O chef da cibersegurança:

criando o melhor livro de receitas para resiliência a ataques de DDoS da Camada 7

Índice

Introdução

Planejar a defesa certa contra os ataques de DDoS (negação de serviço distribuída) atuais pode ser um desafio até mesmo para os melhores profissionais de segurança. Isso se aplica principalmente a ataques de DDoS da Camada 7, que trazem complicações adicionais. Por isso, pode ser útil ter um conjunto de instruções detalhadas com diferentes abordagens para diferentes ameaças ou, em outras palavras, um manual sobre DDoS da Camada 7.

Cada adversário prepara ataques de DDoS de maneiras diferentes. Ataques nas Camadas 3 e 4 são uma questão de força. Quem tem melhor capacidade de rede, o invasor ou a defesa? Por outro lado, os ataques da Camada 7 visam a camada de aplicativo do modelo OSI (Open Systems Interconnection), responsável por interagir diretamente com aplicativos de software. O objetivo desses ataques é sobrecarregar servidores da Web, bancos de dados ou aplicativos, explorando capacidade, alocações de memória ou fraquezas na forma como esses sistemas lidam com solicitações.

Os ataques de DDoS da Camada 7 apresentam desafios específicos em relação à mitigação porque essas solicitações normalmente se parecem com o tráfego legítimo, o que dificulta a filtragem de solicitações mal-intencionadas sem afetar usuários legítimos. Além disso, a disponibilidade de recursos de automação e nuvem facilita ainda mais para os invasores realizarem esses ataques de forma rápida e em grande escala.

Neste documento, abordamos os desafios de mitigar os ataques de DDoS da Camada 7 com orientações detalhadas que incluem as ferramentas e técnicas que os invasores usam, táticas de detecção e mitigação para combatê-los e sugestões de análise e recuperação pós-evento.

Graças ao histórico da Akamai em entrega de conteúdo, cibersegurança e uma plataforma de nuvem distribuída com mais de 4.200 pontos de presença em todo o mundo, temos uma perspectiva única sobre os ataques de DDoS atuais. Conforme os ataques de DDoS na camada de aplicativo continuam a se tornar mais complexos e multifacetados, é importante reconhecer esse perigo e ter uma estratégia completa para defesa. É isso que oferecemos.

Seja você um profissional de segurança de linha de frente buscando ajuda com uma ameaça ou vulnerabilidade específica ou um profissional responsável pela segurança da informação que visa melhorar sua postura de segurança, este manual oferece a receita para o sucesso.

Alvos comuns e exemplos de ataques de DDoS da Camada 7

Os ataques de DDoS da Camada 7 têm como alvo a camada superior do modelo OSI, a camada de aplicativo. Esses ataques têm como objetivo sobrecarregar os recursos do alvo, explorando a maneira como os aplicativos da Web processam solicitações. Alguns alvos comuns de ataques de DDoS da Camada 7 incluem:

Servidores da Web: os invasores atacam servidores da Web para interromper a entrega de conteúdo a usuários legítimos. Isso pode causar carregamento lento de websites ou até mesmo inacessibilidade total.

Aplicativos da Web: os aplicativos que dependem de bancos de dados ou serviços de back-end estão vulneráveis a esse tipo de ataque, já que ele pode explorar pontos fracos na forma como os aplicativos analisam consultas, processam solicitações ou gerenciam sessões.

APIs (interfaces de programação de aplicativos): as APIs são um componente essencial de serviços da Web e aplicativos móveis modernos. Os invasores atacam as APIs para interromper a interação entre diferentes serviços de software, o que afeta a funcionalidade dos aplicativos que dependem dessas APIs.

Serviços de DNS (Sistema de Nomes de Domínio): embora os ataques a DNS também possam ocorrer em outras camadas, os ataques de Camada 7 podem bombardear o serviço de DNS com solicitações mal-intencionadas para interromper a resolução de nomes de domínio, causando problemas de acessibilidade generalizados. O aumento da adoção do DNS por HTTP/TLS pode resultar em um aumento desses ataques.

Servidores de e-mail: ataques a servidores de e-mail podem interromper comunicações, afetando e-mails enviados e recebidos.

Gateways de pagamento e serviços financeiros: esses são alvos lucrativos para invasores que visam interromper transações e semear o caos nas operações financeiras.

Os relatórios SOTI (State of the Internet) e os insights de segurança da Akamai analisam o cenário em evolução dos ataques de DDoS da Camada 7 regularmente, destacando os diversos vetores de ataque e os principais setores em risco.

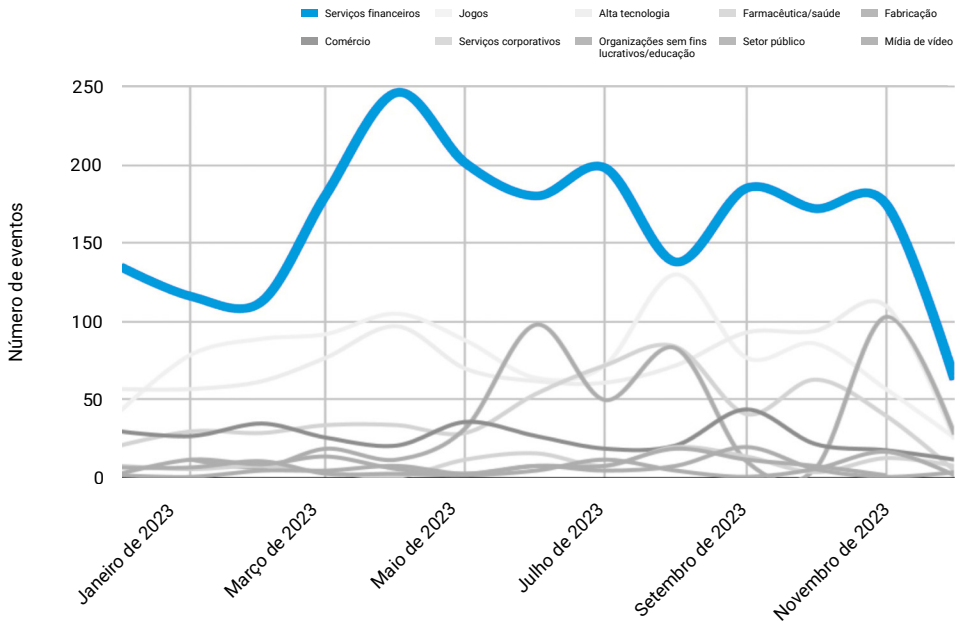
Vetores de ataque

- Ataques contra aplicativos da Web e APIs: os adversários normalmente direcionam seus ataques aos pontos de entrada de website, incluindo pontos de extremidade de API que normalmente não são armazenados em cache devido ao seu conteúdo ou configuração. Entre os caminhos que são mais atacados, podemos mencionar "/", "/home", "/en-us" e "/pricing".
- É comum ver vetores de ataque como:
  • Inundação de HTTP GET / POST em páginas iniciais
  • Inundação de HTTPS GET em caminhos aleatórios e cadeias de consulta
  • Ataques de leitura lenta
  • Grandes inundações de upload de arquivos

Além disso, o número de empresas que enfrentam ataques de DDoS tem aumentado historicamente ano após ano, mas agora a forma é diferente. Primeiro, o tipo e o volume das propriedades que estão sendo atacadas mudaram. Por exemplo, em vez de 10 ataques contra pontos de extremidade iguais ou semelhantes, agora pode haver 100 ataques direcionados a diferentes IPs no espaço de rede. Esses ataques não visam apenas a Camada 3, mas também a Camada 7 ao mesmo tempo.

Setores em risco

O número de eventos de ataque de DDoS (negação de serviço distribuída) contra os setores de serviços financeiros, jogos de azar e manufatura teve um pico em 2023, principalmente na região da EMEA, em que os ataques excederam em número em comparação a todas as outas regiões combinadas.

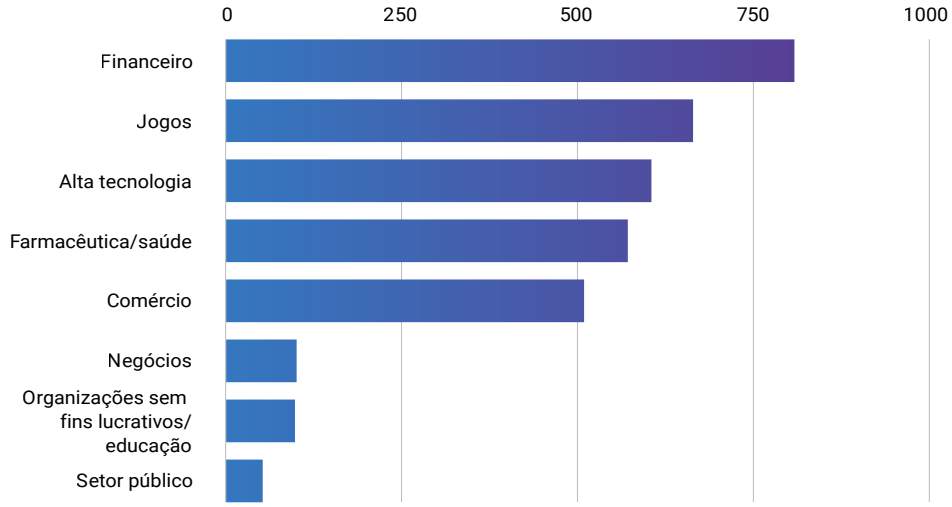


DDoS: Here to Stay, março de 2024

Os serviços financeiros, em particular, tornaram-se um alvo crescente para ataques de DDoS da Camada 7. Desde 2021, a Akamai notou um aumento distinto e perceptível no número de ataques de DDoS contra empresas de serviços financeiros. Em 2023, mais de um terço (35%) dos ataques contra todos os setores foram realizados contra instituições de serviços financeiros, tornando o setor um alvo mais atraente do que o setor de jogos. A análise da Akamai mostra que o setor bancário foi alvo de 63% dos ataques de DDoS em todo o mundo. Quase três quartos (72%) dos ataques na EMEA e 91% na APAC foram direcionados ao setor bancário. Nas Américas, no entanto, os ataques de DDoS foram distribuídos de forma mais uniforme entre instituições bancárias, de seguros e de outros serviços financeiros.

Américas: os serviços financeiros são alvo de 28% dos ataques de DDoS

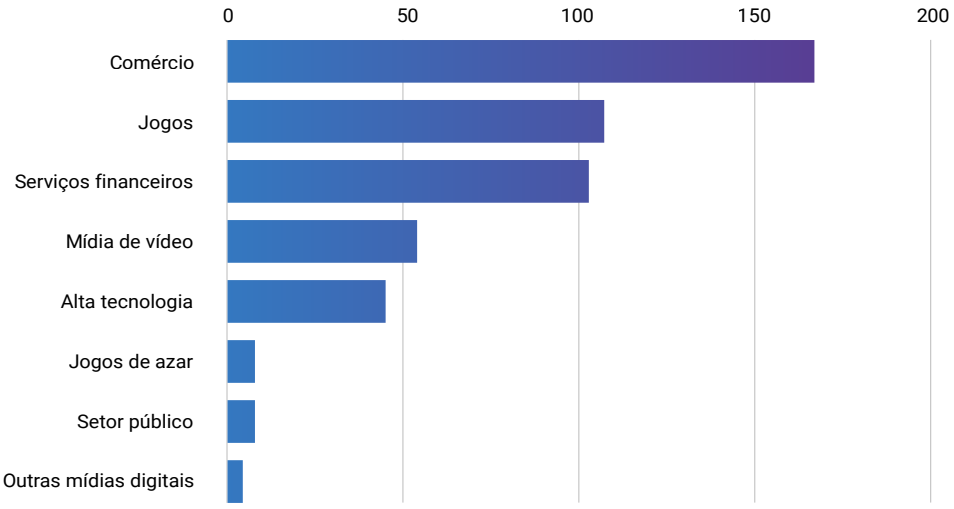
Junho a dezembro de 2023



DDoS: Here to Stay, março de 2024

APAC: os serviços financeiros são alvo de 11% dos ataques de DDoS

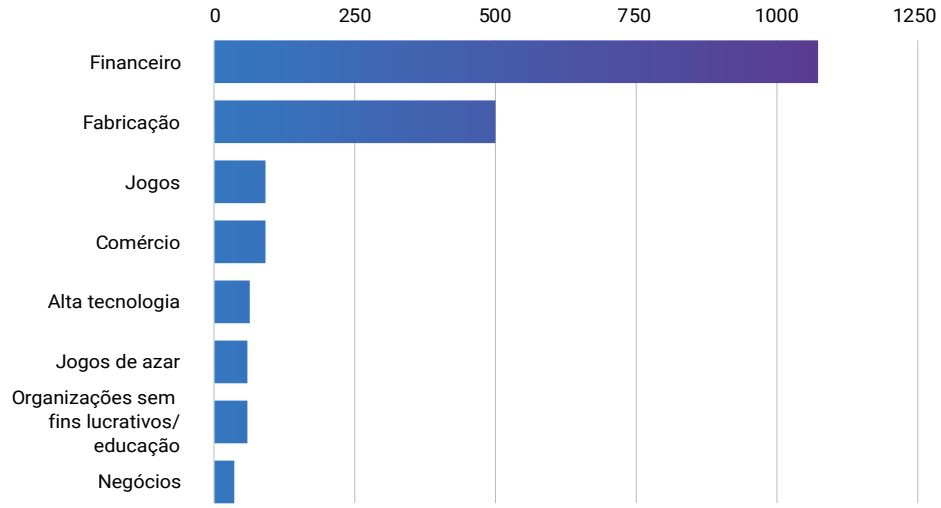
Junho a dezembro de 2023



DDoS: Here to Stay, março de 2024

EMEA: os serviços financeiros são alvo de 66% dos ataques de DDoS

Junho a dezembro de 2023



DDoS: Here to Stay, março de 2024

Um exemplo recente de um sofisticado ataque de DDoS da Camada 7 tinha como alvo um dos clientes de serviços financeiros da Akamai. Os adversários cibernéticos utilizaram a automação e criaram um ataque altamente distribuído. Esse ataque usou uma inundação de HTTP GET visando principalmente URLs que não podiam ser armazenados em cache (como página inicial e pontos de extremidade de login). Utilizando vários controles proativos, este ataque foi mitigado com sucesso sem qualquer impacto na origem do cliente. Este mapa de fonte de calor de ataques ressalta o uso crescente de provedores de serviços de nuvem, nós de saída Tor e nós de proxy anônimos ou abertos:

Ataques de DDoS por sistema autônomo

Visualização de ataques na camada de aplicativo em instituições financeiras ocorridos no primeiro trimestre de 2024 em mais de 100 países, que a Akamai ajudou a mitigar

Os invasores DDoS conseguem construir e coordenar uma infraestrutura de ataque amplamente dispersa, aproveitando endereços IP dinâmicos em redes extensas, abrangendo vários países e regiões em todo o mundo.

Ferramentas e técnicas usadas pelos invasores

Infelizmente, os invasores e seus métodos não permanecem os mesmos. À medida que os invasores continuam a encontrar maneiras de monetizar seus atos, eles adaptam suas técnicas, aproveitam novas ferramentas e encontram novos métodos. Há vários fatores que demonstram essa evolução.

Automação: os invasores estão usando scripts e bots automatizados para imitar o comportamento de um usuário legítimo, dificultando ainda mais a detecção. Além disso, agora eles estão usando algoritmos de aprendizado de máquina que se adaptam e evitam a detecção tradicional.

Ataques multivetoriais: os adversários estão cada vez mais usando estratégias multivetoriais, combinando diferentes tipos de ataque (como inundações de GET e POST) e alvos de DNS (como amplificação e ataques de fragmentos) com outras combinações para sobrecarregar os recursos de rede e de aplicativos.

Ataques a APIs: como cada vez mais as empresas dependem das APIs para alimentar seus aplicativos, os invasores estão encontrando novas oportunidades de invasão explorando as vulnerabilidades das APIs em seus ataques de DDoS. O objetivo desses ataques é esgotar os recursos do servidor solicitando centenas de conexões simultaneamente, ou explorar falhas lógicas, causando interrupções no serviço.

Exploração de dispositivos de Internet das coisas: o aumento de dispositivos de IoT (Internet das coisas) mal protegidos cria um vasto exército de botnets. Esses dispositivos são frequentemente sequestrados e usados para lançar ataques de DDoS massivos que exploram sua conectividade de rede e poder computacional.

Aumento da sofisticação

Com todas essas novas ferramentas e técnicas, houve um aumento correspondente na complexidade e frequência dos ataques de DDoS, que agora exploram métodos sofisticados para contornar defesas tradicionais. Algumas notáveis tendências incluem:

Criptografia: uma evidente mudança para ataques de DDoS baseados em HTTPS tornou a mitigação mais desafiadora. Esses ataques se disfarçam como tráfego legítimo, visto que são criptografados, o que dificulta sua detecção e filtragem, já que as medidas tradicionais de proteção contra DDoS têm limitações para descriptografar o tráfego SSL/TLS da camada de aplicativo.

Botnets e proxies: devido ao crescimento significativo de botnets de DDoS e à prevalência de proxies anônimos de invasores, as solicitações agora estão sendo enviadas de uma infinidade de endereços IP (normalmente, mais de 10 mil IPs por ataque). Os invasores usam essa estratégia para contornar medidas de mitigação que contam as solicitações de um único IP.
A prevalência de plataformas de hospedagem em nuvem e a adoção de serviços baseados em nuvem facilita muito a elaboração desses ataques de alta intensidade e altamente distribuídos.

Ataques de DDoS por sistema autônomo

Visualização de um recente ataque de DDoS na camada de aplicativo contra um cliente financeiro da Akamai: 650 mil TPS (transações por segundo), 20 Gbps, mais de 9 bilhões de solicitações no total

Os invasores DDoS conseguem criar e coordenar uma infraestrutura de ataque extremamente distribuída, principalmente de provedores de nuvem.

Uma abordagem em evolução que os defensores estão empregando é o rastreamento de solicitações por impressão digital de TLS, que é composta por vários sinais de camada de TLS, como tipos de cifra e sua ordem. Embora essa abordagem seja suscetível a falsos positivos, se usada corretamente, ela pode fornecer uma mitigação mais eficaz quando um invasor está operando em várias máquinas e IPs, porque o mesmo software é instalado nos dispositivos comprometidos. Esses dispositivos exibem características de ambiente semelhantes, sendo uma delas a biblioteca compartilhada de TLS.

Fornecimento de ingredientes

Embora as ferramentas disponíveis mudem constantemente, a evolução das técnicas de ataque indica uma transição para métodos mais sofisticados e menos detectáveis. Entre eles estão:

- **Dispositivos de IoT comprometidos:** os invasores continuam a usar dispositivos de IoT comprometidos em botnets como um método para lançar ataques de DDoS em grande escala, evidenciando a vulnerabilidade contínua desses dispositivos.
- **Serviços de DDoS por encomenda:** a disponibilidade de serviços de DDoS por encomenda reduziu a barreira de entrada para realizar os ataques, permitindo que indivíduos sem amplo conhecimento técnico conduzam ataques em escala significativa.

- **Técnicas de evasão:** técnicas avançadas de evasão, como parâmetros de cabeçalho aleatórios e argumentos de solicitação dinâmica, tornaram-se mais comuns. Essas técnicas desafiam abordagens tradicionais de detecção e mitigação, dificultando a distinção entre tráfego mal-intencionado e solicitações legítimas.

Vulnerabilidades normalmente exploradas nesses ataques

As vulnerabilidades que os invasores exploram nos ataques de DDoS da Camada 7 normalmente estão relacionadas às maneiras como os aplicativos da Web processam entradas dos usuários e gerenciam dados. É essencial implementar uma combinação de medidas de segurança para mitigar essas vulnerabilidades.

Nos últimos anos, uma das principais vulnerabilidades que os invasores exploraram ao realizar ataques de DDoS na camada de aplicativos foi a falha HTTP/2 Rapid Reset, amplamente publicada no final de 2023. Esses ataques exploraram uma falha no protocolo HTTP/2, que é essencial para o funcionamento da Internet e de todos os websites. A exploração dessa vulnerabilidade causou um aumento global de 65% no tráfego de ataques de DDoS HTTP em um trimestre em comparação com o anterior, evidenciando a gravidade e o impacto desse tipo de ataque.

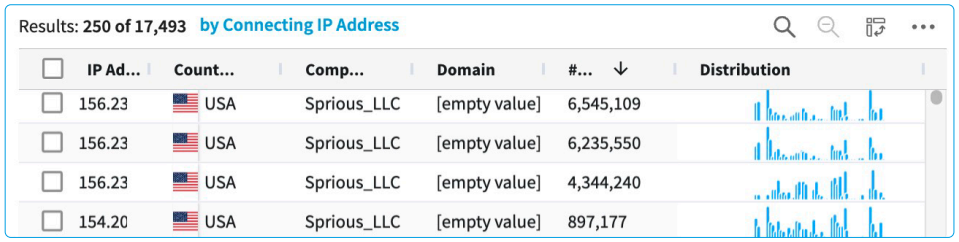
Essa vulnerabilidade em particular permitiu que os invasores gerassem maior impacto, aproveitando as plataformas de computação em nuvem e explorando o HTTP/2, possibilitando ataques de DDoS extremamente volumétricos com botnets relativamente pequenos. Os setores mais afetados incluem os setores de jogos, TI, criptomoeda, software de computador e telecomunicações, sendo os EUA, a China, o Brasil, a Alemanha e a Indonésia os maiores alvos desses ataques.

Em resposta a esses ataques, um esforço coordenado coletivo dos setores revelou a vulnerabilidade HTTP/2 Rapid Reset (CVE-2023-44487) para trazer à tona os ataques de DDoS que se aproveitavam dessa falha. Diversos provedores foram alvo desse tipo de ataque, incluindo provedores líderes de serviços de nuvem e CDN (Rede de Entrega de Conteúdo).

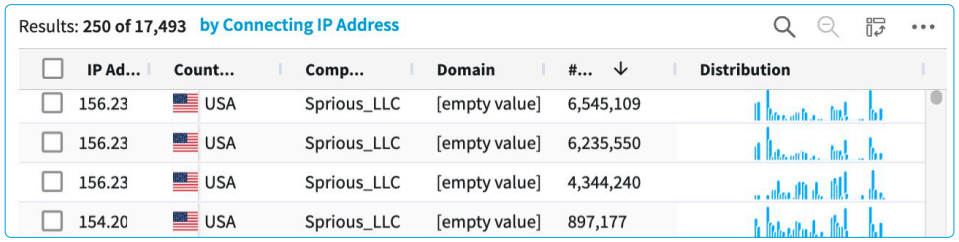
Exemplos da vida real: uso da automação em ataques de DDoS

Os invasores geralmente usam várias ferramentas de DDoS para realizar os mesmos ataques de DDoS, cada uma aproveitando várias técnicas combinadas para sair do radar de produtos de segurança ou, pelo menos, torná-los menos eficientes. Um exemplo de um ataque é descrito abaixo usando o Akamai Web Security Analytics.

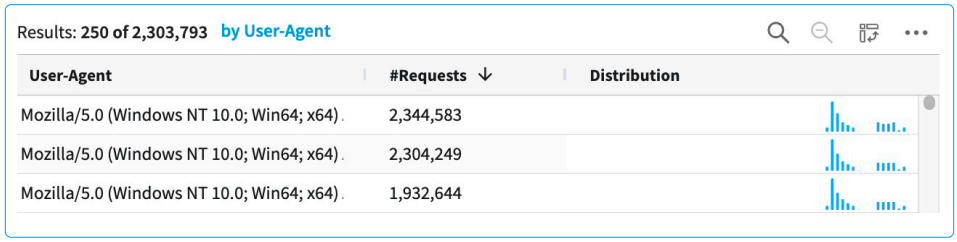
- Ataque observado em mais de 17 mil endereços IP



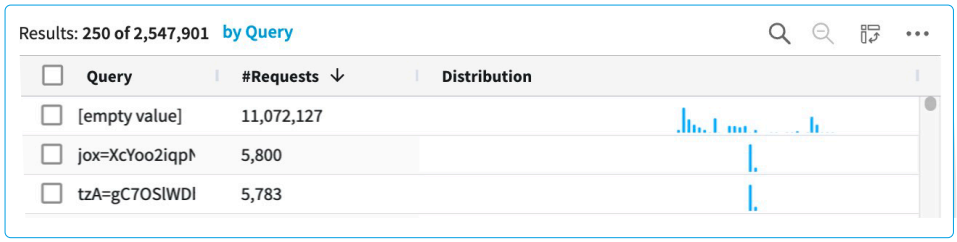
- Fontes de ataque de mais de 400 redes



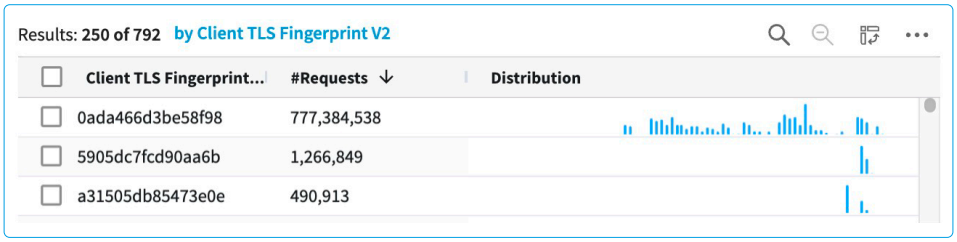
- 2.303.793 agentes de usuário exclusivos



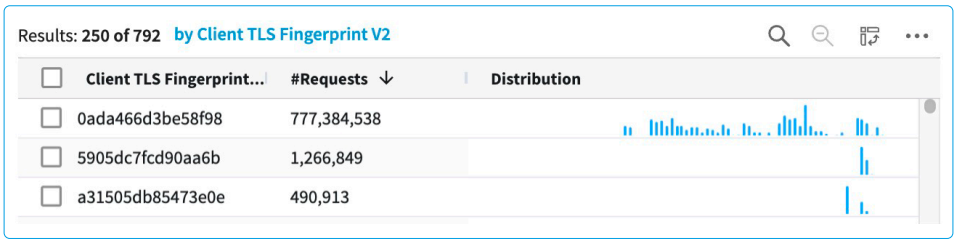
- 2.547.901 strings de consulta únicas e aleatórias



- Rotação de cabeçalho HTTP (por exemplo, Accept-Language, Referer)



- Rotação de configuração de TLS



Para mitigar esses ataques sofisticados, é preciso ter uma estratégia de proteção em camadas. Pode ser útil usar controles proativos e reativos, como uma combinação avançada de correspondências de solicitações e características de tráfego de origem na limitação de taxa ou controles de reputação de origem.

Adversários mais fortes: apropriação indevida de sinal de TLS

Observações recentes mostraram que agentes mal-intencionados cada vez mais usam sinais de TLS em suas ferramentas de DDoS para evitar detecções, fazendo com que essas conexões pareçam vir de navegadores Chrome legítimos. Em vez de usar uma versão headless do Chrome com uso intenso de recursos, que pode retardar o ataque, os invasores podem ter empregado uma versão modificada da biblioteca de TLS, permitindo que eles definam e simulem os sinais de TLS de qualquer navegador genuíno. Embora existam ferramentas criadas para replicar a impressão digital de TLS, elas não são comumente encontradas em ferramentas de ataque de DDoS. O uso deste tipo de ataque sugere crescimento na proeza técnica dos invasores e um profundo conhecimento das defesas. É por isso que as estratégias de defesa aos ataques de DDoS da Camada 7 devem incluir pesquisas regulares sobre as tendências mais recentes de ataque. Isso também parece sugerir que as ferramentas de DDoS que incluem falsificação de TLS estão se tornando mais comuns.

Análise da situação: avaliação de risco e identificação de vulnerabilidades

Você pode aprimorar significativamente sua estratégia de mitigação de ataques de DDoS da Camada 7 identificando seus ativos críticos e determinando onde eles podem estar vulneráveis a um ataque de DDoS. Esta avaliação de risco ajuda a priorizar quais recursos proteger com base em sua importância e vulnerabilidade. Ao compreender potenciais vetores de ataque e seus impactos, as organizações podem implementar contramedidas específicas, como limitação de taxas, firewalls de aplicativos da Web e análise de comportamento, para mitigar os riscos de forma eficaz. Além disso, uma avaliação contínua de riscos permite uma estratégia de defesa que evolui em resposta a novas ameaças e mudanças nos requisitos comerciais.

Diferentes setores e empresas podem adotar diferentes abordagens para avaliações de risco de DDoS na camada de aplicativo. Por exemplo:

> **Comércio eletrônico:** antes de um grande evento de venda, uma avaliação de riscos pode identificar o processo de finalização de compra como uma vulnerabilidade crítica. As medidas de mitigação podem incluir a implementação de um WAF (firewall de aplicativos da Web) e limitação de taxa para proteger o serviço.
>
> **Serviços financeiros:** em um aplicativo bancário, a avaliação de riscos pode determinar que a página de login é um alvo principal para ataques de DDoS. O banco poderia então implementar combinação de limitação da taxa personalizada de ponto de extremidade e detecção de comportamento para diferenciar usuários legítimos e tráfego de ataque.

A compreensão de vulnerabilidades específicas permite a implementação de defesas direcionadas e aumenta os serviços críticos durante um ataque.

Equipe centralizada: funções e responsabilidades

Estabelecer funções e responsabilidades claras são etapas cruciais para uma estratégia eficaz de DDoS da Camada 7, pois maximiza a oportunidade de uma resposta coordenada e eficiente em caso de ataque. Sem funções claras, os esforços de resposta podem se tornar caóticos, com sobreposições de deveres e lacunas na defesa. Responsabilidades bem definidas ajudam na identificação das tarefas específicas de cada membro da equipe, desde o monitoramento de tráfego e identificação de anomalias até a implementação de estratégias de mitigação e comunicação com as partes interessadas. Essa coordenação ajuda a minimizar o impacto dos ataques, manter a disponibilidade do serviço e proteger ativos críticos.

Ter muitos tomadores de decisão sem funções claras pode causar respostas atrasadas durante um ataque de DDoS. Por exemplo, se as equipes de operações de rede e cibersegurança decidirem seguir abordagens diferentes de mitigação de forma independente e sem coordenação entre as equipes, pode ser que uma estratégia anule os esforços da outra equipe ou que ambas ignorem vulnerabilidades críticas. A estratégia correta envolve funções predefinidas, como designar um líder de resposta a incidentes, um coordenador de comunicação e uma equipe de resposta técnica, garantindo ações rápidas e unificadas contra ataques, minimizando o tempo de inatividade e agilizando a análise pós-incidente.

As ferramentas certas para suas necessidades

Detectar e mitigar um ataque da camada de aplicativo pode ser desafiador, pois é muito difícil diferenciar tráfego legítimo do mal-intencionado. Em resposta a essas ameaças em evolução, recomendamos uma abordagem multifacetada para a defesa:

- **Foque no sempre ativo vs. sob demanda:** certifique-se de que os controles de segurança de DDoS estejam sempre ativos e atualize os planos de resposta a incidentes para lidar rapidamente com ameaças emergentes.
- **Estabeleça uma arquitetura resiliente e confiável:** antecipe um único ponto de falha, já que os invasores provavelmente atacarão vários serviços, incluindo DNS, aplicativos da Web, APIs e infraestruturas de data center e rede. Usar a arquitetura certa é essencial para se proteger contra ataques de DDoS da Camada 7. Essas considerações de arquitetura podem incluir a escolha de proteção contra DDoS baseada em edge ou CDN (Rede de Entrega de Conteúdo), que estão sempre ativas. Não superestime a confiabilidade. A escala dos ataques de DDoS atuais pode facilmente sobrecarregar a maior parte da infraestrutura.
- **Avalie os SLAs do seu provedor** e os alinhe com sua estratégia.
- **Analise a prontidão do seu provedor:** escolha um provedor que regularmente demonstre que revisa seus componentes críticos de rede e avalia diferentes mecanismos de proteção contra DDoS para obter informações sobre sua eficácia contra os métodos de ataque atuais.
- **Revise seu manual de resposta a ataques de DDoS:** reúna suas equipes de TI, operações, segurança e comunicação com o cliente para aprimorar sua prontidão no caso de um ataque.
- **Proteção de emergência contra DDoS:** tenha um plano pronto para integrar um provedor de soluções de mitigação de DDoS em caso de crise. Se você tem um parceiro fornecedor em proteção contra DDoS, ligue para a linha direta de suporte a DDoS.

Receitas para detecção e mitigação

Uma proteção eficiente contra DDoS na Camada 7 exige diversas estratégias de detecção e mitigação. Você pode aplicar várias metodologias, cada uma das quais tem seus pontos fortes e considerações importantes.

Detecção comportamental e baseada em anomalias

Pontos fortes: essa abordagem depende do uso de aprendizado de máquina e análise estatística para assimilar seus padrões de tráfego normais e, em seguida, identificar desvios que podem indicar um ataque de DDoS. Ela é altamente eficaz contra ataques complexos que antes passavam despercebidos.

Considerações: a detecção eficaz requer um período de aprendizagem que pode levar várias semanas para estabelecer uma linha de base de tráfego "normal". Durante esse período, a detecção pode não ser tão eficaz. O modelo pode retornar falsos positivos se não for treinado com precisão.

Detecção baseada em taxas e taxa de transferência

Pontos fortes: é um método simples de implementar que monitora a taxa e o volume de solicitações, acionando alertas ou processos de mitigação quando o tráfego excede os limites predefinidos. É eficaz para identificar rapidamente ataques volumétricos em grande escala.

Considerações: picos de tráfego legítimos, como os que ocorrem durante eventos promocionais, podem ser confundidos com ataques de DDoS. Esse método pode não detectar ataques de baixo volume e taxa lenta que não acionam alarmes.

Detecção baseada em assinatura

Pontos fortes: ao comparar o tráfego com um banco de dados de padrões de ataque conhecidos, este método pode rapidamente identificar e bloquear ameaças reconhecidas. Ele é altamente eficaz contra vetores de ataque comuns e previamente identificados.

Considerações: ele não detecta ataques novos ou modificados que não correspondem às assinaturas existentes. É preciso atualizar regularmente para manter sua eficácia.

Testes de resposta a desafios

Pontos fortes: essa abordagem envia desafios para o tráfego de entrada, seja ele gerado por humanos ou bots. Cálculos CAPTCHA ou JavaScript podem efetivamente mitigar bots e ferramentas de ataque automatizadas.

Considerações: os desafios podem atrapalhar a experiência do usuário se forem implementados de forma agressiva. Bots mais sofisticados podem conseguir realizar testes de resposta a desafios, o que exige que você faça atualizações regulares aos mecanismos de desafio.

Abordagens híbridas

A combinação de várias estratégias de detecção e mitigação pode oferecer uma proteção mais abrangente. Por exemplo, o uso de detecção baseada em anomalias para sinalizar possíveis ataques, complementado por métodos baseados em taxas e em assinaturas para uma cobertura mais ampla, permite a implementação de mecanismos de defesa mais robustos. Testes de resposta a desafios podem filtrar bots sofisticados de usuários legítimos.

Métodos convencionais

Filtragem geográfica e por IP: bloquear ou limitar o tráfego de determinados intervalos IP/CIDR e regiões geográficas não relevantes para a sua empresa pode reduzir sua exposição a ataques provenientes dessas áreas. Embora esse método possa ser útil quando a origem dos usuários da empresa é conhecida e limitada, ele pode muitas vezes representar desafios na manutenção contínua e na atualização da lista de fontes aceitas. Além disso, hackers experientes podem fazer uso de proxies para contornar o bloqueio geográfico. No entanto, esse método continua sendo uma escolha popular e uma estratégia de defesa inicial contra ataques de DDoS da Camada 7.

Análise do protocolo da camada de aplicativo: esse método pode mitigar ataques de DDoS da Camada 7 ao examinar dados dentro de protocolos de camada de aplicativo para detectar anomalias ou padrões mal-intencionados, possibilitando mecanismos de defesa proativos. Esse método pode evitar ataques de DDoS sofisticados que contornam medidas de segurança convencionais. No entanto, ele pode consumir muitos recursos para realizar a inspeção profunda de pacotes e tem maiores chances de apontar falsos positivos, o que poderia bloquear indevidamente o tráfego legítimo.

Elaboração da receita certa e equilibrada para uma estratégia de defesa contra DDoS de várias camadas

Criar uma estratégia de defesa contra DDoS de várias camadas envolve uma abordagem diferenciada, adaptada ao perfil de risco específico de uma organização e ao cenário em evolução das ciberameaças. Fundamentalmente, essa estratégia exige uma avaliação inicial para identificar os ativos críticos e possíveis vetores de ataque, além da implementação de proteções base, como limitação de taxa e firewalls. Etapas avançadas exigem uma combinação de detecção baseada em anomalias para novas ameaças, detecção baseada em assinaturas para ataques conhecidos e mecanismos de resposta a desafios para filtrar bots.

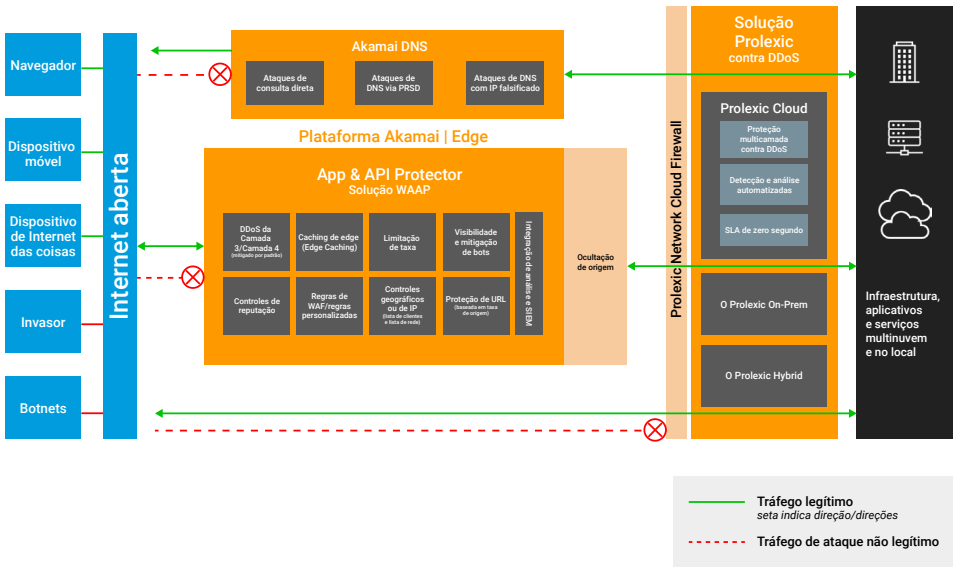
Incorporando inteligência adaptativa contra ameaças, como algoritmos que determinam padrões de impressão digital de TLS de fontes de ataque de DDoS conhecidas e emergentes, o sistema de segurança pode adaptar automaticamente a mitigação para bloquear ou desafiar o tráfego que exibe essa impressão digital, mitigando efetivamente o ataque. Um plano abrangente de resposta a incidentes e recuperação é essencial para minimizar os danos e manter a confiança durante e após um ataque. A aprendizagem contínua e os ajustes baseados em ataques anteriores e tendências emergentes mantêm a estratégia de defesa eficaz e resiliente.

Uma instituição financeira que lida com ataques de DDoS sofisticados e multivetoriais é um exemplo nítido da importância de ter uma estratégia de defesa equilibrada e multicamada. O impacto que o tempo de inatividade pode ter em suas operações e na confiança do cliente torna essas instituições os principais alvos.

Ao integrar uma combinação de métodos de detecção e mitigação, como detecção de anomalias de tráfego, usando métodos convencionais, como limitação de taxa, filtragem geográfica ou por IP, reputação do IP e inteligência contra ameaças em tempo real, juntamente com um plano robusto de resposta a incidentes, é possível proteger ativos essenciais contra interrupções e garantir a continuidade do serviço aos clientes. Esta ampla abordagem exemplifica como as organizações podem se defender contra a natureza multifacetada dos ataques de DDoS no cenário digital atual.

Preparo: estratégia de defesa em profundidade com a arquitetura de edge da Akamai

A abordagem da Akamai para a proteção contra DDoS na camada de aplicativo é multicamada, abrangente e adaptável, pensada para proteger websites, aplicativos e APIs contra os ataques mais sofisticados. Nosso App & API Protector aproveita vários recursos essenciais que fornecem proteção abrangente, combinando um firewall de aplicativos da Web, visibilidade e mitigação de bots, segurança de APIs e proteções contra ataques de DDoS da Camada 7 em um único produto para oferecer proteção ampla.



Arquitetura de referência para proteção holística contra DDoS usando DNS de edge, o App & API Protector e soluções Prolexic

A estratégia de proteção contra DDoS da Akamai é desenvolvida com base em uma arquitetura de defesa de edge que direciona o tráfego para a plataforma altamente distribuída da Akamai, onde cada solicitação é inspecionada em tempo real. Esta configuração cria uma proteção contra ataques de DDoS, app da Web e API, e bots mal-intencionados na edge, e é ela que impede que eles cheguem aos aplicativos ou à infraestrutura. Isso aumenta a continuidade dos negócios, mantendo uma arquitetura rápida, altamente segura e sempre disponível que se escala com ataques.

O conjunto de ferramentas e soluções robusto da Akamai fornece controles proativos e reativos, cada um servindo um propósito distinto na estratégia geral de defesa.

Controles proativos

Os controles proativos ajudam a evitar ataques antes que eles aconteçam, focando no fortalecimento da postura de segurança para minimizar vulnerabilidades. Estão incluídos:

- **Controles de IP (bloquear IP, intervalos CIDR e ASNs):** esses controles constituem uma camada fundamental de defesa, pois bloqueiam endereços IP mal-intencionados conhecidos ou intervalos identificados por meio de inteligência contra ameaças.
- **Controles geográficos (bloquear locais determinados):** ao permitir ou limitar o tráfego de regiões específicas, as organizações podem limitar preventivamente a exposição a ataques provenientes de áreas de alto risco.
- **Regras de WAF (firewall de aplicativos da Web):** implementar regras contra vulnerabilidades conhecidas e vetores de ataque, como ferramentas como o FiberFox, oferece uma forte primeira linha de defesa.
- **Controles de reputação de IP:** o uso de inteligência por meio de heurísticas de recursos mal-intencionados conhecidos de DDoS, web scraping e outras atividades mal-intencionadas permite o bloqueio preventivo ou a análise minuciosa do tráfego suspeito.
- **Plataforma de inteligência contra DDoS:** as informações de ataques de DDoS da plataforma de edge da Akamai, distribuída globalmente, podem ajudar a criar uma estratégia de mitigação proativa no combate a ataques de DDoS da camada de aplicativo.
- **Armazenamento em cache:** otimizar o armazenamento de conteúdo em cache pode reduzir significativamente a carga nos servidores de origem, mitigando indiretamente o impacto de DDoS ao atender solicitações do cache de edge.
- **Site Shield:** a ocultação de origem permitindo apenas solicitações de origens da rede de edge da Akamai pode reduzir ainda mais as cargas do servidor.

Controles reativos

Os controles reativos são respostas a um ataque detectado. O objetivo desses controles é mitigar o impacto do ataque e manter a disponibilidade do serviço.

- **Limitação de taxa (políticas de taxa):** são essenciais para mitigar picos súbitos de tráfego que podem indicar um ataque de DDoS. A configuração pode ser definida e adaptada para perfis de tráfego específicos do cliente. A limitação de taxa muitas vezes funciona como a primeira linha de defesa na proteção da origem do cliente contra ataques de DDoS volumétricos e distribuídos.
- **Proteção de Slow POST:** especificamente visando ataques de HTTP POST, esse controle reage a padrões de tráfego anormais que têm como objetivo esgotar os recursos do servidor.

- **Regras personalizadas no WAF:** é possível adaptar as regras rapidamente em resposta a ameaças emergentes, oferecendo mecanismos de defesa flexíveis e dinâmicos.
- **Visibilidade e mitigação de bots:** com aprendizado de máquina para detectar a apropriação indevida do navegador, é possível identificar e bloquear ataques de DDoS sofisticados que usam automação.
- **Proteção de URL com eliminação inteligente de carga:** controles que limitam solicitações excessivas à origem e priorizam usuários legítimos em relação ao tráfego mal-intencionado podem ajudar a manter o tempo de atividade do serviço durante um ataque de DDoS.
- **Plataforma de inteligência contra DDoS:** a eliminação de carga é uma categoria na proteção de URL que usa informações de ataques de DDoS da plataforma Akamai distribuída globalmente e permite que nossos clientes criem uma estratégia de mitigação proativa para combater ataques de DDoS da camada de aplicativo.

A mistura de ingredientes para uma receita equilibrada

- **Exemplo:** uma grande organização de serviços financeiros elabora uma estratégia de defesa aprofundada com a solução Akamai WAAP

Algumas organizações podem ser alvos mais frequentes de ataques de DDoS. De acordo com pesquisas da Akamai, mais de um terço dos ataques de DDoS em 2023 foram efetuados em instituições de serviços financeiros. Uma grande organização de serviços financeiros, um cliente da Akamai, enfrentou um ataque direcionado à sua página de login. Mas ela seguiu uma receita comprovada para defesa. Você pode fazer o mesmo.


Perfil do invasor: hacktivista


Meta: ponto de extremidade de login


Método: inundação de HTTP POST


Fontes de ataque: aprox. 66 mil endereços IP e cerca de 140 países

Receita

Mitigação de um ataque de inundação de HTTP POST

Ingredientes:

Controles proativos:

- **Controles de IP**: use a inteligência contra ameaças para bloquear endereços IP ou intervalos CIDR associados a entidades mal-intencionadas conhecidas.
- **Controles geográficos**: coloque certas regiões conhecidas por abrigar grupos de hacktivistas, como regiões associadas ao "Anonymous Sudan", na lista de negações.
- **Regras de WAF (firewall de aplicativos da Web)**: implemente regras especificamente projetadas para neutralizar as ferramentas e táticas conhecidas de DDoS, incluindo padrões típicos de inundações de HTTP GET.
- **Controles de reputação de IP**: monitore ou bloqueie ativamente o tráfego (em tempo real) de fontes com má reputação.
- **Plataforma de inteligência contra DDoS**: aplique informações dos dados globais de ataques de DDoS da Akamai para antever e neutralizar vetores de ameaças emergentes.
- **Site Shield**: ative ACLs (listas de controle de acesso) de firewall para permitir apenas o tráfego da rede de edge Akamai e bloquear o resto.

Controles reativos:

- **Limitação de taxa**: estabeleça políticas de taxas para mitigar picos repentinos no tráfego, definindo limites apropriados para solicitações por segundo à página inicial. Você pode otimizar sua limitação de taxa das seguintes formas: (1) reduzir as janelas de tempo para medir a velocidade da solicitação para uma solicitação por segundo e (2) aplicar a limitação de taxa com base na geografia e na pontuação de reputação das fontes de IP conectadas enquanto permite a listagem de fontes, como endereços IP corporativos e parceiros da instituição financeira.
- **Regras personalizadas no WAF**: crie regras personalizadas em resposta às características específicas do ataque detectado. O uso de controles de amostragem de tráfego em suas regras personalizadas ajudará na análise de tráfego para, desta forma, analisar de forma mais eficiente as principais fontes de ataque. Já os controles geográficos ou de IP nas regras personalizadas podem ajudar na mitigação rápida.
- **Visibilidade e mitigação de bots**: use a detecção de falsificação de navegador para identificar e bloquear solicitações que imitam o comportamento legítimo do usuário, mas fazem parte da inundação.
- **Proteção de URL**: aplique controles para limitar as taxas de solicitação especificamente ao URL de login, preservando a largura de banda para usuários legítimos. Configurar a eliminação inteligente de carga com categorias como proxies, nós de saída Tor, bots básicos, IPs de baixa reputação etc. ajudará a priorizar o tráfego real do usuário.

Método de preparo:

Fase de análise:

- **Análise da configuração**: conduza uma revisão completa de sua postura de segurança atual. Configure os controles proativos com base no que você encontrar, garantindo que todos os controles geográficos e de IP relevantes sejam gerenciados adequadamente.
- **Otimização da configuração**: ajuste a configuração para reconhecer e mitigar padrões de tráfego incomuns, incluindo os característicos de ataques de inundação de HTTP POST.

Fase de detecção e mitigação:

- **Monitoramento e alertas**: a arquitetura de defesa de edge da Akamai pode monitorar o tráfego de entrada para identificar padrões que podem indicar um ataque de DDoS. Você pode configurar alertas para picos de tráfego anormais ou padrões que correspondem aos métodos de DDoS conhecidos, como inundação de HTTP POST.
- **Detecção e mitigação**: vários controles proativos, como reputação de IP, armazenamento em cache e controles geográficos ou de IP, fornecem automaticamente recursos de detecção e mitigação, se configurados corretamente.

  Quando um ataque é detectado, controles como limitação da taxa, proteção de URL e detecção de falsificação de navegador são acionados automaticamente, sem precisar de intervenção do usuário.
- **Análise e adaptação**: analise continuamente os padrões de ataque e adapte suas medidas defensivas em tempo real para neutralizar as táticas em evolução. Por exemplo, crie regras personalizadas ou políticas de limitação de taxa com base na análise recente do tráfego de ataques.

Recuperação e análise pós-ataque:

- **Análise de registros**: após o ataque, realize uma análise detalhada do registro de tráfego para identificar os vetores de ataque e a eficácia dos controles implantados.
- **Ajustes**: faça os ajustes necessários aos controles proativos e reativos com base nas informações obtidas na análise de ataque.

Sugestões de consumo:

- Analise e atualize regularmente sua estratégia de defesa para se adaptar às táticas de DDoS em evolução. Essas análises podem variar significativamente entre diferentes organizações, já que são influenciadas pelas necessidades específicas da organização, pela exposição a ameaças e pelas práticas recomendadas do setor. Uma organização de serviços financeiros pode precisar dessas avaliações a cada trimestre, enquanto uma plataforma de comércio eletrônico pode precisar de avaliações semestrais para se preparar para picos de compras sazonais.
- Participe de treinamento contínuo para que a equipe de segurança reconheça e responda a novos vetores de ataque de DDoS.
- Conduza ataques simulados para testar a eficácia das medidas implementadas e preparar a equipe para incidentes do mundo real.

Recuperação e análise pós-ataque

Quando se trata da defesa contra ataques de DDoS na camada de aplicativo (Camada 7), a fase pós-ataque é essencial para fortalecer defesas futuras e entender seu adversário. Ela envolve duas etapas críticas: analisar o padrão de ataque e melhorar suas defesas com base na análise. Estas etapas são fundamentais para criar uma estratégia de defesa resiliente e garantir a continuidade e integridade dos serviços online.

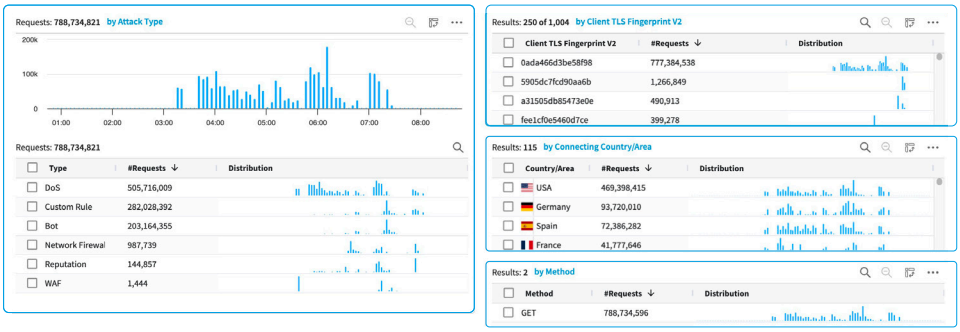
Análise do padrão de ataque e tráfego

Depois de lidar com um ataque, a próxima etapa é analisar o incidente para entender qual estratégia funcionou e qual não funcionou como previsto. Esta avaliação abrange fatores de longo prazo, como o impacto na confiança do cliente, a integridade dos dados e as potenciais perdas financeiras. Sistemas abrangentes de análise de segurança, como o Akamai Web Security Analytics, são ferramentas indispensáveis nesta fase, pois permitem que as organizações entendam o tráfego de ataques e seus impactos.

Esta análise envolve o destrinchamento de TTPs (táticas, técnicas e procedimentos) usados pelos invasores. As principais perguntas que devem ser feitas incluem:

- Qual foi a natureza do pico de tráfego?
- Foram alvo funcionalidades específicas do aplicativo?
- O ataque explorou vulnerabilidades conhecidas?

O Akamai Web Security Analytics pode identificar anomalias nos padrões de tráfego, identificar a origem geográfica do ataque e classificar o tipo de ataque com base em comportamentos observados. O exemplo a seguir mostra algumas das características ou dimensões de tráfego que podem ser aplicadas para investigar um ataque de DDoS.



As imagens exibidas são do Web Security Analytics, que fornece visibilidade sem precedentes e análise proativa de eventos de segurança

Revisão e atualização de estratégias de defesa com base na análise do ataque

Revisar e atualizar as estratégias de defesa com base na análise de ataques é essencial para fortalecer a postura de cibersegurança de uma organização. Ao examinar as especificidades de um ataque anterior, as organizações podem identificar vulnerabilidades em suas defesas atuais e fazer ajustes embasados. Aqui estão alguns exemplos de como esse processo pode ser aplicado usando o Akamai Web Security Analytics.

Exemplo 1: atualização das regras de WAF com base em padrões de ataque

Cenário: uma organização enfrenta um ataque de DDoS da Camada 7 visando seu aplicativo da Web com uma enxurrada de solicitações mal-intencionadas para a página inicial do aplicativo.

Análise: a análise de ataque revela que as regras existentes do WAF (firewall de aplicativos da Web) detectaram e bloquearam adequadamente mais de 90% do tráfego de ataque, mas os 10% restantes passaram porque havia uma lista de permissões geográficas explícita permitindo que fontes de ataque desse local sobrecarregassem o aplicativo.

Atualização: com base nesta análise, a organização atualizou suas configurações de WAF para usar uma regra de WAF personalizada que corresponde às características específicas do tráfego de ataque a partir desse local específico. Modificações podem continuar permitindo a localização, mas bloquear os atributos específicos do tráfego de ataque. Além disso, as configurações de limitação de taxa para esse local específico ficaram mais rigorosas.

Exemplo 2: aprimoramento da proteção da origem

Cenário: o processo de login de um website de varejo é alvo de um ataque de DDoS altamente distribuído e sofisticado da Camada 7, que utiliza bots automatizados.

Análise: a análise pós-ataque indica que o tráfego de ataque foi altamente distribuído, proveniente de mais de 150 países e centenas de impressões digitais de TLS que se parecem com navegadores legítimos. Uma boa parte do tráfego se originou de provedores de nuvem, alguns dos quais estavam na lista de permissões como fontes de parceiros confiáveis. Embora o ataque tenha sido efetivamente mitigado, a análise revelou a necessidade de medidas adicionais de defesa.

Atualização: para proteger URLs de alta computação, como um processo de finalização de compra, a organização implementou a proteção de URL, um recurso projetado especificamente para proteger URLs e pontos de extremidade de API que utilizam muita computação contra ataques de DDoS da camada de aplicativo altamente distribuídos. Um arquiteto de segurança também habilitou a eliminação inteligente de carga para bots, proxies, reputação de IP etc. Esse sub-recurso de proteção de URL ajuda a priorizar o tráfego real do usuário, negando solicitações de fontes mal-intencionadas.

A organização também decidiu habilitar a funcionalidade de proteção de bots integrada no WAF que anteriormente não foi considerada pela empresa devido à presença de uma solução de bot no local que não foi capaz de escalar durante esse ataque de alta velocidade.

Exemplo 3: implementação de limitação de taxa para pontos de extremidade de API

Cenário: um ponto de extremidade de API de um aplicativo de serviços financeiros foi sobrecarregado com uma inundação de solicitações de transações fraudulentas, o que indica um ataque de DDoS da Camada 7 destinado a esgotar os recursos do servidor.

Análise: a análise do padrão de ataque mostra que os invasores visaram especificamente os pontos de extremidade de API menos protegidos, incapazes de processar um alto volume de solicitações.

Atualização: em resposta, a organização implementou uma limitação rigorosa de taxa em todos os pontos de extremidade de API, especialmente nos identificados como vulneráveis. A organização também adotou um complemento de segurança de APIs dedicado que fornece camadas avançadas para segurança de APIs, incluindo abuso de lógica de API, ameaça de APIs sombra e monitoramento de vulnerabilidades de API.

Conclusões estratégicas

- **Monitoramento e registros contínuos:** defina sistemas robustos de monitoramento e registro para detectar prontamente anomalias e avaliar com precisão os danos durante e após um ataque.
- **Gerenciamento de vulnerabilidades:** atualize e corrija sistemas regularmente para mitigar vulnerabilidades conhecidas, reduzindo o risco de exploração.
- **Análise de padrão de ataque:** use ferramentas de visibilidade apropriadas para uma análise profunda dos padrões de ataque para entender as metodologias e intenções dos invasores.

Análise pós-ataque

Entre os componentes essenciais de uma estratégia de robusta de defesa contra DDoS da Camada 7, está a avaliação do dano e a análise do padrão de ataque. Essas etapas não só ajudam a compreender e mitigar os impactos imediatos de um ataque, mas também fundamentam a melhoria contínua dos mecanismos de defesa, garantindo uma melhor preparação para futuras ameaças.

Manutenção e atualização das receitas

Manter uma forte defesa contra DDoS da Camada 7 exige monitoramento constante das tendências e técnicas mais recentes.

Os invasores consistentemente misturam padrões de ataque, aproveitando novas ferramentas e vulnerabilidades. Para combater proativamente essas ameaças, as organizações devem investir tempo e esforços em pesquisas, monitoramento, avaliação de defesas, automação de proteções e colaboração com a comunidade de inteligência contra ameaças.

O monitoramento dos principais fóruns de cibersegurança é apenas um bom ponto de partida. Sugerimos uma abordagem mais prescritiva:

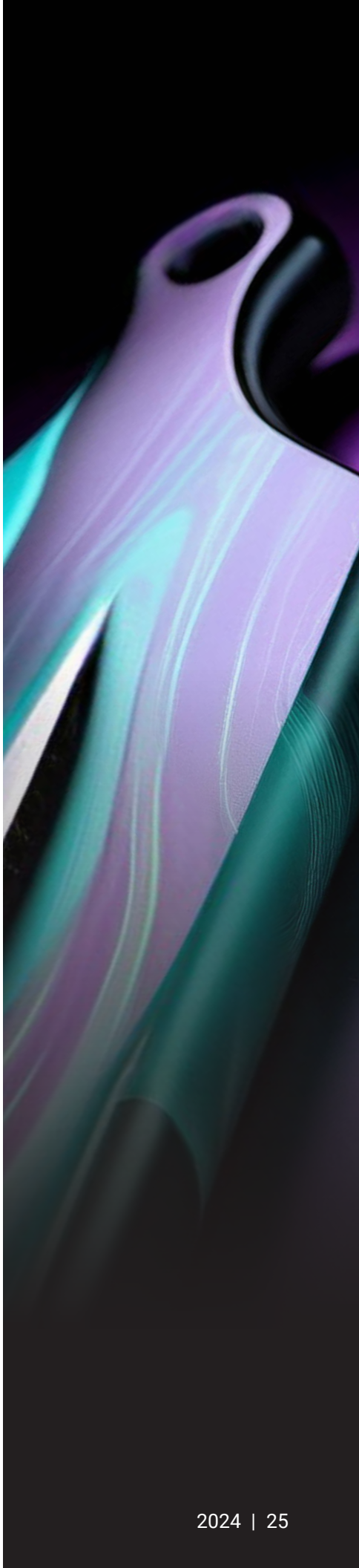
Monitoramento e avaliação contínuos: monitore regularmente o desempenho da sua rede e dos aplicativos para detectar novos padrões ou anomalias que indiquem ameaças emergentes. Use esses dados para avaliar a eficácia dos mecanismos de defesa existentes, identificando áreas de melhoria ou ajustes.

Formação de uma equipe anti-DDoS: defina a pessoa ou a equipe dentro da organização que vai pesquisar e monitorar o cenário de ataques de DDoS e reportar à organização em geral pelo menos trimestralmente quaisquer descobertas e recomendações importantes.

Participação na comunidade de inteligência contra ameaças: os invasores se comunicam entre si sobre os métodos mais recentes e eficazes. Não há motivos para você não se comunicar com colegas em outras empresas e setores sobre as melhores defesas. Fique por dentro da mais recente inteligência contra ameaças. Assine feeds de segurança, participe de fóruns de cibersegurança e colabore com colegas de seu setor. Essas informações ajudarão você a antever novos vetores de ataque e ajustar suas defesas conforme necessário.

Suporte do seu fornecedor de cibersegurança: os fornecedores de tecnologia geralmente têm grupos dedicados de pesquisa de ameaças, e os que têm uma rede de entrega de conteúdo podem fornecer informações que não estão disponíveis em nenhum lugar. Aproveite essas oportunidades de aprendizagem sempre e onde você puder. Também é importante falar com especialistas em consultoria de segurança periodicamente.

Testes em suas próprias defesas: "falhar em se preparar é se preparar para falhar", "a prática leva à perfeição"... Qualquer que seja o clichê, a mensagem é a mesma: realizar testes e simulações regulares compensa.



Realize revisões periódicas e cenários de ataque simulados (exercícios de equipe vermelha) para testar a resiliência de suas estratégias de defesa. Esses exercícios podem revelar pontos fracos em sua configuração atual e fornecer insights sobre como os invasores podem explorar seu sistema.

Faça um teste da sua rede pelo menos uma vez por ano. Perfis de ataques recentes também podem ser uma boa referência para um caso de teste, particularmente um que aconteceu com uma empresa em seu setor.

Compartilhamento dos aprendizados com a comunidade: vale a pena reiterar: assim como os invasores compartilham suas ferramentas e táticas, as organizações também devem se envolver no compartilhamento de conhecimento sobre estratégias de defesa bem-sucedidas.

Ao documentar sucessos e fracassos, os profissionais de cibersegurança podem fornecer informações do mundo real que enriquecem a base de conhecimento coletiva. Envolver-se em fóruns do setor, oferecer orientação para colegas mais novos e participar de projetos colaborativos é fundamental para promover um ecossistema de defesa robusto. Tais esforços não só contribuem para o desenvolvimento de estratégias e ferramentas mais eficazes, mas também possibilitam um conjunto diversificado de experiências e informações que podem se adaptar às táticas de mudança dos agentes de ameaças. Esse espírito colaborativo é essencial para se manter à frente no cenário de cibersegurança, tornando cada contribuição valiosa na construção de um mundo digital mais forte e resiliente.

Principal conclusão

O cenário das ameaças de DDoS é dinâmico, com os invasores constantemente buscando novas maneiras de burlar as defesas. Manter e atualizar suas estratégias de proteção contra DDoS da Camada 7 é um processo contínuo que requer vigilância, adaptabilidade e uma abordagem proativa. Ao se atualizar, participar de testes e avaliações regulares e promover uma cultura de melhoria contínua, você pode manter uma defesa robusta contra ameaças presentes e futuras.

Conclusão

É evidente que os ataques de DDoS da Camada 7 não só estão mais sofisticados, como também estão mais fáceis de serem lançados graças aos avanços na automação e à coordenação entre os invasores. Enquanto isso, as organizações precisam defender um cenário maior e mais complexo, mesmo quando os custos do fracasso aumentam.

De fato, elaborar uma receita de defesa não é uma tarefa fácil. Nenhum método oferece uma solução totalmente eficiente para ataques de DDoS da Camada 7. Como demonstramos, uma abordagem multifacetada que combina várias estratégias de detecção e mitigação fornece a defesa mais robusta.

Além disso, a escolha dos métodos deve ser guiada pelas necessidades específicas, pelos padrões de tráfego e pelo perfil de risco do aplicativo ou serviço que está sendo protegido. Não é possível implementar uma defesa sem entender sua empresa, seu tráfego e suas vulnerabilidades. Atualizações e ajustes regulares a essas estratégias são essenciais para se adaptar ao cenário em evolução das ameaças de DDoS.

Por fim, também é evidente que o trabalho não acaba só porque o ataque acabou. A análise e os ajustes pós-ataque são fundamentais para o sucesso contínuo e podem ajudar a desempenhar um grande papel no compartilhamento de conhecimento e no desenvolvimento de carreira.

Felizmente, a Akamai está bem posicionada para fornecer assistência em cada etapa do caminho. Desde a proteção de aplicativos e APIs, até informações incomparáveis sobre o tráfego global e análises especializadas pós-ataques, muitas empresas estão aproveitando a oportunidade de obter todas as proteções contra DDoS da Camada 7 de que precisam em um único provedor.

Veja as proteções contra DDoS da Camada 7 da Akamai em ação.
Inicie uma avaliação gratuita do App & API Protector.

Créditos

Editorial e redação

Aseem Ahmed
Barney Beal

Revisão e contribuição especializada

Abdeslam Bella
Sean Flynn
Alex Marks-Bluth
Nitesh Shrivastava
Prathmesh Verma
Dennis Birchard
Ryan Gao
Pawan Sajnani
Patrick Sullivan
Danielle Walter

Marketing e publicação

Georgina Morales Hampe
Shivangi Sahu

As soluções de segurança da Akamai protegem os aplicativos que impulsionam seus negócios em cada ponto de interação, sem comprometer o desempenho ou a experiência do cliente. Ao aproveitar a escala de nossa plataforma global e sua visibilidade de ameaças, trabalhamos com você para evitar, detectar e mitigar ameaças, permitindo que você construa a confiança na sua marca e opere de acordo com a sua visão. Saiba mais sobre as soluções de computação em nuvem, segurança e entrega de conteúdo da Akamai em akamai.com/ e akamai.com/blog, ou siga a Akamai Technologies no X, antigo Twitter, e LinkedIn. Publicado em 10/24.