Czy transakcje finansowe online mogą być bezpieczne?

Kategoria: Aktualności
Opublikowano: piątek, 27, wrzesień 2013 00:00
Rafał Rudka

Wprowadzenie bankowości online doprowadziło do powstania nowej formy cyberprzestępczości - kradzieży informacji dotyczących płatności. Oszuści nieustannie opracowują nowe sposoby obchodzenia systemów ochrony danych finansowych. W jaki sposób ich szkodliwe oprogramowanie kradnie twoje pieniądze? Jak możemy się przed nim zabezpieczyć? Czy jest to w ogóle możliwe? Po przestudiowaniu mechanizmów stosowanych w atakach na systemy bankowości online eksperci z Kaspersky Lab udzielają odpowiedzi na te pytania.

Trojany bankowe to najbardziej niebezpieczny rodzaj wyspecjalizowanego szkodliwego oprogramowania. Po zainstalowaniu na komputerze ofiary trojan zwykle automatycznie gromadzi wszystkie dane dotyczące płatności, a czasem nawet przeprowadza transakcje finansowe w imieniu ofiary. Przestępcy wykorzystują trojany bankowe, które potrafią atakować klientów różnych banków i systemów płatniczych, jak również trojany, których celem są klienci konkretnego banku.

Przestępcy mogą wysyłać trojany w wiadomościach phishingowych, za pomocą których podstępnie nakłaniają użytkownika do kliknięcia odsyłacza lub otwarcia załączonego pliku, który okazuje się szkodliwy. Do masowej dystrybucji trojanów bankowych wykorzystywane są również aktywnie luki w zabezpieczeniach systemu Windows i w popularnych aplikacjach. Po ukradkowym wniknięciu do systemu szkodliwe programy umieszczają na zainfekowanym komputerze trojana. W celu przeprowadzania skuteczniejszych ataków przestępcy wykorzystują pakiety szkodliwych programów - zestawy potrafiące infekować za pośrednictwem luk w zabezpieczeniach wielu różnych aplikacji.

Po znalezieniu się na zainfekowanym komputerze trojany stosują następujące techniki:

- Przechwytywanie znaków wprowadzanych z klawiatury. Trojany identyfikują wciskane klawisze, co pozwala atakującym kraść dane dotyczące kont użytkowników bankowości online.
- Zrzuty ekranu formularza z wprowadzonymi danymi finansowymi.
- Obchodzenie klawiatury wirtualnej oraz przekazywanie cyberprzestępcom szczegółów dotyczących symboli klikanych na klawiaturze ekranowej.
- Zmienianie ustawień systemu, na skutek czego użytkownicy są przekierowywani na fałszywe strony internetowe, nawet jeśli adres legalnej strony został wpisany ręcznie.
- Wstrzykiwanie szkodliwego kodu uruchomionej przeglądarki - technika ta pozwala trojanom kontrolować transmisję danych między przeglądarką a serwerem.

Cyberprzestępcy mogą uzyskać dane dotyczące konta, które użytkownik wprowadza na stronie bankowej, jak również zmodyfikować zawartość strony systemu bankowości online o dodatkowe formularze, prosząc np. o numer karty kredytowej, nazwę właściciela, datę wygaśnięcia, kod CVV, tajne słowo itd. Tym samym osoby przeprowadzające ataki uzyskują dostęp do dodatkowych poufnych informacji.

Trojany bankowe potrafią również obejść dodatkowe warstwy ochrony, takie jak uwierzytelnianie dwuskładnikowe przy użyciu jednorazowych haseł (tzw. kody TAN). Jedna z metod stosowanych przez trojana ZeuS działa w następujący sposób: gdy ofiara wejdzie do systemu bankowości online i poda jednorazowe hasło, szkodliwe oprogramowanie wyświetli fałszywy komunikat informujący, że aktualna lista kodów TAN jest nieważna i zachęcający użytkownika do uzyskania nowej listy haseł. W tym celu ofiara musi podać w odpowiednim formularzu stworzonym przez trojana wszystkie dostępne kody TAN, które zostaną następnie zablokowane. W wyniku tego działania cyberprzestępcy zdobędą wszystkie kody ofiary i będą mogli od razu je wykorzystać do przelania pieniędzy na swoje konta. W samym tylko 2012 r. eksperci z Kaspersky Lab wykryli ponad 3,5 miliona prób ataków przy użyciu ZeuSa na 896 000

komputerów zlokalizowanych w różnych państwach.

Chociaż sytuacja może wydawać się beznadziejna, istnieją rozwiązania, które pozwalają na skuteczną ochronę transakcji finansowych online - należy do nich, np. technologia "Bezpieczne pieniądze" opracowana przez firmę Kaspersky Lab.

"Do skutecznego zabezpieczenia transakcji finansowych online niezbędne jest użycie kilku mechanizmów. Dane finansowe powinny być chronione przed trojanami bankowymi przy użyciu rozwiązań antywirusowych oraz specjalnych technologii, takich jak 'Bezpieczne pieniądze', chroniony tryb przeglądarki oraz dodatkowe zabezpieczenie klawiatury. Z kolei autentyczność systemu płatności lub bankowości online powinna być weryfikowana poprzez sprawdzenie jej certyfikatu cyfrowego i odsyłaczy" - powiedział Nikołaj Griebiennikow, dyrektor ds. technicznych w Kaspersky Lab.

Źródło: Kaspersky Lab Polska