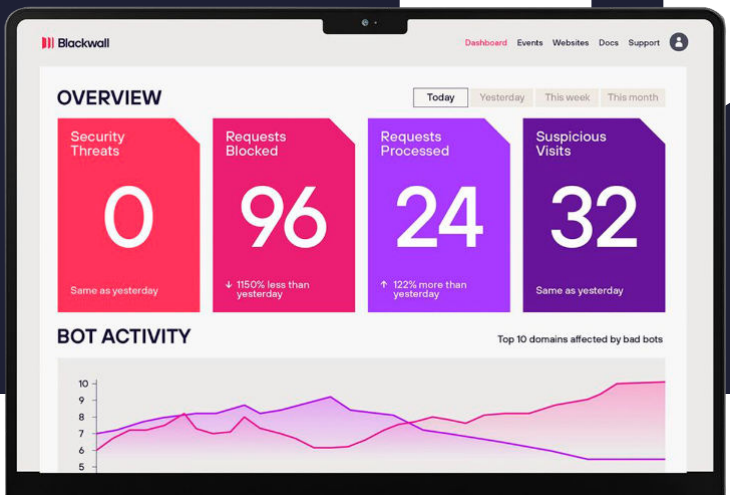


Blackwall

Bezpieczeństwo ruchu internetowego

Czym jest bezpieczeństwo ruchu na stronie internetowej?

Cyberbezpieczeństwo jest tematem ważnym, ale też złożonym i skomplikowanym. Jednak, jeśli chodzi o ochronę przedsiębiorstw oraz ich działań online, kluczowe jest bezpieczeństwo ruchu na stronie internetowej.

Złośliwe działania na stronach internetowych, inicjowane przez hakerów i zagrożenia internetowe, przekształciły się w pełnoprawny biznes na czarnym rynku, na który większość organizacji nie jest gotowa. Najnowsze szacunki wskazują, że do 2025 r. globalny koszt cyberprzestępczości osiągnie rocznie 10,5 biliona dolarów amerykańskich. Tak alarmująca liczba powinna stanowić ważne ostrzeżenie dla przedsiębiorstw, aby wzmocniły pierwszą linię obrony, w przeciwnym razie poniosą poważne konsekwencje, takie jak działania prawne, kary finansowe, utraty danych naruszeń, straty finansowe, szkody w reputacji i ciągłości działania.

Problem leży w reaktywnej postawie decydentów, którzy skupiają się na konsekwencjach działań, zamiast szukać ich pierwotnych przyczyn. Każdy atak DDoS, hakerski, spamowy lub scraperowy jest starannie planowany i obejmuje rozległe wyszukiwania lub wykorzystanie luk. Z uwagi na wyrafinowane, nowoczesne zagrożenia internetowe, które naśladują ludzkie zachowanie, proces ich wykrywania staje się coraz trudniejszy i omijają one starsze typy zabezpieczeń.

Jeśli firmy nie rozumieją swojego ruchu, nie są w stanie rozszyfrować charakteru cyberzagrożeń, przed którymi stoją. Bez tego zaniedbują pierwszy krok obrony w Internecie i często wdrażają szersze środki ochronne, które dają fałszywe poczucie bezpieczeństwa i nie wzmacniają skutecznie ich obrony. Bezpieczeństwo ruchu w witrynie ma na celu wypełnienie tej luki.

Czym są boty?

Ruch internetowy nie jest generowany wyłącznie przez człowieka. Ruch inny niż ludzki, czyli ruch botów, stanowił prawie połowę ruchu internetowego w 2022 r. i liczba ta stale rośnie. Ponadto sposób, w jaki współdziałamy w Internecie, znacznie się zmienił w ciągu ostatnich kilku lat wraz z rozwojem wyszukiwarek, takich jak Google, Yahoo czy Bing oraz asystentów cyfrowych, takich jak Siri, Alexa czy Asystent Google, zapewniających poczucie wygody i prostoty naszej codzienności.

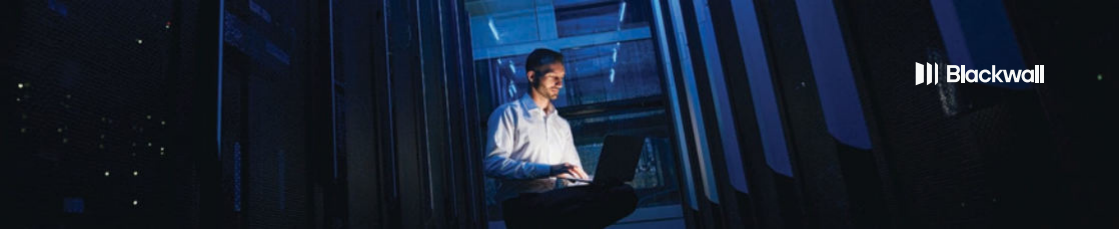
Mimo tych pozytywnych zmian, cyberprzestępcy również dokonali znacznego postępu w wykorzystaniu mocy oprogramowania. Zły ruch botów, który stanowił 30% całego ruchu internetowego, jest teraz powszechnym zjawiskiem, często pozostając niezauważony. Staje się on pierwszym elementem skoordynowanego planu ataku na strony internetowe i aplikacje, stanowiąc jedno z głównych zagrożeń dla firm w erze cyfrowej. Od oszustw reklamowych po blokowanie dostępu do zasobów czy kradzież danych uwierzytelniających – lista współczesnych zagrożeń internetowych jest długa i prognozowana jest jej dalsza ekspansja.

Zagrożenia wynikające z ignorowania ruchu złośliwych botów

Boty często kojarzone są z wyprzedażami limitowanych edycji sneakersów lub koncertami, na które bilety wyprzedają się w ciągu kilku sekund, jednak wpływ nikczemnego ruchu botów wykracza daleko poza sferę sprzedaży detalicznej online. Byliśmy świadkami jego wpływu na najważniejsze towary, takie jak niepokojący niedobór odżywek dla niemowląt, szaleństwo wokół zapasów konsol do gier i manipulacje rabatami z okazji Czarnego Piątku. Przypadki te podkreślają wszechobecny charakter złośliwych botów i ich zdolność do zakłócania nie tylko handlu, ale także życia konsumentów.

Działanie botów może prowadzić do blokowania stanu magazynowego, co z kolei prowadzi do frustracji klientów, którzy nie mogą kupić produktu. Boty mogą również wpływać na ceny, prowadząc do sztucznego podniesienia lub obniżenia ich poziomu. Może to prowadzić do strat finansowych zarówno dla przedsiębiorców jak i konsumentów. Dodatkowo boty mogą obniżać komfort użytkowników przez spowalnianie działania stron internetowych. Mogą powodować awarie, przejmować konta użytkowników, niszczyć dane oraz spamować.

Jeszcze bardziej niepokojące jest to, że boty mogą zagrażać ciągłości biznesowej. Bezpośredni wpływ finansowy i reputacyjny naruszenia danych lub ataków DDoS powinien przyprawić firmy każdej wielkości o dreszcze. Uwzględnij dodatkowe koszty związane z kontrolą szkód, karami regulacyjnymi i utratą zaufania klientów, a obraz stanie się tylko ciemniejszy.



Wpływ botów na moją firmę

Skalper bot (bot skalpujący)

Bot skanuje cały Internet w poszukiwaniu atrakcyjnych produktów. Następnie porównuje ich ceny dostępne w różnych sklepach i na aukcjach internetowych i wykupuje wszystkie produkty w cenie promocyjnej. W efekcie sklep, który zdecydował się na wystawienie produktu w niższej cenie, sprzedaje cały zapas nieuczciwej konkurencji, która później sprzedaje te produkty po wyższej cenie. Sklep nie tylko ponosi stratę finansową, ale również traci zaufanie klientów, którzy myślą, że sklep ich oszukał i wcale nie oferuje tego produktu w tej cenie.

Wpływ na przedsiębiorstwo:

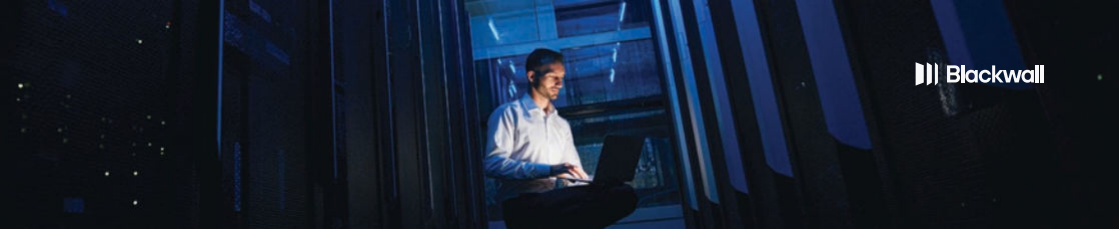
- **Zniechęcenie klienta**
- **Strata lojalności klientów**
- **Marnowanie środków marketingowych**
- **Błędy w planowaniu zapasów**
- **Straty reputacyjne**

Credential Cracker (łamacz haseł)

Bot łamie poświadczenia użytkowników poprzez wielokrotne wprowadzanie różnych kombinacji loginu i hasła. Oczywiście robi to błyskawicznie podejmując kilkaset a nawet kilka tysięcy prób na sekundę. Manipulacja kontami, przejęcie kontroli nad kontami oraz kradzież towarów to skutki jego aktywności w naszym sklepie www.

Wpływ na przedsiębiorstwo:

- **Straty finansowe bezpośrednie**
- **Zniechęcenie klienta**
- **Naruszenie prywatności danych**
- **Strata lojalności klientów**



AD Fraud (oszustwo reklamowe)

Proceder polega na wyklikaniu budżetu marketingowego przez boty. Wykorzystywany przez nieuczciwą konkurencję oraz właścicieli stron internetowych i aplikacji.

Wpływ na przedsiębiorstwo:

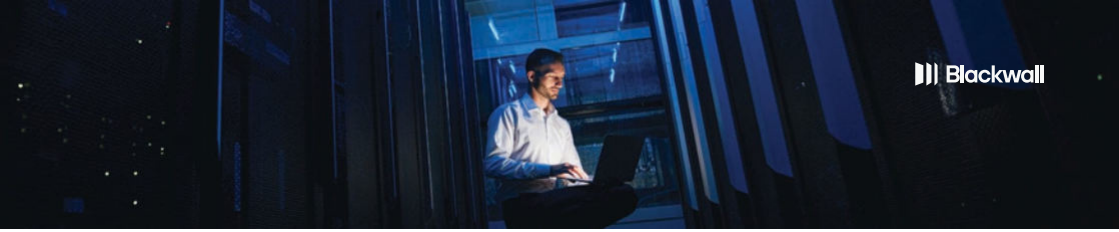
- **Utrata budżetów reklamowych i marketingowych**
- **Modyfikacja statystyk i danych analitycznych**
- **Błędy marketingowe i planistyczne wynikające z nieprawidłowych danych**

Spam Bot (bot spamujący)

Bot spamujący wykorzystuje oprogramowanie do rozpowszechniania złośliwych lub wątpliwych informacji w treściach publicznych lub prywatnych, bazach danych lub wiadomościach użytkowników. Zagrożenie to występuje we wszystkich witrynach handlu elektronicznego, które zawierają opinie użytkowników, w tym oceny i recenzje.

Wpływ na przedsiębiorstwo:

- **Fałszywe opinie o produktach i usługach mogą prowadzić do nieprzewidywalnych sytuacji**
- **Zniekształcenie analizy prowadzące do błędów marketingowych**
- **Problemy z nawigacją użytkownika na stronie internetowej**



Scarper Bot (bot skrobak)

Bot kopiuje zawartość naszej aplikacji internetowej (treści, zdjęcia, cenniki oraz wrażliwe dane) aby następnie wykorzystać je gdzie indziej. Takie działanie jest trudne do wykrycia i jest masowo wykorzystywane przez firmy konkurencyjne do monitorowania cen, dostępności produktów, ocen konsumentów jak i stanów magazynowych, zwłaszcza w dynamicznym środowisku.

Wpływ na przedsiębiorstwo:

- Znaczące obciążenie serwera pasożytniczym ruchem
- Monitorowanie konkurencji
- Modyfikacja statystyk i danych analitycznych
- Hakowanie systemów dynamicznych cen zazwyczaj prowadzi do bezpośredniego zabezpieczenia strat finansowych
- Często stosowane do przygotowywania skoncentrowanych ataków

Denial of Inventory (blokowanie stanu magazynowego)

Bot dodaje wszystkie nasze produkty do koszyka i nigdy nie finalizuje zakupu. Takie działanie blokuje nasz stan magazynowy i towary nie są dostępne dla realnych klientów

Wpływ na przedsiębiorstwo:

- **Zwykli klienci tracą dostęp do produktów i usług**

Czy boty wpływają na moją witrynę?

Aby ocenić wpływ botów na Twoją witrynę, konieczne są specjalne narzędzia programowe. Istnieje kilka symptomów, które mogą wskazywać na potencjalne zakłócenia spowodowane działaniem złośliwych botów i wagę ich skutków:

1

Niespójne wzorce zachowań gości

Grupy użytkowników zachowują się w określony sposób i nie odbiegają od niego zbytnio. W przypadku zauważenia znacznego odstępstwa od standardowych wyników istnieje wysokie prawdopodobieństwo, że masz do czynienia z botami. Przykłady obejmują wzrost liczby odwiedzanych produktów, większą głębokość przeglądanych stron, nieregularny harmonogram wizyt na stronie internetowej lub znaczną liczbę porzuceń zakupów, które nie wynikają z żadnych zmian na stronie.

2

Wzorce powtarzające się dla różnych kont użytkowników

Innym sposobem zakłóceń jest powtarzanie wzorców na różnych kontach użytkowników, których nie można wytłumaczyć przyczynami naturalnymi. Najczęstszymi przykładami są udostępnianie danych konta i adresu dostawy na wielu kontach, jednoczesna zmiana danych, zmiana zakresów adresów IP krajów na wielu kontach, powtarzające się sformułowania lub szybkie zmiany w proporcjach urządzeń użytkownika.

3

Anomalia wielkości ruchu internetowego

Wysokie wzrosty ruchu w przypadku towarów i usług o ograniczonej dostępności, szczyty wyświetleń i kliknięć w połączeniu z niezwykle niskimi odsłonami stron i konwersją, gwałtownie rosnąca liczba utworzonych kont lub gwałtowny wzrost liczby ocen i recenzji to tylko niektóre ze wskaźników, na które powinieneś zwrócić uwagę, aby zapewnić prawidłowe funkcjonowanie Twojej witryny internetowej.

4

Niska wydajność strony internetowej

Jeśli nie potrafisz wyjaśnić słabego funkcjonowania swojej strony spowodowanego nieprawidłową konfiguracją, może dojść do przeciążenia zasobów przez boty.
W tego rodzaju sytuacjach aktualizacja serwera nie jest wystarczająca, gdyż konieczne będą specjalistyczne narzędzia do monitorowania ruchu.

5

Skargi klientów

Poza omówionymi wskaźnikami, opinie klientów mogą stanowić istotne źródło informacji. Skargi klientów, które nie poddają się standardowym procedurom, powinny być traktowane jako bodziec do analizy ewentualnych nieprawidłowości. Nasze doświadczenie wskazuje, że opinie klientów często sygnalizują problemy.

Jak postępować w przypadku problemu dotyczącego mojej firmy

Brak priorytetowego traktowania bezpieczeństwa ruchu w witrynie może mieć poważne konsekwencje dla firm. Od bezpośrednich skutków finansowych i reputacyjnych, po kary regulacyjne lub potencjalną utratę zaufania klientów – konsekwencje mogą być druzgocące.

Poza przyjęciem proaktywnego podejścia i stosowaniem prostych środków, takich jak regularne aktualizowanie i łatanie oprogramowania witryny internetowej lub monitorowanie ruchu, należy wdrożyć odpowiednie środki bezpieczeństwa. Przede wszystkim należy wdrożyć skuteczne rozwiązanie zabezpieczające ruch, które może pomóc w wykrywaniu i blokowaniu złośliwego ruchu, takie jak to dostarczane przez Blackwall. Usuwając boty, organizacje mogą zarówno chronić firmę, jak i zapewnić bezproblemowe zakupy prawdziwym użytkownikom. Brak botów pomaga również firmom podejmować bardziej wnikliwe decyzje w oparciu o autentyczne interakcje z klientami, optymalizować działania marketingowe i poprawiać ogólną satysfakcję klientów.

Wraz z rosnącym ruchem internetowym, wzrasta ryzyko zatorów i zakłóceń w ruchu online spowodowanych złośliwą działalnością. Brak odpowiednich środków bezpieczeństwa naraża przedsiębiorstwa na ataki oraz przyczynia się do przeciążenia i niestabilności Internetu.

Blackwall

Kim jesteśmy?

Blackwall (dawniej BotGuard) to firma europejska założona w 2019 roku z siedzibą w Tallinie, w Estonii. Działająca globalnie, z klientami i partnerami w ponad 30 krajach, specjalizuje się w opracowywaniu rozwiązań zabezpieczających ruch na stronach internetowych, chroniących firmy przed współczesnymi zagrożeniami internetowymi, takimi jak złośliwe boty, ataki hakerów i inne szkodliwe działania w Internecie.

Zapewniając webmasterom i właścicielom witryn proste i niezawodne narzędzie umożliwiające podjęcie decyzji, kogo chcą wpuścić, zabezpieczamy infrastrukturę i działanie, jednocześnie zmniejszając ryzyko dla Twojej firmy i jej klientów.

Liczby kluczowe:

Ponad 2,1 miliona aplikacji internetowych jest chronionych
Wliczając niewielkie strony internetowe MŚP, które odwiedzane są przez kilka tysięcy osób dziennie oraz klastry na poziomie przedsiębiorstw o dużej szybkości transferu.

Ponad 30 państw
Obejmuje kraje Beneluksu, DACH, Wielką Brytanię, Irlandię, kraje nordyckie, kraje bałtyckie, USA, Kanadę, Meksyk, Brazylię, Argentynę, Australię, Nową Zelandię, RPA, Izrael, Polskę, Francję, Hiszpanię, Grecję i Włochy.

Ponad 50 ekspertów bezpieczeństwa
We wszystkich głównych strefach czasowych, zapewniając ochronę Twojej firmy przez 24 godziny na dobę, 7 dni w tygodniu.

Porozmawiajmy!

Systemy Informatyczne ITXON Sp. z o.o.
Dystrybutor produktów firmy Blackwall

ul. Garncarska 34,
42-200 Częstochowa
handel@itxon.pl | www.itxon.pl

Wpisana do rejestru przedsiębiorstw w Krajowym Rejestrze Sądowym w Częstochowie, XVII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000968078 z kapitałem 600 000 zł, NIP 573-250-72-21