aut. Andrzej Kozłowski 25.01.2019

PROWADZIMY WYŚCIG ZBROJEŃ Z FRAUDSTERAMI [WYWIAD]

„Karta płatnicza jako nośnik płatności nie została stworzona do działania w Internecie. Stąd taka popularność fraudów". O tym zjawisku, sposobach jego zwalczania oraz o tym jak sztuczna inteligencja może okazać się pomocna mówi w rozmowie z CyberDefence24.pl Hubert Rachwalski, CEO firmy Nethone.

Andrzej Kozłowski: Jak dużym problemem w Polsce są fraudy?

Hubert Rachwalski: Mimo że w Polsce użycie kart kredytowych jako sposobu płatności jest względnie niewielkie w porównaniu do innych krajów, przede wszystkim do Stanów Zjednoczonych, to problem ten jest coraz poważniejszy. Obserwujemy rosnące zagrożenie związane z wystąpieniem fraudów płatniczych z użyciem kart kredytowych i debetowych. Wynika to z coraz częstszego wykorzystania modelu subskrypcyjnego przez wielu dostawców innowacyjnych metod nabywania dóbr i usług, takich jak np. Uber, Taxify, czy różnego rodzaju dostępu do prasy w internecie. Sposób dystrybucji dóbr i usług cyfrowych oraz korzyści wynikające z modelu subskrypcyjnego powodują, że udział kart (red. kredytowych i debetowych) w rynku rośnie. Wierzymy, że powinniśmy mówić o problemie fraudów. Firmy, które działają w Polsce powinny o tym wiedzieć i coraz częściej o tym rozmawiać, również w obliczu tego, że coraz więcej polskich firm działających w sieci wychodzi na rynki zagraniczne.

Wspomniał Pan przykład Stanów Zjednoczonych. Dlaczego w tym państwie ten problem jest poważniejszy niż w Polsce? Czy wynika to tylko z popularności tego rozwiązania płatniczego?

Po pierwsze, jeśli chodzi o konsumpcję to Stany Zjednoczone są wielokrotnie większe niż Polska. Ponadto, Amerykanie wśród preferowanych metod płatności zdecydowanie częściej wskazują karty kredytowe. Jest to związane z uwarunkowaniami historycznymi i ewolucją samych systemów płatniczych, ale też ze świadomością i edukacją, z czym wiąże się wykorzystanie tego sposobu płatności. Niektórzy złośliwie mówią, że Amerykanie rodzą się z umiejętnością rozliczania karty kredytowej i zgłaszania chargebacków (tzw. obciążeń zwrotnych). W Polsce nie jest to dostatecznie spopularyzowane.

Polski system finansowy, przeskoczył bardzo szybko etap kart i skupił się na płatnościach elektronicznych, takich jak przelewy ekspresowe. Polska w tej kategorii zajmuje bardzo wysokie miejsce na świecie w różnego rodzaju rankingach czy konkursach finansowych, a banki detaliczne działające w Polsce zdobywają liczne nagrody. W związku z tym, że przeskoczyliśmy w pewnym sensie erę kart, to karta kredytowa jako nośnik nie zdążyła się tak spopularyzować jak w innych krajach.

Czy to może się zmienić? Czy obecnie obserwujemy popularyzację kart jako nośników czy jednak to bankowość elektroniczna będzie cały czas dominować?

Subskrypcje i usługi cyfrowe świadczone z poziomu aplikacji są coraz popularniejsze, a płacenie z poziomu karty płatniczej jest bardzo wygodną metodą korzystania z nich. Moim zdaniem karty kredytowe czy płatnicze nie staną się najpopularniejszym środkiem płatności w Polsce. Obserwując trendy wierzymy jednak, że wykorzystanie kart będzie dalej rosnąć. Duży nacisk na popularyzację płatności bezgotówkowych czy płatności kartami kładzie VISA i Mastercard czyli najwięksi gracze w tym ekosystemie.

W Polsce zdecydowanie popularniejsze są karty debetowe niż kredytowe. Czy one w takim samym stopniu są narażone na fraudy?

Profil ryzyka i mechanizmy są zgoła inne. Niemniej, to o czym się bardzo często mówi, to, że karta płatnicza jako nośnik płatności nie została stworzona do działania w Internecie. Teoretycznie jest ona przypisana do konkretnej osoby, ale tak na dobrą sprawę wystarczy, że ktoś przeczyta to co jest na niej napisane i może te dane wprowadzić do sieci. Rodzi to duże ryzyko dla właściciela danej karty. Ten nośnik wartości okazał się bardzo wygodny i dlatego tak szybko się spopularyzował w Internecie. Jeszcze raz jednak zaznaczę, nie został do tego zaprojektowany. Oczywiście wdrażane są dodatkowe zabezpieczenia, np. 3DS, ale wtedy pojawia się kwestia potencjału utraty konwersji sprzedażowej, ale to temat na zupełnie oddzielną dyskusję.

Regulacje i pierwsze dokumenty związane z wprowadzaniem kart kredytowych bardzo mocno eksponowały fakt, że na drugiej stronie był podpis w celu osobistej weryfikacji posiadacza karty. Intencją było, że ten nośnik płatności miał być pierwotnie wykorzystywany jeszcze przed erą Internetu. Wraz z pojawieniem się Internetu i e-commerce, który stał się niezwykle popularny. Z jednej strony oczywiście biznes korzysta z możliwości dawanych przez sieć, z drugiej strony pojawiła się ogromna rzesza użytkowników Internetu, dla których to olbrzymia szansa na wyłudzenia.

Jak taki potencjalny fraud wygląda w praktyce?

Fraud płatniczy to sytuacja, kiedy ktoś w nieprawowity sposób wchodzi w posiadanie danych karty kredytowej (lub płatniczej) i posługuje się nią, np. w Internecie. Przykładowo, wchodzi na stronę linii lotniczej, gdzie próbuje kupić bilet korzystając z nie swojej karty kredytowej. Zjawisko fraudów płatniczych jest ogromne, bo mówimy o 30 miliardach dolarów związanych ze stratami finansowymi na całym świecie. W 2017 roku straty wynosiły 27 miliardów, ale jak widać problem tylko się powiększa m.in. z uwagi na dynamiczny wzrost transakcyjności w sieci. Sam fakt, że e-commerce rośnie będzie powodował, że liczba fraudów będzie stale się zwiększać.

Pierwsze pytanie, która się pojawia to jak zdobyć dane kartowe? Zaczynając od koncepcyjnie najprostszych sposobów mamy do czynienia z fizycznym wejściem w posiadanie danej karty kredytowej i spisanie danych. Zdecydowanie powszechniejsze są jednak kradzieże w Internecie. Praktycznie codziennie czytamy o wyciekach z baz danych, gdzie te informacje są przechowywane nie zawsze w odpowiedni sposób. Oczywiście wdrażanych jest mnóstwo najlepszych praktyk, certyfikacji, systemów zabezpieczeń, w jaki sposób przechowywać dane. Wiemy jednak, że w rzeczywistości różnie bywa i wciąż wiele stron narażonych jest na ataki. Bez przerwy słyszymy o milionach danych (również kart kredytowych) wyciekających Internecie.

Czyli czasami jest tak, że użytkownik tej karty, pomimo że zachowa wszystkie standardy bezpieczeństwa, ze względu na to, że dane wypłyną ze strony trzeciej może być narażony na taki fraud?

Oczywiście takie sytuacje się zdarzają. Obecnie jednak coraz rzadziej mają one miejsce. Wynika to z presji, którą wywiera się na instytucjach, żeby wprowadziły odpowiednie zabezpieczenia. Należy jednak pamiętać, że fraudsterzy są bardzo kreatywni i szukają innych metod. Od lat mamy do

czynienia też z atakami, które są bardzo prozaiczne. W momencie, kiedy ktoś korzysta z karty to przykładowo w bankomacie może być ona zeskanowana i odczytana, o czym też wielokrotnie słyszeliśmy. Oczywiście najczęściej są to ataki o zdecydowanie mniejszej skali niż ta, o której przed chwilą mówiłem. Ciągle również taka fizyczna penetracja ma miejsce i tak na dobrą sprawę, dopóki będzie jakaś możliwość jej stosowania to będzie miała miejsce.

Fraudster ma dużą dostępność danych kartowych. Wystarczy wejść w zakamarki Dark Web i znaleźć strony, które oferują sprzedaż pakietów kart kredytowych. To co jest ciekawe i podkreśla skalę tego problemu, to fakt, że mamy do czynienia z zespołami stron, na których dostępne są najróżniejsze pakiety kart, np. klasyfikowane geograficznie. Mamy też karty obywateli konkretnego kraju czy karty określonej klasy np. Visa Gold. Oczywiście kluczową informacją z perspektywy fraudstera jest data wystąpienia wycieku, ponieważ z każdą minutą, godziną czy dniem szansa na to, że prawowity właściciel danej karty zda sobie sprawę z kradzieży, zwiększa się. W sposób naturalny wpływa to na wartość danych, która wraz z upływem czasu zmniejsza się. Część z tych stron idzie nawet krok dalej i udostępnia system do losowego sprawdzenia ważności tych kart, żeby ocenić jakość danej paczki kart, którą kupują. Często tego typu witryny dużo inwestują w funkcje "obsługi klienta". Możemy więc mówić o całej branży obsługi konsumenckiej w obszarze fraudów. Fraudster może sobie sprawdzić jakość danej paczki czy porównywać recenzję źródeł. Rynek podażowy jest ogromny. Mamy więc konkurencję walczącą o to, żeby dana oferta z danymi kart kredytowych była lepsza niż inne.

Sytuacja wygląda trochę podobnie do tego co mieliśmy w latach 90. i na początku XXI wieku oraz rywalizacji Max Butlera i Dark Marketu i wielkiej konkurencji między nimi. Czyli pomimo tego, że te podmioty zostały wykluczone z branży to pojawią się nowe i problem fraudów cały czas istnieje i nic się nie zmieniło?

Niewiele się zmieniło. Powstał dobrze zorganizowany rynek w oparciu o to, co z tymi danymi można zrobić i z perspektywy analizowania tego procederu, bariera wejścia w naszej ocenie jeszcze się obniżyła. Naszym celem jest podniesienie tej bariery. Oferowany przez nas system antyfraduowy jest zdecydowanie bardziej zaawansowany niż najlepsze z funkcjonujących wcześniej.

Zawsze mówiąc o fraudzie płatniczym w naszych głowach powstaje obrazek wyścigu zbrojeń. Z jednej strony mamy do czynienia z dużą inicjatywą z perspektywy oszustów. Oni podchodzą do tego kreatywnie, poszukując nowych sposób złamania zabezpieczeń, są coraz lepiej wykształceni, zorganizowani oraz finansowani. Z drugiej strony merczanci, czyli podmioty które sprzedają dobra i usługi oraz akceptują daną formę płatności, widząc, że skala zagrożenia jest coraz większa, podnoszą sposób zabezpieczeń, co powoduje, że fraudsterzy muszą być jeszcze lepiej zorganizowani, przygotowani i są zmuszeni korzystać z bardziej zaawansowanych narzędzi.

Fraudster w swojej działalności zwraca uwagę na trzy główne elementy:

- Po pierwsze chce ukryć swoją tożsamość, czyli zanonimizować swoje działania. Zależy mu na tym, żeby mógł prowadzić swój proceder w powtarzalny sposób, więc nie chce odkryć swojej tożsamości;
- Drugą istotną rzeczą jest charakterystyka fraudów. Mamy do czynienia z ciągłą innowacją i szukaniem nowych metod polegających m.in. na zmianie deklaratywnych parametrów urządzenia, połączenia sieciowego czy zmianie częstotliwości prób ataków. raudster cały czas musi szukać nowych metod. Główny (niestety wciąż dominujący na rynku) sposób zwalczania fraudów polega na tzw. systemie regułowym. Pojawia się jakiś atak, a analitycy pracując na ograniczonym zestawie danych historycznych tworzą reguły, które blokują próby transakcji o konkretnych znamionach. W skrócie, przygotowują regułę, która ma zabezpieczyć przed danym określonym atakiem. Gdy jest ona wdrożona to atak przeprowadzony w dokładnie taki sam

sposób zostanie udaremniony. Wymusza to od fraudsterów ciągłą konieczność modyfikowania sposobów działania przysłowiowe wchodzenie oknem, gdy nie mozna drzwiami.
- Trzeci wymiar jest związany z warstwą ekonomiczną - tak jak powiedziałem, wartość danej paczki kart kredytowych maleje z czasem. Jeżeli fraudster kupuje paczkę 1000 kart i próbuje zmaksymalizować zwrot z tej inwestycji, myśli on jak typowy przedsiębiorca. W związku z tym musi mieć metody, żeby w miarę automatyczny (lub półautomatyczny) sposób spróbować dokonać zakupu i wykorzystać te środki.

Obserwujemy fraudsterów, którzy próbują kombinować, w jaki sposób ukryć swoją tożsamość poprzez zmianę swojego zachowania lub jak automatyzować swoje działania. Była to dla nas jedna z głównych przesłanek, żeby zacząć budować narzędzia tzw. głębokiego profilowania. Trzymaliśmy się filozofii, aby zejść jak najniżej się da i żeby móc powiedzieć jakie dane jesteśmy w stanie zebrać o danym użytkowniku. Robimy to w sposób wyczerpujący całe spektrum źródeł danych o danym momencie zakupowym. Patrzymy bowiem jednocześnie na specyfikę urządzenia (od strony hardware i software), charakterystykę połączenia sieciowego (w jaki sposób dane urządzenie łączy się z witryną / aplikacją natywną) oraz cały wymiar behawioralny interakcji użytkownika z serwisem merchanta (tempo / takt pisania, wklejanie ze schowka, poruszanie myszą, popełnianie błędów w wpisywaniu na formularzu, zapisy akcelerometru / żyroskopu dla urządzeń mobilnych i wiele innych). W każdym z tych trzech wymiarów szukamy efektywnych danych, tzn. takich, które nie są nam deklarowane, a tych które pozwalają nam samodzielnie zweryfikować użytkowników. Tym samym szukamy niskopoziomowych przesłanek o tym, że ktoś anonimizuje / wirtualizuje / emuluje / automatyzuje dany kontekst zakupowy.

Mówił Pan, że wartość danych ze skradzionych kart kredytowych maleje z czasem. Jest to niewątpliwie związane z pewną świadomością użytkowników. Jak to wygląda w Polsce?

Mówiąc o malejącej wartości w czasie miałem na myśli, że jeżeli kupuję paczkę tysiąca kart teraz, to ta sama paczka jest aktualnie warta X. Ale już za 2 godziny będzie warta X-1, bo istnieje szansa, że jeden z tysiąca właścicieli tych kart zauważy, że coś jest nie tak.

Jednak, żeby zauważyć, że coś jest nie tak, to trzeba mieć świadomość, że w ogóle coś takiego może zaistnieć.

Jak najbardziej tak i dlatego przekaz jest faktycznie istotny. Jednym z celów naszego raportu „Bezpieczny handel w internecie” była analiza świadomości przedsiębiorców. Trzeba podkreślić, że odpowiedzialność związana z fraudami spoczywa na merczantach. Mamy bardzo silne instytucje kartowe takie jak VISA czy Mastercard, którym zależy na tym, żeby Kowalscy tego świata jak najwięcej korzystali z kart. Dlatego nie chcą ich winić lub obciążać odpowiedzialnością za kradzież karty. Doszło do tego, że merczant jest odpowiedzialny za proceder fraudowy. To on jest zobowiązany regulacyjnie do tego, żeby wprowadzić odpowiednie metody zabezpieczeń, czyli przeciwdziałać fraudom, a w sytuacji niepowodzenia pokrywa straty z własnej kieszeni. W sytuacji, kiedy moja karta zostanie skradziona jestem w stanie właśnie przez procedurę chargebacku odzyskać środki od swojego banku, który z kolei otrzyma zwrot od merchanta (nie bezpośrednio, często po drodze będą jeszcze pośrednicy płatności i bank merchanta). Tym kosztem na koniec dnia obciążony jest właśnie merczant.

Jak można wykorzystać technologię sztucznej inteligencji do walki z fraudami?

H. R.: Typowe schematy czy elementy działań fraudsterskich są inspiracją do naszych działań. Tak jak wspominałem, w chwili obecnej fraudy są zwalczane w sposób konwencjonalny: systemami regułowymi, które są statyczne i bazują na ograniczonej możliwościami manualnej analizy liczbie cech. Obserwując jak bardzo dynamicznie zmienia się sposób działania fraudersów, potrzebny okazał

się automatyczny mechanizm, która przygląda się ich działaniom poprzez wykorzystanie właściwych danych. Zwraca on uwagę na zachowanie i sposób konfiguracji sprzętu czy połączenia z inną stroną, żeby w adaptacyjny, automatyczny sposób uwrażliwiać nas na to co się dzieje.

Stwierdziliśmy, że poza wymiarem zbierania właściwych danych, czyli profilowaniem przydatne będzie uczenie maszynowe, tak żeby w procesie podejmowania decyzji wykorzystywać model czy zestaw modeli decyzyjnych, które wraz z przepływającym ruchem dostosowują się do obserwowanych wzorców. Wykorzystywanie uczenia maszynowego i odpowiednich klas modeli wrażliwych na poszczególne cechy i zagwarantowanie im odpowiedniej pętli zwrotnej w sposób automatyczny umożliwia bardziej precyzyjne i jednocześnie adaptacyjne rozumienie użytkowników naszych merchantów. To jest jedna z wielu dużych innowacji. Cieszymy się, że coraz większa liczba merczantów dostrzega, że jest to właściwszy, czyli bardziej skuteczny sposób na wykrywanie prób fraudów, bo lepiej odpowiada ich sposobowi działania. Jednocześnie system nie generuje tak wielu „fałszywych alarmów” jak system regułowy, więc merchant jest w stanie akceptować zdecydowanie więcej prób transakcji, maksymalizując swój potencjał. To jest właśnie Nethone Guard.