BIOMETRIA BEHAWIORALNA LEKIEM NA WYŁUDZENIA FINANSOWE? [TEST TECHNOLOGII]

Analiza zachowania użytkowników napędza nowe technologie wymierzone w oszustów działających na rynku płatniczym. Biometria behawioralna coraz silniej zaznacza swoją obecność w branży. Czy stanowi skuteczny lek na problemy branży? Test technologii proponowanej przez Nethone, prezentuje Aleksander Kijek, Chief Product Officer, Nethone

Technologia Nethone opiera się na analizie zachowania użytkowników stron internetowych poprzez wykorzystanie uczenia maszynowego do wykrywania fraudu płatniczego online. Dzięki połączeniu maszyny i ludzkiej kreatywności zespołu specjalistów ds. danych, którzy skupili się na ekspozycji *feature importance*, tłumaczeniu modeli uczenia maszynowego Nethone stanowi tzw. white box. Jednym z filarów technologii jest unikatowy profiler zbierający dane, które można wzbogacić o zewnętrzne źródła danych w celu utworzenia "centrum danych" unikatowego dla każdego sprzedawcy. Są one przedstawione wraz z wynikami analizy uczenia maszynowego na czytelnym, graficznym panelu.

Nethone wykorzystując Profilera zbiera ponad 5000+ atrybutów, które wykorzystywane są w modelach uczenia maszynowego. To urządzenie, oparte na naszych badaniach w dark webie i różnych forach, zbiera dane z czterech domen. Po pierwsze sprawdza specyfikę urządzenia (od strony sprzętu i oprogramowania) w tym m.in.

- rozpoznanie hardware'u i systemu,
- charakterystyka i wykrycie GPU,
- wykrycie wirtualnych maszyn,
- liczba rdzeni w procesorze,
- wykrywanie urządzeń mobilnych lub ich emulacji,
- informacje o baterii.

Po drugie, określenie połączenia sieciowego (w jaki sposób dane urządzenie łączy się z witryną / aplikacją natywną – w tym wypadku firmy pożyczkowej lub linii lotniczej) i wszelkie próby anonimizacji tego połączenia. Do najpopularniejszych elementów należy:

- geolokacja z użyciem IP,
- analiza stosu sieciowego TCP/IP i wykrywanie anomalii,
- rozpoznanie typ połączenia na podstawie niskopoziomowym i/lub charakterystyk przeglądarki,
- cyfrowy odcisk palca systemu, tzw. fingerprint systemu,
- wykrycie technologii VPN/Proxy/Tunelowania,
- wykrywanie sieci TOR,
- informacja o typie IP
- charakterystyka połączenia od strony sieciowej (np. router w domu/pracy/serwerowni)

Trzecia kategoria danych dotyczy przede wszystkim przeglądarki jako narzędzia wykorzystywanego do przeglądania stron internetowych, w tym witryn sklepów internetowych, linii lotniczych itd. Najważniejszymi są:

- Anomalie w sposobie Renderowania DOM (układu HTML, kodów JS)
- Nietypowe kody HTML
- Specjalne pliki cookie (bazowane na technologiach HTML, samoistnie przywracalne)
- Wykrywanie popularnych dla oszustów narzędzi (wtyczek, dodatków)
- Wykrywanie ukrywania swojej tożsamości w sieci
- Wykrywanie korzystania z trybu Incognito w przeglądarce
- Nietypowe cechy przeglądarki
- Różne fingerprinty

Narzędzie - Nethone Guard - ma możliwość stać się centrum danych dla firmy, koncentrując w sobie nie tylko dane o kliencie, ale także informacje zewnętrzne: m.in. Paay, Ethoca, Emailage, Geo IP, BIN Intelligence. Deweloperzy w Nethone stworzyli API, które może stać się centrum analizy danych - pozwala podłączyć dowolne źródła danych firm zewnętrznych lub po prostu przesłać więcej danych o danej sesji, z których modele mogą się uczyć.

Profiler zbierając informacje pozostawione przez użytkownika przy korzystaniu ze strony pozwala na weryfikację użytkownika od strony behawioralnej, czyli badanie interakcji użytkownika z serwisem m.in.

- jego tempo i takt pisania,
- ruchy myszką/touchpadem
- przesunięcia/dotknięcia i przewijanie
- dynamika naciskania klawiszy
- odczyty żyroskopu i akcelerometru w wypadku sprzętu mobilnego
- wklejanie w pola zamiast wpisywania.

Uczenie maszynowe zapewnia bardziej kompleksowy ogląd biznesu, wyraźne wskazanie KPI, szybszą adaptację i dokładniejsze decyzje. Techniki oszustów, polegające na fałszowaniu systemów zapobiegania fraudom, ciągle się zmieniają i stają się coraz bardziej wyrafinowane. Co więcej, nieustannie udoskonalają swoje metody, pozostawiając systemy statycznych reguł firmy daleko w tyle. Obecnie, aby odnieść większy sukces w walce z oszustwami internetowymi, więcej danych (w zakresie wielkości i różnorodności) należy analizować w krótszym czasie - niezbędne są do tego bardziej zaawansowane technologie. Dla każdego użytkownika strony są one w stanie przeanalizować tysiące atrybutów w ciągu sekundy odkrywając skomplikowane wzorce i relacje. W wyniku ich analizy sprzedawca/usługodawca internetowy otrzymuje decyzje, czy dana transakcja jest uczciwa, czy nie. Dzięki zastosowaniu uczenia maszynowego system bierze pod uwagę wszystkie dostępne atrybuty, przypisuje im i ich relacjom wagi wpływu prowadząc do niespotykanie precyzji rekomendacji.

Siła uczenia maszynowego wynika ze zdolności przeanalizowania takiego bogactwa informacji w krótkim czasie. Dla najlepszej jakości predykcji, Nethone wykorzystuje najbardziej zaawansowane algorytmy uczenia maszynowego - xgboost czy sieci neuronowe. Jednocześnie staramy się odkrywać jak najwięcej w kontekście ich sposobu działania. Jednak trzeba pamiętać, że wdrożenie uczenia maszynowego pozwalającego na analizę tysięcy atrybutów i zrozumienie nieliniowych zależności między nimi, uniemożliwia predykcję zrozumiałą dla ludzkiego mózgu. Nethone stara się odkryć rąbka tajemnicy przez ekspozycję *feature importance,* a nawet przekazywanie wag atrybutów dla każdej z predykcji.

Materiał przygotowany we współpracy z Nethone