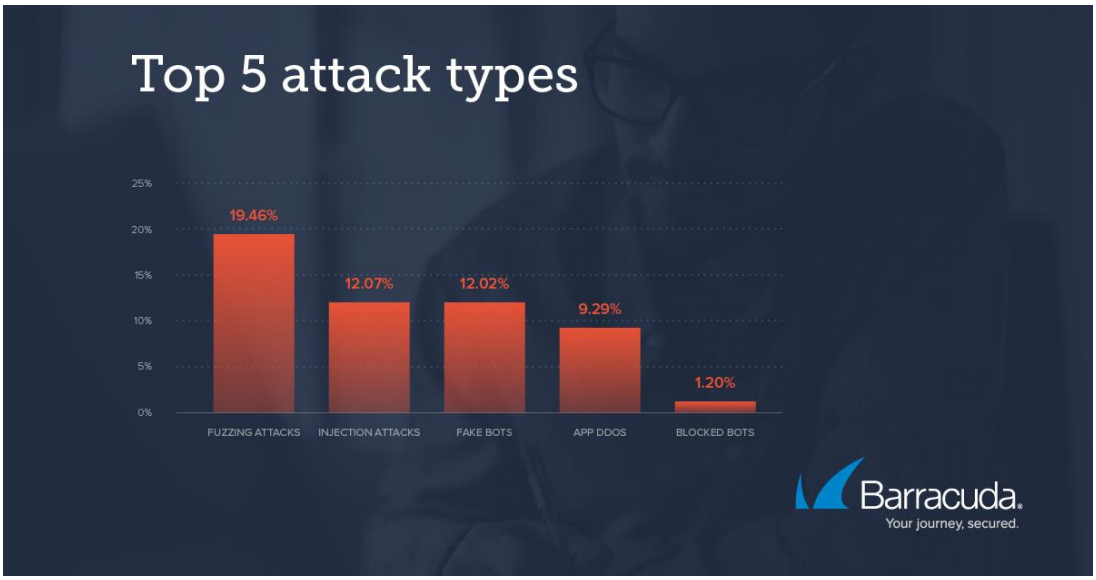
Informacje o zagrożeniach: zautomatyzowane ataki na aplikacje internetowe

Cyberprzestępczość stała się wielkim biznesem, a oszuści coraz częściej sięgają po boty i automatyzację, aby ich ataki były bardziej wydajne, skuteczne i trudne do wykrycia.

W grudniu 2020 r. analitycy firmy Barracuda przeanalizowali próbkę danych z ataków przeprowadzonych w ciągu dwóch miesięcy na aplikacje internetowe zablokowane przez systemy Barracuda. Wyniki pokazały ogromną liczbę ataków zautomatyzowanych. Pięć najpopularniejszych ataków było zdominowanych przez ataki wykonywane przy użyciu narzędzi automatycznych.



Prawie 20% wykrytych ataków stanowiły ataki fuzzingowe, które są realizowane automatycznie w celu wykrycia przypadków, w których aplikacje załamują się, i wykorzystania wykrytych w ten sposób luk do przeprowadzenia ataku. Kolejnych ok. 12 proc. ataków polegało na wstrzyknięciu kodu, przy czym większość atakujących używała do tego zautomatyzowanych narzędzi, takich jak sqlmap. Wiele z tych ataków było realizowanych na poziomie script kiddies – bez wcześniejszego rozpoznania, który pozwoliłby je zoptymalizować.

Niemal ex aequo, na trzecim miejscu, również stanowiąc nieco ponad 12% ataków, były boty podszywające się pod roboty indeksujące Google lub innych wyszukiwarek. Zaskakująco powszechne, stanowiąc ponad 9% analizowanej przez analityków z firmy Barracuda próbki, były też ataki typu DDoS, czyli rozproszonej blokady dostępu – które były stosowana we wszystkich obszarach geograficznych. Natomiast boty zablokowane przez administratorów strony miały znaczenie marginalne (poniżej 2% ataków).

A oto trendy wykryte przez analityków w atakach na aplikacje internetowe oraz sposoby, w jaki cyberprzestępcy wykorzystują ataki zautomatyzowane.

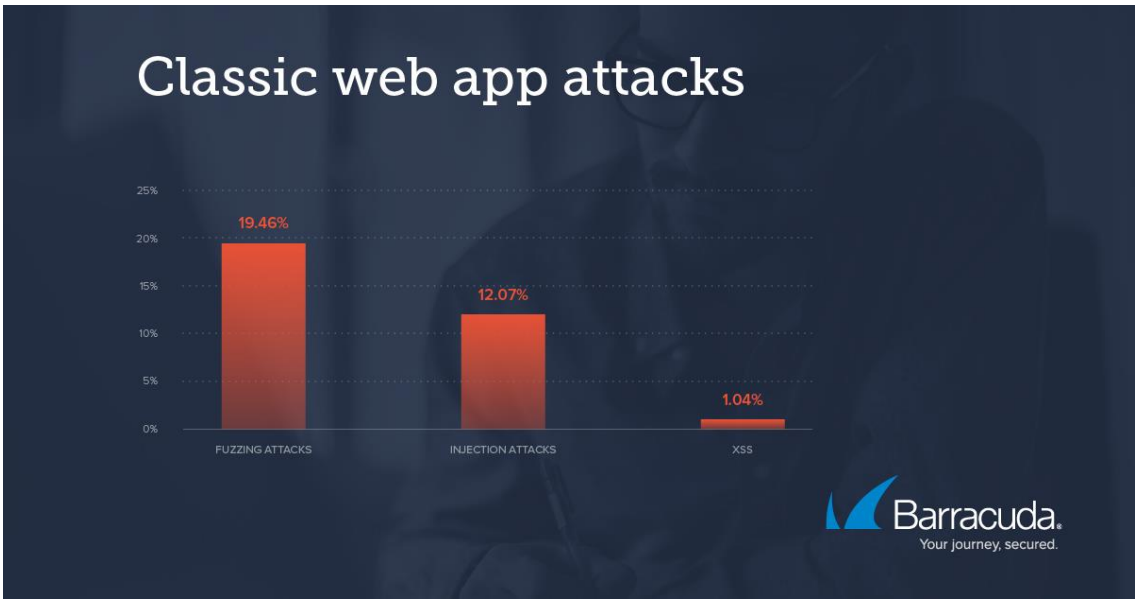
Wyróżnione zagrożenia

Ataki zautomatyzowane – w atakach zautomatyzowanych stosowane są boty, które próbują wykorzystywać luki i podatności aplikacji internetowych. Obejmują one szerokie spektrum zagrożeń, od botów udających szperacze Google w celu uniknięcia wykrycia, po ataki DDoS, które przeciążając aplikację usiłują doprowadzić do awarii witryny.

Chociaż ruch botów jest szybko rosnącym problemem, nie oznacza to, że cyberprzestępcy zarzucają stare metody. Duża część ataków przeanalizowanych przez analityków z firmy Barracuda to ataki klasyczne, takie jak

wstrzykiwanie kodu (12%) i cross-site scripting (XSS) (1%). Jednak większość ruchu związanego z atakami pochodziła z narzędzi stosowanych do prowadzenia rekonesansu lub wspomnianego narzędzia fuzzing do sondowania aplikacji.

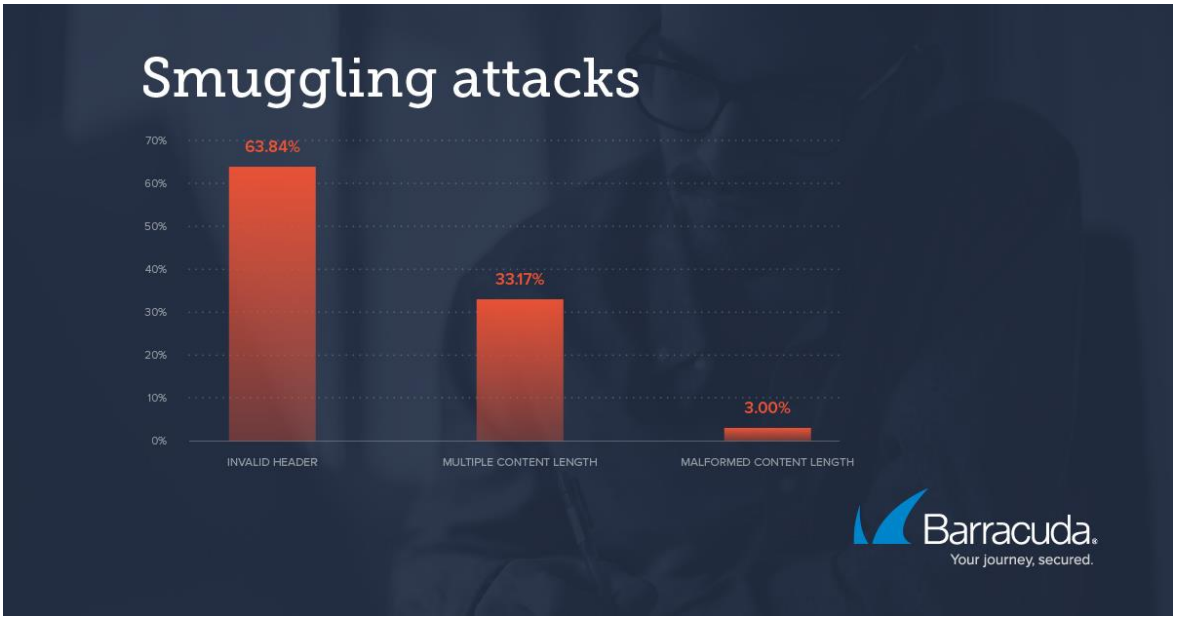
Wstrzykiwanie kodu otwiera najnowszą listę dziesięciu najpoważniejszych zagrożeń przygotowywaną przez fundację Open Web Application Security Project (*OWASP Top 10*) i odkąd istnieje ta lista, są obecne w każdej kolejnej jej edycji. Nie ma też żadnych oznak zarzucania ich ze względu na relatywną łatwość wykonania i potencjalnie duże korzyści dla cyberprzestępców. Dość częste były również ataki typu cross-site scripting (XSS) –trzeci najczęściej stosowany atak w tej grupie.



Szczegóły

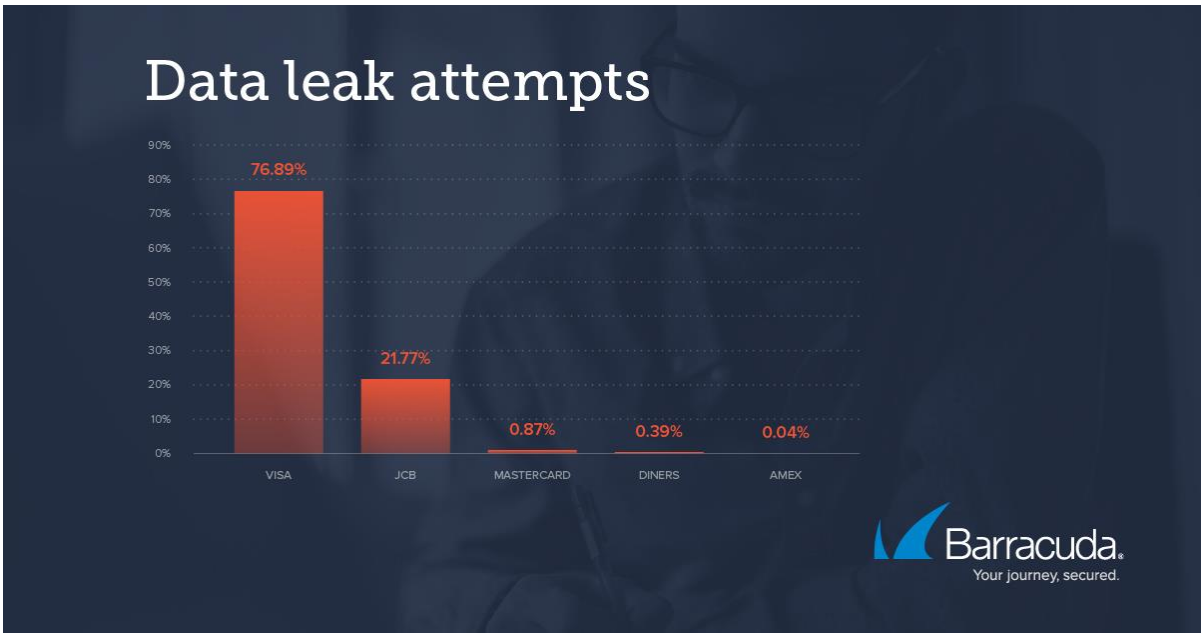
Znaczna część analizowanego ruchu związanego z atakami miała na celu wykorzystanie podatności aplikacji WordPress (popularny CMS wykorzystywany przez twórców stron internetowych) lub PHP (zwykle były to strony phpMyAdmin stosowane do zarządzania bazą danych MySQL) – było to odpowiednio 6,1% oraz 1,05% ataków. Spora część z nich została przeprowadzona przeciwko stronom niewykorzystującym PHP lub WordPressa, co prowadzi do wniosku, że były one dziełem tzw. „*script kiddies*" – osób korzystających z gotowych, dostępnych w Internecie narzędzi hackerskich, lecz nie mających pojęcia na temat ich działania. Niewykluczone jednak, że osoby te wkrótce nauczą się przeprowadzać rekonesans przed przeprowadzeniem ataku.

Atakiem, którego popularność spadła do pomijalnego poziomu, ale który po ujawnieniu ataku HTTP Desync powraca na skalę masową, jest przemycanie zapytań http (*HTTP Request Smuggling*). Według badania firmy Barracuda, ponad 60% tego typu ataków wykorzystywało nieprawidłowy nagłówek protokołu http, jedna trzecia wykorzystywała zwielokrotnianie wartości w polu *Content-Length*, a 3% miało źle sformatowaną wartość w tym polu.



Większość zaobserwowanych ataków przeciwko API JSON polegała na testowaniu warunków brzegowych, czyli w gruncie rzeczy były to próby zmylenia tego API. W 95% tego typu ataków przekraczano dopuszczalną wielkość liczb (*Max Number*), a w prawie 4% – dopuszczalną długość napisów (*Max Value Length*). Zaobserwowano również inne próby ataków – ataki XSS i SQL Injection – ale ich liczba w próbce była pomijalna. Analitycy spodziewają się jednak, że w ciągu najbliższego roku może ona wzrosnąć.

Próby wycieku danych dotyczyły głównie prób ujawnienia wrażliwych danych, takich jak numery kart kredytowych, ubezpieczenia społecznego (używanych w wielu krajach do potwierdzania tożsamości, analogicznie jak polski PESEL), itp. Dominowały próby eksfiltracji numerów kart kredytowych. Głównym celem była Visa, przeciwko której zanotowano ponad trzy czwarte wszystkich ataków tego typu. Daleko w tyle była firma JCB (ponad 20% ataków), natomiast Mastercard, Diners i American Express były atakowane znacznie rzadziej.



Szyfrowanie

Analitycy firmy Barracuda przeanalizowali również szyfrowanie ruchu, które zapobiega różnym atakom, takim jak man-in-the-middle, oraz zapewnia warstwę ochrony użytkowników odwiedzających strony internetowe.

Prawie 92% ruchu analizowanego przez naukowców Barracuda w okresie dwóch miesięcy od października do grudnia 2020 r. to szyfrowany ruch HTTPS, a nieszyfrowany protokół HTTP był odpowiedzialny za mniej niż 10% ruchu. To obiecujący postęp i dobra wiadomość dla bezpieczeństwa aplikacji internetowych.

Preferowanym protokołem stosowanym w przeglądarkach jest obecnie TLS1.3, co zaczyna mieć wpływ na bezpieczeństwo użytkowników. Starszy protokół SSLv3 był rzadko stosowany, ponieważ nie jest on zbyt skuteczny. Nawet wśród organizacji, które korzystają z tego protokołu, ruch SSLv3 był niewielki. To samo dotyczy protokołów TLS1.0 i TLS1.1, których popularność gwałtownie spada – a z których każdy odpowiada za mniej niż 1% analizowanego ruchu.

Najbezpieczniejszy obecnie protokół TLS1.3 stanowił całe 65% całego analizowanego ruchu HTTPS. Około jednej trzeciej stanowił starszy protokół TLS1.2, ale jego popularność powoli spada.

Analizując przeglądarki korzystające z TLS1.3 (w oparciu o informacje zgłaszane przez same przeglądarki w nagłówkach User Agent), najpopularniejszą przeglądarką, odpowiedzialną za 47% ruchu zaszyfrowanego tym protokołem, była Chrome. Na drugim miejscu było Safari, które odpowiadało za 34% ruchu TLS1.3. Co zaskakujące, Edge wyprzedził Firefoksa i znalazł się na podium z 16% ruchu, natomiast Firefox wygenerował zaledwie 3% ruchu. Firefox przegrywa z Edge prawdopodobnie z dwóch powodów:

- Dominacja Chrome
- Systemy korporacyjne, które dotychczas preferowały przeglądarkę Internet Explorer, obecnie przechodzą na Edge

Analiza ruchu TLS1.2 przyniosła bardziej zaskakujące wyniki. W tym protokole Internet Explorer generuje wyższy ruch niż Chrome – odpowiadając za ponad połowę ruchu – natomiast Chrome ma nieco poniżej 40%. Dla porównania, Safari generuje poniżej 10% ruchu, a Firefox – jeszcze mniej.

Analitycy z firmy Barracuda odkryli, że dość często stosowane są automatyczne aktualizacje przeglądarek Chrome i Firefox. Większość tych przeglądarek to najnowsza lub jedna z dwóch najnowszych wersji.

Nadal wiele osób korzysta z Internet Explorera, przy czym zdecydowanie najczęściej była to wersja IE11, co pokazuje poprawny trend w kierunku używania bardziej aktualnych i bezpiecznych przeglądarek.

Dla kontrastu, ruch generowany automatycznie rzadko wykorzystuje TLS1.3 – zwykle jest to jednak TLS1.2. Obejmuje to monitory witryn, boty i narzędzia, takie jak curl.

Jak się chronić przed atakami zautomatyzowanymi

W obszarze ochrony przed najnowszymi atakami, takimi jak boty i czy ataki przeciwko API, można być przytłoczonym liczbą wymaganych rozwiązań. Na szczęście są one łączone w takich produktach, jak WAF / WAF-as-a-Service, znanymi również jako usługi ochrony aplikacji webowych i usługi ochrony API (WAAP).

Jak to zdefiniował Gartner w raporcie WAF Magic Quadrant 2020:

„Gartner definiuje usługi WAAP jako ewolucję usług WAF w chmurze. Usługi WAAP obejmują usługi WAF, ochronę przed botami, ochronę przed DDoS i ochronę API, dostarczane w chmurze w modelu subskrypcyjnym”.

Organizacje powinny więc poszukać rozwiązania WAF-as-a-Service lub WAAP, które obejmuje ochronę przed botami, ochronę przed DDoS, ochronę API i ochronę przed zapychaniem poświadczeniami – oraz upewnić się, że zostało ono odpowiednio skonfigurowane.

Należy też być na bieżąco z aktualnymi zagrożeniami i śledzić ich zmiany. Na przykład podczas niedawnego webinarium (dostępnego obecnie na żądanie) firma Barracuda podzieliła się prognozami dotyczącymi trzech najważniejszych typów ataków, których częstszego stosowania spodziewa się w tym roku: zautomatyzowanych ataków botów, ataków na interfejsy API i ataków na procesy tworzenia oprogramowania. Ochrona przed tymi typami ataków jest słabsza, więc zwykle są one przepuszczane czy to z ich niedoceniania czy – w niektórych przypadkach – wdrażania aplikacji poza kontrolą działu IT i bez odpowiednich zabezpieczeń.