vivo empresas

Guia completo sobre DDoS

Entenda, proteja-se e minimize os riscos

Sumário

Introdução

Os ataques cibernéticos são uma ameaça crescente à segurança digital das empresas em todo o mundo. Entre as diversas modalidades de ataques, os ataques de negação de serviço distribuído (DDoS) se destacam pela capacidade de causar interrupções significativas nos serviços online, afetando diretamente a continuidade dos negócios.

Um ataque DDoS ocorre quando múltiplos dispositivos, geralmente comprometidos por meio de malware e organizados em uma botnet, são utilizados para enviar um grande volume de requisições maliciosas a um servidor, rede ou aplicação. O objetivo é sobrecarregar a capacidade de processamento e os recursos do sistema alvo, resultando em lentidão ou na completa indisponibilidade dos serviços. A diferença fundamental entre um ataque de negação de serviço (DoS) e um DDoS está na origem: enquanto o DoS provém de um único ponto de ataque, o DDoS é orquestrado a partir de várias fontes simultâneas, dificultando a detecção e mitigação.

A gravidade e a frequência dos ataques DDoS têm aumentado nos últimos anos, impulsionadas pela crescente digitalização das empresas e pela proliferação de dispositivos conectados à Internet. Em setores como finanças, saúde e serviços de internet, os impactos de um ataque podem ser devastadores, causando desde perda de receita até danos à reputação. Neste e-book, exploraremos os aspectos essenciais dos ataques DDoS, desde os conceitos básicos até estratégias avançadas de mitigação, para capacitar empresas e profissionais de TI a se protegerem contra essa ameaça crescente.

Sobre a Telefónica Tech

Somos a Telefónica Tech, transformamos o seu negócio através dos nossos serviços de Cibersegurança, Cloud, IoT, Big Data, Inteligência Artificial e Blockchain.

Habilitamos a transformação digital dos processos e negócios dos nossos clientes com uma combinação única dos melhores profissionais, tecnologias e plataformas. Além disso, contamos com o apoio de um ecossistema global de parceiros líderes no mercado.

Fazemos isso de forma simples para novos clientes, para facilitar e acelerar a adoção da tecnologia e fazer uma diferença real em cada negócio.

CAPÍTULO 1

Como funciona um ataque DDoS?

Um ataque de negação de serviço distribuído (DDoS) é uma tentativa maliciosa de interromper o funcionamento normal de um serviço online, sobrecarregando o servidor ou a rede com um fluxo massivo de tráfego. Diferente de um ataque de negação de serviço simples (DoS), que provém de uma única origem, os ataques DDoS são orquestrados a partir de múltiplas fontes, muitas vezes utilizando uma rede de dispositivos comprometidos, conhecidos como botnets. Esses dispositivos podem incluir computadores, servidores e até mesmo dispositivos da Internet das Coisas (IoT), como câmeras de segurança e roteadores.

A principal característica de um ataque DDoS é a capacidade de gerar tráfego volumoso e diversificado, dificultando a distinção entre requisições legítimas e maliciosas. Isso torna a mitigação mais desafiadora e aumenta o potencial de danos à infraestrutura do alvo.

Vetores de ataque comuns

Os ataques DDoS podem ser classificados em diferentes tipos, dependendo do método utilizado para gerar tráfego malicioso. Alguns dos vetores de ataque mais comuns incluem:

- **Amplificação de DNS**: esse tipo de ataque funciona como aquele amigo que transforma uma simples história em uma epopeia. Pequenas requisições de dados são amplificadas em pacotes gigantescos, inundando o alvo com tráfego malicioso e fazendo parecer que a rede está tentando contar a versão completa de 'O Senhor dos Anéis' de uma só vez. A técnica de amplificação explora a diferença entre o tamanho da solicitação enviada e o tamanho da resposta recebida, o que permite que os atacantes gerem um volume massivo de dados com pouco esforço.

- **HTTP Flooding**: consiste em enviar um grande número de requisições HTTP legítimas para esgotar os recursos do servidor. Este tipo de ataque é particularmente eficaz contra aplicações web e pode ser difícil de detectar, pois o tráfego pode parecer genuíno.

- **Ataques Volumétricos (L3/L4)**: exploram vulnerabilidades em protocolos de rede (como UDP, ICMP) para gerar tráfego de alta intensidade, sobrecarregando a capacidade de banda do alvo e causando indisponibilidade. Em 2023, observou-se um aumento significativo no uso de múltiplos vetores de ataque em investidas volumétricas, com picos recordes de tráfego chegando a centenas de gigabits por segundo.

Processo de execução de um ataque DDoS

O processo de um ataque DDoS pode ser dividido em três etapas principais:

1. Construção da Botnet

- Os cibercriminosos infectam dispositivos com malware, transformando-os em 'zumbis' digitais. É como se você estivesse liderando um exército de mortos-vivos da série 'The Walking Dead', mas, em vez de grunhidos e mordidas, eles lançam requisições de dados para sobrecarregar a infraestrutura digital. Essas redes de dispositivos comprometidos, chamadas de botnets, são usadas para gerar grandes volumes de tráfego contra um alvo específico.

- O crescimento das botnets de IoT tem aumentado significativamente a escala e a sofisticação dos ataques DDoS, pois dispositivos como câmeras, smart TVs e assistentes virtuais são frequentemente menos protegidos do que servidores convencionais.

2. Direcionamento do tráfego

- Os atacantes utilizam técnicas de spoofing para mascarar a origem do tráfego e dificultar a mitigação. Spoofing é uma técnica em que os invasores falsificam endereços de origem dos pacotes de dados para parecerem legítimos, dificultando a identificação de sua verdadeira origem. Em seguida, eles coordenam os dispositivos infectados para gerar um fluxo simultâneo de requisições ao servidor alvo.

- As requisições podem ser adaptadas para atingir pontos específicos da infraestrutura do alvo, como a largura de banda da rede ou a capacidade de processamento de uma aplicação específica.

3. Resultado do ataque

- O tráfego malicioso sobrecarrega os recursos do servidor ou da rede, resultando em lentidão, falhas ou até mesmo indisponibilidade completa dos serviços. Em casos extremos, o impacto pode durar horas ou dias, dependendo da intensidade do ataque e da capacidade de resposta da equipe de segurança.

- Algumas técnicas, como ataques de "bombardeio em massa", visam esgotar rapidamente os recursos, enquanto ataques mais sofisticados podem usar múltiplos vetores simultaneamente para prolongar o tempo de indisponibilidade.

Processo de execução de um ataque DDoS

O processo de um ataque DDoS pode ser dividido em três etapas principais:

- **Ataques contra serviços críticos em Israel (2023)**: durante um conflito, grupos de hacktivistas lançaram ataques coordenados contra websites e infraestruturas governamentais, utilizando múltiplos vetores de ataque para gerar até 1 milhão de solicitações por segundo. A complexidade e a intensidade dos ataques aumentaram a dificuldade de mitigação;

- **Testes de ataques em larga escala no Brasil (2024)**: empresas brasileiras enfrentaram uma série de ataques DDoS massivos com tráfego de amplificação de DNS, o que indica uma preparação cuidadosa para ataques futuros mais intensos. Esses testes demonstraram o alto "poder de fogo" dos cibercriminosos e a necessidade urgente de estratégias de mitigação eficazes.

O nascimento do DDoS

O conceito de ataques DDoS surgiu antes mesmo de existir uma internet como conhecemos hoje. Em 1974, um jovem estudante de apenas 13 anos, David Dennis, acidentalmente realizou uma versão primitiva de um ataque ao derrubar 31 terminais PLATO (sistema educacional online). Embora não tenha sido intencional, o incidente demonstrou o potencial disruptivo de sobrecarregar sistemas com tráfego indesejado.

Nos anos 90, os ataques DDoS começaram a tomar forma mais concreta com o desenvolvimento de ferramentas e técnicas mais sofisticadas. Um dos primeiros grandes ataques registrados aconteceu em 1999, quando a Universidade de Minnesota foi alvo de um ataque DDoS chamado Trinoo. Esse ataque utilizava pacotes UDP (User Datagram Protocol), um protocolo de comunicação que envia dados sem exigir uma conexão prévia, tornando-o mais rápido, mas também mais suscetível a abusos. Desde então, a evolução desses ataques seguiu em paralelo com o crescimento da conectividade global, aproveitando as vulnerabilidades da internet e a proliferação de dispositivos conectados.

O início dos anos 2000 marcou a popularização do DDoS como arma de ciberataques, com casos notórios como o "Mafiaboy", um adolescente canadense de 15 anos que lançou uma série de ataques contra grandes empresas, gerando prejuízos bilionários. Esses primeiros incidentes mostraram ao mundo a gravidade e o impacto potencial dos ataques DDoS, que se tornaram uma preocupação central para a segurança cibernética.

CAPÍTULO 2

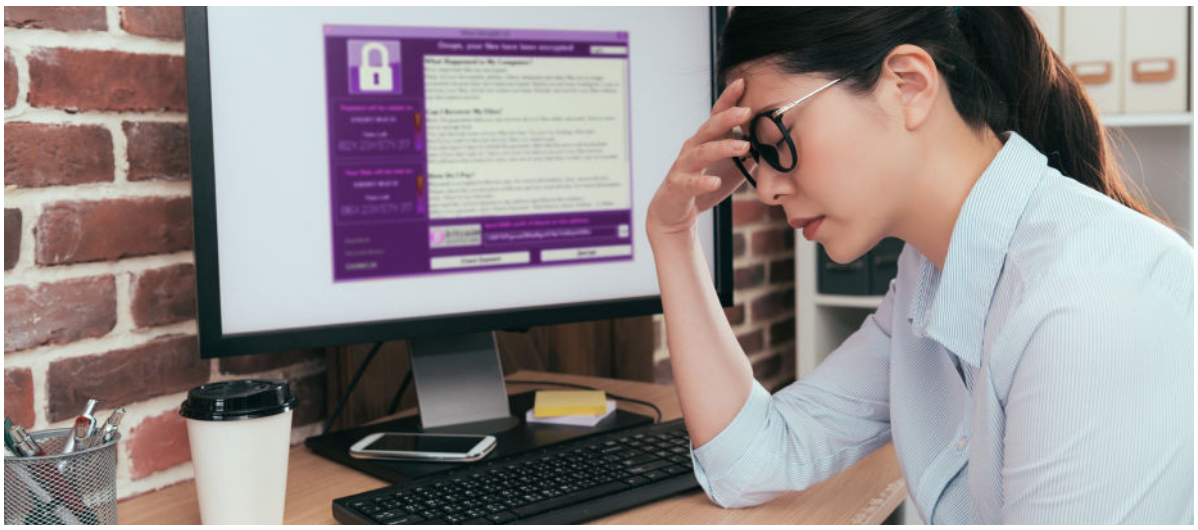
Impactos de um Ataque DDoS

Os ataques DDoS podem causar uma série de impactos significativos que vão além da simples indisponibilidade de um site ou serviço. Entre as consequências mais imediatas estão:

Interrupção de serviços: A sobrecarga de tráfego malicioso gerada pelos ataques DDoS pode levar à indisponibilidade temporária ou total de sistemas online. É como se um estádio lotado de fãs tentasse acessar o mesmo Wi-Fi ao mesmo tempo durante o intervalo do Super Bowl: nada funciona e todo mundo fica frustrado. Isso afeta diretamente a experiência do usuário e pode resultar em perda de clientes, reputação e oportunidades de negócio. Para empresas que dependem fortemente de sua presença digital, até mesmo uma breve interrupção pode causar prejuízos substanciais;;

Perda de receita: negócios que operam online, como e-commerces, provedores de serviços financeiros e plataformas de entretenimento, são particularmente vulneráveis. Durante um ataque DDoS, os clientes podem ser incapazes de concluir transações ou acessar informações importantes, resultando em perda direta de vendas e receita. De acordo com relatórios recentes, uma interrupção causada por ciberataques pode custar, em média, US$ 1,42 milhão para uma organização;

Sobrecarga de recursos de TI: quando ocorre um ataque DDoS, as equipes de TI são frequentemente desviadas de suas tarefas cotidianas para mitigar o impacto, gerenciar a recuperação dos sistemas e identificar a origem do problema. Isso pode sobrecarregar os profissionais e gerar atrasos em outras atividades críticas.



Danos reputacionais

A reputação de uma empresa pode ser severamente afetada quando seus serviços se tornam indisponíveis, especialmente se os clientes e o público percebem que a organização não está preparada para lidar com ameaças cibernéticas. Alguns dos principais danos à reputação incluem:

- **Perda de confiança dos clientes**: quando serviços críticos ficam fora do ar por longos períodos, a confiança dos clientes pode ser abalada. É como prometer uma festa épica e, na hora H, o som para de funcionar. Ninguém quer ser o anfitrião que deixou o DJ sem energia elétrica. A percepção de que uma empresa não possui uma infraestrutura segura e confiável pode levar os clientes a buscar alternativas concorrentes. Em casos onde informações sensíveis estão envolvidas, a preocupação com a segurança aumenta, resultando em maior dano à marca.

- **Impacto na imagem de inovação e competência**: empresas que se posicionam como líderes em tecnologia ou inovação podem sofrer mais danos reputacionais, já que os clientes esperam que essas organizações estejam à frente em termos de segurança e resiliência digital. Um ataque DDoS pode minar essa imagem, gerando a impressão de falta de preparo ou falhas de segurança.

Custos de recuperação e mitigação

Além da perda de receita e danos à reputação, os custos financeiros para recuperar a normalidade após um ataque DDoS podem ser elevados. Isso inclui:

- **Custos diretos de mitigação**: empresas precisam investir em serviços de mitigação de DDoS, ferramentas de segurança e equipes especializadas para conter e remediar os efeitos de um ataque. Em alguns casos, soluções emergenciais podem ser necessárias, como o uso de redes de distribuição de conteúdo (CDN) ou firewalls adicionais, o que pode aumentar as despesas.

- **Investimentos em infraestrutura de segurança**: após sofrerem um ataque, muitas organizações optam por reforçar sua infraestrutura para prevenir incidentes futuros. Isso pode envolver a contratação de novos serviços de segurança, atualização de sistemas e até mesmo a reformulação completa da arquitetura de rede para melhorar a resiliência.

- **Tempo de inatividade e produtividade perdida**: quando sistemas ficam fora do ar, funcionários que dependem dessas plataformas para executar seu trabalho podem enfrentar períodos de inatividade. Isso resulta em perda de produtividade e pode afetar outros departamentos, além da equipe de TI.

Uso de Ataques DDoS como distração para outros cibercrimes

Em muitos casos, os ataques DDoS não são apenas fins em si mesmos, mas atuam como uma “cortina de fumaça” para distração, permitindo que cibercriminosos realizem outras atividades ilícitas enquanto a equipe de segurança está ocupada lidando com a mitigação. Entre as atividades comuns estão:

Exfiltração de dados: enquanto a equipe de segurança está concentrada em mitigar o ataque DDoS, os invasores podem explorar outras vulnerabilidades para roubar dados sensíveis ou confidenciais. Isso pode resultar em vazamentos de informações críticas que podem ser exploradas para extorsão ou vendidas na dark web.

Investimentos em infraestrutura de segurança: após sofrerem um ataque, muitas organizações optam por reforçar sua infraestrutura para prevenir incidentes futuros. Isso pode envolver a contratação de novos serviços de segurança, atualização de sistemas e até mesmo a reformulação completa da arquitetura de rede para melhorar a resiliência.

Tempo de inatividade e produtividade perdida: quando sistemas ficam fora do ar, funcionários que dependem dessas plataformas para executar seu trabalho podem enfrentar períodos de inatividade. Isso resulta em perda de produtividade e pode afetar outros departamentos, além da equipe de TI.

Exemplos de impacto no mundo real

Para exemplificar os efeitos devastadores de ataques DDoS, podemos citar casos recentes:

- **Incidente com provedores de internet no Brasil (2023)**: provedores enfrentaram ataques massivos que causaram instabilidades em suas redes, resultando em interrupções no serviço para milhares de usuários. Esse tipo de ataque pode resultar em reclamações de clientes, multas e danos à imagem da empresa.

- **Ataques de distração combinados com Ransomware**: hackers têm usado cada vez mais ataques DDoS para distrair as equipes de segurança enquanto implantam ransomware nas redes - durante o ano de 2023, os setores bancário e de serviços financeiros foram os mais visados. Isso cria um duplo impacto, forçando as empresas a lidar com duas ameaças ao mesmo tempo, e aumentando os custos de recuperação.

Os maiores ataques DDoS da História

Os ataques DDoS variam em escala e complexidade, mas alguns casos históricos se destacam pelo seu impacto e pelas volumetrias atingidas. A seguir, estão alguns dos maiores ataques DDoS já registrados:

CLOUDFLARE (2024)

o maior ataque de DDoS da história foi mitigado, atingindo impressionantes 5,6 Tbps e 666 milhões de pacotes por segundo em seu pico. O ataque durou aproximadamente 80 segundos e fez parte de uma campanha mais ampla de ataques DDoS hipervolumétricos;

GOOGLE CLOUD (2023)

em outubro de 2023, o Google relatou ter mitigado o que considerou o maior ataque DDoS já visto, até então: um ataque HTTP/2 “Rapid Reset” que alcançou o pico de 398 milhões de solicitações por segundo (RPS). Este ataque explorou uma falha no protocolo HTTP/2, demonstrando a evolução sofisticada das técnicas de ataque cibernético;

AZURE (2021)

em novembro de 2021, a Microsoft Azure sofreu um ataque DDoS que atingiu 3,47 Tbps, originado de aproximadamente 10 mil fontes distribuídas em pelo menos 10 países. Na época, foi considerado um dos maiores ataques já registrados;

AMAZON AWS (2020)

um dos maiores ataques já registrados até hoje aconteceu contra a infraestrutura da Amazon AWS, com uma volumetria de 2,3 Tbps. O ataque utilizou amplificação do protocolo CLDAP, gerando pacotes até 70 vezes maiores que os pacotes legítimos, e durou três dias. O impacto potencial foi significativo, mesmo para uma gigante da computação em nuvem;

GOOGLE CLOUD (2017)

a Google enfrentou um ataque que atingiu 2,54 Tbps, tornando-o o maior já documentado em termos de volumetria. O ataque envolveu a falsificação de milhões de pacotes por segundo e utilizou múltiplos vetores, como CLDAP, DNS e SNMP. A origem foi atribuída a agentes de ameaça patrocinados por um estado, o que demonstrou a escala que um atacante com muitos recursos pode alcançar;

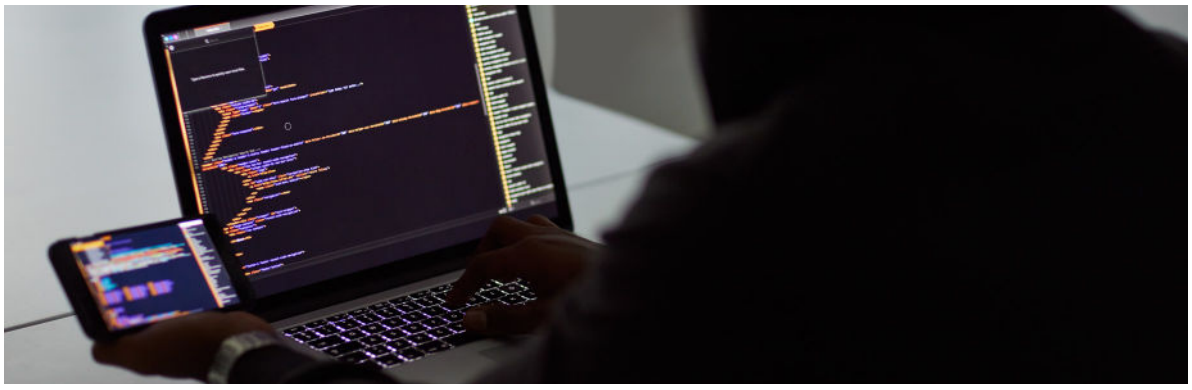
MIRAI BOTNET (2016)

esse botnet utilizou dispositivos IoT para lançar ataques massivos contra alvos como a Dyn, uma empresa de serviços DNS, causando a queda de grandes sites como GitHub, Twitter e Netflix. O ataque atingiu uma volumetria de 1,5 Tbps e expôs as vulnerabilidades de dispositivos conectados à internet;

ATAQUES AOS BANCOS NOS EUA (2012)

seis grandes bancos dos Estados Unidos foram alvos de uma série de ataques coordenados, que utilizaram múltiplos vetores para atingir a volumetria de 60 Gbps. Esses ataques, atribuídos a uma organização ligada ao Hamas, não apenas geraram prejuízos financeiros, mas também afetaram a confiança pública nas instituições.

Esses incidentes evidenciam como os ataques DDoS se tornaram mais potentes e sofisticados ao longo do tempo, exigindo defesas cada vez mais robustas para mitigar os riscos e manter a integridade dos serviços online.



CAPÍTULO 3

Métodos de prevenção e contenção

A prevenção e a contenção de ataques DDoS exigem uma estratégia proativa que integre ferramentas de segurança, práticas recomendadas e um plano de resposta ágil. É fundamental que as organizações adotem medidas preventivas para minimizar a vulnerabilidade a ataques e garantir que, se um incidente ocorrer, os impactos sejam mitigados rapidamente. A combinação de soluções locais e em nuvem, conforme veremos, é uma abordagem eficiente para lidar com ataques de diferentes intensidades e complexidades.

Soluções locais vs. soluções em nuvem

Os métodos de prevenção e mitigação de ataques DDoS podem ser classificados em três tipos principais: soluções locais (on-premises), soluções em nuvem e soluções híbridas de backbone. Cada abordagem oferece vantagens específicas, e uma combinação dessas soluções pode proporcionar a maior proteção possível.
Esses passos incluem:

1. **Soluções locais (On-Premises):**

- Os cibercriminosos infectam dispositivos com malware, transformando-os em Essas soluções são implementadas diretamente na infraestrutura do cliente, filtrando o tráfego malicioso antes que ele alcance os servidores internos. Ferramentas comuns incluem firewalls de aplicação, sistemas de detecção de intrusão e appliances especializados em mitigação de DDoS.

Vantagens: maior controle sobre a configuração e personalização, resposta imediata a ataques de pequena escala.

Limitações: capacidade limitada para lidar com ataques volumétricos massivos, que podem saturar a banda disponível antes de chegarem à infraestrutura de mitigação.

2. Soluções em nuvem (Cloud DDoS):

- As soluções em nuvem são particularmente eficazes para mitigar ataques volumétricos de grande escala, uma vez que o tráfego malicioso é filtrado em centros de limpeza distribuídos globalmente, agindo como um guarda-chuva de última geração. Não importa o tamanho da tempestade digital, com um bom sistema em nuvem, você fica sempre seco. A Telefónica Tech, por exemplo, oferece uma solução com capacidade de mitigação de até 7 Tbps, utilizando uma infraestrutura de vários centros de mitigação.

Vantagens: escalabilidade para lidar com grandes picos de tráfego, proteção geograficamente distribuída que reduz a latência e permite respostas automáticas.

Limitações: menor controle direto sobre as configurações específicas de mitigação, podendo depender da disponibilidade e localização dos centros de mitigação.

3. Soluções híbridas de backbone:

- Atualmente, muitas empresas estão adotando soluções híbridas que protegem o link de backbone antes de ele atingir as redes do cliente. Este modelo envolve uma combinação de soluções locais e em nuvem, com o tráfego sendo filtrado antes de chegar à infraestrutura interna do cliente, muitas vezes através de uma rede de proteção dedicada fornecida pelo provedor de serviços de internet ou pelas operadoras de backbone.

Vantagens: proteção avançada para tráfego de alta volumetria, redução do impacto no link de comunicação entre o cliente e o provedor, e mitigação de ataques antes que eles sobrecarreguem a infraestrutura interna.

Limitações: pode exigir um gerenciamento mais complexo e dependência de terceiros para garantir a efetividade da mitigação. A coordenação entre a solução local do cliente e a proteção do backbone é essencial para a eficácia do sistema.

Práticas recomendadas para prevenção de ataques DDoS

A implementação de medidas proativas é essencial para proteger as empresas contra ataques DDoS. A seguir estão algumas práticas recomendadas:

1. Monitoramento contínuo e análise de tráfego:

- O monitoramento em tempo real é uma das defesas mais importantes contra ataques DDoS, permitindo a detecção precoce de atividades suspeitas. Pense nisso como um alarme de carro extremamente sensível – sempre pronto para disparar no menor sinal de problema. Não é à toa que todo mundo quer ter aquele 'vizinho vigilante' em versão digital. A coleta de dados de fluxo ajuda a identificar padrões anômalos e ativar alertas automáticos para iniciar a mitigação.

2. Uso de soluções híbridas:

- Combinar soluções on-premises com mitigação em nuvem proporciona uma camada adicional de segurança. Por exemplo, ataques menores podem ser mitigados localmente, enquanto ataques de grande escala são desviados para a nuvem para serem filtrados em centros de limpeza.

3. Redundância de redes e balanceamento de carga:

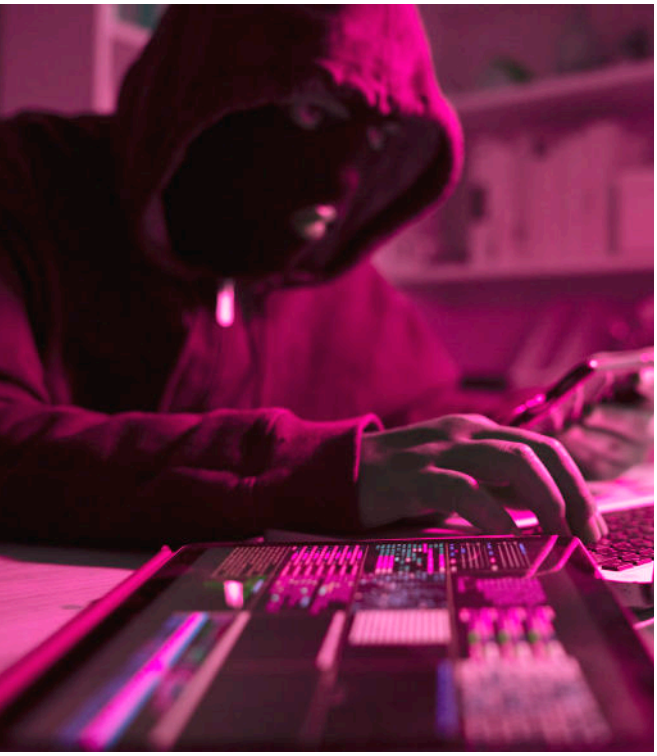
- A implementação de redes de distribuição de conteúdo (CDNs) e balanceadores de carga pode ajudar a distribuir o tráfego, evitando que um único ponto de falha comprometa a disponibilidade dos serviços. Isso é particularmente útil para mitigar ataques DDoS focados em camadas de aplicação.

4. Planos de resposta a incidentes::

- As organizações devem ter planos de resposta a incidentes bem definidos e praticados regularmente. Isso inclui instruções claras sobre como isolar o tráfego malicioso, comunicar o incidente internamente e com clientes, e restaurar os serviços afetados. Empresas que não possuem essa capacidade interna podem contar com o serviço especializado da Telefónica Tech, que oferece suporte completo para a mitigação de ataques DDoS, com monitoramento contínuo e um time de especialistas pronto para atuar de forma rápida e eficaz, garantindo a continuidade dos seus serviços e a proteção da infraestrutura digital.

CAPÍTULO 4

Evolução dos ataques DDoS



Os ataques DDoS evoluíram significativamente nos últimos anos, tornando-se mais frequentes, sofisticados e prejudiciais. O que antes era considerado um incômodo técnico, hoje representa uma ameaça global à continuidade de negócios em diversos setores. Inclusive, segundo a Nescout Systems divulgou nos resultados de seu Relatório de Inteligência de Ameaças DDoS 2024.1, no primeiro semestre de 2024 foi observado um aumento dramático de 43% no número de ataques de nível de aplicação e aumento de 30% nos ataques volumétricos, especialmente na Europa e no Oriente Médio.

As tendências atuais apontam para um aumento no uso de múltiplos vetores de ataque, a exploração de dispositivos IoT, e a utilização de DDoS como serviço (DDoS-as-a-Service), que facilita o acesso a essas ferramentas por cibercriminosos de todos os níveis de habilidade.

Crescimento em volume e complexidade

De acordo com relatórios recentes, o tamanho médio dos ataques DDoS está aumentando exponencialmente, com picos que ultrapassam centenas de gigabits por segundo. É como se os cibercriminosos tivessem trocado baldes por caminhões-pipa para inundar os sistemas digitais. Um estudo de 2023 revelou que os maiores ataques atingiram 170 Gbps, um aumento significativo em comparação aos 124 Gbps registrados em anos anteriores.

TENDÊNCIA 1
Ataques Multivetoriais

- Ataques DDoS estão se tornando mais complexos, frequentemente utilizando múltiplos vetores simultâneos para sobrecarregar diferentes camadas da infraestrutura alvo (L3, L4, L7). Isso exige uma resposta mais coordenada e eficiente das equipes de segurança.

Internet das Coisas (IoT) como vetor de ataques

Com o crescimento da Internet das Coisas (IoT), a superfície de ataque aumentou drasticamente. Dispositivos conectados à rede, como câmeras de segurança, eletrodomésticos e sistemas de controle industrial, muitas vezes não possuem segurança robusta, tornando-se alvos fáceis para a formação de botnets.

TENDÊNCIA 2
Botnets de Dispositivos IoT

- O uso de botnets IoT em ataques DDoS continua a crescer. Segundo relatório de 2023, o número de dispositivos IoT comprometidos usados em ataques DDoS conduzidos por botnets, aumentou de 200 mil para aproximadamente 1 milhão, representando, atualmente, mais de 40% de todo o tráfego DDoS.

Ataques DDoS como Serviço (DDoS-as-a-Service)

Outra tendência preocupante é a profissionalização do cibercrime por meio da comercialização de ataques DDoS. Plataformas DDoS-as-a-Service permitem que até mesmo pessoas com conhecimento técnico limitado possam comprar ataques personalizados, aumentando a frequência e a facilidade de lançamento de ofensivas.

TENDÊNCIA 3
Cibercrime como serviço

- No mercado ilegal, serviços DDoS são oferecidos a preços acessíveis, permitindo que qualquer pessoa, ou organização mal-intencionada, lance ataques volumétricos ou focados com apenas alguns cliques. Essa “democratização” do cibercrime intensifica os riscos para empresas de todos os setores.

DDoS combinado com outros ataques

Conforme discutido anteriormente, os ataques DDoS estão frequentemente sendo utilizados como distrações para outros tipos de cibercrime, como exfiltração de dados ou implantação de ransomware. O uso de DDoS como parte de um ataque combinado está se tornando uma técnica comum entre grupos de hackers sofisticados.

TENDÊNCIA 4
Ataques combinados:

- Em um cenário típico, os invasores iniciam um ataque DDoS para desviar a atenção das equipes de segurança, enquanto, em segundo plano, realizam a invasão de redes para roubar dados ou implantar malware. Em muitos casos, as empresas não percebem a invasão secundária até que os dados já tenham sido comprometidos.

Automação e Machine Learning no combate a DDoS

Por fim, a evolução das tecnologias de defesa também está moldando o futuro da mitigação de DDoS. Soluções baseadas em automação e machine learning estão sendo integradas as plataformas de segurança, para identificar padrões de tráfego anormais e responder de forma mais rápida e precisa a ataques em andamento, agindo como o 'Sherlock Holmes' digital. Com seu poder de análise, elas identificam padrões suspeitos mais rápido do que o famoso detetive poderia dizer 'Elementar, meu caro Watson'.

TENDÊNCIA 5
Automação na defesa

- Plataformas como a Anti-DDoS em Nuvem da Telefónica Tech utilizam machine learning para monitorar e detectar padrões de tráfego maliciosos em tempo real. Isso permite que as soluções adaptem suas respostas automaticamente, mitigando ataques de forma proativa.

À medida que os ataques DDoS continuam a evoluir em volume, sofisticação e alcance, as organizações precisam acompanhar as tendências emergentes para garantir sua resiliência digital. Desde a exploração de dispositivos IoT até o uso de inteligência artificial para detectar e mitigar ameaças, a próxima geração de ataques exigirá que as empresas adotem abordagens de segurança mais robustas e dinâmicas.

CAPÍTULO 5

Portfólio Telefónica Tech

Em um cenário digital onde a disponibilidade constante de serviços tornou-se imperativa, a proteção contra ataques de Negação de Serviço Distribuído (DDoS) emerge como um componente crítico da segurança cibernética moderna. A Telefónica Tech, reconhecendo essa necessidade fundamental, utiliza uma tecnologia amplamente reconhecida no mercado e a oferece como serviço em sua solução robusta e adaptativa: o Cloud Anti-DDoS.

Os ataques DDoS modernos utilizam redes globais de computadores infectados, conhecidos como “zumbis”, para gerar um volume massivo de requisições simultâneas, simulando acessos legítimos a aplicações e sites. Esta sofisticação crescente demanda soluções igualmente avançadas, capazes de proteger infraestruturas digitais de maneira eficaz e inteligente.

Cloud Anti-DDoS: Uma Solução Robusta

A solução utilizada pela Telefónica Tech se destaca por sua abordagem tríplice à proteção DDoS:

1. Detecção inteligente

O sistema realiza uma análise contínua do tráfego, identificando padrões anormais que possam indicar um ataque em andamento. Esta vigilância constante permite uma resposta rápida e precisa a ameaças emergentes.

2. Mitigação eficiente

Quando um ataque é detectado, a plataforma separa automaticamente o tráfego malicioso do legítimo, garantindo que apenas requisições autênticas alcancem a infraestrutura do cliente. Como um segurança de festa que deixa passar apenas os convidados com convite – enquanto os ‘penetras digitais’ ficam do lado de fora –, este processo é realizado por meio de uma rede global de centros de limpeza, estrategicamente posicionados para minimizar a latência.

3. Adaptação contínua

O sistema evolui constantemente, identificando novos padrões de ataque e adaptando suas defesas. Esta capacidade de aprendizagem garante proteção contra ameaças emergentes e em evolução.

Capacidades e benefícios diferenciados

A solução oferece um conjunto impressionante de recursos:

- **Capacidade massiva de mitigação:** capacidade massiva de mitigação: 7Tbps de capacidade total – imagine uma soluçãol capaz de bloquear um tsunami digital. Essa proteção de grande escala garante que o tráfego malicioso vá direto para o ralo, enquanto o tráfego legítimo navega tranquilo;
- **Flexibilidade de conexão:** suporte a túneis GRE e conexões diretas, adaptando-se à infraestrutura existente;
- **Escalonamento inteligente:** utilização do método 95 percentil, permitindo picos de até 10 vezes do tráfego contratado em até 5% do tempo dentro do mês;
- **Cobertura abrangente:** proteção simultânea para múltiplas sub-redes;
- **Automatização avançada:** detecção e desvio automático de ataques, minimizando a necessidade de intervenção manual.

Diferenciais estratégicos

- **Infraestrutura global com toque local:** a solução mantém centros de limpeza distribuídos globalmente, incluindo uma instalação dedicada no Brasil. Isso garante que o tráfego legítimo originado no país permaneça em território nacional, otimizando a latência e atendendo a requisitos regulatórios.
- **Modelo flexível de contratação:** a plataforma oferece pacotes escaláveis, desde 50Mbps até 5Gbps de banda limpa, com a possibilidade de expansão conforme necessidade. O modelo de precificação baseado no 95º percentil permite picos de utilização sem custos adicionais, oferecendo flexibilidade financeira e operacional.

Monitoramento e gestão avançada

O console de gerenciamento dedicado permite:

- Monitoramento em tempo real
- Análise detalhada de ataques
- Geração de relatórios abrangentes

Suporte especializado

A solução é respaldada por uma equipe global de profissionais altamente especializados, que operam por meio de:

- Diversos Centros de Operações de Segurança (SOCs)
- Centros de Operações Digitais (DOCs)
- Laboratórios e Centros de Inovação dedicados à pesquisa e ao desenvolvimento de soluções de segurança

Essa estrutura robusta permite o monitoramento contínuo de dispositivos críticos e o processamento de um grande volume de eventos de segurança, garantindo a proteção eficiente contra as mais diversas ameaças cibernéticas.

O Cloud Anti-DDoS da Telefónica Tech representa uma solução completa e madura para a proteção contra ataques DDoS. Combinando tecnologia avançada, infraestrutura global e expertise local, a plataforma oferece a segurança e a flexibilidade necessárias para manter operações digitais resilientes no cenário atual de ameaças cibernéticas em constante evolução.

Conclusão

A evolução dos ataques DDoS, tanto em frequência quanto em complexidade, exige que as organizações adotem uma abordagem estratégica e proativa para proteger seus ativos digitais. A ameaça é constante, e os métodos dos atacantes estão se tornando cada vez mais sofisticados, utilizando múltiplos vetores, aproveitando botnets IoT e oferecendo ataques DDoS como serviço. Essa realidade impõe a necessidade de investir em soluções abrangentes e escaláveis, capazes de responder a ataques de diferentes tipos e intensidades.

Ao longo deste e-book, abordamos os fundamentos dos ataques DDoS, seus impactos, e as práticas recomendadas para prevenção e mitigação. Também destacamos a importância de uma estratégia híbrida que combina soluções locais e em nuvem, além de serviços gerenciados que ofereçam monitoramento contínuo e automação para detecção e resposta rápidas. A Telefónica Tech, com seu portfólio de proteção Anti-DDoS, se posiciona como uma parceira confiável na defesa contra essas ameaças, oferecendo soluções adaptáveis e personalizadas para diversos setores e tamanhos de empresas.

Para enfrentar os desafios impostos pelos ataques DDoS, as organizações devem ir além da proteção básica, adotando práticas proativas de segurança, como monitoramento constante, revisão de políticas de mitigação e a implementação de soluções avançadas. A preparação e a resiliência digital são essenciais para garantir a continuidade dos negócios e minimizar os impactos de incidentes cibernéticos.

Com a crescente sofisticação das ameaças, estar informado e preparado faz toda a diferença. Esperamos que este material tenha proporcionado insights valiosos para fortalecer suas defesas e proteger seus sistemas contra os ataques DDoS. Para conhecer mais sobre as soluções da Telefónica Tech e como elas podem ajudar a sua organização, entre em contato com nossos especialistas.

vivo empresas

Mais informações em Telefonicatech.com

Telefónica Tech