Akamai

WHITE PAPER

Vetores de ataque que ameaçam a confiança do seu cliente

A segurança e a confiança da marca nunca foram mais interdependentes. Com aplicativos e APIs impulsionando a forma como as marcas aparecem no mundo, e o volume de ataques cibernéticos que disparou globalmente, a proteção de aplicativos digitais sem prejudicar a experiência do cliente se tornou a primeira tarefa para equipes de segurança em todo o mundo.

Experiências robustas do cliente constroem a confiança da marca, o que tem um impacto mensurável sobre o desempenho dos negócios. Desde o desempenho do website até a proteção de dados e tudo o que há entre eles, as escolhas de segurança que as organizações fazem afetam a experiência do cliente com muita frequência para pior. Controles trabalhosos que protegem a empresa podem introduzir áreas de atrito para o cliente, resultando em perda de confiança e, por fim, perda de receita.

As escolhas de segurança também afetam o crescimento e a inovação. À medida que as empresas continuam a expandir digitalmente e migrar dados e aplicativos para a nuvem, inúmeros agentes de ameaça estão focados em vetores de ataque abertos por essas mudanças. As soluções de segurança agora devem ter como objetivo evoluir à frente das táticas em constante mudança e ataques multivetoriais sofisticados (diferentes tipos de ataques ao mesmo tempo ou em rápida sucessão) desses agentes, selecionando soluções que trabalham juntas para proteger sua empresa e a confiança que seus clientes depositaram em sua marca.

Quais vetores de ataque devem estar no topo da sua lista?

O mais novo grande alvo no pedaço: APIs

Os aplicativos impulsionam quase todos os aspectos de sua empresa, e as APIs (interfaces de programação de aplicativos), que conectam elementos de software e permitem a comunicação entre vários aplicativos, tornaram-se um novo alvo favorito para os agentes de ameaça. Por quê? Muitas vezes, os aplicativos e processos de negócios que envolvem APIs são iniciados e implantados mais rapidamente do que as equipes de segurança podem avaliá-los, levando a configurações incorretas e vulnerabilidades. Essas falhas são o que os agentes de ameaça procuram: usando abuso de lógica de negócios, os ataques a APIs bem-sucedidos permitem que eles consigam acesso ao seu ambiente, onde podem roubar dados e até lançar ataques adicionais. Além disso, eles não são apenas direcionados a APIs que passam pelo firewall de aplicativos da Web. Mesmo quando autenticadas pelo WAF, as APIs ainda podem se tornar vulneráveis a ataques, indicando que os invasores estão realizando regularmente o reconhecimento para identificar APIs específicas a serem exploradas.

É importante lembrar que qualquer API pode ser um alvo potencial. Em setores como a saúde, a interoperabilidade de dispositivos de Internet das coisas, por exemplo, tornou as APIs um alvo enorme para criminosos que buscam roubar informações de identificação pessoal (PII) ou lançar ataques de ransomware. Assim, a proteção de APIs começa com a obtenção de uma visão de cada API associada à sua organização, o que também é conhecido como patrimônio de APIs.

O Akamai API Security realmente ajuda você a fazer o inventário de seu patrimônio e, em seguida, fornece visibilidade do comportamento histórico de cada API para que você possa saber como é o comportamento normal da API em comparação com o abusivo. Com esse conhecimento, você pode procurar por ameaças ativas para poder interromper o abuso rapidamente, antes que os agentes de ameaça atinjam suas metas.

Mais sofisticado e mais fácil de implantar do que nunca: bots maliciosos

Os bots estão passando pelo seu website o tempo todo. Na verdade, todos os seus esforços de otimização de mecanismos de busca são direcionados para obter benefícios dos bots. Os bots mal-intencionados que realizam uma série de ataques cibernéticos estão misturados entre os bots bons. Os bots maliciosos são talvez mais conhecidos por monopolizar o inventário limitado, como comprar calçados esportivos de edição limitada ou grandes quantidades de ingressos para concertos ou reservas de hotéis, mas eles usam praticamente o mesmo método ao sobrecarregar sua empresa com um número excessivo de solicitações em um ataque de negação de serviço distribuída, ou DDoS, que é projetado para deixar sua empresa offline.

O que muitas pessoas não sabem é que o DDoS se tornou uma forma de ataque relativamente fácil e barata que está sendo usada por uma nova cultura de invasores para derrubar corporações multibilionárias e infraestrutura pública crítica, incluindo escolas, hospitais, aeroportos e provedores de serviços públicos. Esses ataques criam enormes interrupções de serviço que custam às vítimas enormes quantidades de receita por minuto. Em uma mudança marcante de invasores tradicionais do passado, esses ataques são quase sempre realizados por agentes sofisticados de estados-nação, hacktivistas políticos e cibercriminosos profissionais com a ajuda de botnets, ou seja, grandes redes de dispositivos conectados (que podem ser dispositivos de usuário ou dispositivos simples de Internet das coisas) infectadas e controladas por bots.

Os bots também são usados para iniciar ataques de preenchimento de credenciais que levam a ataques de apropriação indevida de contas. O preenchimento de credenciais ocorre quando um invasor usa uma lista de nomes de usuário e senhas obtidas durante uma grande violação de dados e envia essas credenciais em grandes tentativas de fazer login em outras instituições. Os bots são implantados para realizar milhões de tentativas de apropriação de contas e, como muitas pessoas tendem a reutilizar nomes de usuário e senhas, uma pequena fração funcionará. Depois que o invasor obtém acesso a uma conta, isso se torna um ataque de apropriação indevida de contas.

O preenchimento de credenciais é apenas um dos muitos métodos que os agentes de ameaça usam para se apropriar de contas legítimas. Uma vez que controlam uma conta, podem desviar pontos de fidelidade e transferir os ativos digitais, esgotar os saldos de vales-presentes e fazer compras fraudulentas usando as informações armazenadas do cartão de crédito. Eles podem até mesmo vender toda a conta para outro agente de ameaça. Se isso acontecer com seus clientes, a confiança é quase sempre irrevogavelmente quebrada. Mas até mesmo ataques malsucedidos de preenchimento de credenciais podem ser prejudiciais à sua marca, porque o tráfego de bots que inunda seu website durante essas tentativas pode reduzir significativamente a disponibilidade de recursos e causar tempos de resposta lentos, criando experiências frustrantes para seus clientes e visitantes do website.

Finalmente, os bots de scraper são usados para bons fins e para fins mal-intencionados, mas o menos óbvio é que sua presença pode diminuir o desempenho do website e poluir as métricas de que as empresas precisam para tomar decisões importantes, tornando seus efeitos colaterais potencialmente piores para sua marca do que o que elas capturam.

A Akamai tem um conjunto de soluções desenvolvidas especificamente para mitigar as ameaças introduzidas por bots maliciosos:

O Akamai App & API Protector com proteção contra malware é a base para a proteção contra roubo de seus dados, PII e outras informações de conta, e para bloquear ataques de DDoS orientados por bots, bem como ransomware, malware e muito mais. Ele permite que seus clientes tenham acesso constante às suas propriedades da Web e garante que o desempenho do website não seja reduzido quando você enfrentar um ataque.

O Akamai Bot Manager detecta todo o tráfego de bots e mitiga bots mal-intencionados na edge. Ele usa modelos de IA para analisar o comportamento dos bots e implanta algoritmos de impressão digital do navegador e machine learning (ML) para tornar a detecção cada vez mais precisa, reduzindo o atrito para os usuários e os protegendo contra atividades fraudulentas.

O Akamai Content Protector evita que scrapers roubem seu conteúdo da Web que pode ser usado para fins mal-intencionados, além de reduzir a degradação do desempenho do website. Com a detecção orientada por ML, a atividade de scraper de bots potencialmente mal-intencionados é classificada por risco para informar a resposta apropriada.

Outra solução fundamental para proteger seus clientes é aprimorar o acesso seguro à conta. O Akamai Account Protector impede fraudes humanas que geralmente são coordenadas por bots, ao mesmo tempo em que permite que usuários confiáveis tenham acesso seguro e sem atritos ao seu website, o que os incentiva a permanecer conectados por mais tempo e a retornar com frequência.

O custo de scripts mal-intencionados: ameaças do lado do cliente

Assim como os bots, scripts de terceiros são majoritariamente positivos. Eles permitem funcionalidade, ferramentas de marketing, análises e muito mais para aprimorar a experiência geral do usuário (UX). Mas eles também transformam o navegador da Web em uma superfície crítica de ameaça no lado do cliente.

As ameaças do lado do cliente têm como objetivo enganar seus clientes para que eles acessem conteúdo mal-intencionado. Eles aproveitam os pontos fracos em aplicativos que estão sendo executados no computador que está sendo operado diretamente pelo usuário (geralmente seu cliente), referido aqui como o cliente. A segurança do lado do cliente abrange, assim, as tecnologias e as políticas usadas para proteger os clientes contra atividades mal-intencionadas que ocorrem em páginas da Web.

Os ataques de script podem causar danos financeiros significativos às organizações e diminuir a confiança de clientes, parceiros e processadores de pagamento. Não é de se admirar que a segurança do lado do cliente seja o foco principal dos novos requisitos do PCI DSS v4.0 (Padrão de segurança de dados do setor de cartões de pagamento). Para estar em conformidade, qualquer organização que processa cartões de pagamento online deve saber quais scripts estão sendo executados em seu website, quando eles mudam e quando param de funcionar.

Defender-se contra esses ataques não é fácil. Scripts de terceiros são numerosos e mudam continuamente, o que os torna extremamente difíceis de monitorar. Os próprios ataques de script também assumem várias formas, como skimming e formjacking da Web. Todos os grupos criminosos (mais notoriamente, o Magecart) se organizaram em torno desses tipos de técnicas para roubar dados de cartões de pagamento e PII.

Em nosso mundo de pagamentos digitais e compras e pesquisas online, a segurança do lado do cliente é mais crítica do que nunca, especialmente em páginas de finalização de compra e de pagamento, nas quais dados pessoais e financeiros estão sendo coletados. Você precisa ter visibilidade de todos os scripts em execução em seu website, capacidade de detectar comportamentos suspeitos e medidas de mitigação implantadas para se defender contra ataques. A Akamai oferece uma solução específica para cobrir essas ameaças:

O Client-Side Protection & Compliance mantém a privacidade e a confiança do cliente dentro do navegador, protegendo todos os seus usuários contra ataques no lado do cliente, como skimming da Web, formjacking e Magecart.

Proteger a infraestrutura para proteger a experiência do cliente

No centro da experiência do cliente está a infraestrutura digital subjacente que potencializa tudo sobre sua marca. Segurança, confiabilidade e desempenho de DNS são as garantias de que seus clientes possam acessar seus serviços sempre que precisarem. Os sistemas DNS praticamente equivalem à sua presença online. Quando eles ficam inativos, sua presença digital também fica. É por isso que os agentes de ameaça atacam constantemente os sistemas DNS de seus alvos com ataques de DDoS. Considerando o campo de atuação supercompetitivo que todos os setores enfrentam, você precisa de nada menos que disponibilidade ininterrupta de DNS e 100% de tempo de atividade para garantir que os clientes e possíveis clientes experimentem o melhor que sua marca tem a oferecer.

A Akamai oferece um portfólio de excelência de soluções para proteger sua infraestrutura digital contra diversos ataques de DDoS:

Para a defesa contra DDoS mais poderosa, o Akamai Prolexic oferece várias opções de proteção, incluindo centros de depuração em mais de 32 locais globais, e impressionantes 20 Tbps de capacidade de defesa dedicada.

O Akamai Edge DNS oferece uma solução de DNS confiável, abrangente e de uso específico que usa a escala, a segurança e a capacidade da Akamai Connected Cloud para gerenciar suas zonas de DNS.

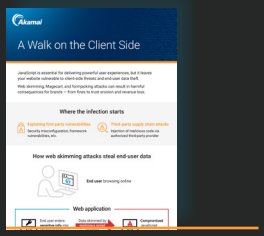
O Akamai Shield NS53, uma solução de proxy DNS bidirecional com aplicação dinâmica de políticas de segurança, pode ser usado para proteger os principais componentes de sua infraestrutura de DNS de origem, seja no local, na nuvem ou híbrida, contra ataques de esgotamento de recursos.

Somos seu parceiro para garantir a confiança do cliente

Na Akamai, estamos focados em como as marcas aparecem há mais de 25 anos. Começando como pioneira na CDN (Rede de Entrega de Conteúdo), resolvemos problemas de velocidade para as primeiras vitrines digitais. Na última década, usamos a visibilidade do tráfego proporcionada pela nossa rede de entrega de conteúdo, uma das maiores do mundo, para monitorar e analisar as ameaças diariamente, pesquisas que nos permitem desenvolver organicamente nossas soluções de segurança à medida que os vetores de ataque continuam a crescer e a mudar. Como um importante parceiro de segurança para nossos clientes, compartilhamos um compromisso de manter seus negócios em funcionamento e proteger sua experiência com o cliente, enquanto você oferece a ele a confiança de experimentar novas experiências digitais que lideram seus setores.

Próximas etapas

Aqui estão alguns recursos para ajudar você a considerar o próximo passo ideal para proteger sua marca:



Fortaleça a integridade de sua página da Web com a proteção do lado do cliente.

Consiga segurança completa e sem comprometimento para websites, aplicativos e APIs.

Conheça as principais considerações para uma estratégia de gerenciamento de bots.

A Akamai protege sua experiência do cliente, sua força de trabalho, seus sistemas e seus dados ajudando a incorporar a segurança em tudo o que você criar, em qualquer lugar que você criar e entregar. A visibilidade da nossa plataforma em relação às ameaças globais nos ajuda a adaptar e desenvolver sua postura de segurança para permitir Zero Trust, interromper ransomware, proteger aplicativos e APIs ou combater ataques DDoS, dando a você a confiança para inovar, expandir e transformar continuamente o que é possível. 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 06/24.