Momentum Solutions S.A.

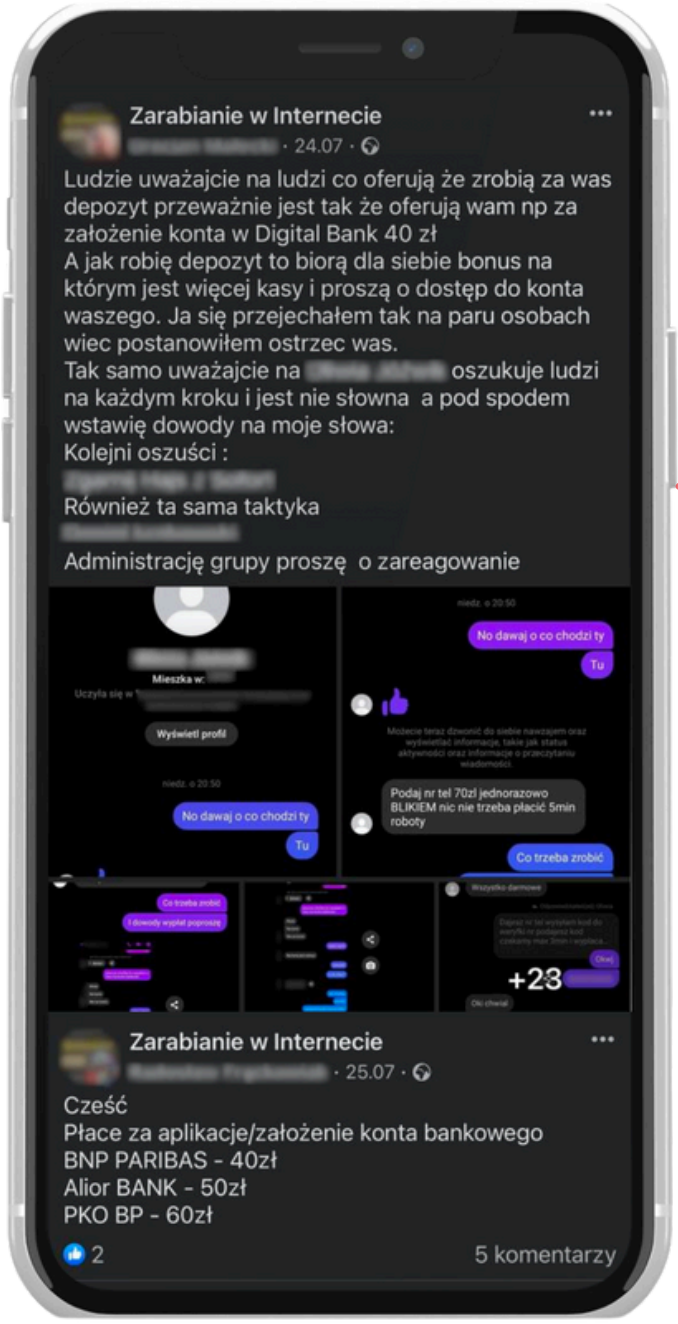
KAIROS™ FRAUD DETECTOR

SYSTEM WSPARCIA DECYZYJNEGO W OBSZARZE BEZPIECZEŃSTWA DOSTĘPU DO SERWISÓW WEB

Momentum Solutions S.A.

momentumsolutions.pl

Niekontrolowany handel kontami bankowymi



W Internecie – zwłaszcza na portalach społecznościowych – coraz częściej dochodzi do nielegalnego obrotu kontami bankowymi. Podobnemu procederowi podlegają również konta podmiotów prowadzących rachunki płatnicze na podstawie licencji MIP lub KIP.

Przykład skali problemu:

Konta bankowe (zarówno prywatne, jak i firmowe) „bez zajęć komorniczych" można kupić już za 20 zł!

Dlaczego handluje się kontami bankowymi?

1. **Wyłudzanie bonusów bankowych**

   Banki oferują premię za założenie konta online lub za pomocą kuriera. „Sprzedawcy" kont przechwytują te bonusy, co prowadzi do nieoptymalnej alokacji środków marketingowych po stronie banku. W skrajnych przypadkach może to skutkować wyłączeniem opcji zakładania rachunków online w trakcie trwającej kampanii.

2. **Legalizacja nieuczciwych środków**

   „Kupione" konto umożliwia uwiarygodnienie nielegalnego pochodzenia pieniędzy, co narusza procedury AML i naraża banki na odpowiedzialność.

3. **Transakcje kryptowalutowe**

   Anonimowość transakcji w kryptowalutach, w połączeniu z cudzym kontem, służy do zaciemniania źródła pochodzenia środków oraz obchodzenia regulacji.

4. **Potwierdzenie tożsamości**

   Część osób używa „zakupionych" rachunków, by posłużyć się danymi innej osoby i zyskać pozorne potwierdzenie tożsamości.

5. **Wyłudzenia finansowe**

   Kredyty, pożyczki, fałszywe sprzedaże na platformach e-commerce (Allegro, OLX), – takie operacje są łatwiejsze, gdy wykorzystuje się nie swoje, a kupione konto.

Wnioski z analizy odporności systemu bankowego na fraudy

Na podstawie przeprowadzonych badań wynika:

1.Brak możliwości ustalenia beneficjenta rzeczywistego

Klienci świadomie przekazują dane logowania do kont, co powoduje, że bank nie jest w stanie stwierdzić, kto realnie korzysta z rachunku.

2.Procedury AML a skala zjawiska

Ze względu na skalę procederu, dotychczasowe procedury AML okazują się niewystarczające. Osoby dokonujące oszustw z łatwością obchodzą standardowe zabezpieczenia.

3.Ryzyko trudnych do oszacowania strat

Banki mogą ponosić znaczące straty finansowe i wizerunkowe w związku z takimi nadużyciami.

4. Znaczenie wykrycia przestępstwa na wczesnym etapie

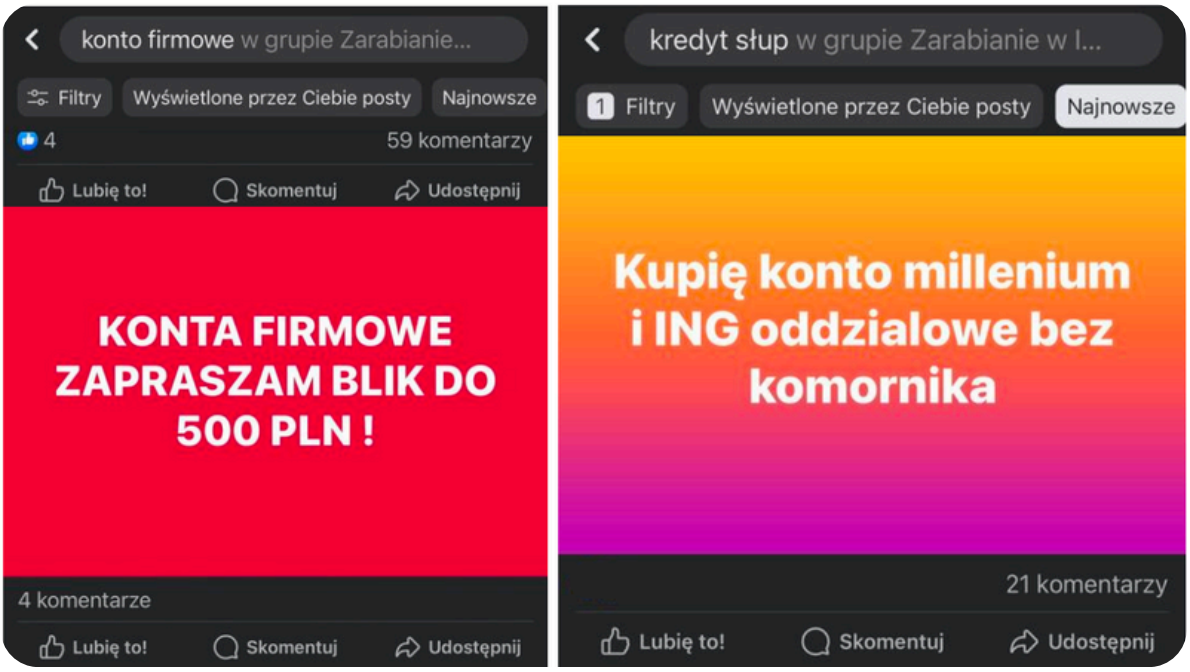
Kluczowe jest rozpoznanie, że doszło do fraudu w momencie jego rozpoczęcia, aby natychmiast zablokować dalsze operacje i zapobiec stratom.

Źródło danych:

Kilkanaście publicznych grup na Facebooku (m.in. „Zarabianie w Internecie”), liczących od kilkunastu do kilkudziesięciu tysięcy członków każda. Analitycy Momentum Solutions S.A. zidentyfikowali szereg zróżnicowanych charakterystyk powyższych fraudów, co pozwala na ich kategoryzację i precyzyjną identyfikację w systemach bankowych.

Brak skutecznych narzędzi zapobiegawczych

Handel danymi do logowania do aplikacji bankowych jest prowadzony na ogromną skalę i brak jest dostępnych rozwiązań technologicznych zapobiegających tego typu działaniom, obecnie funkcjonujące systemy nie dają możliwości zapobiegania realizacji opisanych fraudów, z uwagi na fakt, iż fraud opiera się o realne dane oraz o dobrowolne przekazanie danych do logowania.



Zjawisko to w szczególności dotyczy rachunków otwieranych za pośrednictwem aplikacji mobilnych np. konto na selfie. Jeden ze schematów fraudu, w dużym uproszczeniu, można przedstawić następująco: osoba sprzedająca konto zakłada je za pośrednictwem aplikacji mobilnej podając swoje prawdziwe dane, z wyjątkiem numeru telefonu i adresu e-mail, które należą do „fraudstera”. Po udanej weryfikacji tożsamości i zalogowaniu się do aplikacji sprzedający konto przekazuje dane do logowania, w zamian za umówione wynagrodzenie. Osoba nabywającą konto dokonuje logowania na swoim urządzeniu mobilnym, a następnie zmienia hasło i przejmuje konto bankowe wykorzystywane do procedur opisanych w niniejszym dokumencie.

momentumsolutions.pl

Kairos Fraud Detector – zaawansowany system wsparcia decyzyjnego

Kairos Fraud Detector jest systemem wsparcia decyzyjnego, bazującym na silniku analitycznym opracowanym w architekturze BIG DATA, z komponentami analizy strumieniowej - analiza danych w czasie rzeczywistym podczas ich napływania oraz algorytmami z zaszytą wiedzę o modelach działań fraudowych.

Architektura Systemu Kairos pozwala na identyfikację zdarzeń potencjalnych naruszeń w czasie rzeczywistym, tj. w milisekundach od otrzymania zdarzenia na wejściu. Tym samym Kairos umożliwia wykrycie fraudu ex-ante, czyli przed jego popełnieniem, co umożliwi zablokowanie fraudu przed jego wystąpieniem.

System powstał w oparciu o wieloletnią wiedzę zespołu programistów i analityków wytwarzających narzędzia informatyczne do walki z przestępczością zorganizowaną oraz w oparciu o doświadczenie z zaawansowanych systemów fraudowych związanych z oszustwami w transporcie dóbr akcyzowych oraz dóbr szczególnej wartości lub znaczenia.

Identyfikacja fraudów w czasie rzeczywistym bazująca na analizie wielokryterialnej zachowań użytkownika. Dane analizowane są z wykorzystaniem algorytmów ang. data quality - analizujących ich jakość pochodzącą od różnych typów urządzeń mobilnych, co umożliwia poprawne zakwalifikowanie okoliczności wpływających na prawidłowe określenie zdarzenia fraudowego. Zastosowanie analityki wielokryterialnej obejmuje między innymi dane o urządzeniu użytkownika, parametrach jego pracy i jego otoczeniu. Wykorzystanie rozbudowanych algorytmów badających sekwencje i dynamikę wykrywanych zmian stanu atrybutów pracy aplikacji. Wykrywanie tak zwanych ognisk naruszeń dzięki analizom korelacji oraz klasteryzacji schematów zachowywania się użytkowników. Całość procesu zakończona jest nadaniem klasyfikacji zdarzenia z uwzględnieniem metodologii KAIROS_FRAUD_STAMP.

System oprócz integracji z modułem detekcji anomalii oraz zdarzeń fraudowych w logice ex-ante, posiada również moduł analiz ex-post, celem definiowania nowych funkcjonalności oraz algorytmów z wykorzystaniem ang. machine learning.

Doświadczenie

Zespół z doświadczeniem implementacyjnym BIG DATA opartym na przetwarzaniu strumieniowym z analityką ang. real-time, w systemach infrastruktury krytycznej.

Doświadczenie w tworzeniu Systemów przetwarzania strumieniowego danych pozyskiwanych między innymi z urządzeń mobilnych klasy smartphone. Dzięki doświadczeniu przy współtworzeniu aplikacji mobilnych przekazujących dane telematyczne posiadamy szeroką wiedzę dotyczącą niedoskonałości poszczególnych klas sprzętu dostępnych na rynku oraz sposobów optymalizacji występowania anomalii w danych wysyłanych przez te urządzenia na poziomie oprogramowania.

Innowacja

- Analityka zdarzeń w „strumieniu na wejściu”
- Czas reakcji systemu na wykrycie naruszenia/anomalii na poziomie milisekund umożliwiające wykrycie fraudu w czasie rzeczywistym, a w efekcie zablokowanie fraudu przed jego wystąpieniem.

Skuteczność

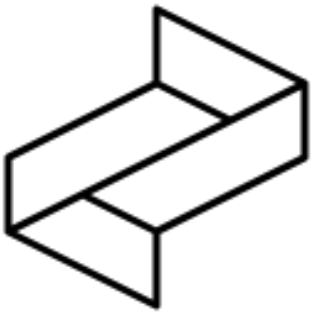
Wykonywanie alertów lub dyrektyw kontrolnych do systemów dostawcy usług o podejrzeniu fraudu zanim on wystąpi.

Ciągły rozwój

Identyfikacja schematów fraudów oraz ciągły rozwój algorytmów.

Możliwość wdrażania zmian bez wpływu na ciągłość przetwarzania głównego potoku danych.

Wysoka dostępność oraz elastyczność systemu pod kątem integracji z systemami dostawców usług.



O nas

Momentum Solutions S.A. to firma technologiczna specjalizująca się w systemach przeciwdziałania fraudom. Oferujemy takie produkty jak Kairos Fraud Detector dla branży finansowej i Kairos Inspector dla branży transportowej.

Modernizujemy systemy infrastruktury krytycznej dla Ministerstwa Finansów.

Nasz zespół współtworzył jeden z największych w Europie systemów antyfraudowych – system infrastruktury krytycznej ministerstwa finansów służący do monitoringu towarów szczególnego znaczenia.

Obsługujemy podmioty funkcjonujące w ramach NFZ w zakresie platformy automatyzującej proces zarządzania opieką koordynowaną.

Wytarzamy również innowacyjny system paszportyzacji i zarządzania procesem recyklingu oraz system automatyzacji procesu ofertowania dla branży budowalnej

[Pozostańmy w kontakcie]

Momentum Solutions S.A.

TOMASZ ZYGMAŃSKI
CEO

+48 601 888 007
biuro@momentumsolutions.pl

WWW.MOMENTUMSOLUTIONS.PL