Akamai

WHITE PAPER

Como evitar o caos em uma festa

com a plataforma certa de DDoS na camada de aplicação

O que o DDoS na camada de aplicação significa para nós hoje

Como os especialistas em segurança de todo o mundo sabem, DDoS, ou negação de serviço distribuída, é um ataque cibernético que tenta tornar um website ou recurso de rede indisponível, inundando-o com tráfego mal-intencionado para que ele não possa operar. Os ataques DDoS ainda são a técnica de ataque mais popular usada por agentes de ameaça e tem estado em ascensão nos últimos cinco anos. Por exemplo, um dos grandes ataques mais recentes (em termos de pacotes por segundo [PPS]) atingiu um pico de 809 MPPS em cerca de dois minutos.

Uma tendência que observamos nesse crescimento de ataques é o aumento das instâncias de ataques DDoS na camada de aplicação. Também conhecidos como DDoS na camada 7, esses ataques visam e interrompem aplicações da Web específicas (não redes inteiras). Portanto, embora a prevenção e a mitigação sejam difíceis para os defensores, a alta adoção de tecnologias como automação e serviços em nuvem deu aos invasores acesso fácil às ferramentas necessárias para lançar esses ataques, facilitando, mais do que nunca, comprometer a camada de aplicação.

A realidade é que as solicitações usadas neste tipo de ataque parecem solicitações normais do usuário final, portanto não há maneira fácil de avaliar a sofisticação de um ataque. A eficiência de afetar o servidor de destino e a rede significa que um ataque gera mais danos com menos largura de banda total. Em resumo, os ataques à camada de aplicação são fáceis de implementar, difíceis de desacelerar ou interromper e específicos para um alvo.

Para entender como os ataques DDoS na camada de aplicação estão afetando exclusivamente nossas organizações, precisamos saber como os eles nos afetam em todas as categorias. Considere as categorias de ataques DDoS como as armadilhas de uma festa. Por exemplo, você pode abrir sua casa para alguns convidados para comemorar uma ocasião especial ou se divertir no fim de semana. No entanto, algumas situações podem ocorrer:

tipos de ataques DDoS

Cenário 1
Ataque volumétrico

Seus convidados estão animados com sua festa e compartilham informações demais (talvez em mídias sociais). A notícia de que sua festa é o evento que ninguém quer perder se espalha e, no dia da festa, inúmeros estranhos chegam. Isso representa um ataque DDoS volumétrico, porque todos os seus recursos estão sendo consumidos por pessoas que você não convidou.

Cenário 2
Ataque de protocolo

Um convidado em quem você achava que confiava foi comprometido! Pessoas que querem ser convidadas para sua festa (e não receberam um convite) sobrecarregam um de seus convidados com exigências para saber detalhes do evento. O convidado cede, e um grupo de pessoas não convidadas tem acesso à sua festa. Isso representa um ataque DDoS de protocolo porque alguém que deveria manter a confidencialidade de sua festa não o fez.

Cenário 3
Ataque de aplicação

Uma pessoa mal-intencionada ouve sobre sua festa e decide entrar em sua casa disfarçada de convidado para planejar e cometer um roubo. Isso representa um ataque DDoS de aplicação, porque a pessoa está se fazendo passar por um convidado real.

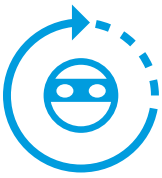
Em todos esses cenários, há uma vulnerabilidade comum: você abriu sua casa para um evento. Essa é a vulnerabilidade inevitável da qual os ataques DDoS da camada de aplicação se beneficiam porque é a camada na qual sua organização interage com o usuário. Além disso, como essa é uma camada sobre a qual você tem menos controle, pois atende diretamente aos usuários, pode ser mais difícil mitigar os ataques DDoS na camada de aplicação.

Além disso, se algum desses problemas ocorrer, você terá um custo adicional. Seja lidando com a despesa de mais comida e bebida consumida, com estranhos descobrindo informações pessoais sobre você ou com as consequências de um ataque à sua casa, uma festa que dá errado custa caro.

Muitas soluções de segurança prometem cada vez mais proteger seus sistemas, recursos e informações confidenciais contra ataques DDoS na camada de aplicação, que agora são mais comuns e um dos mais difíceis de se defender. Você confiou nelas para proteger o que você tem a oferecer. Portanto, no final, suas proteções contra DDoS são tão boas quanto a plataforma à qual você empresta suas proteções. Vejamos as últimas mudanças e tendências a serem observadas ao procurar a plataforma certa de proteção contra DDoS na camada de aplicação.

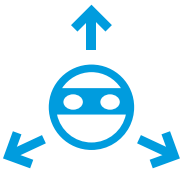
O que é tendência e o que está mudando

Como sempre, quando criamos soluções para um ataque específico, os invasores adaptam suas estratégias para combatê-las. Monitoramos essa concorrência, e aqui estão as quatro tendências e mudanças que vemos no momento:



1. Mudança para ataques repetidos e de curta duração

Os ataques DDoS estão se tornando menos prolongados e se tratam mais sobre o tamanho e a frequência. A Akamai observou ataques complexos com mais de nove vetores diferentes que combinam ARMs, inundação SYN, reflexão UDP (DNS, WS-Discovery etc.), inundação HTTP e muito mais.

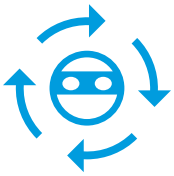


2. Uso mais frequente de ataques multivetoriais

Mais de 20% dos invasores estão usando ataques DDoS multivetoriais, combinando diferentes métodos em um ataque curto e repetindo-o logo em seguida. De acordo com o Link11, o maior número de vetores simultâneos observados foi de 18 – um aumento de 50% em relação a 2021.

3. Aumento da capacidade de evitar detecção e a mitigação subsequente

É difícil distinguir entre o tráfego de ataque e o tráfego normal, especialmente no caso de uma camada de aplicação. Por exemplo, um botnet realiza um ataque de inundação HTTP contra o servidor de uma vítima. Como cada bot em um botnet faz solicitações de rede aparentemente legítimas, o tráfego não é falsificado e pode parecer "normal" na origem.



4. Automatizar primeiro e depois adaptar as táticas

Com a prevalência de plataformas de nuvem e IaaS/PaaS, os invasores têm acesso fácil à automação e ao poder de computação, e é fácil automatizar e lançar ataques forma rápida e em escala. Portanto, esses ataques não são apenas volumétricos, mas mais distribuídos, aleatórios e inteligentemente criados (randomizando parâmetros em solicitações etc.).

Conforme observado no cenário de uma festa, sua casa pode ser comprometida de três maneiras: pelo consumo de recursos, um convidado vulnerável ou um agente de ameaça disfarçado. Com as tendências e mudanças nos ataques à camada de aplicação, sua casa pode estar enfrentando um caos projetado para passar sob seu radar. Em vez disso, tudo é orquestrado entre essas três categorias para desenvolver a ação furtiva, como conferir sua casa com antecedência para ver quantas entradas existem; descobrir a regra de vestimenta da festa com antecedência; ou criar perfis de mídia social falsos para saber mais sobre você a fim de enganar todos os convidados de sua festa para que eles pensem que os agentes de ameaça são seus amigos íntimos.

Devido ao aumento da complexidade com ataques DDoS na camada de aplicação, é útil ter uma estratégia mais holística de proteção do que você poderia ter no passado. Antigamente, qualquer proteção de aplicações Web e APIs (WAAP) poderia atender às suas necessidades, mesmo as WAAPs criadas internamente. Agora, sua WAAP precisa exceder a complexidade dos ataques à camada de aplicação que acontecem atualmente.

Uma abordagem holística para a proteção contra DDoS na camada de aplicação

O que dificulta a detecção de ataques DDoS na camada de aplicação é que, mesmo quando ataques multivetoriais contêm padrões óbvios, um invasor motivado monitorará a resposta do ataque e a modificará para se esquivar de um defensor determinado. Para lidar com esse desafio de forma mais consistente e precisa, é necessário melhorar seus recursos de WAAP em termos de detecção, mitigação e autoatendimento.

Em última análise, você não quer que sua WAAP proteja apenas a porta da frente de sua casa. Você quer que ela seja capaz de defender cada ponto de entrada, entenda como identificar agentes de ameaça disfarçados como convidados e seja escalável se você estiver enfrentando vários ataques de uma só vez. A boa notícia é que: é possível adotar a plataforma certa para mitigar o caos do DDoS na camada de aplicação e continuar os negócios como de costume. Sua estratégia de alívio de DDoS deve se tornar mais holística e se concentrar no seguinte:

A escalabilidade de sua plataforma

Não importa o quanto sua WAAP funciona no dia a dia, se ela não puder ser dimensionada para absorver um ataque volumétrico, falhará rapidamente. É por isso que a plataforma sob a WAAP é tão importante quanto a própria WAAP. Você também quer saber onde a plataforma é executada. Por exemplo, a Akamai tem locais de edge no mundo todo, geralmente nas regiões em que os ataques se originam. É muito mais fácil interromper um ataque DDoS se ele puder ser mitigado exatamente onde começou. Além disso, a escalabilidade tornará muito mais fáceis as operações decisivas, como limitação de taxas e regras personalizadas.

Os recursos de dados e a saída que informam suas proteções

Enquanto qualquer WAAP pode monitorar o tráfego e relatar dados que você gera, considere uma solução capaz de agregar dados de uma perspectiva global. Quando seu provedor de soluções tem visibilidade do tráfego em milhares de empresas, os dados que você gera podem ser contextualizados entre as organizações que enfrentam as mesmas ameaças e podem informar melhor os sistemas de machine learning em vigor em sua solução. Em seguida, suas próprias equipes internas podem obter esses dados e usá-los para iterar e personalizar sua solução.

Visibilidade e precisão da sua solução

Alguns métodos de detecção devem vir por padrão, incluindo detecções comportamentais/baseadas em anomalias, que se concentram além do tráfego de clientes recebidos para a taxa de conexão de origem e os parâmetros de desempenho do servidor. No entanto, quando você tem uma solução escalável informada por um conjunto de dados robusto, sua WAAP será muito mais direcionada e precisa. Além disso, você terá uma compreensão mais detalhada do que está acontecendo em seu tráfego porque a solução é adaptável e capaz de entender se um ataque está oculto (como ataques que se escondem atrás de um proxy aberto na Internet). Tudo isso ajudará a garantir que as pessoas certas sejam notificadas e, ao mesmo tempo, reduzirá drasticamente os falsos positivos.

Então, para resumir, se você fosse planejar uma festa que não corresse o risco de ficar sobrecarregada, você gostaria que sua casa fosse grande o suficiente (escalável) para receber pessoas extras que talvez não tenham sido convidadas. Você deve conversar com outras pessoas que tiveram experiências ruins com festas (recursos de dados) para saber antecipadamente as proteções que devem ser implementadas. Você vai querer compartilhar a lista de convidados com antecedência e cumprimentá-los antes que eles entrem em sua casa (visibilidade e precisão) para garantir que todos estejam seguros.

Se você não quiser fazer todo esse trabalho por conta própria, poderá contratar reforços de confiança para fazer o trabalho para você. Os serviços gerenciados podem monitorar todos os sinais aos quais você precisa estar muito atento para distinguir um convidado comum de um mal-intencionado. Além disso, você elimina o estresse de ter que dedicar o tempo e a experiência de sua equipe na prevenção contra ataques 24 horas por dia para esse tipo de ataque cada vez mais comum e difícil de detectar.

A conversa sobre DDoS na camada de aplicação é repleta de variáveis e vulnerabilidades que vêm naturalmente como parte da camada de aplicação. É uma conversa importante porque os ataques DDoS na camada de aplicação podem ser os mais prejudiciais para a sua organização. No entanto, a defesa contra esse tipo de ataque não precisa ser complicada ou caótica. Tudo o que você precisa é de uma solução estratégica, escalável e orientada por dados, e então você pode se divertir na festa.

Saiba mais sobre como a Akamai pode oferecer suporte a você com proteções contra DDoS da Camada 7.