CLOUDFLARE

백서

악성 봇 플레이북: 조기 경고 신호 및 대응 방법

목차

서론

오늘날 봇은 온라인 트래픽의 약 30%를 차지하며, 이 봇들 중 상당수는 귀사와 같은 조직에 피해를 입히기 위해 활동하고 있습니다. 추정치에 따르면, 해당 봇 트래픽의 약 93%는 검증되지 않았으며 잠재적으로 악성입니다. 콘텐츠 및 가격 스크래핑, 계정 탈취, 자격 증명 및 신용 카드 스터핑, 재고 사재기, 봇넷 기반 분산 서비스 거부(DDoS) 공격의 만연은 악성 봇 행위자가 매년 더욱 복잡해지고 정교해지고 있음을 시사합니다.

또한 위치 차단, IP 주소 차단 및 CAPTCHA와 같은 기존 봇 방지 대책은 오늘날 그 효과가 미비합니다. 실제로 CAPTCHA는 사람보다 봇이 해결하기가 더 쉽습니다.[1]

따라서, 단 하나의 전술로 모든 봇을 막고 사용자와 회사 브랜드를 저해하는 것도 막을 수는 없습니다. 효과를 볼 수 있는 유일한 접근법은 데이터를 수집한 다음, 대상 응답, 패턴 감지, 예측 분석 등의 보완적 전략을 활용하여 숨길 수 없는 다양한 봇의 경고 신호를 지켜보고 있다가 개별적으로 대응하는 것입니다.

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

봇 문제의 경고 신호

다양한 잠재적 지표들을 추적하게 되면, 악성 봇이 심각한 손상을 입히기 전에 발견할 가능성을 크게 높일 수 있습니다. 다음의 신호를 찾아 보시기 바랍니다.

사업 성장은 없는데 인프라 비용이 증가하는 경우

웹 사이트로 유입되는 모든 트래픽에는 비용이 수반됩니다. 누가 회사의 콘텐츠에 액세스하는지와 무관하게 스토리지 및 계산 비용을 부담해야 하기 때문입니다. 하지만 악성 봇이 작동하면, 회사에 아무런 수익도 내지 않으면서 트래픽 관련 비용이 증가할 수 있습니다. 검색 엔진이 이용하는 좋은 봇은 사이트의 콘텐츠를 색인화하여 SEO 등급에 도움이 되지만, 악성 봇이 있으면 매년 상당한 초과 대역폭 비용을 부담하게 됩니다.

수요가 높은 재고의 비정상적 소량 구매

매우 적은 수의 구매자가 재고 중 의심스러울 정도로 높은 비율을 구매한다는 것이 발견되면, 싹쓸이 구매 봇이 범인일 가능성이 있습니다. 단순히 장바구니를 채웠다가 포기해 합법적인 고객을 차단하는 봇도 있지만, 실제 물건을 구매했다가 다른 사이트에서 높은 가격에 재판매하는 봇도 있습니다.

고객 불만 증가

계정 폐쇄 및 사기성 거래에 관련된 지원 티켓이 증가한다면, 이는 자격 증명 스터핑 봇의 신호일 수 있습니다. 이러한 봇은 과거 정보 유출을 통해 획득한 정보를 이용해 합법적인 사용자 계정을 탈취합니다. 이러한 사기성 거래가 발생하면, 고객 경험에 부정적 영향을 미치는 것은 물론이고 서버에 과부하가 발생하게 되어 페이지 로드 시간이 길어지고 웹 사이트를 사용할 수 없게 되기도 합니다.

실패한 로그인 시도의 증가

고객은 누구나 암호를 잘못 입력할 수 있습니다. 하지만 실패한 로그인이 갑자기 증가한다면 봇의 문제일 가능성이 큽니다. 자격 증명 스터핑 봇은 훔친 자격 증명을 이용해 합법적인 고객 계정에 액세스하려 합니다. 널리 쓰이는 단순한 기법으로 무작위 대입 공격이 있지만, 이는 봇이 널리 쓰이는 수천 가지의 사용자 이름과 암호 사전을 이용해 속사포처럼 로그인 시도를 하는 것입니다. 봇이 사이트의 특정 계정에 대해 로그인 실패 한계를 넘어서게 되면, 해당 계정의 실제 사용자는 이 문제가 해결될 때까지 계정이 폐쇄되고 이는 사용자 경험에 심각한 문제를 가져옵니다.

광고 지출에 대한 낮은 수익률

디지털 광고는 사이트로 트래픽을 끌어오는 효과적인 방법이지만, 악성 봇에게는 수익성이 좋은 무기이기도 합니다. 인간 사용자를 흉내내어 광고를 반복적으로 클릭함으로써 클릭당 결제(PPC) 지출을 늘려놓고 구매는 하지 않고 떠나는 트래픽 봇이 많습니다. 광고 플랫폼 중에는 기계 학습 알고리즘을 배포해 클릭 사기를 방지하는 경우도 있지만, 이러한 봇이 감지되지 않는 경우도 많습니다.[2]
따라서 광고를 통한 클릭은 하나하나 적극적으로 모니터링해야 합니다.

페이지 조회수 분석의 왜곡

명확한 이유 없이 페이지 조회수가 급증한다면, 악성 봇이 범인일 수 있습니다. 신제품이나 이벤트 프로모션을 출시한 지 얼마 되지 않을 때 사용자의 트래픽이 급증할 수 있지만, 악의적인 봇 운영자는 정확히 이 시기에 콘텐츠 스크래핑 봇을 배포하는 등 점점 더 스마트해지고 있습니다. 이들은 콘텐츠를 탈취해 전체적인 분석 데이터에 악영향을 미칩니다.

계정 생성의 갑작스러운 증가

수백 또는 수천 개의 새로운 사용자 계정이 갑자기 증가했다면, 봇이 배후에 있을 가능성이 있습니다. 이들은 가짜 프로필을 이용해 사이트의 공공 평가 점수를 낮추고 다양한 형태의 사기 행위를 저지를 수 있어, 수익과 사용자 유지는 물론 브랜드의 신뢰도에도 위협이 됩니다.

승인 받지 않은 사이트에 자신의 콘텐츠가 복제되는 경우

내 사이트의 콘텐츠를 다른 사이트에서 공유하는 것은 좋은 일일 수 있지만, 콘텐츠가 그대로 복제된 것이 많아진다면 이는 콘텐츠 스크래핑 봇의 전형적인 특징입니다. 이러한 봇은 오랜 시간 수집하고 정리한 정보를 탈취한 후, 악의적 사이트 운영자들이 소유한 도메인에 호스트하게 하여 자체 트래픽은 늘리면서 원래 사이트에 타격을 입힙니다.

비정상적인 지리적 위치에서 오는 트래픽

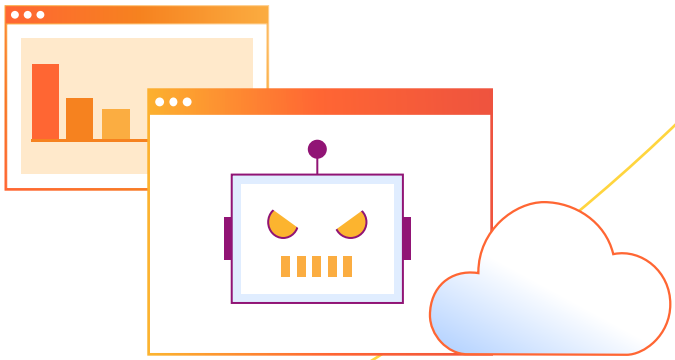
예상치 않은 지역에서 트래픽이 갑자기 급증하면, 악성 봇의 활동인 경우가 있습니다. 고객이 살고 있지 않는 경우나 내가 서비스를 제공하지 않는 지역을 중심으로 집단으로 이러한 활동이 발생한다면, 그럴 가능성이 더욱 큽니다. 정상적인 사용자 집단과 관련이 없어 보이는 의심스러운 활동을 면밀히 주시해야 합니다.

전형적인 위치에서의 트래픽이지만, 비정상적인 시간인 경우

예상치 않은 지역에서의 트래픽 급증이 악의적 봇의 신호일 수 있듯, 정상적인 위치이지만 비정상적인 시간에 트래픽이 급증한다면 그것 또한 봇이 일반 사용자로 위장한 것일 수 있습니다. 예를 들어 고객이 많은 지역이지만, 야간에 활동이 급증한다면 해당 트래픽을 눈여겨보는 것이 좋습니다.

카드 유효성 검증 실패의 증가

악성 봇의 활동에 대해 특히 위험한 신호는 유효성 검증에 실패한 신용 카드 거래가 증가하는 것입니다. 신용 카드 스터핑 봇은 훔친 수천 개의 신용 카드 번호를 테스트해 작동하는 것을 찾으려 합니다. 보안이 잘 안 되어 있는 웹 사이트에서 저가 구매를 통해 이를 수행한 후, 큰 사이트에서 고가의 구매를 하거나, 유효성이 확인된 카드를 다크웹에서 팔기도 합니다. 어떠한 사이트도 이러한 계획의 희생자가 될 수 있으며, 실패한 거래가 과도한 경우라면, 결제 서비스 공급업체가 벌금을 부과할 수도 있습니다.



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

봇과 싸우기 위한 전술

어떠한 봇 공격도 다른 봇 공격과 동일하지 않으므로 봇을 중간에 차단하려면 다양한 전술을 조합해서 활용해야 하는 경우가 많습니다. 다음 전략들을 고려해볼 수 있습니다.

악성 봇을 파악하는 즉시 차단

가장 명백한 대응이지만, 가장 효과적인 방법이기도 합니다. 악의적 봇 활동으로 확인된 트래픽을 모두 차단하는 것입니다. 이 전술만으로도 상당한 대역폭 비용 및 스토리지 비용을 절감할 수 있습니다. 소비자의 신뢰나 브랜드 평판을 보호하는 것은 당연합니다. 동시에 기억해야 할 것은 동기가 상당한 봇 조작자라면, 전술을 바꾸어서 다른 공격 전략으로 다시 올 가능성이 있다는 점입니다.

알고 있는 모든 좋은 봇의 허용 목록 작성

악성 봇을 감지하여 차단하더라도 검색 엔진이나 파트너가 보내는 좋은 봇은 사이트를 스크래핑할 수 있도록 허용해야 합니다. 이렇게 하여야 SEO 순위가 굳건하게 유지되기도 하지만, 내 사이트로 트래픽을 보내는 타사 서비스로부터 오는 합법적인 고객 트래픽을 원활하게 받아들일 수도 있습니다. 허용 목록을 작성하면, 진짜 인간 방문자의 액세스에 부정적 영향을 주지 않는 봇 차단 규칙을 설정하기도 훨씬 용이해집니다.

감지된 의심스러운 봇에는 인증 질문 제시

의심스러운 로그인 패턴, 조회하는 페이지 수준이 낮은 경우, 페이지에 머무는 시간이 짧은 경우, 실패한 신용 카드 유효성 인증 등 전형적인 봇 활동의 신호를 감지하면 보안 검사를 배포하는 것이 중요합니다. 과거에는 CAPTCHA 챌린지를 보내는 것이 모범 사례로 여겨졌습니다. 하지만 고도화된 봇 중에는 이러한 퍼즐을 실제 인간 사용자보다 훨씬 더 빠르고 정확하게 풀어내는 봇도 많습니다.

오늘날 가장 좋은 방법은 CAPTCHA가 필요 없는 인증 방식을 사용하는 것입니다. 이러한 인증 방식에서는 '인증' 소프트웨어가 여러 요소를 고려하여 사용자가 네트워크, 장치, JavaScript 핑거프린트 등 실제로 봇인지 판단합니다.
이와 같은 "CAPTCHA 없는" 인증은 완전한 봇 관리 솔루션과 이상적으로 통합되어 정확도를 극대화합니다(자세한 내용은 결론을 참조).

사용자가 정보를 요청할 수 있는 레이트 리미팅

레이트 리미팅은 정교하지 않은 봇을 궁지에 몰아넣는 유효한 방법이 될 수 있습니다. 특정 IP 주소가 요청을 제출할 수 있는 수에 절대적인 제약을 두면, 수천 개의 사전 단어 및 많이 쓰이는 암호를 이용해 로그인을 시도하는 단순한 무차별 대입 봇 공격을 방지할 수 있습니다. 하지만, 최근의 고도화된 봇들은 요청 수를 레이트 리미트 바로 아래로 유지해 감지되지 않으면서 손상을 가할 수 있기도 합니다.

모든 사이트 트래픽의 상세한 로그 유지

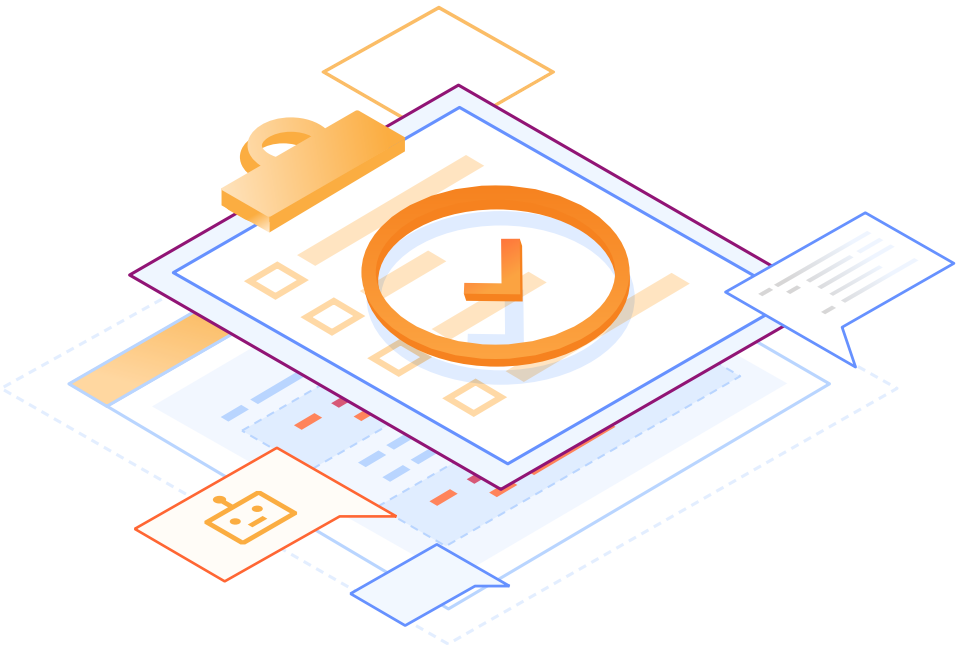
이미 페이지 조회나 계정 로그인 등에 대한 로그를 유지하는 경우도 많겠지만, IP 주소, 브라우저, 장치, OS, 지리적 위치, 참조자, 네트워크, 페이지 보기 등의 상세한 사용자 정보에 대한 로그를 유지하면 모호한 활동 패턴을 찾아낼 수 있는 경우도 많습니다. 로그를 이용하면 봇이 사이트에서 어떻게 행동하는지 명확하게 이해할 수 있어 효과가 높은 보안 정책을 설정할 수 있게 됩니다. 또한, 실제 데이터 침해가 발생한 경우에도 로그는 보고 및 규제 준수에 중요한 경우가 많습니다.

봇을 대체 콘텐츠로 리디렉션

특정 트래픽 원천이 봇인 게 상당히 확실하다면, 대체 콘텐츠를 이용해 봇의 컴퓨팅 자원을 소모시킬 수도 있습니다. 콘텐츠 스크래핑 봇에게는 틀린 가격 정보 등 가짜 데이터를 줘서, 조작자에게 무용지물로 만들어도 좋습니다. 이러한 기법을 이용하게 되면, 각 봇의 행태를 지켜보면서 활동 패턴을 이해하고 이를 영원히 해결할 수 있는 전략을 세울 시간을 벌 수 있습니다.

모든 사용자에게 추가 인증 요구

봇 공격이 만연하게 되면서 합법적인 인간 로그인에도 엄격한 보안 대책을 실시하는 사이트가 늘어나고 있습니다. 예를 들어, 2단계 인증(2FA)에서는 다수의 기기 또는 계정에서 사용자의 신원을 확인하며, 1회용 암호(OTP)는 계정을 해킹하기 어렵게 만들어 자격 증명 스터핑 봇을 좌절시킵니다. 하지만, 이러한 기법을 이용하면 로그인 절차가 복잡해져 사용자 경험에 악영향이 있을 수 있으니 유념해야 합니다.

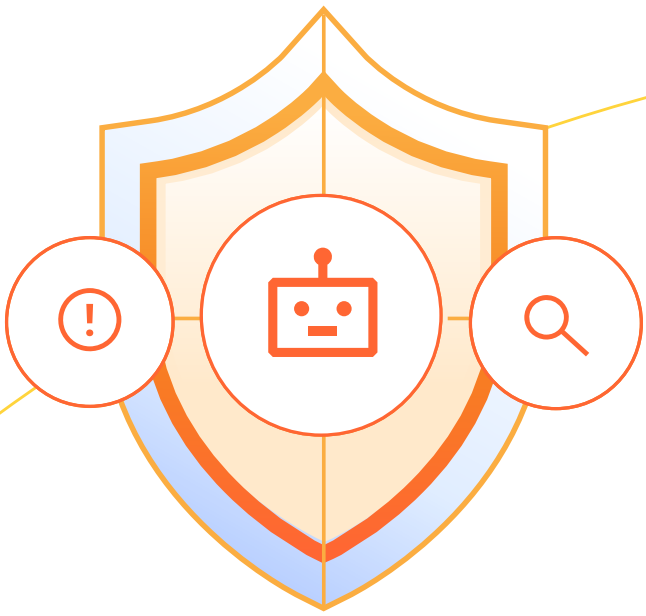


결론

이러한 전술을 검토함에 있어서 이들 중 어떤 것도 단독으로는 모든 봇을 막을 수 없다는 사실을 기억해야 합니다. 사업을 보호하기 위해서는 다수의 전술을 결합하여 이용해야 하며, 고급 다변량 패턴 분석을 추가해야 합니다. 다양한 업계의 조직들이 Cloudflare Bot Management를 이용해서 다중 접근법을 시행할 수 있습니다. 이 기능은 수백만 개의 인터넷 자산을 지원하며 전 세계 330여 개의 도시에 걸쳐 있는 Cloudflare의 광범위한 네트워크에 통합되어 있습니다.

Cloudflare Bot Management는 이러한 네트워크에서의 지속적인 위협 인텔리전스를 활용하므로 행태 분석, 기계 학습, 지문 인식 등을 통해 악성 봇과의 전투를 위한 노력을 줄이는 데 상당한 도움이 됩니다. 또한 Cloudflare는 몇 줄의 코드로 모든 웹 애플리케이션에 통합할 수 있는, 거의 마찰이 없고 CAPTCHA가 필요 없는 봇 방어 시스템인 Turnstile도 제공합니다.

Cloudflare Bot Management에 대해 자세히 알아보세요.



CLOUDFLARE

007-9814-2030-192 | enterprise@cloudflare.com | www.cloudflare.com/ko-kr/

REV:BDES-6333.2024SEPT03