CLOUDFLARE

KRÓTKI OPIS ROZWIĄZANIA

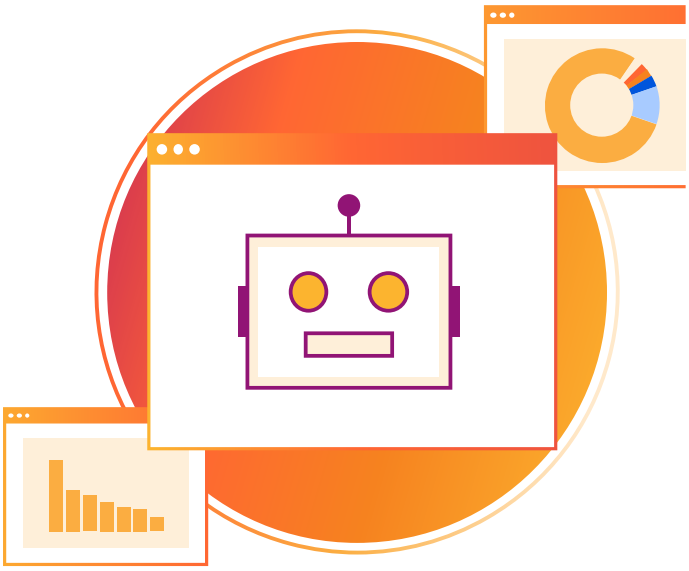
Cztery strategie zarządzania złośliwymi botami

Unikaj kosztownych szkód i strat finansowych spowodowanych przez niepożądane boty

Boty są wszędzie w Internecie

Współczesny Internet jest wypełniony botami pomagającymi w automatyzacji ważnych zadań. Szacuje się, że około 40–50% całego ruchu Internetu generują boty, z których wiele pełni uzasadnione funkcje biznesowe.

Jednak boty są również często wykorzystywane przez przestępców do atakowania zasobów internetowych i powodowania kosztownych szkód. Złośliwe boty mogą kraść dane, uzyskiwać nieautoryzowany dostęp do kont użytkowników, przesyłać niechciane dane za pośrednictwem formularzy online i wykonywać inne szkodliwe działania. Te złośliwe boty marnotrawią cenne zasoby obliczeniowe i związane z witrynami, kradną dane oraz zniekształcają analizy ruchu.



Czym jest zarządzanie ruchem botów?

Zarządzanie ruchem botów polega na blokowaniu niepożądanego lub złośliwego ruchu generowanego przez boty przy jednoczesnym umożliwieniu przydatnym botom dostępu do zasobów internetowych. Osiąga się to poprzez wykrywanie aktywności botów, rozróżnianie pożądanych i niepożądanych zachowań oraz identyfikację źródeł niepożądanej aktywności.

Dlaczego to jest ważne?

Zarządzanie ruchem botów jest niezbędne, ponieważ niekontrolowane boty mogą powodować poważne i kosztowne problemy. Podczas próby odfiltrowania złośliwego ruchu generowanego przez boty w zasobach internetowych organizacje muszą upewnić się, że nie blokują niezbędnych botów, takich jak boty indeksujące wyszukiwarek.

Co można zrobić?

Identyfikacja i blokowanie złośliwych botów zanim rozpoczną atak to kluczowy element każdej dobrej strategii bezpieczeństwa. Przedstawiamy cztery historie prawdziwych klientów Cloudflare, którzy zmierzyli się z wyzwaniami w zakresie zarządzania ruchem botów, stosując cztery różne strategie oparte na produktach Cloudflare.

Blokowanie botów

Takie podejście wymaga ostrożności, ponieważ wiele uzasadnionych procesów biznesowych, takich jak indeksowanie przez wyszukiwarki, wymaga, aby boty miały dostęp do zasobów firmy.

Blokowanie botów		
Wyzwanie	**Rozwiązanie**	**Wyniki**
Jedna z firm z branży iGamingowej odnotowała znaczny wzrost liczby reklamacji od użytkowników. Ich konta były atakowane, a informacje o kartach kredytowych kradzione. Cyberprzestępcy wykorzystywali zautomatyzowane boty do ataków brute-force na dane logowania, uzyskując dostęp do kont użytkowników i w efekcie je przejmując.	Zespół ds. bezpieczeństwa zastosował **ograniczanie częstotliwości żądań** wraz z zaawansowanym **zarządzaniem ruchem botów**, aby wykryć wielokrotne próby logowania w krótkim czasie. Po wykryciu nietypowego zachowania funkcja ograniczania częstotliwości żądań automatycznie rozpoczynała blokowanie złośliwych żądań. Od czasu wdrożenia tej funkcji firma iGamingowa nie odnotowała ani jednego ataku typu „credential stuffing”.	Wszystkie firmy muszą zachowywać równowagę między rygorystycznym bezpieczeństwem a optymalnym komfortem użytkowania. Odpowiedni zestaw narzędzi pomaga wykrywać złośliwy ruch botów i zapobiegać mu, minimalizując jednocześnie fałszywe alarmy i utrudnienia dla prawdziwych użytkowników.

Spowalnianie przeciwnika

Ta technika maksymalizuje czas odpowiedzi na wszystkie podejrzane żądania sieciowe.

Spowalnianie przeciwnika		
Wyzwanie	**Rozwiązanie**	**Wyniki**
Firma zajmująca się zakładami sportowymi odnotowała znaczny spadek liczby transakcji. Podczas analizy problemu zidentyfikowano aktywność złośliwych botów, które pobierały dane o kursach z firmowej witryny internetowej i wykorzystywały te informacje, aby uzyskać przewagę konkurencyjną.	Firma nie blokowała botów, ponieważ cyberprzestępcy znaleźliby sposób na obejście blokady. Zamiast tego spowolniono pobieranie danych dla zakładów. Firma wykorzystała funkcję **nadpisywania nagłówków** do oznaczania podejrzanych żądań na podstawie analizy **zarządzania ruchem botów**, a następnie skrypty **Workers** w celu reagowania na te nagłówki i spowalniania żądań.	Ta metoda umożliwiła firmie przywrócenie normalnej aktywności użytkowników. Inne metody obejmują używanie weryfikacji CAPTCHA dla dużych żądań lub modyfikowanie znaczników HTML w regularnych odstępach czasu. Działania te zakłócają przepływ pracy botów, przez co pozyskiwanie danych staje się bardziej skomplikowane.

Wprowadzanie botów w błąd

Chociaż wiele firm wdraża środki zaradcze przeciwko botom, prawdziwie zdeterminowany atakujący może je obejść. Zamiast tego niektóre firmy postanawiają się bronić.

Wprowadzanie botów w błąd		
Wyzwanie	**Rozwiązanie**	**Wyniki**
Pewna firma oferująca zakłady sportowe próbowała znaleźć rozwiązanie problemów z wykorzystywaniem przez boty danych o zakładach sportowych w jej witrynie internetowej. Po przeanalizowaniu dostępnych możliwości zdecydowano się na wdrożenie obejścia wykorzystującego kilka produktów Cloudflare, które umożliwiało podawanie botom losowych informacji.	Po wykryciu, że żądanie zostało wygenerowane przez złośliwego bota, system akceptował je i generował nowy proces roboczy: Żądanie → **WAF** (zidentyfikowany bot) → **Zarządzanie ruchem botów** (przypisana ocena zagrożenia) → **Workers** (generowanie losowych danych) → **Workers** (zwracanie losowych danych do bota)	Nowy proces roboczy generował nowe, losowe dane, które były zwracane złośliwym botom. W rezultacie boty, których celem było zbieranie danych i wyrządzanie szkód, odchodziły z niczym, co zniechęcało do dalszych nadużyć.

Analiza dynamiczna

Wraz z rosnącą złożonością botów firmy muszą gromadzić dane na ich temat i przeprowadzać dynamiczną analizę przed podjęciem jakichkolwiek działań. Cele mogą obejmować wykrywanie nieprawidłowych rejestracji, kursów, roszczeń dotyczących premii itp. Dla wykonania szczegółowej analizy zespoły ds. bezpieczeństwa mogą potrzebować połączenia wielu źródeł danych z narzędzi wewnętrznych i zewnętrznych w celu zbadania parametrów ruchu generowanego przez boty.

Analiza dynamiczna		
Wyzwanie	**Rozwiązanie**	**Wyniki**
Firma bukmacherska rozpoczęła kampanię marketingową mającą na celu przyciągnięcie nowych użytkowników poprzez nagrody za rejestrację. Niedługo po uruchomieniu kampanii zauważono, że boty dokonują fałszywych rejestracji. Firma posiadała już pewne wewnętrzne narzędzia analityczne, ale nie zapewniały one pełnego wglądu w zachowanie botów.	Zespół wdrożył zaawansowane rozwiązanie Cloudflare do **zarządzania ruchem botów** z sygnaturami JA3, aby generować **dzienniki nieprzetworzone** całego ruchu internetowego przychodzącego na stronę rejestracji. Firma wzbogaciła swoje systemy wewnętrzne o oceny botów i sygnatury JA3, co pozwoliło jej dokładniej identyfikować boty.	Po przeprowadzeniu szczegółowej analizy firma była w stanie anulować fałszywe rejestracje i uniknąć zawyżania statystyk nowo pozyskanych użytkowników. W efekcie do najlepszych praktyk firmy dodano regularną analizę botów z użyciem sygnatur JA3.

O krok przed złośliwymi botami

Cloudflare Bot Management

Proste wdrażanie
Brak złożonej konfiguracji i konserwacji

Niskie opóźnienia
Mediana opóźnień poniżej 0,3 ms

Rozbudowana analiza danych
Koreluj dzienniki ruchu z innymi źródłami danych, takimi jak systemy SIEM lub narzędzia BI

Precyzyjne mechanizmy kontrolne
Dostosuj reguły, użyj wizualnego narzędzia do tworzenia reguł lub napisz własne reguły dopasowywania wzorców

Zatrzymaj szkodliwe boty, zanim zaszkodzą Twojej firmie

Z każdym dniem boty stają się coraz bardziej zaawansowane. Wraz z rosnącym poziomem wyrafinowania cyberprzestępców próby wykrycia i zablokowania botów napotykają ograniczenia. Współczesne firmy muszą nieustannie dostosowywać swoje strategie, aby reagować na zmiany taktyk stosowanych przez atakujących, jednocześnie dążąc do znalezienia równowagi między solidnym bezpieczeństwem a minimalizacją utrudnień dla użytkowników.

Niezależnie od strategii, którą wybierzesz, upewnij się, że Twój partner dysponuje elastycznym zestawem narzędzi do efektywnego zarządzania ruchem botów. Aby dowiedzieć się więcej o tym, jak Cloudflare może pomóc w rozwiązaniu problemów z botami, skontaktuj się z nami w celu uzyskania spersonalizowanej oceny szacunkowej.

Informacje, którym możesz zaufać

Cloudflare pełni funkcję serwera proxy dla około 20% całego globalnego Internetu, co zapewnia rozległą analizę w czasie rzeczywistym zachowań złośliwych botów w sieci Cloudflare.
Ponadto firma Cloudflare współpracuje z wieloma partnerami, którzy wymieniają się informacjami o skradzionych danych uwierzytelniających, co ułatwia wykrywanie prób przejęcia kont, zanim doprowadzą do naruszenia bezpieczeństwa.

Rozpocznij podróż do szybszej, bardziej niezawodnej i bezpiecznej sieci

Umów się na konsultację

Nie potrzebujesz jeszcze oceny szacunkowej?

Dowiedz się więcej o Cloudflare One