Ochrona konta bankowego za pomocą technologii „Bezpieczne pieniądze”

Wszystko sprowadza się do pieniędzy. Trudno wyobrazić sobie nowoczesne środowisko internetowe bez płatności online. Według prognoz IDC w roku 2012 będziemy świadkami ponad miliarda zakupów dokonanych online o łącznej wartości ponad 1,2 biliona dolarów. W dzisiejszych czasach ponad 60% użytkowników korzysta regularnie z internetu przeprowadzając transakcje bankowe i dokonując zakupów.

Niestety, wzrostowi ilości płatności dokonywanych online towarzyszy równie gwałtowna eskalacja oszustw internetowych. Istnieją różne metody pozbawiania ludzi gotówki, ale chyba najbardziej popularną techniką stosowaną przez oszustów jest przekonanie systemu płatności online, aby wierzył on, że oszust jest prawdziwym właścicielem konta. Kiedy ta akcja się powiedzie, cyberprzestępca będzie mógł bez przeszkód wykonywać operacje z użyciem funduszy swojej ofiary.

Jak oszuści zdobywają dane osobowe?

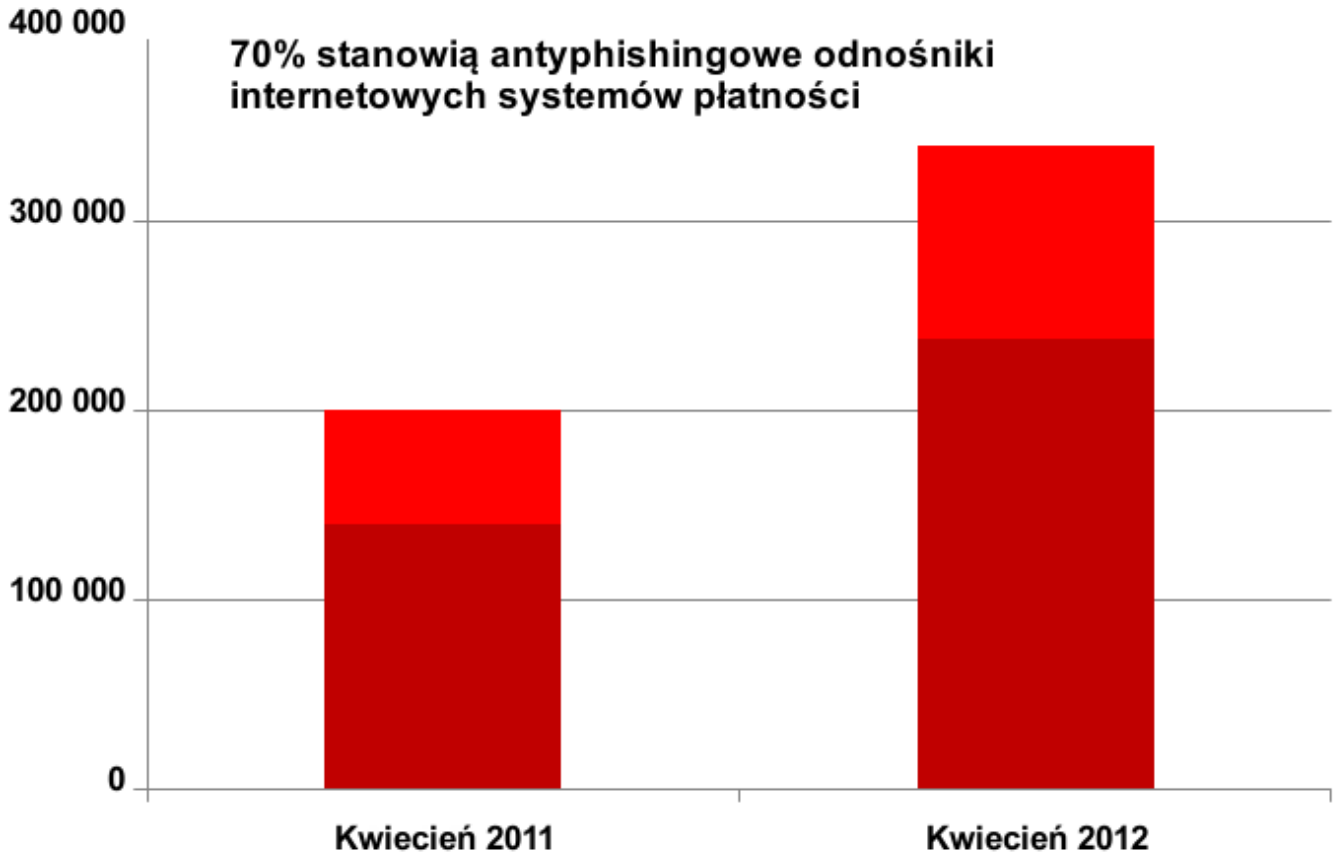
Oszust wprowadza dane osobowe ofiary (plus np. numer karty kredytowej) i prawidłowe hasło (może być to PIN, tajne hasło lub inna forma autoryzacji). To wystarczy, aby przekonać system płatności, że użytkownik jest prawdziwy.

Ale zastanówmy się w pierwszej kolejności, w jaki sposób cyberprzestępcy uzyskują te dane? Różne narzędzia i techniki są stosowane do tego celu, ale najpopularniejszą metodą jest użycie konia trojańskiego. Gdy komputer zostanie już zainfekowany trojanem, oszuści mogą ukraść prawie wszystkie informacje, które są im potrzebne. Robią to:

- poprzez wprowadzenie złośliwego kodu, odczyt pamięci lub inne operacje w przeglądarce internetowej w celu uzyskania loginu i hasła lub zastąpienia zawartości pól (kwota, konto bankowe itp.) transakcji bankowych;
- poprzez wyświetlanie na ekranie użytkownika fałszywych okien, które imitują prawdziwą stronę internetową, aby przechwycić prywatne dane;
- poprzez zbieranie zrzutów ekranu;
- poprzez rejestrację naciśnięć klawiszy klawiatury i kliknięć myszy;
- poprzez przechwytywanie ruchu internetowego za pomocą różnych technik, a wszystko to w celu gromadzenia danych wprowadzanych użytkownika.

W większości przypadków użytkownik nie zdaje sobie sprawy, że jego dane osobowe zostały naruszone, dopóki nie sprawdzi swojego wyciągu z konta bankowego. Niemniej jednak, płatności online

są częścią współczesnego życia. Według danych eBay, handel online stanowi 15% globalnego indeksu CAGR (rocznej stopy wzrostu). Natomiast ostatnie doniesienia firmy Harris Interactive wskazują, że ponad 60% wszystkich użytkowników internetu uważa kradzież danych bankowych za najpoważniejsze zagrożenie w sieci. Powstaje pytanie: gdzie użytkownicy mogą znaleźć niezawodną ochronę?



Powyższy rysunek ilustruje liczbę odnośników antyphishingowych dodanych do bazy danych Kaspersky Lab. 70% z nich stanowią odnośniki do phishingowych systemów płatniczych. Łatwo można zauważyć, że liczba phishingowych odnośników wykrytych przez Kaspersky Internet Security wzrosła o 100% w pierwszym kwartale 2012 r. w porównaniu z poprzednim kwartałem.

Tradycyjna ochrona antywirusowa

Tradycyjne programy antywirusowe oferują zestawy narzędzi, które znacznie zmniejszają ryzyko zarażenia trojanami. Technologie, takie jak: **Anti-Phishing**, **Ochrona WWW** i **Ochrona plików** przeciwdziałają wniknięciu szkodliwego kodu do systemu użytkownika. Jednak, oszuści stają się coraz bardziej pomysłowi i wprowadzają wiele modyfikacji złośliwego oprogramowania, aby było ono w stanie ominąć tradycyjne środki ochrony. Istotne jest, aby użytkownicy posiadali wszechstronne i wielopoziomowe zabezpieczenia. Każdy etap, na którym złośliwe oprogramowanie może przeniknąć do komputera użytkownika lub próbować wykonywać podejrzane działania, musi być ściśle kontrolowany.

Dodatkowo, wszystkie poziomy bezpieczeństwa muszą być zintegrowane ze sobą. Z tego właśnie powodu najnowszy produkt Kaspersky Internet Security, z nową technologią „Bezpieczne pieniądze", nie tylko łączy w sobie najlepsze tradycyjne narzędzia antywirusowe, ale oferuje również całą gamę nowych technologii, opracowanych specjalnie w celu ochrony komputera podczas transakcji i płatności online.

Technologia „Bezpieczne pieniądze”

Technologia „Bezpieczne pieniądze”, zaprojektowana przez Kaspersky Lab, posiada trzy główne aspekty:

Zaufane witryny internetowe

Użytkownik wchodzi na stronę internetową swojego banku lub systemu płatności online w jeden z następujących sposobów — poprzez pocztę e-mail, zakładkę przeglądarki internetowej, wpisując adres URL w polu adresowym przeglądarki lub wybierając witrynę z listy stron w oknie Kaspersky Internet Security. Lista stron jest wcześniej opracowywana przez użytkownika.

Przed załadowaniem strony, jej adres URL jest automatycznie sprawdzany w bazie danych zaufanych adresów URL prowadzonej przez Kaspersky Lab lub określonej przez użytkownika. Jeżeli zostanie odnaleziona zgodność, przeglądarka przełącza się w tryb **Bezpiecznych pieniędzy**, który zapewnia specjalną ochronę podczas wszelkich operacji online. Gwarantuje to, że użytkownik otwiera prawdziwą stronę systemu bankowego lub płatności online, a nie fałszywą stroną hostowaną przez oszustów.

Zaufane połączenie

Ważne jest również, aby sprawdzać autentyczność serwera, z którym użytkownik łączy się podczas korzystania z kanałów bankowości elektronicznej lub podczas płatności online. Usługa weryfikacji cyfrowego certyfikatu, wprowadzona przez Kaspersky Lab, może zostać wykorzystana do ustalenia ponad wszelką wątpliwość, że strona jest autentyczna. Jeżeli certyfikat nie może zostać potwierdzony, produkt Kaspersky Internet Security zablokuje dostęp do serwisu płatności online.

Zaufane środowisko

Przed każdą transakcją online technologia „Bezpieczne pieniądze” sprawdza bezpieczeństwo komputera, na którym transakcja ma zostać wykonana. Dotyczy to skanowania systemu operacyjnego w poszukiwaniu luk. Duża szybkość działania to wynik poszukiwania luk określonego typu, takich, które mogą zagrozić bezpieczeństwu korzystania z bankowości elektronicznej (na przykład: luk, które mogą być wykorzystywane do zwiększenia przywilejów). Obecność luki sprawia, że transakcje bankowe nie są bezpieczne, a użytkownik zostanie poproszony o ich usunięcie w trybie automatycznym przy użyciu usługi Windows Update. Po uruchomieniu przeglądarki w trybie „Bezpieczne pieniądze”, użytkownik musi upewnić się, że wszystkie dane osobowe są chronione przed kradzieżą lub modyfikacją przez oszustów. Kaspersky Internet Security realizuje to poprzez blokowanie wszelkich prób wprowadzenia złośliwego kodu za pośrednictwem przeglądarki, odczytu pamięci, wyświetlania fałszywych okien lub wykonywania zrzutów ekranu.

Jednocześnie, w celu ochrony przed przechwyceniem poufnych danych wejściowych, wprowadzanych z klawiatury sprzętowej, dostępne są dwie opcje:

- **Klawiatura wirtualna**, która jest wyświetlana na ekranie komputera użytkownika i sterowana za pomocą myszy.
- **Bezpieczne wprowadzanie danych z klawiatury**, nowa funkcja, która wykorzystuje specjalny sterownik do ochrony danych wprowadzanych z klawiatury sprzętowej.

Gdy transakcja płatnicza zostanie zrealizowana za pośrednictwem modułu „Bezpieczne pieniądze”, użytkownik zostanie automatycznie przekierowany do standardowego okna przeglądarki w celu dokończenia procesu lub kontynuowania zakupów w sklepie internetowym.

Korzyści

Technologia „Bezpieczne pieniądze” funkcjonuje dla dowolnej witryny wymagającej identyfikacji i łączy się z systemami płatności za pośrednictwem protokołu **https**. Co więcej, użytkownik może samodzielnie dodawać do listy zaufanych witryn strony banków, systemy płatności i sklepy internetowe.

Główne zalety technologii „Bezpieczne pieniądze” polegają na tym, że:

- mechanizmy ochronne działają automatycznie – w odpowiednim czasie i właściwym miejscu;
- zmodyfikowane okno przeglądarki pozwala użytkownikowi zobaczyć, że mechanizm ochronny jest aktywny i działa prawidłowo;
- technologia nie wymaga jakiejkolwiek wcześniejszej konfiguracji, aby aktywować mechanizm ochronny (lub tylko minimalnej konfiguracji i jednorazowego potwierdzenia użycia „Bezpiecznych pieniędzy” dla danej strony internetowej). Elastyczne ustawienia zawsze pozwalają, aby moduł „Bezpieczne pieniądze” był włączony lub wyłączony dla różnych stron, w zależności od ich zawartości;
- szybkie uruchamianie trybu „Bezpieczne pieniądze” jest również dostępne dla witryn internetowych, wybranych wcześniej przez użytkownika za pomocą specjalnego skrótu na pulpicie. Stwarza to bezpieczny punkt wejścia do tych obiektów.

Technologia „Bezpieczne pieniądze”, opracowana przez Kaspersky Lab, gwarantuje maksymalną ochronę bankowości elektronicznej i transakcji płatniczych online. Jest to realizowane za pomocą mechanizmów Zaufane witryny internetowe, Zaufane połączenie i Zaufane środowisko, które zapewniają szczegółowy poziom kontroli na wszystkich etapach procesu płatności online. Te innowacyjne technologie, zintegrowane w Kaspersky Internet Security 2013, gwarantują maksymalne bezpieczeństwo i ochronę nie tylko internetowych transakcji bankowych, ale i wszystkich innych działań w internecie.