**Zagrożenia związane z bankowością online – trzy krótkie historie**

**Według danych Kaspersky Lab ponad 90% użytkowników internetu korzysta z bankowości online. Niestety - na popularności tego typu usług żerują cyberprzestępcy, którzy nieustannie wymyślają sposoby uzyskania dostępu do danych finansowych użytkowników. Eksperci z Kaspersky Lab przygotowali trzy wzięte z życia historie z zagrożeniami finansowymi w roli głównej oraz metody, dzięki którym użytkownicy uniknęliby szkód.**

**Podmieniony formularz na stronie bankowej**

Wyobraźmy sobie klienta banku, który podaje swoje dane na stronie banku i niedługo potem stwierdza, że z jego konta zniknęła spora suma pieniędzy – co więcej, transakcja ta została przeprowadzona przy użyciu jego danych uwierzytelniających. Okazuje się, że szkodliwy program zainstalowany w systemie użytkownika w locie podmienił pola wprowadzania danych i zebrane w ten sposób informacje wysłał cyberprzestępcom. Tego rodzaju funkcjonalność zawiera np. niesławny trojan bankowy ZeuS. W samym tylko 2013 r. produkty firmy Kaspersky Lab ochroniły przed tym konkretnym zagrożeniem około 1,3 miliona użytkowników.

W tej sytuacji przydatne byłoby oparte na serwerze rozwiązanie bezpieczeństwa działające w infrastrukturze IT banku. Technologia taka nie tylko analizuje transakcje i oznacza te podejrzane, ale również chroni użytkowników przed kilkoma rodzajami cyberataków, nawet jeśli na komputerze klienta nie ma wyspecjalizowanego oprogramowania. Możliwości takie posiada na przykład platforma [Kaspersky Fraud Prevention](http://www.kaspersky.pl/about.html?s=news_products&amp;amp;cat=5&amp;amp;newsid=2199), która w czasie rzeczywistym sprawdza, czy strona bankowości online, z której korzysta użytkownik, została zmodyfikowana przez szkodliwe oprogramowanie.

**Przypadkowy przelew, którego nie było**

W kolejnym hipotetycznym ataku użytkownik otrzymuje powiadomienie wysłane rzekomo przez jego bank, w którym zostaje poinformowany, że na jego konto zostały omyłkowo przelane pieniądze i muszą zostać zwrócone. Klient sprawdza swoje konto za pośrednictwem systemu bankowości online i stwierdza, że rzeczywiście znajdują się na nim „dodatkowe” środki, które następnie przelewa z powrotem do nadawcy, wykorzystując do tego swój kod jednorazowy (z SMS-a, karty-zdrapki lub tokena). Wkrótce jednak odkrywa, że tak naprawdę nie było żadnego omyłkowego przelewu i wysłał własne środki na konto cyberprzestępcy. Strona, którą widział, była fałszywa – została dynamicznie stworzona w przeglądarce przez trojana bankowego, który zainfekował komputer. Mógł to być SpyEye, który został wykorzystany do kradzieży milionów dolarów na całym świecie.

W momencie gdy użytkownik przeprowadza jakiekolwiek operacje bankowości online, wyspecjalizowane rozwiązanie powinno przełączyć przeglądarkę w bezpieczny tryb, blokując jakąkolwiek aktywność osób trzecich na stronie. Co więcej, powinno chronić przed szkodliwym oprogramowaniem, które rejestruje znaki wprowadzane z klawiatury i przechwytuje zrzuty ekranu. Platforma Kaspersky Fraud Prevention spełnia wszystkie te wymagania.

**Niechciany przelew z iPada**

Ostatnia historia dotyczy użytkownika, który korzysta z serwisu bankowości online na swoim iPadzie i po krótkim czasie zauważa, że z jego konta została przelana ogromna suma na konto bankowe na Wyspach Kanaryjskich.

Kradzież bankowych danych uwierzytelniających ułatwiają luki w zabezpieczeniach platform mobilnych. Na przykład, firma [FireEye](http://plblog.kaspersky.com/2014/03/05/szpiedzy-klawiatury-teraz-takze-na-iphonie/) wykryła lukę w systemie iOS, która pozwala aplikacji osób trzecich przechwytywać dane wprowadzane za pośrednictwem klawiatury wyświetlanej na ekranie. Powstaje także wiele szkodliwych programów dla systemu operacyjnego Android - na przykład, wykryty przez Kaspersky Lab trojan bankowy [Svpeng](http://securelist.pl/threats/7264%2Cewolucja_mobilnego_szkodliwego_oprogramowania_2013.html#svpeng), który wyświetla fałszywe okno przypominające legalną aplikację bankowości i prosi użytkownika o jego dane finansowe, a następnie wysyła je cyberprzestępcom.

Aby mobilne płatności online były bezpieczne, na smartfonie/tablecie powinna być zainstalowana skuteczna ochrona, która uniemożliwia cyberprzestępcom uzyskanie dostępu do informacji poufnych. Technologia Bezpieczna klawiatura firmy Kaspersky Lab za każdym razem losowo zmienia rozkład symboli na wirtualnej klawiaturze, przez co przechwytywanie danych wprowadzanych dotykiem staje się bezużyteczne. Bezpieczna klawiatura jest zawarta w Kaspersky Fraud Prevention SDK – zestawie komponentów służących do tworzenia bezpiecznych aplikacji mobilnych w ramach platformy Kaspersky Fraud Prevention.

Więcej informacji o platformie Kaspersky Fraud Prevention znajduje się na anglojęzycznej stronie <http://kaspersky.com/fraudprevention>.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie <http://www.kaspersky.pl/news>.