CLOUDFLARE

ARTIGO TÉCNICO

O guia de bots maliciosos: primeiros sinais de alerta e o que fazer a respeito

Conteúdo

Introdução

Os bots representam cerca de 30% do tráfego on-line atualmente e muitos deles pretendem prejudicar organizações como a sua, com cerca de 93% desse tráfego de bots não verificado e possivelmente malicioso. A prevalência de raspagem de conteúdo e de preços, controle de conta, preenchimento de credenciais e cartões de crédito, acumulação de estoque e ataques de DDoS (negação de serviço distribuída) acionados por botnets indica que agentes de bots maliciosos estão se tornando mais complexos e sofisticados a cada ano.

Além disso, as medidas tradicionais contra bots, como bloqueio de localização, bloqueio de endereço de IP e CAPTCHAs tradicionais, são ineficazes atualmente. Aliás, os CAPTCHAs são mais fáceis de resolver para bots do que para humanos.[1]

Por esse motivo, nenhuma tática isolada pode parar todos os bots e impedir que prejudiquem seus usuários e sua marca. A única abordagem eficaz é ficar atento para uma variedade de sinais reveladores de alerta de bots e responder a cada um coletando dados e, em seguida, implantando respostas direcionadas, detecção de padrões, análise preditiva e outras estratégias complementares.

1. https://www.usenix.org/conference/usenixsecurity23/presentation/searles

Sinais de alerta de um problema com bots

Ao rastrear uma série de possíveis indicadores, você tem grandes chances de detectar bots ruins antes que possam causar danos graves. Veja o que procurar:

Maior custo de infraestrutura sem aumento de negócios

Todo tráfego para o seu site implica em algum custo. Não importa quem ou o quê acessa seu conteúdo, você precisa pagar a conta de armazenamento e computação. No entanto, os bots ruins podem aumentar seus custos relacionados ao tráfego sem gerar nenhuma receita para a sua empresa. Enquanto os bots bons são usados por mecanismos de pesquisa para indexar conteúdo em seu site e, assim, facilitar sua classificação de SEO, os bots ruins provocam cobranças excessivas e significativas de largura de banda todos os anos.

Compras incomuns de estoque de baixo volume e alta demanda

Se você perceber que está vendendo um percentual extremamente alto de seu estoque para um subconjunto surpreendentemente pequeno de compradores, os culpados podem ser os bots de acumulação de estoque. Alguns desses bots simplesmente enchem carrinhos de compras e em seguida os abandonam para bloquear clientes legítimos. Já outros realmente comprarão seu estoque com o objetivo de revendê-lo por um preço mais alto em outros sites.

Aumento de reclamações de clientes

Um aumento nos tickets de suporte relacionados a bloqueios de conta e transações fraudulentas pode ser um sinal de bots de preenchimento de credenciais. Esses bots assumem o controle de contas de usuários legítimos com informações que coletaram em vazamentos anteriores. Além de afetarem negativamente a experiência do cliente, essas transações fraudulentas sobrecarregam seus servidores, criando tempos de carregamento de página mais longos, ou podem até tornar seu site indisponível.

Aumento de tentativas fracassadas de login

Todo cliente erra sua senha de vez em quando. Porém, se você perceber um aumento repentino de tentativas fracassadas de login, é provável que você tenha um problema envolvendo bots. Enquanto alguns bots de preenchimento de credenciais tentam acessar contas legítimas de clientes por meio de credenciais roubadas, uma técnica mais simples e mais comum é lançar um ataque de tentativas de quebra de senha com força bruta no qual os bots tentam muitos logins rápidos usando dicionários de milhares de nomes de usuário e senhas populares. Quando um bot excede o limite de logins com falha no seu site para uma conta específica, o verdadeiro proprietário humano dessa conta será bloqueado até que você resolva a questão. É um grande problema em termos de experiência do usuário.

Baixo rendimento em gastos de publicidade

A publicidade digital pode ser uma ferramenta eficaz para direcionar o tráfego para o seu site, mas também é uma arma lucrativa para bots ruins. Muitos bots de tráfego imitam o comportamento de usuários humanos, clicando em seus anúncios repetidamente para aumentar seus gastos de pagamento por clique (PPC) e, em seguida, saem sem fazer uma compra. Embora algumas plataformas de publicidade tenham implantado algoritmos de aprendizado de máquina para reduzir as fraudes de cliques, muitas delas não são detectadas.[2]
Por isso, é crucial ser proativo e monitorar cada clique resultante de seus anúncios.

Análise de visualizações de página distorcida

Se suas visualizações de página apresentarem um pico repentino sem um motivo aparente, bots ruins podem ser os culpados. Embora um pico no tráfego possa vir de usuários humanos, se você acabou de lançar um novo produto ou uma promoção de evento, operadores de bots maliciosos estão ficando mais inteligentes e capazes de implantar bots de raspagem de conteúdo exatamente nesses momentos, roubando seu conteúdo e afetando negativamente seus dados de análise agregados.

Aumento repentino na criação de contas

Quando centenas ou mesmo milhares de novas contas de usuários aparecem do nada, esse influxo pode ser obra de bots. Os bots podem usar esses perfis falsos para fazer spam em suas classificações públicas e cometer várias outras formas de fraude, ameaçando não apenas sua receita e a retenção de usuários, mas também a credibilidade de sua marca.

Duplicatas de seu conteúdo em sites não aprovados

Ter seu conteúdo compartilhado por outros sites pode ser positivo. Porém, um aumento repentino no conteúdo duplicado é sinal de bots de raspagem de conteúdo. Esses bots roubam informações que você se dedicou a preparar e organizar, permitindo que operadores de sites maliciosos as hospedem em seus próprios domínios e aumentem o respectivo tráfego, enquanto o seu é prejudicado.

Tráfego proveniente de regiões incomuns

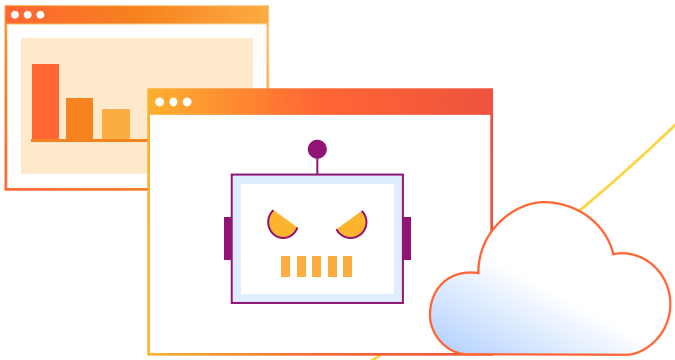
Picos repentinos originários de locais inesperados podem indicar uma atividade de bots ruins, especialmente se essa atividade aparecer em clusters, centrada em regiões nas quais você não tem clientes ou seus serviços não estão disponíveis. Fique de olho em qualquer atividade suspeita que pareça não ter relação com sua base de usuários regular.

Tráfego de locais típicos em horários incomuns

Assim como picos de tráfego de locais inesperados podem indicar bots maliciosos, picos de locais normais em horários fora do comum podem indicar bots que tentam se disfarçar como seus usuários regulares. Caso observe um pico na atividade de uma região comum no meio da noite, por exemplo, investigue esse tráfego com mais atenção.

Aumento das falhas de validação de cartão

Um sinal particularmente perigoso de bots ruins é um aumento nas transações de cartão de crédito que não são validadas. Os bots de preenchimento de cartão de crédito testam milhares de números de cartões de crédito roubados na tentativa de encontrar um que funcione. Para isso, realizam compras de baixo valor em sites menos seguros antes de fazer transações maiores em sites maiores ou de vender os números de cartão validados na dark web. Seu site pode ser incluído nesses planos em qualquer ponto da cadeia e se houver um excesso de transações com falha seu provedor de pagamentos poderá multá-lo.



2. https://www.entrepreneur.com/article/313943

Táticas para combater bots

Nenhum ataque de bots é igual ao outro. Você geralmente precisará de uma combinação de várias táticas para parar todos eles. Considere algumas das estratégias abaixo:

Bloqueie os bots ruins assim que os detectar

A resposta mais evidente a um bot é também uma das mais eficazes: basta bloquear todo o tráfego que você identificou como proveniente de atividades de bots maliciosos. Essa tática, por si só, pode economizar custos significativos em termos de largura de banda e armazenamento, sem mencionar a proteção da confiança do consumidor, além da reputação de sua marca. Ao mesmo tempo, lembre-se de que, se for altamente motivado, um operador de bot poderá mudar suas táticas e voltar mais tarde com uma estratégia de ataque diferente.

Inclua todos os bots bons que você conhece em uma lista de permissão

Mesmo que você detecte e bloqueie bots ruins, é essencial garantir que bots bons de mecanismos de busca e parceiros ainda consigam rastrear seu site. Isso não só garante que sua classificação de SEO permaneça sólida, mas também mantém o tráfego legítimo de clientes fluindo sem problemas a partir de serviços de terceiros que encaminham tráfego para você. A lista de permissão também ajuda a definir regras de bloqueio de bots que não afetam negativamente o acesso de visitantes humanos reais.

Desafie os bots suspeitos que você detectar

Assim que você perceber um padrão de logins suspeitos, acessos com baixa profundidade de página ou pouco tempo na página, validações de cartão de crédito com falha ou qualquer outro comportamento típico de bots, é fundamental implantar um teste de segurança. No passado, enviar desafios CAPTCHA era considerado uma prática recomendada. No entanto, muitos bots avançados agora podem resolver esses quebra-cabeças ainda mais rápido e com mais precisão do que os usuários humanos.

Atualmente, a melhor abordagem é usar desafios sem CAPTCHA, nos quais o software de “desafio” leva em consideração uma série de fatores para determinar se o usuário é realmente um bot (por exemplo, rede, dispositivo, impressões digitais JavaScript). Desafios "sem CAPTCHA" como esse são idealmente integrados a uma solução completa de gerenciamento de bots para máxima precisão (veja a conclusão para mais informações)

Limite a taxa de solicitação de informações pelos usuários

A limitação de taxa pode ser uma técnica eficaz para manter bots menos sofisticados à distância. Definindo limites rígidos para o número de vezes que qualquer endereço de IP pode enviar solicitações para o seu site, você evita muitos ataques simplistas de bots de força bruta, que tentam entrar usando milhares de palavras do dicionário e senhas comuns. No entanto, os bots mais avançados da atualidade podem manter o número de solicitações logo abaixo do limite de taxa, permanecendo não detectados enquanto continuam infligindo danos.

Mantenha logs detalhados de todo o tráfego do site

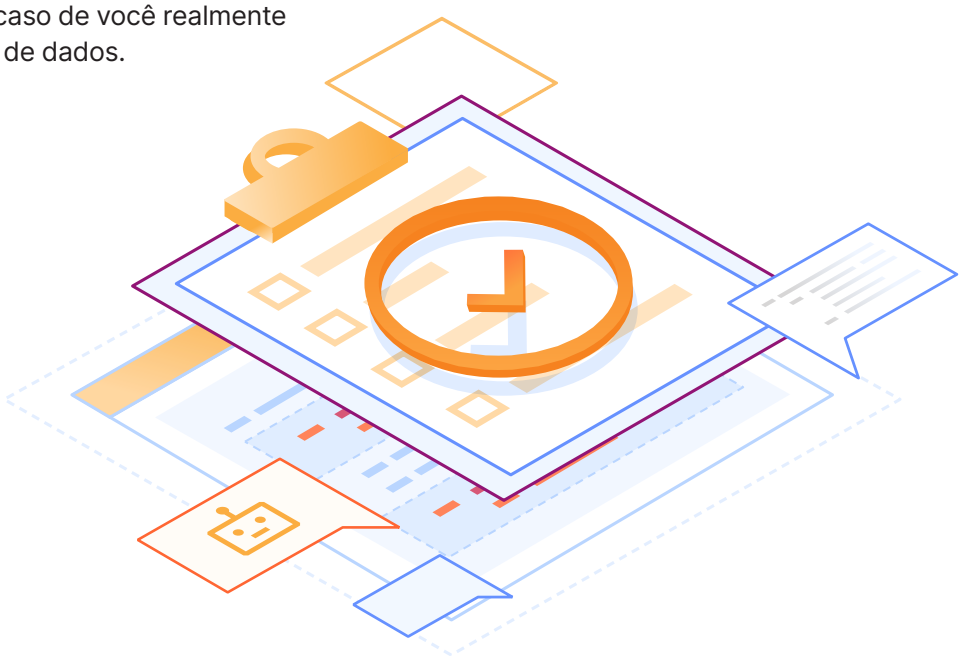
É provável que você já mantenha logs diários de visualizações de página e logins de conta. No entanto, logs mais detalhados de informações de usuários, como endereços de IP, navegadores, dispositivos, sistemas operacionais, geolocalizações, referenciadores, redes e visualizações de página, podem ser inestimáveis para detectar padrões de atividade mais sutis. Os logs podem dar uma ideia clara de como os bots tendem a se comportar em seu site, permitindo que você configure políticas de segurança mais eficazes. Além disso, os logs geralmente são essenciais para relatórios e conformidade no caso de você realmente sofrer uma violação de dados.

Redirecione os bots para um conteúdo alternativo

Quando você tiver certeza de que uma determinada fonte de tráfego é um bot, forneça um conteúdo alternativo que consuma os recursos computacionais do mesmo. Você pode até fornecer dados falsos, como informações errôneas sobre preços, para bots de raspagem de conteúdo, tornando-os inúteis para seus operadores. Técnicas como essas proporcionam o tempo necessário para ver como cada bot se comporta, entender seu padrão de atividade e preparar uma estratégia para lidar com ele de uma vez por todas.

Exija autenticação adicional para todos os usuários

À medida que os ataques de bots se tornam mais prevalentes, um número crescente de sites está buscando medidas de segurança intensificadas, mesmo para logins de humanos legítimos. Por exemplo, a autenticação de dois fatores (2FA) exige que os usuários confirmem sua identidade em vários dispositivos ou contas, enquanto as senhas de uso único (OTPs) podem desencorajar bots de preenchimento de credenciais, tornando as contas mais difíceis de invadir. Porém, lembre-se de que essas técnicas podem afetar negativamente sua experiência do usuário ao adicionar atrito ao seu processo de login.

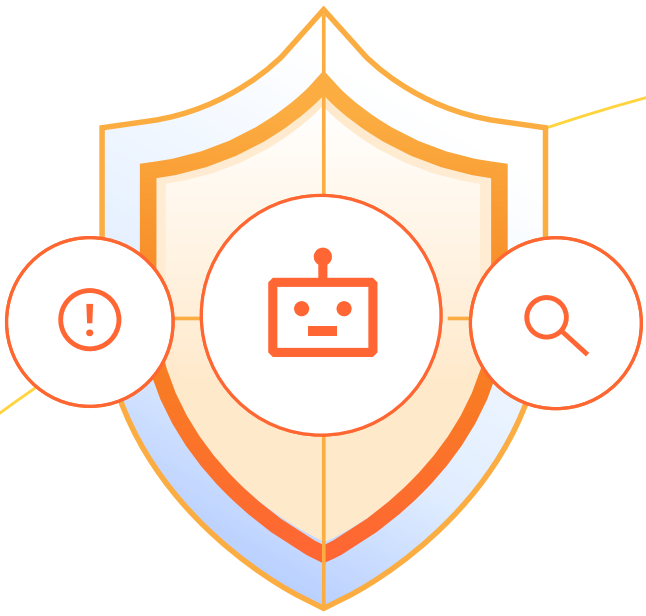


Conclusão

À medida que você explora essas táticas, lembre-se: nenhuma delas por si só irá parar todos os bots. Para proteger sua empresa, você provavelmente precisará combinar táticas e adicionar uma análise avançada de padrões multivariáveis. O Cloudflare Bot Management pode ajudar organizações de vários setores a adotarem essa abordagem multifacetada. Ele está incorporado à rede mais ampla da Cloudflare, que oferece suporte a milhões de ativos da internet e abrange mais de 330 cidades em todo o mundo.

Com base na inteligência contra ameaças contínua em toda a rede, o Cloudflare Bot Management oferece análise de comportamento, aprendizado de máquina e impressão digital do lado do cliente para eliminar grande parte do esforço de combate a bots ruins. Além disso, a Cloudflare oferece o Turnstile, um desafio de bots quase sem atrito e sem CAPTCHA, que pode ser integrado a qualquer aplicativo web com apenas algumas linhas de código.

Saiba mais sobre o Cloudflare Bot Management.



CLOUDFLARE

+55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

REV:BDES-6333.2024SEPT03