Citrix ADC ochroni Twoje aplikacje i strony internetowe przed atakami botów

Zautomatyzowane ataki zdarzają się coraz częściej. Szacuje się, że 38% całego ruchu internetowego to ruch botów - połowa z tego to szkodliwe boty atakujące wrażliwe treści i dane. Twoja firma każdego dnia musi stawiać czoła wielu takim atakom. W najlepszym przypadku będą one jedynie obciążać infrastrukturę firmy, ale mogą też wyrządzić dużo większe szkody.

Ataki botów na aplikacje mogą sparaliżować Twoją firmę

Boty i botnety są wykorzystywane do przeprowadzania złośliwych działań przeciwko stronom internetowym i aplikacjom. Przybierają one różnorodne formy i mogą na wiele sposobów szkodzić Twojej firmie. Typowe ataki to:

- **Content scraping:** Należące do firmy treści są zagrożone przez boty, które mogą je kopiować w nielegalnych celach. Konkurencja może na przykład wykradać cenniki, żeby wykorzystać je do nieuczciwej rywalizacji. Skopiowana treść może też zostać użyta do tworzenia fałszywych stron w celu podprowadzenia klientów czy zniszczenia reputacji firmy.
- **Ataki DDoS L7:** Są to ataki bardziej wyrafinowane niż ataki DDoS w warstwie sieciowej. Boty wykorzystują aplikacje internetowe do wysyłania zapytań, które obciążają serwery ponad granice ich wydajności. W ten sposób uniemożliwiają aplikacjom obsługiwanie normalnego ruchu, a nawet mogą spowodować ich wyłączenie, co oczywiście może w istotny sposób zaszkodzić firmie.
- **Przejmowanie kont i tworzenie fałszywych kont:** Przestępcy wykorzystują boty w celu uzyskania dostępu do kont w systemach wymagających logowania. Jeśli uda im się złamać zabezpieczenie konta, mogą nadużywać Twoich usług, transferować środki, sprzedawać pozyskane dane osobowe. Może to wpłynąć na przychody Twojej firmy, a także narazić Cię na odpowiedzialność prawną, jeśli zostanie naruszona ochrona danych osobowych.
- **Oszustwa reklamowe:** Boty, które "klikają" na Twoje reklamy, generują ruch, za który płacisz, ale nie otrzymujesz zwrotu. To może prowadzić do wzrostu kosztów reklamy i obniżenia wskaźników ROI. To również zaburza miarodajność prowadzonej analityki marketingowej.
- **Ataki typu Credit card stuffing:** Boty mogą atakować Twoją witrynę i próbować dokonywać niewielkich zakupów w celu sprawdzenia skuteczności użycia danych skradzionej karty kredytowej. To może prowadzić do bezpośrednich strat finansowych, a także zwiększenia opłat transakcyjnych przez wystawców kart kredytowych.
- **Chomikowanie zapasów:** Przestępcy atakują sklep internetowy poprzez masową rezerwację towarów w koszyku na etapie przed dokonaniem zapłaty. Uniemożliwia to sprzedaż towarów rzeczywistym klientom, co prowadzi do strat finansowych. Może także negatywnie wpłynąć na planowanie popytu i zatowarowania.

Ochrona przed botami: kompleksowe, inteligentne i zintegrowane rozwiązanie

Łagodzenie skutków działania botów jest wbudowane w Citrix Application Delivery Controller (ADC) jako część ogólnego rozwiązania bezpieczeństwa. Polega to na ograniczaniu możliwości działania złośliwych botów poprzez ich identyfikację w ruchu przychodzącym, a następnie odpowiednie odfiltrowanie. Istnieje kilka mechanizmów wykorzystywanych przez Citrix ADC do wykrywania botów o różnym stopniu zaawansowania. Najprostsze metody opierają się na wykorzystaniu adresów IP klientów.

- **Czarne i białe listy:** Definiuje się czarną listę znanych złych botów, aby mieć pewność, że nie zostaną wpuszczone na stronę. Jednocześnie należy ustawić białą listę z dobrymi botami (np. porównywarkami, wyszukiwarkami, itp.), ponieważ mogą one mieć korzystny wpływ na działanie firmy, np. pomagać w jej promocji.
- **Reputacja IP:** Ponieważ boty często zmieniają adresy IP, Citrix ADC ma wbudowany filtr reputacji IP, który jest dynamicznie aktualizowany w miarę odkrywania nowych zagrożeń związanych z botami.
- **Geolocation data:** Adres IP może być użyty w celu określenia lokalizacji klienta. Jeśli firma nie ma odbiorców w danym regionie geograficznym, można zablokować ruch pochodzący z tamtego obszaru.

Bardziej wyrafinowane boty wymagają inteligentniejszych metod wykrywania, które nie opierają się tylko na adresie IP. Citrix ADC wykorzystuje dodatkowe techniki do rozpoznawania ruchu botów.

- **Sygnatury:** Dzięki informacjom z nagłówka (adres IP, domena źródłowa, aplikacja kliencka) Citrix stworzył bazę sygnatur ponad 3500 znanych botów. Przychodzące żądania są sprawdzane pod tym kątem w celu zidentyfikowania ruchu botów.
- **Odciski palców:** Przy pomocy 34 różnych parametrów, takich jak wtyczki przeglądarki, czcionki, aplikacja kliencka czy rozdzielczość ekranu, Citrix tworzy unikalne odciski palców dla urządzeń klientów. Ponieważ urządzenia ludzi i boty mają bardzo różne kryteria identyfikacji, odcisk palca jest przydatną techniką rozpoznawczą w przypadku bardziej zaawansowanych botów.
- **Analiza zachowania:** Wyrafinowane boty dobrze naśladują ludzi. Citrix wykorzystuje uczenie maszynowe do ustalenia charakterystyki aplikacji, a następnie wykrywa anomalie w zachowaniu, aby wykryć boty. Na przykład:
  - Transakcje klienta - Czy ich liczba wygląda na realną w przypadku człowieka?
  - Pobieranie danych - Czy ilość pobieranych danych wykracza poza normalne parametry?
  - Wskaźniki udanych i nieudanych uwierzytelnień - Boty, zwłaszcza te, które stosują techniki typu "credential stuffing", będą miały wyższy niż normalnie wskaźnik niepowodzeń przy próbach uwierzytelniania.

Walka z botami

Oprócz wykrywania botów Citrix udostępnia szereg mechanizmów łagodzących skutki ich działań, tak aby zapobiegać obciążaniu infrastruktury i chronić aplikacje przed nadużyciami.

- **Blokady:** Blokowanie żądania ruchu przychodzącego od bota. Ta prosta czynność powstrzymuje ruch botów i zapobiega atakom. Pozwala to również na odciążenie infrastruktury firmy i obniżenie kosztów hostingu.
- **Przekierowanie:** Przekierowanie żądań do alternatywnej strefy objętej kwarantanną w celu dalszej analizy i monitorowania - np. serwer honeypot.

- **Ograniczanie liczby żądań:** Ograniczanie liczby żądań od klienta może pomóc w kontrolowaniu ruchu botów i chronić back-end przed przeciążeniem.
- **Mechanizmy typu Challenge:** W przypadku wątpliwości, czy dany klient to nie jest bot, można zastosować test CAPTCHA. Określenie czy ruch pochodzi od człowieka, czy od bota, umożliwia ochronę aplikacji przed zautomatyzowanymi atakami.

Określenie, czy ruch pochodzi od człowieka czy od bota, umożliwia ochronę aplikacji przed zautomatyzowanymi atakami. Oferowana przez Citrix funkcja łagodzenia skutków ataków botów może chronić witrynę przed różnymi rodzajami ataków. Oto kilka przykładów:

- Ochrona przed atakami, które mają na celu przejęcie konta, dzięki monitorowaniu wskaźników udanych i nieudanych prób uwierzytelniania klienta.
- Powstrzymywanie botów, które usiłują kopiować treści, poprzez określenie tempa żądań do serwera.
- Wykorzystanie oferowanych przez Citrix danych dotyczących proporcji liczby botów i ludzi w stosunku do liczby użytkowników, aby skorygować wyniki analityki biznesowej zniekształcone przez ruch botów. Pozwoli to na podejmowanie bardziej racjonalnych decyzji.

Elastyczne i proste opcje wdrożenia w środowisku wielochmurowym

Łagodzenie ataków botów jest jednym z elementów rozwiązania Citrix ADC, dostępnym w przypadku nabycia licencji premium. Citrix ADC jest oferowane w wielu wariantach oraz jako usługa dostępna w wiodących chmurach publicznych (AWS, Azure, GCP), co ułatwia jego wdrażanie. Jednolita podstawa kodu dla całego portfolio Citrix ADC umożliwia zachowanie spójności operacyjnej we wszystkich wdrożeniach i aplikacjach. Zastosowanie jednej licencji, obejmującej różnorodne funkcje bezpieczeństwa, takie jak WAF, łagodzenie skutków ataków botów i ochrona API, pozwala na uproszczenie obsługi i obniża TCO. Im mniej skomplikowane rozwiązania tym lepsza ochrona.

Citrix Systems Poland

e-mail: poland@citrix.com
WWW | https://www.citrix.com/pl-pl/