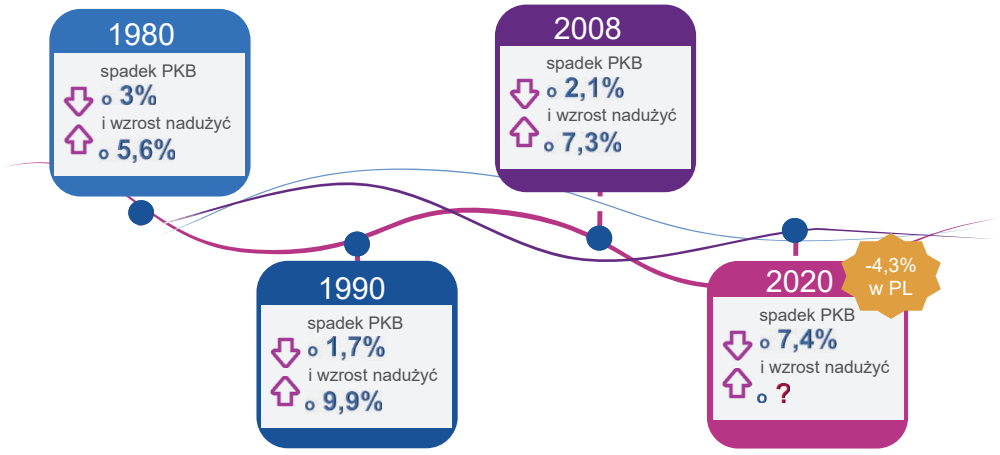
Cyberprzestępczość – poważny skutek uboczny kryzysu

Obecny kryzys na rynkach finansowych niesie wiele zagrożeń dla funkcjonowania globalnej gospodarki. Dotyka wszystkich bez wyjątku – korporacje, firmy prywatne, gospodarstwa domowe, osoby indywidualne. Jest przy tym wyjątkowy, nie spowodowały go żadne kataklizmy finansowe, a niewidoczny gołym okiem wirus – SARS-CoV-2, wywołujący chorobę COVID-19.

Iga SIKORSKA
Główny Analityk Experian CEE

Bartosz WÓJCICKI
dyrektor Biura Usług Antyfraudowych BIK SA

1. Spadek PKB a wzrost nadużyć



Źródło: szacunki Komisji Europejskiej, ec.europa.eu

W przypadku wcześniejszych kryzysów, choćby tego z lat 2008–2009, wszystko wydawało się jasne, zwłaszcza gdy dziś patrzymy na to z perspektywy 12 lat. Ówczesna sytuacja budziła strach, niepewność ludzi o swój majątek, dorobek życia oraz o pracę. Przyrównywano ją do największego kryzysu od Wielkiej Depresji lat 20. Podłożem tamtych zawirowań były czynniki ekonomiczne, zatem można było korzystać z doświadczeń przeszłości. Obecnie gospodarką wstrząsa pandemia koronawirusa i nie bardzo wiadomo, jak sobie z tym radzić. Mamy do czynienia ze zjawiskiem dużo bardziej nieznanym i wielowymiarowym, którego przebieg każdego dnia mocno daje się gospodarce we znaki. Świat stanął w obliczu nowego wyzwania – chronić trzeba ludzkie życie i zdrowie, a przy tym nie można zapominać o ekonomii.

Trudno dziś szacować straty, wynikające z gwałtownego zamrożenia niemal wszystkich aktywności gospodarczych. Jeszcze trudniej przewidzieć skalę recesji, na którą wpływ miał zarówno drastyczny spadek popytu (wzrost bezrobocia, ograniczenie dochodów gospodarstw domowych, możliwe zubożenie klasy średniej), jak i wyhamowanie podaży (przerwane ciągi dostaw oraz nierealizowane procesy produkcyjne).

Taktyka i scenariusze działań hakerów

Skutkiem ubocznym trwającej pandemii jest wzrost przestępczości gospodarczej. Na dodatek przestępcy niezwykle szybko adaptują się do aktualnych, mocno przecież zmiennych, uwarunkowań. Przodują tu zwłaszcza cybergangsterzy. Podobnie było w przypadku poprzednich kryzysów, z tym że tamte miały charakter czysto finansowy.

Widzimy dostosowywanie się działań przestępców do chaosu wywołanego zagrożeniem zdrowotnym i groźbą utraty stabilności ekonomicznej. Wykorzystując informacyjny szum, lęk przed zakażeniem czy utratą pracy, tworzą skuteczne kampanie socjotechniczne, celem których jest pozyskanie czyjejś tożsamości, dostępu do rachunków bankowych i kodów autoryzacyjnych, docelowo zaś wyłudzenie cudzych pieniędzy.

Z danych historycznych wynika, że poziom wyłudzeń zawsze był wyższy niż spadek PKB. Ten prognozowany dziś jest bardzo wysoki, jednak skali wzrostu przestępczości z wykorzystaniem skradzionych danych nikt nie potrafi przewidzieć.

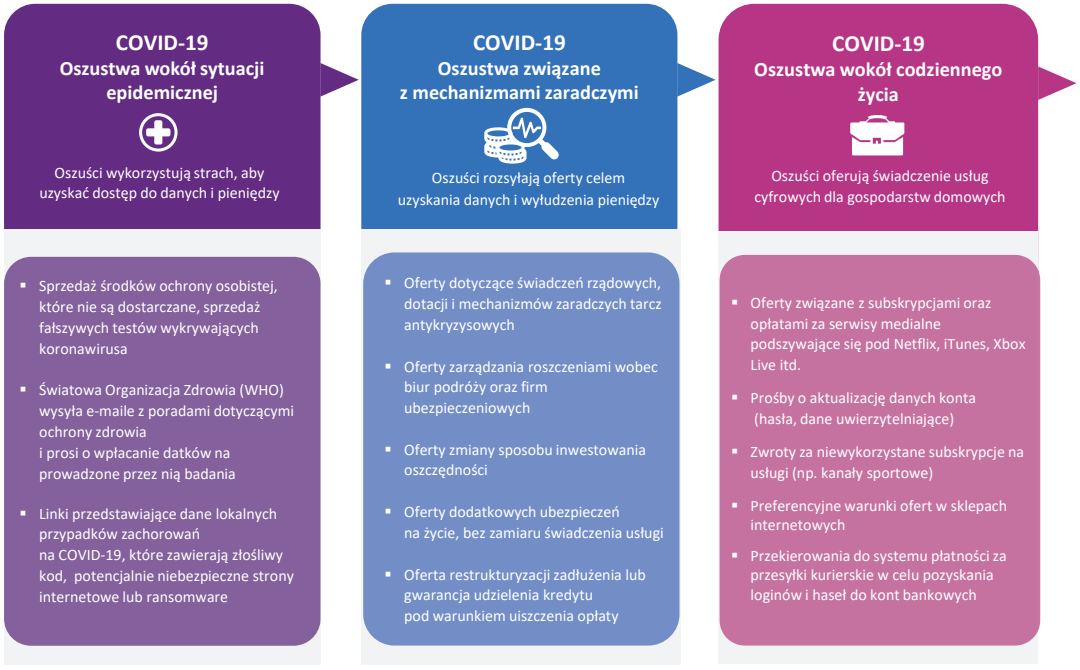
Nasilenie działań przestępczych w okresie pandemii koronawirusa potwierdza m.in. Międzynarodowa Organizacja Policji Kryminalnych. W swoim raporcie Interpol wskazuje m.in. na wzrost liczby zarejestrowanych domen ze słowami kluczowymi „COVID" lub „corona". To element socjotechniczny, cyberprzestępcy wykorzystują wzmożone zainteresowaniem pandemią do zbierania danych osób wchodzących na te strony. Co gorsza, to tylko jeden z nowych scenariuszy ich działań.

Eksperci firmy Experian podkreślają, że oszuści rzadko kiedy zaprzestają działalności, a niepewność związana z koronawirusem COVID-19 może potrwać nawet i 24 miesiące. Z dużym prawdopodobieństwem założyć zatem można, że kiedy wyjdziemy z obecnego kryzysu, przestępcy znowu zmodyfikują schematy oszustw, by czerpać zyski z nowej post-pandemicznej sytuacji.

Działaniom przestępczym sprzyja anonimowość, w dobie COVID-19 oszuści stali się mniej zauważalni, a użytkownicy internetu, pochłonięci nowymi wyzwaniami związanymi z organizacją życia prywatnego i zawodowego, mniej niż zwykle czujni.

Manipulacje, phishing i złośliwe oprogramowanie, to tylko niektóre z metod stosowanych przez hakerów dla wyłudzenia danych osobowych, środków finansowych oraz dostępu do kont i rachunków. Statystyki z krajów

2. Scenariusze działań przestępczych w czasie pandemii



Źródło: Experian

EMEA potwierdzają, że w okresie pandemii wyraźnie wzrósł wolumen handlu danymi w DarkNecie. Dobrze zorganizowane grupy przestępcze często wykorzystują osoby prywatne, działające jako tzw. słupy. Posługują się nimi przy ubieganiu się o kredyt (którego rzecz jasna i tak nie mają zamiaru spłacić) – zwłaszcza przy fałszowaniu danych poświadczających zdolność kredytową, czy też o nieprzysługujące im środki finansowe – dotacje lub zapomogi, świadczenia ubezpieczeniowe itp. Wzrosła także liczba tzw. mułów, czyli osób (nieświadomych, że biorą udział w przestępstwie), które pomagają w transferowaniu skradzionych środków, np. poza system bankowy. Z zagrożeniami w cyberprzestrzeni borykają się tak osoby fizyczne i małe firmy, jak i duże przedsiębiorstwa oraz korporacje. Oszustwa w sektorze finansowym mają wspólny mianownik – zawsze chodzi o wyłudzenie. Dla instytucji finansowej dodatkowym obciążeniem w takiej sytuacji jest możliwość utraty reputacji i zaufania klientów. To dlatego wiele z nich decyduje się na podjęcie działań zmierzających do wzmacniania procesów i narzędzi zarządzania ryzykiem wyłudzeń w działalności kredytowej. Chcą w ten sposób ograniczyć straty finansowe oraz skrócić czas niezbędny do rozpoznania próby wyłudzenia.

Wzrost roli systemowych narzędzi prewencyjnych

Przed stratami zabezpiecza Platforma Antyfraudowa BIK (PAF) – od początku jej działania sektor bankowy uniknął wyłudzeń sięgających 244,0 mln zł (stan na koniec maja 2020 r.).

Przygotowane przez Biuro Informacji Kredytowej rozwiązanie zabezpiecza uczestników rynku finansowego w Polsce (klientów i instytucje) przed utratą środków finansowych. Wykrywane są rozmaite przypadki, choćby fałszowanie danych czy podawanie informacji niespójnych, niezgodnych z prawdą. Oto kilka z nich:

- kradzież tożsamości – podawanie nieprawdziwych (zwłaszcza skradzionych) danych osobowych,
- podszywanie się pod osoby posiadające pozytywną historię kredytową,
- manipulowanie danymi na wniosku kredytowym, np. zawyżanie dochodów, zaniżanie wydatków itp.,
- podawanie nieprawdziwych, np. niespójnych, danych na wniosku kredytowym.

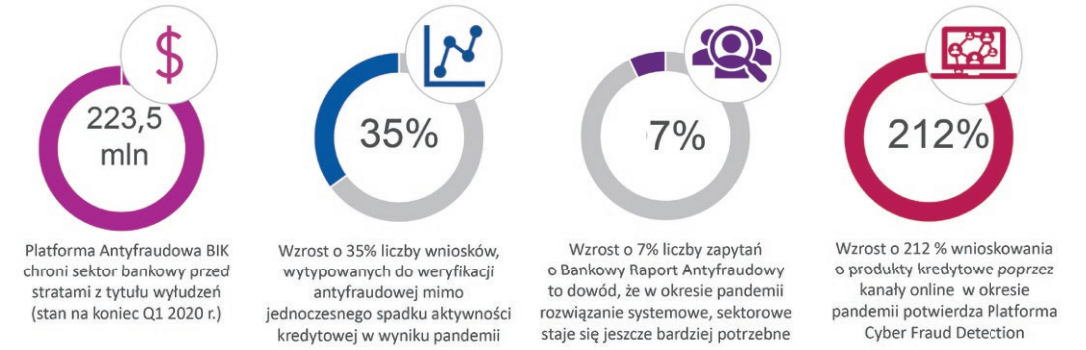
Podstawą technologiczną systemów antyfraudowych oferowanych przez BIK są rozwiązania „Hunter" i „FraudNet", opracowane przez partnerską firmę Experian, światowego lidera usług informatycznych, analitycznych i zarządzania danymi. To scentralizowane i zintegrowane rozwiązanie, które sprawdziło się na rynkach międzynarodowych, stosowane już m.in. w Wielkiej Brytanii, Włoszech, Francji, Hiszpanii czy Stanach Zjednoczonych.

Dzięki zastosowaniu nowoczesnych technologii proces ostrzegania o fraudach działa w czasie rzeczywistym – tylko w taki sposób można zapewnić skuteczną ochronę przed dynamicznie działającymi przestępcami ▸

3. Przebieg działań przestępczych

Źródło: Experian

4. Efekty działania Platformy Antyfraudowej BIK



Źródło: Biuro Informacji Kredytowej

bądź na bieżąco modyfikowanymi schematami oszustw. Gwarantuje to ponad 150 reguł i algorytmów systemu, który weryfikuje wnioski kredytowe i wyszukuje podejrzane powiązania i przejawy nadużyć. Zarówno raporty, jak i alerty antyfraudowe są natychmiast, w trybie online, wysyłane uczestnikom Platformy Antyfraudowej BIK.

Porównując dwa miesiące przedpandemiczne (styczeń i luty 2020 r.) do okresu pandemicznego, trwającego od marca br., zaobserwowano 35-procentowy wzrost liczby wniosków, które Platforma Antyfraudowa BIK wskazała do weryfikacji jako ewentualne próby nadużyć. Stało się tak mimo spadku aktywności kredytowej w sektorze bankowym.

Warto pamiętać, że spowolnienie gospodarcze związane z pandemią koronawirusa może powodować wzrost prób wyłudzeń. Niezmiernie ważne staje się zatem długofalowe działanie firm zapewniające wzmocnienie ochrony systemowej oraz współpraca w ramach sektora finansowego na rzecz przeciwdziałania niepożądanym zjawiskom.

Potwierdza to wynik kwerendy przeprowadzonej przez Experian w krajach EMEA. Wynika z niej, że intensywność działań przestępczych w internecie będzie się nasilała, dlatego inwestowanie w technologie i systemowe rozwiązania służące zapobieganiu oszustwom oraz ograniczaniu ryzyka tym bardziej są niezbędne – tak w dobie kryzysu, jak i w czasach post-pandemicznych.

5. Wnioski z kwerendy w krajach EMEA

Źródło: Experian

Globalizacja przestępczości – czego możemy się spodziewać?

Trudno przewidzieć jak długo potrwa obecny kryzys pandemiczny. Pewne jest tylko jedno – niezależnie od sposobów wychodzenia z recesji i odmrażania gospodarek działania cyberprzestępców nie wyhamują. Dlatego też w najbliższych miesiącach wiele uwagi poświęcać się będzie systemowym rozwiązaniom zapobiegającym cyberoszustwom, zwłaszcza tym zabezpieczającym konta, autoryzującym urządzenia i autentykację tożsamości klienta. Identyfikacja osób fizycznych oraz informacje o tym czy są one klientami, czy przestępcami, to część procesu weryfikacji tożsamości konsumenta, prowadzanego za pomocą cyfrowych danych biometrycznych, jak również rozwiązań analitycznych i uczenia maszynowego.

Przestępcy nigdy nie zaprzestaną prób kradzieży danych. Inwestycje w kompleksowe rozwiązania antyfraudowe to zatem jedyna metoda budowania bezpiecznego rynku i utrzymania zaufania klientów. To zaś przełoży się na przewagę konkurencyjną i zagwarantuje wyjście z kryzysu obronną ręką.

Cóż, musimy się pogodzić z faktem globalizacji przestępczości. Skutecznie przeciwdziałać oszustwom można jednak jedynie wtedy, gdy uczestnicy rynku finansowego zastosują holistyczne podejście do kwestii zabezpieczeń, autentykacji i szeroko rozumianego bezpiecznego korzystania z usług oferowanych w sieci.

Artykuł powstał przy współpracy BIK i Experian.