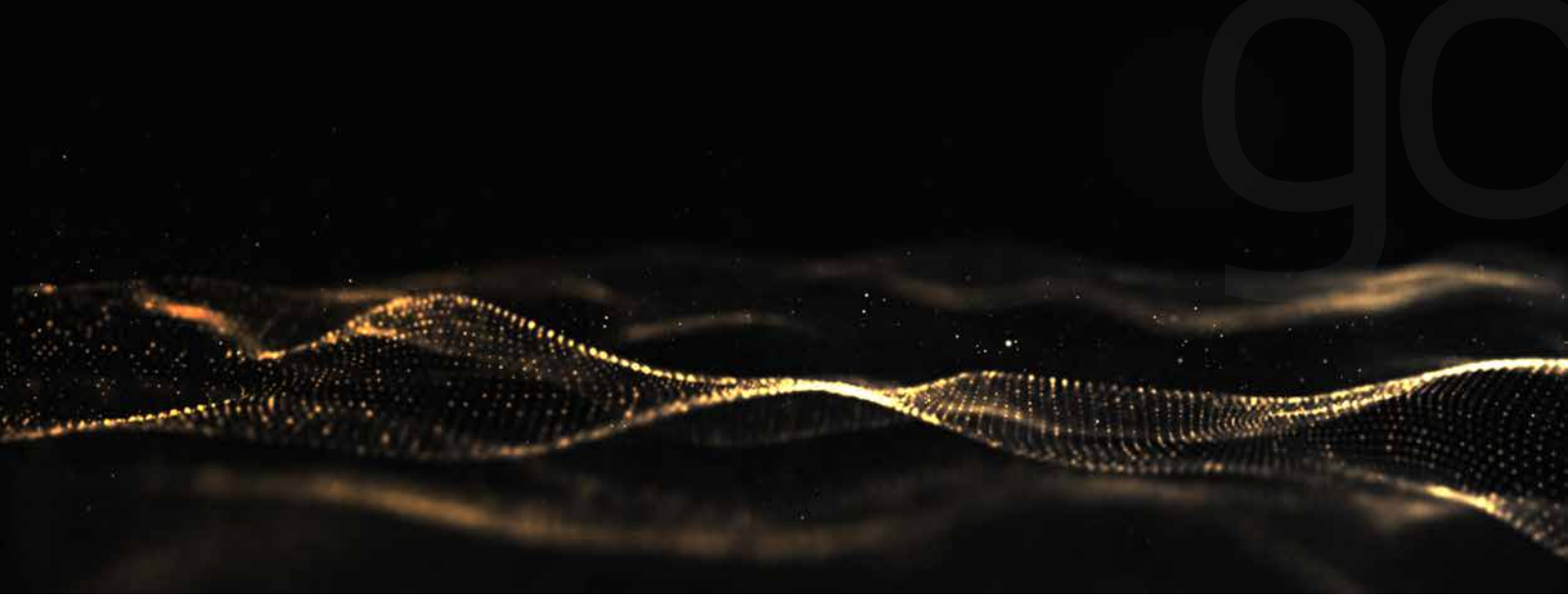
Se você estiver executando um site comercial ou aplicativos online (por exemplo, aplicativos SaaS, banco online, comércio eletrônico), provavelmente desejará proteção 24 horas por dia, 7 dias por semana, sempre ativa. Um grande escritório de advocacia, por outro lado, pode estar mais interessado em proteger sua infraestrutura – incluindo servidores de e-mail, servidores FTP e plataformas de back office – do que o seu site. Este tipo de negócio pode optar por uma solução "on demand".

O segundo passo é escolher o método de implantação. A maneira mais comum e eficaz de implementar proteção contra DDoS sob demanda para os seus principais serviços de infraestrutura em uma sub-rede inteira é por meio do protocolo de gateway de fronteira (BGP - border gateway protocol). No entanto, isso funcionará apenas sob demanda, exigindo que você ative manualmente a solução de segurança em caso de ataque.

Consequentemente, se você precisar da proteção contra DDoS sempre ativa no seu aplicativo da Web, use o redirecionamento de DNS para redirecionar todo o tráfego do site (HTTP/HTTPS) por meio da rede do provedor de proteção contra DDoS (geralmente integrada a uma rede de entrega de conteúdo, conhecidas como CDNs). A vantagem dessa solução é que a maioria das CDNs oferece escalabilidade e plantão NOC para absorver ataques  volumétricos, ao mesmo tempo que minimiza a latência e acelera a entrega de conteúdo.

# Diferença de DDoS para DoS

- Facilidade de detecção/mitigação
- Velocidade de ataque
- Volume de tráfego
- Forma de execução
- Rastreamento das fontes



O primeiro passo para entender a diferença entre ataques DoS vs DDoS é entender o que é um ataque DoS (ataque de negação de serviço). A seção a seguir elucidará o mesmo.

Em um ataque de negação de serviço, um site ou servidor é preenchido com tráfego de bot inorgânico ou é sobrecarregado por um terceiro. O terceiro geralmente é um invasor com intenções maliciosas.

O tráfego sobrecarregado pode ser gerado até vários gigabytes por segundo. Cada site ou servidor é construído com um certo nível de capacidade de hospedagem e o tráfego é gerado para exceder esse limite. Quando o limite é excedido, os usuários orgânicos ou reais têm dificuldade para acessar o site, o acesso é negado ou o servidor ou site trava, deixando de operar.

Um ataque DoS também tem uma versão atualizada no setor, que é conhecida como um ataque DDoS. A seção a seguir elucidará brevemente o que é um ataque DDoS.

A principal diferença entre um DoS e um DDoS é que o primeiro é um ataque sistema a sistema, enquanto o último envolve vários sistemas atacando um único sistema. Existem

outras diferenças, no entanto, envolvendo sua natureza ou detecção, incluindo:

## Facilidade de detecção/mitigação

Como um DoS vem de um único local, é mais fácil detectar sua origem e cortar a conexão. Na verdade, um firewall proficiente pode fazer isso. Por outro lado, um ataque DDoS vem de vários locais remotos, disfarçando a sua origem.

## Velocidade de ataque

como um ataque DDoS vem de vários locais, ele pode ser implantado muito mais rápido do que um ataque DoS originado de um único local. A maior velocidade de ataque torna a detecção mais difícil, o que significa danos maiores ou até mesmo um resultado catastrófico.

## Volume de tráfego

Um ataque DDoS emprega várias máquinas remotas (zumbis ou bots), o que significa que ele pode enviar quantidades muito maiores de tráfego de vários locais simultaneamente, sobrecarregando um servidor rapidamente de uma maneira que escapa à detecção.

## Forma de execução

um ataque DDoS coordena vários hosts infectados com malware (bots), criando uma botnet gerenciada por um servidor de comando e controle (C&C - command-and-control). Em contraste, um ataque DoS normalmente usa um script ou uma ferramenta para realizar o ataque a partir de uma única máquina.

## Rastreamento das fontes

O uso de um botnet em um ataque DDoS significa que rastrear a origem real é muito mais complicado do que rastrear a origem de um ataque DoS.

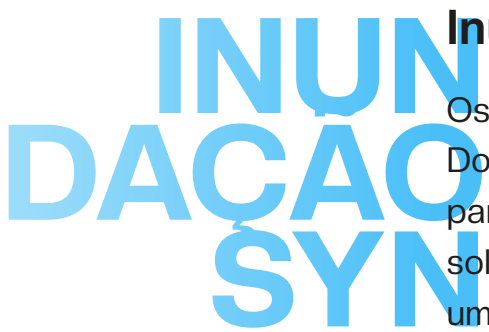
# Quais são os principais tipos de ataque DDoS

- Inundação SYN
- Slowloris
- Inundação HTTP
- Inundações de XML-RPC do WordPress
- SSL Exhaustion
- APIs DDoS

Os ataques DDoS são a mais complexa das duas ameaças, porque usam uma variedade de dispositivos que aumentam a gravidade dos ataques. Ser atacado por um computador não é o mesmo que ser atacado por uma botnet de cem dispositivos ou mais.

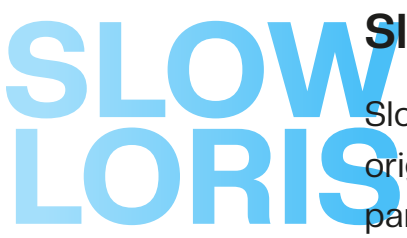
Parte de estar preparado para ataques DDoS é estar familiarizado com o maior número possível de formas de ataque. Nesta seção, veremos isso com mais detalhes para que você possa ver como esses ataques são usados para danificar as redes corporativas.

Os ataques DDoS podem vir de várias formas, incluindo:




## Inundação SYN

Os ataques de inundação SYN são outro tipo de ataque DoS em que o invasor usa a sequência de conexão TCP para tornar a rede da vítima indisponível. O invasor envia solicitações SYN para a rede da vítima, que responde com uma resposta SYN-ACK. O remetente deve responder com uma resposta ACK, mas, em vez disso, o invasor não responde (ou usa um endereço IP de origem falsificado para enviar solicitações SYN). Cada solicitação que não é respondida ocupa recursos de rede até que nenhum dispositivo possa fazer uma conexão.




## Slowloris

Slowloris é um tipo de software de ataque DDoS que foi originalmente desenvolvido por Robert Hansen ou RSnake para derrubar servidores web. Um ataque Slowloris ocorre quando o invasor envia solicitações HTTP parciais sem a intenção de completá-las. Para manter o ataque, o Slowloris envia periodicamente cabeçalhos HTTP para cada solicitação para manter os recursos da rede de computadores vinculados. Isso continua até que o servidor não possa fazer mais conexões. Essa forma de ataque é usada por invasores porque não requer nenhuma largura de banda.


## Inundação HTTP

Em um ataque de Inundação HTTP, os usuários do invasor solicitam HTTP GET ou POST para lançar um ataque a um servidor ou aplicativo da web individual. Inundações HTTP são um ataque de camada 7 e não usam pacotes malformados ou falsificados. Os invasores usam esse tipo de ataque porque exigem menos largura de banda do que outros ataques para tirar a rede da vítima de operação.


## Inundações de XML-RPC do WordPress

Nesse tipo de ataque, o invasor explora pingbacks do WordPress, entre outros, realizando comparativos antes de configurar o ataque. Inundações de HTTP aleatórias e inundações de desvio de cache são os ataques DDoS de Camada 7 mais amplamente reconhecidos.


## SSL Exhaustion

SSL é um método de criptografia, usado por diversos protocolos de comunicação de rede para aprimorar a segurança e aumentar a privacidade. Conforme mais transações e serviços passam a ser protegidos por SSL, naturalmente os ataques a serviços também vem aumentando. Tratam-se de ataques DDoS de exaustão baseados em conexão TCP, utilizados há anos para interromper serviços e que foram adaptados para atacar serviços de SSL.


## APIs DDoS

Em grande maioria, os ataques de API DDoS acabam se concentrando não apenas nos servidores que sua API está sendo executada, mas também em cada endpoint de serviços de API. Isso produz resultados drásticos para a integridade de suas APIs, principalmente em casos de ataques bem-sucedidos.

# O que é um ataque DDoS de Camada 7?

- Como funcionam os ataques de camada
- Diferença de um DDoS em Camada 7 para Camada 3 e 4
- Por que os ataques DDoS da Camada 7 são perigosos?

Ataques DDoS de camada 7, também chamados de ataques DDoS I7, é o termo que descreve um ataque que visa invadir a camada superior em uma construção de modelo OSI onde a solicitação da web, por exemplo, HTTP GET e HTTP POST ocorrem.

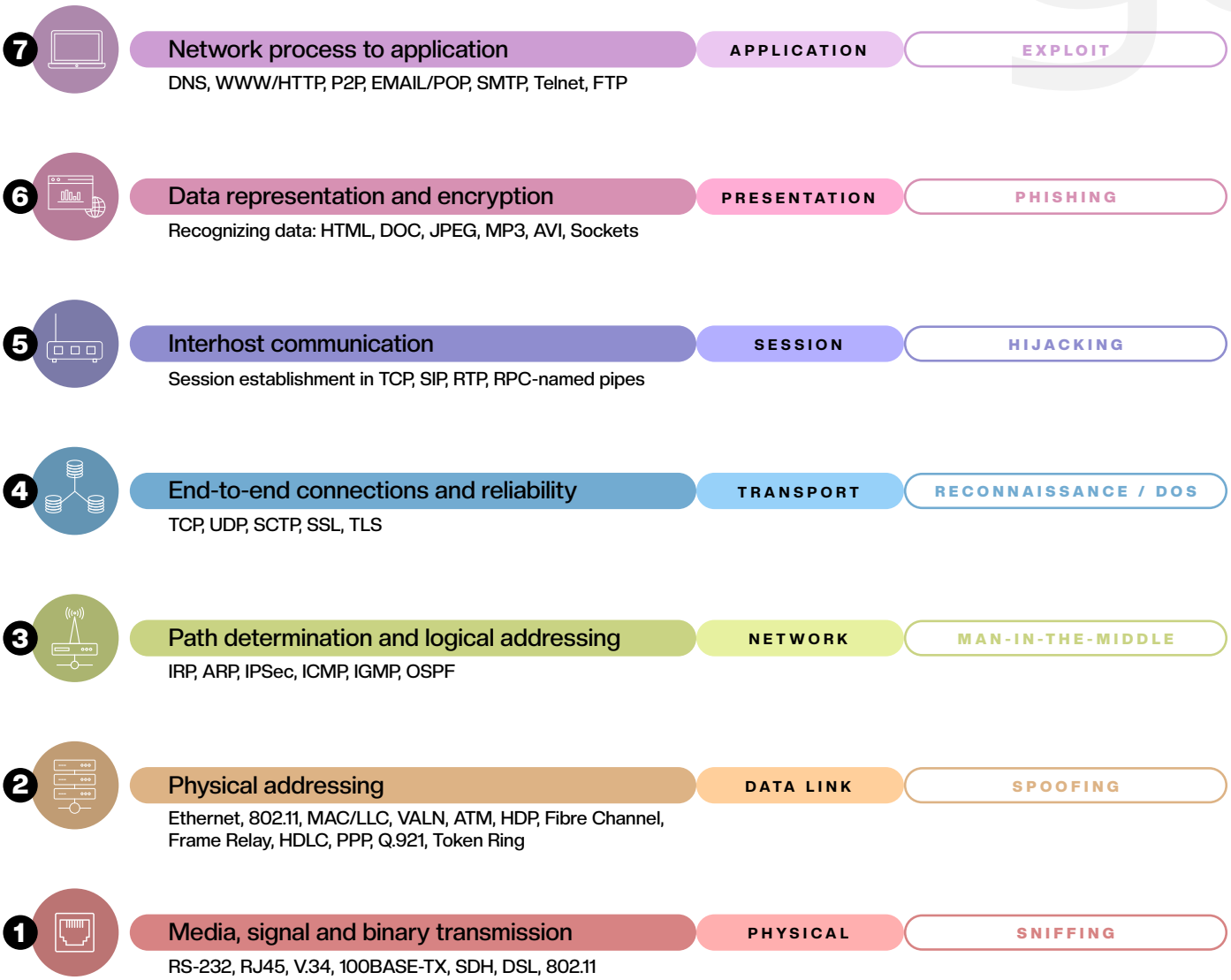
## Diferença de um DDoS em layer 7 para layer 3 e 4

No modelo OSI, a camada 3 compreende os protocolos e tecnologias que tornam as redes interconectadas possíveis. Na camada 3, os dados são divididos em pacotes e esses pacotes são endereçados e enviados aos seus destinos. O protocolo mais importante para esse processo é o Protocolo de Internet (IP).

A camada 4, por sua vez, envolve o uso de protocolos de transporte como o TCP e o UDP, que garante que os dados serão enviados para o lugar certo.

Por fim, a camada 7 é responsável por prover serviços para aplicações, de modo a separar a existência de comunicação em rede entre processos de diferentes computadores.

Os protocolos da camada de aplicação atuam junto com os protocolos da camada de transporte (TCP/IP e UDP), sendo os principais FTP, DNS, HTTP, HTTPS, RTP e TLS.




**Modelo OSI - 7 camadas de rede**

Como a camada 3 não tem conexão, os ataques DDoS não precisam abrir uma conexão com o TCP ou indicar atribuições de portas. Para realizar o ataque, o invasor envia um grande volume de tráfego de rede indesejado por meio dos protocolos de redes. Os ataques DDoS de camada 3 têm como alvo o software de rede que está sendo executado em um computador, em vez de uma porta específica.

O atacante busca se passar como um usuário legítimo distribuindo as requisições web em diferentes pontos para não extrapolar um padrão humano, passando os headers de requisição de forma adequada, entre outros exemplos.

Um ataque em camada 7 tem poder de gerar indisponibilidade com menos uso de banda se comparado aos ataques em camada 3 e 4, principalmente com aplicações que consomem um número alto de APIs que precisa se conectar com banco de dados, entre outros sistemas.

## Por que os ataques DDoS da camada 7 são perigosos?

Isolar o tráfego comum de solicitações maliciosas gera muitos custos em uma infraestrutura, principalmente quando ela está sendo atacada por um botnet executando uma inundação HTTP.

Os ataques à camada de aplicativo visam atingir um sistema versátil que pode incorporar a capacidade de impedir que o tráfego como chegue a um servidor, dependendo das diretrizes pré definidas, e que estão sujeitas a alterações. A utilização de ferramentas, por exemplo, WAF pode ajudar a diminuir qualquer tráfego malicioso de chegar ao servidor de origem, diminuindo o impacto do ataque em geral.

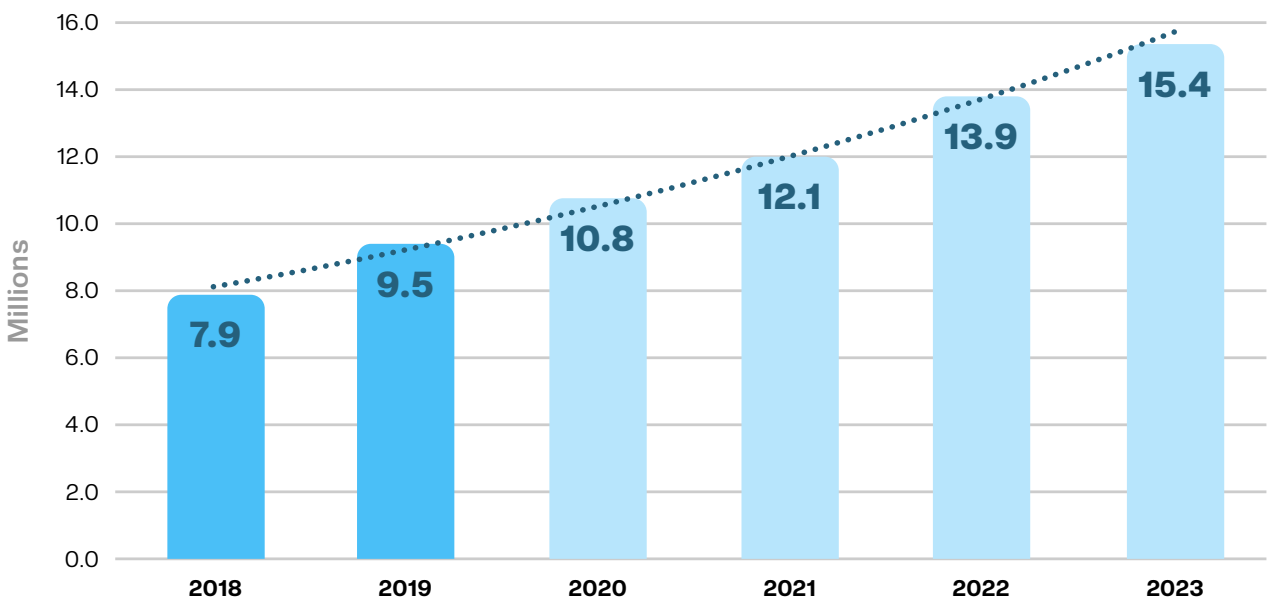
A justificativa de por que os ataques DDoS de camada 7 são tão perigosos é porque a maioria das organizações não estão preparadas para suportar ataques volumétricos e bem estruturados. Atualmente, poucos sites podem lidar e conter o volume de solicitação criado por um ataque de L7.

# Principais DDoS da História

- Google, 2020
- AWS, 2020
- Bryan Krebs e OVH, 2016
- Dyn, 2016
- GitHub, 2018
- Empresa europeia de jogos de azar (sigiloso), 2021
- Occupy Central, 2014
- CloudFlare, 2014
- Spamhaus, 2013
- Seis Bancos, 2012

O primeiro ataque de negação de serviço distribuído conhecido ocorreu em 1996, quando a Panix, agora um dos provedores de serviços de Internet mais antigos, ficou offline por vários dias por uma inundação SYN, uma técnica que se tornou um clássico ataque DDoS.

Nos anos seguintes, os ataques DDoS se tornaram comuns e a Cisco prevê que o número total de ataques DDoS dobrará dos 7,9 milhões vistos em 2018 para em torno de mais de 15 milhões até 2023.




**Relatório Anual Cisco - 2018-2023**

No entanto, não é apenas o número de ataques DDoS que está aumentando. Atores de ameaças estão criando botnets cada vez maiores – os exércitos de dispositivos hackeados que são usados para gerar tráfego DDoS. À medida que as botnets aumentam, a escala dos ataques DDoS também aumenta.

Um ataque de negação de serviço distribuído de um gigabit por segundo é suficiente para tirar a maioria das organizações da Internet, mas agora estamos vendo tamanhos de ataque de pico superiores a um terabit por segundo gerados por centenas de milhares ou mesmo milhões de dispositivos subornados.

## Os dez ataques DDoS mais famosos (por enquanto)

Para fornecer informações sobre como são esses ataques "na natureza selvagem", vamos dar uma olhada em alguns dos ataques DDoS mais notáveis até hoje. Nossas escolhas incluem alguns ataques DDoS que são famosos por sua escala, enquanto outros são por causa de seu impacto e consequências.

2020

### GOOGLE

Em 16 de outubro de 2020, o Threat Analysis Group (TAG) do Google postou uma atualização no blog sobre como as ameaças e os atores de ameaças estão mudando as suas táticas devido às eleições de 2020 nos EUA. No final do post, a empresa se esgueirou em uma nota: "... em 2020, nossa equipe de engenharia de confiabilidade de segurança mediu um ataque recorde de amplificação de UDP proveniente de vários ISPs chineses (ASNs 4134, 4837, 58453 e 9394), que continua sendo o maior ataque de largura de banda de que temos conhecimento."

Montado a partir de três ISPs chineses, o ataque a milhares de endereços IP do Google durou seis meses e atingiu um pico de tirar o fôlego de 2,5 Tbps! Damian Menscher, engenheiro de confiabilidade de segurança do Google, escreveu:

*O invasor usou várias redes para falsificar 167 Mpps (milhões de pacotes por segundo) para 180.000 servidores CLDAP, DNS e SMTP expostos, que então nos enviaram grandes respostas. Isso demonstra os volumes que um invasor com bons recursos pode alcançar: isso foi quatro vezes maior do que o ataque recorde de 623 Gbps do botnet Mirai um ano antes.*

2020

## AWS

O Amazon Web Services foi atingido por um gigantesco ataque DDoS em fevereiro de 2020.

Este é considerado um dos ataques DDoS recentes mais extremos de todos os tempos e teve como alvo um cliente não identificado da AWS, usando uma técnica chamada CLDAP - Connectionless Lightweight Directory Access Protocol.

Essa técnica depende de servidores CLDAP de terceiros vulneráveis e amplifica a quantidade de dados enviados para o endereço IP da vítima em até 70 vezes. O ataque durou três dias e atingiu um pico de 2,3 terabytes por segundo.

2016

## BRIAN KREBS
## OVH

Em 20 de setembro de 2016, o blog do especialista em segurança cibernética Brian Krebs foi atacado por um wwDDoS superior a 620 Gbps. O site de Krebs já havia sido atacado antes. Krebs registrou 269 ataques DDoS desde julho de 2012, mas esse ataque foi quase três vezes maior do que qualquer coisa que seu site ou a internet já tivessem visto antes.

A fonte do ataque foi o botnet Mirai, que, em seu auge no final daquele ano, consistia em mais de 600.000 dispositivos IoT comprometidos, como câmeras IP, roteadores domésticos e

players de vídeo. O botnet Mirai foi descoberto em agosto daquele mesmo ano, mas o ataque ao blog de Krebs foi sua primeira grande aparição.

O próximo ataque de botnet Mirai em 19 de setembro teve como alvo um dos maiores provedores de hospedagem europeus, a OVH, que hospeda cerca de 18 milhões de aplicativos para mais de um milhão de clientes. Este ataque foi contra um único cliente OVH não divulgado e foi impulsionado por cerca de 145.000 bots, gerando uma carga de tráfego de até 1,1 terabits por segundo. Durou cerca de sete dias, mas a OVH não foi a última vítima do botnet Mirai em 2016.

O botnet Mirai foi um avanço significativo em quão poderoso um ataque DDoS poderia ser. O tamanho e a sofisticação da rede Mirai eram sem precedentes, assim como a escala dos ataques e seu foco.

## 2016 DYN

Antes de discutirmos o terceiro ataque DDoS de botnet Mirai notável de 2016, há um evento relacionado que deve ser mencionado. Em 30 de setembro, alguém alegando ser o autor do software Mirai divulgou o código-fonte em vários fóruns de hackers e a plataforma Mirai DDoS foi replicada e alterada dezenas de vezes desde então.

Em 21 de outubro de 2016, a Dyn, uma grande provedora de serviços de nomes de domínio (DNS), foi atacada por uma inundação de tráfego de um terabit por segundo que se tornou o novo recorde para um ataque DDoS na época. Há algumas evidências de que o ataque DDoS pode ter alcançado uma taxa de 1,5 terabits por segundo.

O tsunami de tráfego derrubou os serviços da Dyn, tornando inacessíveis vários sites de alto perfil, incluindo GitHub, HBO, Twitter, Reddit, PayPal, Netflix e Airbnb. Kyle York, diretor de estratégia da Dyn, relatou: "Observamos dezenas de milhões de endereços IP discretos associados ao botnet Mirai que faziam parte do ataque".

O Mirai oferece suporte a ataques complexos e multivetoriais que dificultam a mitigação. Embora o botnet Mirai tenha sido responsável pelos maiores ataques até aquele momento, a coisa mais notável sobre os ataques Mirai de 2016 foi o lançamento do código-fonte do Mirai, permitindo que qualquer pessoa com habilidades modestas em tecnologia da informação criasse um botnet e montasse um ataque de negação de serviço distribuído sem muito esforço.

## 2018 GITHUB

Em 28 de fevereiro de 2018, o GitHub, uma plataforma para desenvolvedores de software, foi atingido por um ataque DDoS que atingiu 1,35 terabits por segundo e durou cerca de 20 minutos. De acordo com o GitHub, o tráfego foi rastreado "mais de mil sistemas autônomos (ASNs) diferentes em dezenas de milhares de endpoints exclusivos".

Embora o GitHub estivesse bem preparado para um ataque DDoS, suas defesas estavam sobrecarregadas. Eles simplesmente não tinham como saber que um ataque dessa escala seria lançado.

Como o GitHub explicou no relatório de incidentes da empresa: "No ano passado, implantamos um sistema de trânsito adicional em nossas instalações. Nós mais que dobramos nossa capacidade de trânsito durante esse

período, o que nos permitiu resistir a certos ataques volumétricos sem impacto para os usuários... Mesmo assim, ataques como esse às vezes exigem a ajuda de parceiros com redes de trânsito maiores para fornecer bloqueio e filtragem."

O ataque DDoS do GitHub foi notável por sua escala e pelo fato de que o ataque foi encenado explorando um comando padrão do Memcached, um sistema de cache de banco de dados para acelerar sites e redes. A técnica de ataque Memcached DDoS é particularmente eficaz, pois fornece um fator de amplificação – a proporção entre o tamanho da solicitação do invasor e a quantidade de tráfego de ataque DDoS gerado de até 51.200 vezes.

## 2021 AKAMI

Em fevereiro, a Akami anunciou que havia lidado com "três dos seis maiores ataques DDoS volumétricos" que a empresa já registrou. Os ataques DDoS foram tentativas de extorsão.

Os hackers lançam um ataque DDoS que o alvo não pode deixar de notar e depois exigem um pagamento para não fazer o mesmo novamente e em uma escala ainda maior. Nesse caso, o ataque de ameaça pesava 800 Gbps.

Este ataque foi notável não apenas por sua escala, mas também por sua novidade. Os invasores usaram um vetor de ataque DDoS inédito que era baseado em um protocolo de rede conhecido como protocolo 33 ou Protocolo de Controle de Congestionamento de Datagrama (DCCP - Datagram Congestion Control Protocol).

O ataque foi volumétrico e, ao abusar do protocolo 33, o exploit foi projetado para contornar as defesas focadas nos fluxos de tráfego tradicionais do Protocolo de Controle de Transmissão (TCP - Transmission Control Protocol) e do Protocolo de Datagrama do Usuário (UDP - User Datagram Protocol).

2014

# OCCUPY CENTRAL HONG KONG

O ataque DDoS PopVote de vários dias foi realizado em 2014 e teve como alvo o movimento popular de Hong Kong conhecido como Occupy Central, que fazia campanha por um sistema de votação mais democrático.

Em resposta às suas atividades, os invasores enviaram grandes quantidades de tráfego para três dos serviços de hospedagem na Web do Occupy Central, além de dois sites independentes, PopVote, um site de eleições simuladas on-line, e Apple Daily, um site de notícias, nenhum dos quais pertencente a Occupy Central, mas apoiou abertamente sua causa. Presumivelmente, os responsáveis estavam reagindo à mensagem pró-democracia do Occupy Central.

O ataque bombardeou os servidores do Occupy Central com pacotes disfarçados de tráfego legítimo. Ele foi executado usando não um, mas cinco botnets e resultou em níveis de tráfego de pico de 500 gigabits por segundo. Embora tenha sido relatado que os atacantes provavelmente estavam ligados ao governo chinês, nunca houve provas conclusivas e, perversamente, o ataque poderia ter a intenção de fazer o governo chinês parecer ruim. O ataque também pode ter fornecido cobertura para hackers que conseguiram extrair detalhes da equipe do Occupy Central de um banco de dados para montar uma extensa campanha de phishing subsequente.

2014

# CLOUD FLARE

Em 2014, CloudFlare, um provedor de segurança cibernética e rede de entrega de conteúdo, foi atingido por um ataque DDoS estimado em aproximadamente 400 gigabits por segundo de tráfego. O ataque, direcionado a um único

cliente CloudFlare e direcionado a servidores na Europa, foi lançado usando uma vulnerabilidade no Protocolo de Tempo para Redes (NTP - Network Time Protocol), que é usado para garantir que os relógios dos computadores sejam precisos. Embora o ataque tenha sido dirigido a apenas um dos clientes da CloudFlare, era tão poderoso que degradou significativamente a própria rede da CloudFlare.

Este ataque ilustra uma técnica em que os invasores usam endereços de origem falsificados para enviar respostas falsas do servidor NTP aos servidores do alvo do ataque.

Esse tipo de ataque é conhecido como "ataque de reflexão", pois o invasor é capaz de "rebater" solicitações falsas do servidor NTP, enquanto oculta seu próprio endereço. Devido a uma fraqueza no protocolo NTP, o fator de amplificação do ataque pode ser de até 206 vezes, tornando os servidores NTP uma ferramenta DDoS muito eficaz. Logo após o ataque, a equipe US Computer Emergency Readiness explicou que os ataques de amplificação de NTP são "especialmente difíceis de bloquear" porque "as respostas são dados legítimos provenientes de servidores válidos".

## 2014 SPAMHAUS

Em 2013, um enorme ataque DDoS foi lançado contra a Spamhaus, um provedor de inteligência de ameaças sem fins lucrativos. Embora a Spamhaus, como organização antispam, seja atacada regularmente e tenha serviços de proteção contra DDoS já implementados, esse ataque - um ataque de reflexão estimado em 300 gigabits de tráfego por segundo - foi grande o suficiente para derrubar site e parte dos serviços offline de e-mail.

O ataque cibernético foi atribuído a um membro de uma empresa holandesa chamada Cyberbunker, que aparentemente tinha como alvo a Spamhaus depois de colocar a empresa na lista negra por spam. Isso ilustra que empresas ou funcionários desonestos podem montar ataques DDoS com imensos danos à marca e sérias consequências legais.

# 2012 SEIS BANCOS

Em 12 de março de 2012, seis bancos dos EUA foram alvo de uma onda de ataques DDoS: Bank of America, JP Morgan Chase, US Bank, Citigroup, Wells Fargo e PNC Bank. Os ataques foram realizados por centenas de servidores sequestrados de uma botnet chamada Brobot, com cada ataque gerando mais de 60 gigabits de tráfego de ataque DDoS por segundo.

Na época, esses ataques eram únicos em sua persistência. Em vez de tentar executar um ataque e depois recuar, os criminosos bombardearam seus alvos com uma infinidade de métodos de ataque para encontrar um que funcionasse. Portanto, mesmo que um banco estivesse equipado para lidar com alguns tipos de ataques DDoS, eles eram impotentes contra outros tipos de ataque.

O aspecto mais notável dos ataques a bancos em 2012 foi que os ataques foram, supostamente, realizados pelas Brigadas Izz ad-Din al-Qassam, a ala militar da organização palestina Hamas. Além disso, os ataques tiveram um enorme impacto nos bancos afetados em termos de receita, despesas de mitigação, problemas de atendimento ao cliente e marca e imagem dos bancos.

# Consequências de um ataque DDoS

- Tempo de inatividade do site
- Problemas de servidor e hospedagem
- Vulnerabilidade do site
- Perda de receita
- Perda de produtividade
- Danos à reputação da marca
- Perda de participação de mercado
- Custos de resgate

Um ataque DDoS pode ter vários efeitos, dependendo da natureza do ataque e de como você está preparado para ele.

## Tempo de inatividade do site

O efeito mais imediato e óbvio é que o seu site fica sobrecarregado e fica indisponível. Isso significa que qualquer negócio obtido por meio do seu site não estará disponível para você até que o site funcione novamente. Isso também afeta a sua reputação como proprietário de um site ou aplicação. E se você não consertar o site rapidamente, isso pode afetar o seu SEO, pois se o Google rastrear o seu site e encontrá-lo indisponível, você perderá a classificação.

Se o seu site estiver indisponível por estar sobrecarregado, ele retornará um erro de gateway 502, o que afetará negativamente as suas classificações de pesquisa se você permitir que ele permaneça assim por muito tempo.

Também existem ataques em que o site não estava disponível há vários dias (porque o proprietário não sabia como corrigi-lo e não mantinha um backup), e quando o site voltou a ficar online, todos os links internos na listagem do Google desse site foram perdidos.

## Problemas em seu servidor de hospedagem

Se o seu site estiver sujeito a ataques regulares e você não toma medidas corretas para mitigar, isso pode levar a problemas com o seu provedor de hospedagem.

Um bom provedor de hospedagem fornecerá ferramentas para proteger o seu site contra ataques DDoS, mas se você não tiver isso e estiver em hospedagem compartilhada, os ataques podem afetar outros sites no mesmo servidor.

## Vulnerabilidade do site

Um ataque DDoS pode tornar o seu site mais vulnerável a hackers, pois todos os seus sistemas ficarão focados em colocar o site novamente online, e os sistemas de segurança podem ter sido desativados pelo ataque.

Os hackers podem achar mais fácil entrar no seu site por meio de uma porta dos fundos (backdoor) assim que o ataque DDoS conseguir paralisar o seu site. Ataques de acompanhamento como este nem sempre virão da mesma fonte que as solicitações que formaram o ataque DDoS: um hacker inteligente saberá como ocultar os seus rastros e usar vários endereços IP para atacar o seu site, bem como ocultar a sua verdadeira localização.

Portanto, se você for vítima de um ataque DDoS, uma das suas primeiras prioridades deve ser garantir que o seu site esteja seguro. Isso é sem dúvida mais importante do que colocar o seu site público em funcionamento novamente, pois outro ataque só o levará de volta à estaca zero (ou pior).

## Perda de receita

O tempo de inatividade pode ser extremamente caro, dependendo do tipo de negócio e do tamanho da organização. Uma hora de inatividade para uma instituição financeira versus uma hora de inatividade para uma rede universitária pode gerar custos muito diferentes, mas o impacto nos clientes ou usuários é significativo em ambos os casos.

No ano passado, o software da Veeam informou que uma hora de inatividade de um aplicativo de alta prioridade custa, em média, US$ 67.651, enquanto esse número é apenas um pouco menor, de US$ 61.642 para um aplicativo normal. Com esse equilíbrio entre alta prioridade e pensando nos custos de impacto, fica claro que "todos os dados são importantes" e que o tempo de inatividade é intolerável em qualquer cenário nos ambientes atuais."

## Perda de produtividade

Quando um aplicativo ou serviço de negócios é degradado, ou pior, fica completamente offline, isso geralmente significa que os funcionários não podem trabalhar com a mesma eficiência ou, em muitos casos, nem trabalhar. Isso ficou particularmente evidente durante a pandemia do COVID-19, pois uma porcentagem muito maior de funcionários agora trabalha remotamente e depende de conectividade confiável para colaborar com os seus colegas. Ao considerar o custo total de um ataque DDoS, os CISOs devem considerar o custo por hora do tempo de inatividade do funcionário.

## Danos à reputação da marca

Alguns setores – como jogos, hospedagem, datacenters e serviços financeiros – dependem muito da própria reputação de disponibilidade de serviço. Se os clientes não puderem confiar que um fornecedor estará on-line e disponível de forma consistente, eles podem facilmente divulgar isso on-line, por meio do Google Reviews ou de outros canais de mídia social. Para adquirir novos clientes em um mercado altamente competitivo, uma empresa deve manter uma reputação positiva.

## Perda de participação de mercado

Ataques DDoS podem criar rotatividade de clientes. Quando um usuário final tem acesso negado a aplicativos voltados

para a Internet ou se problemas de latência obstruem a experiência do usuário, isso pode afetar o resultado final, porque os clientes que não podem confiar em uma empresa para fornecer um serviço consistente podem ir para outro lugar para conduzir os seus negócios.

## Custos de resgate

Embora o ransomware seja um tipo distintamente diferente de ataque cibernético, nos últimos anos os invasores DDoS têm cada vez mais emparelhado ataques DDoS com demandas de resgate, ou seja, os invasores ameaçam uma organização mantendo os seus arquivos como reféns e ameaçando lançar um ataque DDoS em cima disso, a menos que a organização pague uma taxa de resgate exorbitante, normalmente em bitcoin. Não é sensato pagar uma taxa de resgate, mas convenhamos, às vezes as empresas o fazem.

Geralmente não é algo que vira notícia, porque as organizações não querem admitir publicamente que pagaram um resgate. Uma exceção foi o incidente Colonial Pipeline no início deste ano, no qual a empresa pagou US$ 5 milhões em resgate para ser libertada da sua posição de refém. E como foi o caso recentemente com a agência de serviços de saúde da Irlanda, às vezes, os cibercriminosos testam um sistema lançando ataques DDoS antes de instalar o ransomware.


Estratégias para mitigação de DDoS em Camada 7
• Limitação de Requisições
• Cache
• Validação de Requests
• Observabilidade

A camada 7, nos fornece muitas informações e possibilidades de manipulação de dados e requisições. com isso podemos trazer algumas metodologias de mitigação:

## Limitações de requisições

Utilizando o próprio código, é possível criar limitações em determinados pontos críticos da aplicação, como reset de senhas ou cadastro de usuários.

Além disso, é possível utilizar de configurações em WebServer que criem padrões de limitação de requests utilizando NGINX

## Cache

Um dos maiores problemas a serem enfrentados por quem sofre um ataque baseado em volumetria, é a indisponibilidade causada pela necessidade de responder muitas requisições, uma forma de mitigar os dados, é criando uma camada de cache, sendo possível a através de CDNs, plugins no Wordpress, ou até mesmo criando o seu próprio utilizando NGINX Content Caching.

## Validação de Requests

Uma outra forma de diminuir os impactos de um ataque DDoS e DoS, é criando no próprio funcionamento da aplicação validação baseadas em tokens, cookies e checagem de padrões de requests, validando como por exemplo, se há padrões de SQL Injection, usando regexp, pois só de fazer essa checagem e já retornar o 403, diminui o desgaste gerado em processamento, porém é importante salientar que isso ainda sim pode causar danos por depender de recursos da infraestrutura para realizar tal checagem a nível de aplicação

## Observabilidade

Outro ponto a ser considerado para alcançar o objetivo de mitigação de DDoS e DoS, é necessário implementar um sistema de observabilidade, para que possamos manter sobre nossos olhos e nossos radares, qualquer movimento e/ou ação que possa ser considerada suspeita, pois quanto antes detectado o ataque DDoS e DoS, maior é a tranquilidade para análise e mitigação do ataque e seus danos.

Os principais pontos que devem ser observados são:

- **Número geral de requests**

  Ataques por volumetria, costumam aumentar de maneira significativa o número geral de requests, sendo um ótimo ponto para gerar alertas.

- **Número de erros 5XX e 4XX**

  Quando o ataque encontra algum ponto sensível, tende a gerar erros de 5XX, e quando está em fase de escaneamento 4XX, podendo utilizar esses erros para criar uma perspectiva de em que momento está o ataque.

- **Tempo de resposta da hospedagem**

  Quando o ataque é massivo ou quando consegue gerar uma fila muito grande de requisições a serem processadas e respondidas, tende a aumentar o tempo de resposta do servidor, sendo mais em um sintoma de ataques de volumetria.

- **Volatilidade de tamanho médio de requests**

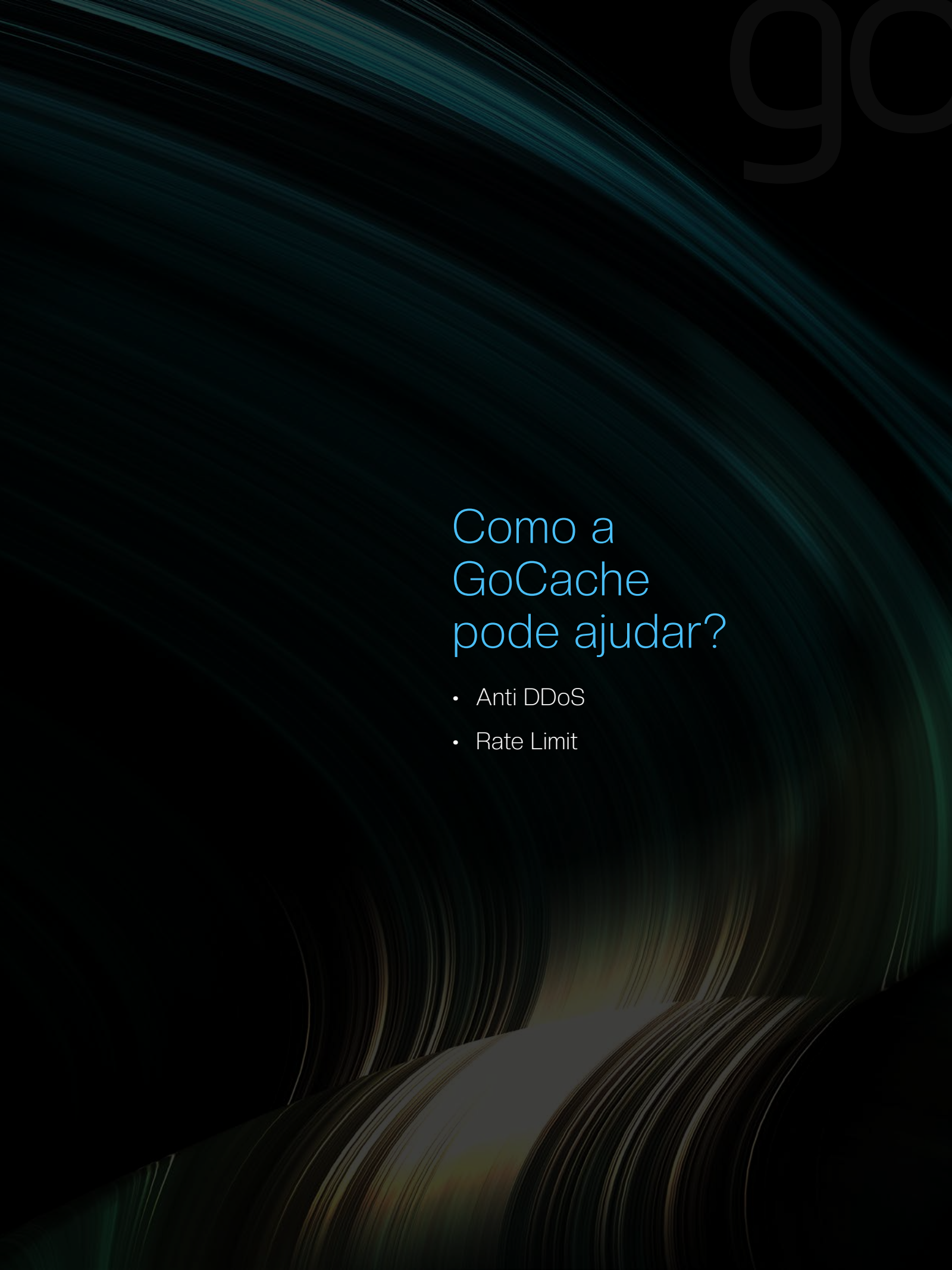
  Algumas estratégias de ataques DDoS tendem a gerar Requests quase vazias para validações de maneira rápida, ou ataques com requests densas, com intenção de causar problemas de processamento.

- **Top User Agents**

  Se atentar a UserAgents com padrões diferentes de navegação, utilizando UserAgends de linguagens de programação ou scrips, exemplo: Curl ou PythonRequests

- **Top URLs de requests**

  As URLs exploradas, tendem a ser URLs diferentes das convencionais, comumente explorando APIs ou URIs sensíveis, devendo fica atento a média de requests diarias das mesmas, para caso haja uma exploração, seja mapeado com tranquilidade.



# Como a GoCache pode ajudar?

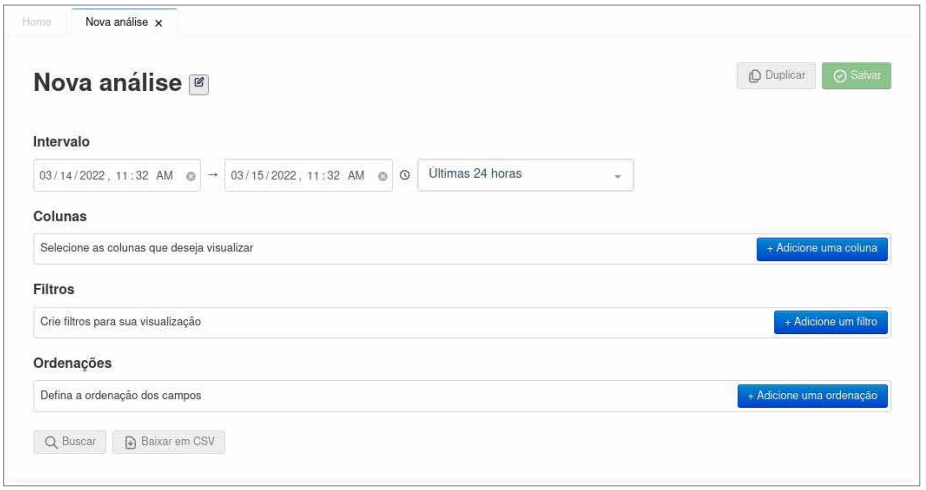
- Anti DDoS
- Rate Limit

O sucesso no combate aos ataques DDoS está diretamente relacionado à estratégia implementada. Independentemente do tamanho ou tipo de ataque, a GoCache oferece soluções inteligentes para reduzir o impacto dos ataques de negação de serviço. Algumas de nossas soluções são:

## Edge Insights

Antes de implementar um plano de ação para interromper qualquer ataque, é necessário que ele primeiramente seja detectado. O Edge Insights é a ferramenta perfeita para isso.

Basicamente, o Edge Insights é uma ferramenta de análises de logs com uma interface gráfica bastante amigável e intuitiva.



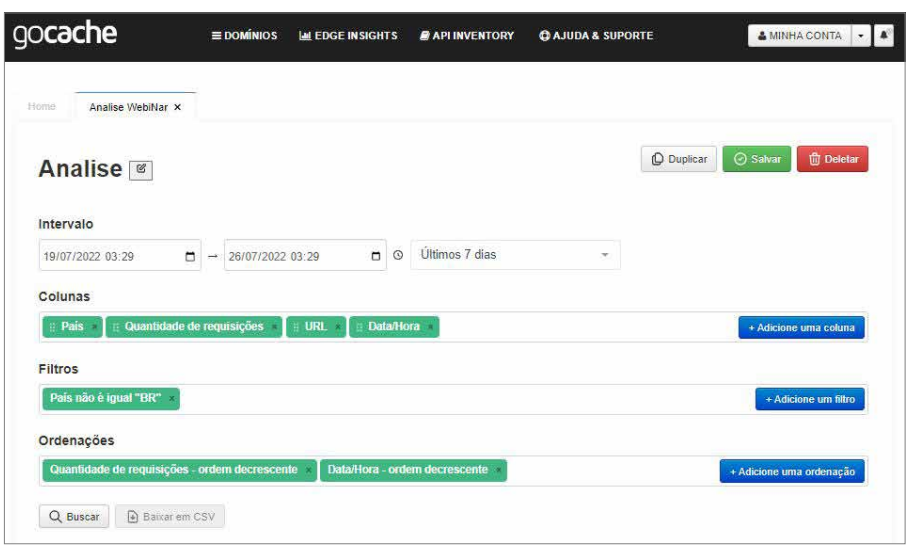

**Personalização de relatórios - Edge Insights**

Uma análise permite coletar dados específicos de sua aplicação, com base em filtros definidos e classificados conforme desejado. Por exemplo, ao definir padrões de acesso quando sua aplicação não estiver sob ataque, você

pode definir restrições seguras que não bloqueiam usuários legítimos. Após analisar e concluir que realmente se trata de um ataque DDoS é só manter  a calma e utilizar o Rate Limit.

## Rate Limit

Basicamente com o Rate Limit você poderá estipular uma taxa de acessos que um IP pode acessar sua aplicação, sendo possível definir diferentes limitação para diferentes endpoints, com diferentes tipos de critérios. Podendo assim ajudar na mitigação de ataques DDos. Vamos ver um exemplo da ferramenta na prática, para isso foi usada uma análise com o seguinte template utilizando o módulo de Edge Insights da GoCache.




**Template Edge Insights**

O Edge Insights retornou o seguinte resultado:

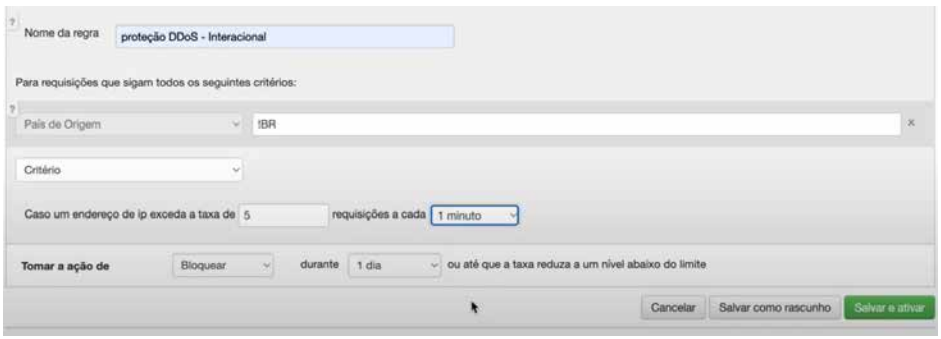
| | | | |
|---|---|---|---|
| Estados Unidos | 2 | http://www.treinamentogc.com.br/xmlrpc.php | 2022-06-22T07:24:19 |
| Estados Unidos | 2 | http://www.treinamentogc.com.br/xmlrpc.php | 2022-06-22T07:24:17 |
| Estados Unidos | 2 | http://www.treinamentogc.com.br/xmlrpc.php | 2022-06-22T07:24:16 |
| Estados Unidos | 2 | http://www.treinamentogc.com.br/xmlrpc.php | 2022-06-22T07:24:14 |
| Estados Unidos | 2 | http://www.treinamentogc.com.br/xmlrpc.php | 2022-06-22T07:24:13 |
| Estados Unidos | 2 | http://www.treinamentogc.com.br/xmlrpc.php | 2022-06-22T07:24:12 |
| Estados Unidos | 2 | http://www.treinamentogc.com.br/xmlrpc.php | 2022-06-22T07:24:11 |
| Estados Unidos | 2 | http://www.treinamentogc.com.br/xmlrpc.php | 2022-06-22T07:24:10 |
| Estados Unidos | 2 | http://www.treinamentogc.com.br/xmlrpc.php | 2022-06-22T07:24:08 |
| Estados Unidos | 2 | http://www.treinamentogc.com.br/xmlrpc.php | 2022-06-22T07:24:07 |

**Resultado Template Edge Insights**

Claramente encontramos um ataque, pois conseguimos elencar alguns fatores:

- Muitos acessos ao "xmlrpc" (uma das partes mais vulneráveis do WordPress);
- Acessos com um padrão de ataque escalável (a cada segundo, 2 acessos são feitos na área sensível da aplicação).

Sendo assim, já podemos criar nossa regra de proteção:




**Criando regra no Rate Limit**

Um ponto interessante a se destacar é que a ferramenta aceita Regex (Expressões Regulares) para criação de suas regras. Perceba que foi criada uma regra nem muito permissiva, nem muito restrita nesse cenário, o ataque consiste em 2 requisições por segundo, foi limitada a aplicação para países diferentes do Brasil (!BR) para que caso um endereço de IP exceda a taxa de 5 requisições por minuto, a ferramenta tome a ação de Bloquear durante 1 dia os acessos desse IP a aplicação. Clicando em salvar e ativar, a aplicação estará protegida contra esse ataque DDos mapeado.

# Estudo de Caso

- Case Evolua Educação


Como estudo de caso, compartilhamos um case de sucesso que temos dentro da GoCache em conjunto com o Grupo Evolua Comunicação, onde utilizamos recursos de segurança e observabilidade da GoCache para bloquear mais de 3 milhões de requisições maliciosas em um único dia.

## A Evolua Educação

Com mais de 20 anos de história, o Evolua Educação promove soluções educacionais, além de pesquisa e desenvolvimento de tecnologia, sendo o principal fornecedor de conteúdo para o mercado de sistema de ensino de qualificação profissional.

Oferecendo uma solução 360°, a Evolua Educação desenvolve soluções para entregar tudo pronto e deixar seus parceiros com tempo livre para uma gestão fluida, minimizando os desafios e multiplicando as chances de sucesso de seus parceiros.

## Qual era o desafio?

Pelo fato do Evolua Educação ser responsável por diversas aplicações web, as quais armazenam dados restritos, o Evolua Educação buscou as soluções de segurança da GoCache visando proteger suas aplicações contra ataques DDoS que poderiam gerar indisponibilidade, além de tentativa de bots invadirem sua aplicação através de brute-force de senha.

## Soluções utilizadas

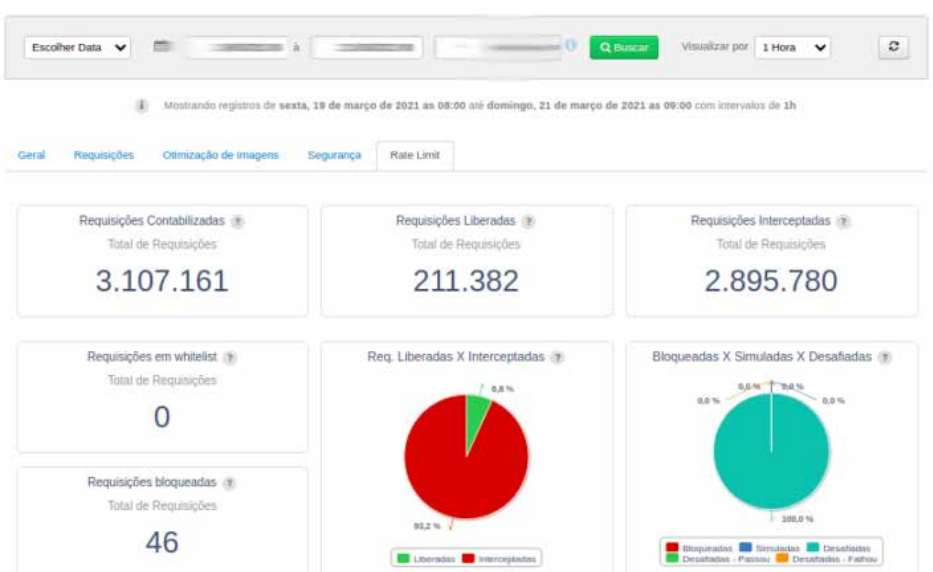
O Grupo Evolua Educação utilizou todo stack de segurança em camada 7 da GoCache visando a resolução dos problemas.

Primeiramente foram definidas nas políticas de segurança algumas regras de controles de acessos utilizando critérios de geolocalização, URI, método HTTP e user-agent, para bloquear o que divergia dos acessos comuns do seu negócio web.

O WAF foi importante na mitigação de acessos maliciosos que apresentavam algumas anomalias no protocolo HTTP, como ausência de headers da requisição, caracterizando-se como um acesso não humano.

A camada anti-ddos da GoCache foi essencial para evitar indisponibilidades geradas por ataques de volumetria. Abaixo, conseguimos identificar variações expressivas entre a média e máxima de requisições em um dia comum VS em um dia sob ataque.


E por último, o rate-limiting para estabelecer diferentes taxas máximas de requisições, para diferentes endpoints, visando bloquear acessos indesejados.



Abaixo vemos o Analytics em tempo real da GoCache com a timeline das requisições com picos superiores a 4 milhões de requests em uma única hora.


Já na imagem abaixo temos a visão em timeline dos recaptchas do rate-limiting em ação.


## Edge Insights: Visão apurada de bots maliciosos

O time da Evolua Educação também utilizou os recursos de Edge Insights da GoCache para observar quais bots maliciosos faziam requisições dentro da aplicação, permitindo entender nos detalhes o volume de requisições por país e user-agent.

| Quantidade de requisições | País | User-Agent | Status code |
|---|---|---|---|
| 547 | Estados Unidos | Mozilla/5.0 (compatible; proximic; +https://www.comscore.com/Web-Crawler) | 403 |
| 78 | Rússia | Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots) | 403 |
| 56 | Singapura | Mozilla/5.0 (compatible;PetalBot;+https://webmaster.petalsearch.com/site/petalbot) | 403 |
| 33 | Alemanha | Mozilla/5.0 (compatible; BLEXBot/1.0; +http://webmeup-crawler.com/) | 403 |
| 12 | Singapura | Mozilla/5.0 (Linux; Android 7.0;) AppleWebKit/537.36 (KHTML, like Gecko) Mobile Safari/537.36 (compatible; PetalBot;+https://webmaster.petalsearch.com/site/petalbot) | 403 |
| 10 | Estados Unidos | Mozilla/5.0 (compatible; Adsbot/3.1; +https://seostar.co/robot/) | 403 |
| 10 | Estados Unidos | Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.1.1 Safari/605.1.15 (Applebot/0.1; +http://www.apple.com/go/applebot) | 403 |
| 9 | Estados Unidos | Mozilla/5.0 (compatible; SurdotlyBot/1.0; +http://sur.ly/bot.html) | 403 |
| 8 | França | INETDEX-BOT/1.5 (Mozilla/5.0; https://inetdex.com/; info at inetdex dot com) | 403 |
| 6 | Rússia | Mozilla/5.0 (compatible; YandexFavicons/1.0; +http://yandex.com/bots) | 403 |
| 6 | França | Mozilla/5.0 (compatible; Barkrowler/0.9; +https://babbar.tech/crawler) | 403 |
| 6 | Irlanda | TprAdsTxtCrawler/1.1 | 403 |
| 6 | Estados | Mozilla/5.0 (compatible; ev-crawler/1.0; +https://headline.com/legal/crawler) | 403 |

## Resultados

Utilizando as ferramentas de Rate Limit da GoCache o time de infraestrutura da Evolua Educação conseguiu interceptar mais de 2.895.780 requisições em um único dia, reduzindo custos com infraestrutura e garantindo que a performance de suas aplicações não fossem prejudicadas.

Já o WAF da GoCache teve importante participação, bloqueando mais de 700 acessos maliciosos em um dia, garantindo que apenas usuários legitimos acessasem determinadas áreas da aplicação.

*"Estávamos sofrendo com alguns ataques web e a GoCache veio pra resolver. Uma ferramenta super granular, fácil de configurar, combinado com a expertise do time técnico foram essenciais para obtermos o sucesso e a tranquilidade da nossa operação."*

**Anderson Ilaris**
COO da Evolua Educação

# Fontes de consulta


**What Is a DDoS Attack?**
https://www.akamai.com/our-thinking/ddos

**9 Miths about DDoS Defense**
https://www.akamai.com/site/en/documents/white-paper/nine-myths-about-ddos-defense.pdf

**DDoS Protection - Reference Architecture**
https://www.akamai.com/site/en/documents/reference-architecture/ddos-protection-reference-architecture.pdf

**Distributed Denial of Service (DDoS)**
https://www.imperva.com/learn/ddos/denial-of-service/

**Prevent DDoS Attacks**
https://www.imperva.com/learn/ddos/how-to-prevent-ddos-attacks/

**DoS vs DDoS Attack: Key Differences**
https://intellipaat.com/blog/dos-and-ddos-attack/

**DoS vs. DDoS**
https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos

**Dos vs DDoS Attacks: The Differences and How To Prevent Them**
https://www.comparitech.com/net-admin/dos-vs-ddos-attacks-differences-prevention/

**Five Most Famous DDoS Attacks and Then Some**
https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

**16 Best DDOS Attack Tools in 2022**
https://lab.wallarm.com/16-best-ddos-attack-tools-in-2022/

**Top 15 DDoS Attack Tools [For Educational Purpose Only]**
https://allabouttesting.org/top-15-ddos-attack-tools/

**DDoS Attacks Explained: Causes, Effects, and How to Protect Your Site**
https://kinsta.com/blog/what-is-a-ddos-attack/

**The Damaging Impacts of DDoS Attacks**
https://www.corero.com/blog/the-damaging-impacts-of-ddos-attacks/

**Layer 7 DDoS Attacks**
https://www.wallarm.com/what/layer-7-ddos-attacks


gocache
your apps safe.
your audience happy.
gocache.com.br
/gocache