KASPERSKY lab

Ochrona płatności online za pomocą technologii Bezpieczne pieniądze

Wszystko sprowadza się do pieniędzy

Trudno wyobrazić sobie nowoczesne środowisko internetowe bez możliwości płacenia online. Według analiz przeprowadzonych przez B2B Interational w 2013 r., 98% użytkowników regularnie dokonuje transakcji bankowych i robi zakupy za pośrednictwem internetu.

Niestety, wzrostowi ilości płatności dokonywanych online towarzyszy gwałtowny wzrost liczby oszustw internetowych. Istnieją różne metody pozbawiania ludzi gotówki. Najczęstszą techniką stosowaną przez atakujących jest „przekonanie" systemu płatności online, że oszust jest prawdziwym właścicielem konta. Jeżeli się to uda, cyberprzestępca będzie mógł wykonywać operacje finansowe z użyciem funduszy swojej ofiary.

W jaki sposób oszuści zdobywają dane osobowe?

Oszust wprowadza dane osobowe ofiary (lub numer karty kredytowej, dane logowania itp.) oraz hasło (PIN, szyfr lub hasło). To wystarczy, aby przekonać system płatności, że użytkownik jest prawdziwy.

W jaki sposób cyberprzestępcy uzyskują te dane? W tym celu stosowane są różne narzędzia i techniki, lecz najpopularniejszą metodą jest użycie konia trojańskiego. Gdy komputer zostanie już zainfekowany trojanem, oszuści mogą ukraść prawie wszystkie informacje, które są im potrzebne. Infekcja komputera może nastąpić:

- poprzez wprowadzenie szkodliwego kodu, odczyt pamięci lub inne operacje w przeglądarce internetowej w celu uzyskania loginu i hasła lub zastąpienia zawartości (kwota, konto bankowe itp.) transakcji bankowych,
- poprzez wyświetlanie na ekranie użytkownika fałszywych okien imitujących prawdziwą stronę internetową,
- poprzez robienie zrzutów ekranu,
- poprzez rejestrację naciśnięć klawiszy klawiatury i kliknięć myszy,
- poprzez przechwytywanie ruchu internetowego za pomocą różnych technik - 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.

Badania przeprowadzone przez B2B International wskazują, że 59% użytkowników internetu obawia się kradzieży danych bankowych online. Gdzie użytkownicy mogą znaleźć niezawodną ochronę?

Tradycyjne narzędzia chroniące przed szkodliwym oprogramowaniem

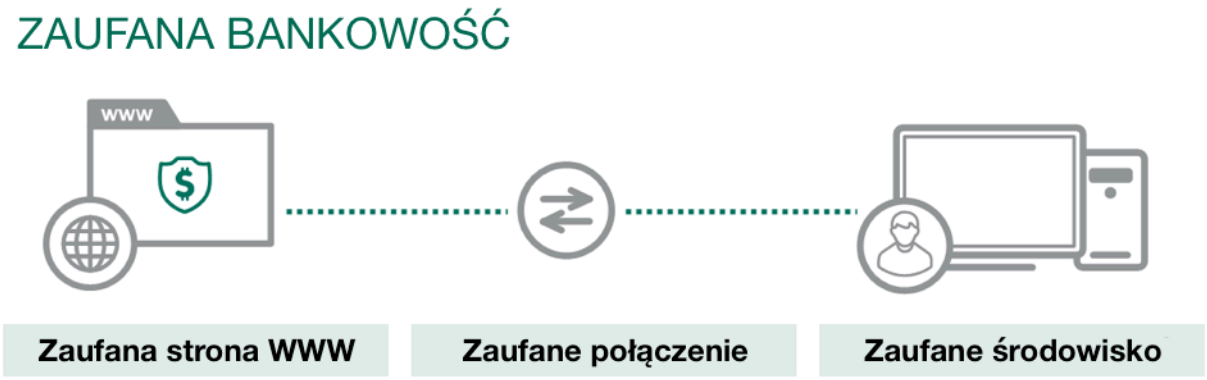
Tradycyjne programy antywirusowe oferują zestawy narzędzi, które znacznie zmniejszają ryzyko zarażenia trojanami. Technologie, takie jak: ochrona przed phishingiem, ochrona WWW i ochrona plików przeciwdziałają wniknięciu szkodliwego kodu do systemu użytkownika. Jednak, oszuści stają się coraz bardziej pomysłowi i wprowadzają wiele modyfikacji szkodliwego oprogramowania, aby było ono w stanie ominąć tradycyjne środki ochrony.

Istotne jest, aby użytkownicy posiadali wszechstronną i wielopoziomową ochronę. Każdy poziom, na którym szkodliwe oprogramowanie może przeniknąć do komputera użytkownika lub próbować dokonywać jakichś zmian, musi być dokładnie kontrolowany. Ponadto, wszystkie poziomy ochrony muszą być ze sobą ściśle zintegrowane.

Z tego właśnie powodu najnowsze produkty firmy Kaspersky Lab posiadają technologię Bezpieczne pieniądze, która nie tylko łączy w sobie najlepsze tradycyjne narzędzia antywirusowe, lecz także oferuje cały pakiet nowych technologii, opracowanych specjalnie w celu ochrony komputera podczas płatności i transakcji online.

Technologia Bezpieczne pieniądze

Technologia Bezpieczne pieniądze składa się z trzech głównych komponentów:



Schemat działania technologii Bezpieczne pieniądze

Zaufane witryny internetowe

Użytkownik uruchamia stronę banku lub systemu płatności online za pośrednictwem poczty elektronicznej, przeglądarki internetowej (wpisując adres URL) lub wybierając stronę z wcześniej opracowanej listy w oknie produktu firmy Kaspersky Lab.

Zanim strona zostanie załadowana, jej adres URL jest automatycznie sprawdzany w bazie danych zaufanych adresów opracowanej przez Kaspersky Lab lub innej, określonej przez użytkownika. Jeżeli adres figuruje w bazie, przeglądarka przełącza się w tryb Bezpieczne

pieniądze, który chroni przed wniknięciem podejrzanego kodu oraz zapewnia dodatkową ochronę podczas wszelkich operacji online. Jeżeli adres URL nie zostanie znaleziony w bazie, strona zostanie sprawdzona przez analizator heurystyczny, którego zadaniem jest wyszukiwanie oszustw phishingowych. Gwarantuje to, że użytkownik otwiera prawdziwą stronę systemu bankowego lub płatności online, a nie fałszywkę stworzoną przez oszustów.

Zaufane połączenia

Ważne jest również, aby sprawdzać autentyczność serwera, z którym użytkownik łączy się podczas korzystania z bankowości elektronicznej lub podczas dokonywania 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 zweryfikowany, produkt wykorzysta technologię Bezpieczne pieniądze, aby zablokować dostęp do serwisu płatności online. W celu przyśpieszenia tego procesu, każdorazowo podczas weryfikacji certyfikatu, technologia Bezpieczne pieniądze lokalnie zachowuje werdykt przez pewien czas. Jeżeli więc przeglądarka przełączy się na tryb Bezpieczne pieniądze podczas nawiązywania połączenia z daną stroną, to pierwszą czynnością będzie sprawdzenie, czy w pamięci podręcznej znajduje się już jakiś werdykt. W przypadku braku werdyktu, zapytanie kierowane jest do bazy danych Kaspersky Security Network.

Zaufane środowisko

Przed każdą transakcją online technologia Bezpieczne pieniądze sprawdza bezpieczeństwo komputera, na którym transakcja ma zostać wykonana. Polega to skanowaniu systemu operacyjnego w poszukiwaniu luk. Szybki proces skanowania to wynik poszukiwania luk określonego typu, czyli takich, które mogą zagrozić bezpieczeństwu korzystania z bankowości elektronicznej (na przykład luk, które mogą zostać wykorzystywane w celu zwiększenia przywilejów szkodliwego oprogramowania w systemie). Obecność luki sprawia, że transakcje bankowe nie są bezpieczne. W takiej sytuacji użytkownik zostaje poproszony o usunięcie luk.

Po uruchomieniu przeglądarki w trybie Bezpieczne pieniądze, użytkownik ma pewność, że wszystkie jego dane osobowe są chronione przed kradzieżą lub modyfikacją przez oszustów. Technologia Bezpieczne pieniądze daje taką gwarancję, ponieważ blokuje wszelkie próby wprowadzenia szkodliwego kodu za pośrednictwem przeglądarki, odczytu pamięci, wyświetlania fałszywych okien, oraz chroni wtyczki i profile przed nielegalną dezaktywacją lub wprowadzeniem zmian. Blokowane są również wszelkie próby wykonywania zrzutów ekranu, łącznie ze zrzutami całego obszaru pulpitu wykonywanymi przy użyciu funkcji API takich jak GDI, DirectX lub OpenGL.

W dodatku, podczas pracy przeglądarki w trybie Bezpieczne pieniądze niezaufane aplikacje nie mają dostępu do schowka, gdzie tymczasowo przechowywane są poufne dane podczas operacji kopiuj/wklej. Dlatego też żadne oprogramowanie innego producenta nie uzyska dostępu do pamięci podręcznej, co wyeliminuje ryzyko kradzieży haseł i loginów.

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

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

Kolejną istotną funkcją technologii Bezpieczne pieniądze jest dodatkowa ochrona przeglądarki, polegająca na ciągłym skanowaniu pola wprowadzania adresu w poszukiwaniu niespodziewanych, niezaufanych modułów, które potencjalnie mogłyby zawierać rootkity. Jeżeli tego rodzaju moduł zostanie wykryty, użytkownik jest o tym fakcie informowany w postaci ostrzeżenia, które pojawia się na nowo otwartej stronie.

Gdy transakcja płatnicza zostanie zrealizowana za pośrednictwem modułu Bezpieczne pieniądze, użytkownik jest automatycznie przekierowany do standardowego okna przeglądarki w celu dokończenia procesu lub kontynuowania zakupów w sklepie internetowym. Tryb Bezpieczne pieniądze jest w pełni kompatybilny ze wszystkimi najnowszymi wersjami najpopularniejszych przeglądarek: Internet Explorer, Apple Safari, Google Chrome i Mozilla Firefox.

Dostępność

Technologia Bezpieczne pieniądze zapewniająca bezpieczeństwo transakcji online jest dostępna w następujących produktach:

- Kaspersky Internet Security
- Kaspersky Internet Security for Mac
- Kaspersky Internet Security – multi-device
- Kaspersky Total Security – multi-device
- Kaspersky Small Office Security

Korzyści

Z technologii Bezpieczne pieniądze można korzystać dla dowolnej witryny wymagającej identyfikacji i łączącej się z systemami płatności za pośrednictwem protokołu HTTPS. Dodatkowo, użytkownik może samodzielnie poszerzać listę zaufanych witryn o strony banków, systemy płatności i sklepy internetowe.

Główne zalety technologii Bezpieczne pieniądze:

- mechanizmy ochronne działają automatycznie – w odpowiednim czasie i we właściwym miejscu;
- wizualne oznaczenie okna przeglądarki pozwala użytkownikowi zobaczyć, że mechanizm ochronny jest aktywny i działa prawidłowo;
- technologia Bezpieczne pieniądze 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, które wcześniej zostały wybrane przez użytkownika za pomocą specjalnego skrótu na pulpicie (systemy Windows). W ten sposób można utworzyć łatwo dostępny i bezpieczny punkt wejścia na określone strony;
- integracja z zaawansowanym rozwiązaniem antywirusowym zapewnia wielowarstwową ochronę przed większością technik wykorzystywanych w oszustwach internetowych.

Technologia Bezpieczne pieniądze opracowana przez Kaspersky Lab gwarantuje maksymalną ochronę bankowości elektronicznej i transakcji płatniczych online. Jest to możliwe dzięki działaniu komponentów takich jak zaufane strony WWW, zaufane połączenie i zaufane środowisko, które zapewniają głęboką kontrolę na wszystkich etapach procesu płatności online. Te innowacyjne technologie gwarantują maksymalne bezpieczeństwo i ochronę, obejmującą nie tylko internetowe transakcje bankowe, lecz także wszystkie inne działania w internecie.

Jakość potwierdzona przez ekspertów

Technologia Bezpieczne pieniądze zajęła czołowe miejsca w niezależnych testach:

- Matousec Online Payments Threats
- AV-TEST Innovation Award 2013
- MRG Effitas Online Banking/Browser Security 2013
- MRG Effitas Online Banking/Browser Security 2014