**Brazylia: jak korzystać z bankomatów i uniknąć klonowania kart kredytowych**

**Jeżeli fani piłki nożnej, którzy wybierają się na tegoroczne mistrzostwa, nie zdecydowali jeszcze, w jaki sposób będą płacić za rachunki w Brazylii – gotówką czy kartą kredytową – najwyższa pora, by przyjrzeli się temu tematowi.**

Kaspersky Lab ostrzega, że w Brazylii działają jedni z najbardziej kreatywnych i aktywnych przestępców specjalizujących się w klonowaniu kart kredytowych. Co więcej, przestępcy ci lubią brać na celownik obcokrajowców, którzy nie wiedzą, jak chronić swoje karty podczas pobierania pieniędzy z bankomatów lub płacenia w restauracji. Eksperci z Kaspersky Lab przygotowali kilka praktycznych wskazówek, które pomogą zabezpieczyć się przed najpopularniejszymi atakami na bankomaty oraz urządzenia umożliwiające dokonywanie płatności (terminale POS) w Brazylii.

**Jak uniknąć klonowania kart kredytowych**

Urządzenia umożliwiające dokonywanie płatności (terminale POS) są powszechnie wykorzystywane w Brazylii – według Brazylijskiego Banku Centralnego karty kredytowe i debetowe odpowiadają za 70% wszystkich płatności dokonywanych w tym kraju. Karty chipowe wymagające kodu PIN są akceptowane przez większość firm, a nawet przez taksówkarzy.

Pomimo pojawiających się ostatnio doniesień o istnieniu luk w zabezpieczeniu tego protokołu, karty chipowe wymagające kodu PIN nadal są bezpieczniejsze i trudniejsze do sklonowania niż karty magnetyczne. Jeśli nie posiadasz jeszcze tego rodzaju karty, zapytaj swój bank, czy możesz ją dostać przed wyjazdem.

W Europie i Ameryce Północnej wiele osób podaje swoje karty personelowi w restauracjach i sklepach. W Brazylii taka praktyka może być niebezpieczna.

**Wskazówki**

Pod żadnym pozorem nie dawaj nikomu swojej karty – w ten sposób dasz oszustom możliwość jej sklonowania, a pokusa jest zbyt silna, żeby się jej oprzeć. Poproś personel, aby przyniósł terminal mobilny, w którym sam dokonasz płatności elektronicznej.

Uważaj na przypadkowe spotkania lub wydarzenia, które mogą sprawić, że na chwilę stracisz kartę z pola widzenia. Jeżeli tak się stanie, upewnij się, że to, co otrzymasz z powrotem, to rzeczywiście Twoja karta. W razie jakichkolwiek wątpliwości natychmiast poinformuj o sprawie swój bank.

**Szkodliwe oprogramowanie, którego celem są urządzenia POS oraz służące do wprowadzania kodów**

Do popularnych szkodliwych programów atakujących terminale POS należą Chupa Cabra oraz SPSniffer - rodzina szkodliwego oprogramowania, która posiada kilka wariantów stworzonych w Brazylii i występuje na wolności od 2010 r. Szkodniki te atakują niezwykle powszechne w Brazylii terminale POS oraz służące do wprowadzania kodów PIN. Urządzenia te są podłączone do komputera za pośrednictwem portu USB lub szeregowego w celu komunikowania się z oprogramowaniem EFT, umożliwiającym elektroniczny transfer środków pieniężnych. Trojan infekuje komputer i oczekuje na dane o karcie płatniczej przesyłane przez te porty.

Kod PIN zostaje zaszyfrowany natychmiast po wprowadzeniu go na terminalu - zwykle przy użyciu potrójnego algorytmu DES. Jednak w przestarzałych urządzeniach nie są szyfrowane takie dane jak numer karty kredytowej, data wygaśnięcia, kod usługi i kod CVV oraz publiczne dane z kart chipowych. Są one wysyłane za pomocą czystego tekstu do komputera PC za pośrednictwem portów USB lub szeregowych. Przechwycenie tych danych wystarczy do sklonowania karty kredytowej.

**Wskazówki**

Sprawdzaj wyciągi z transakcji przy użyciu karty kredytowej i natychmiast powiadom swój bank, jeżeli zauważysz coś podejrzanego.

W miarę możliwości staraj się płacić za pomocą bezprzewodowych terminali POS – są trochę bezpieczniejsze niż te starsze, podłączone do portów szeregowych lub USB.

**Korzystanie z bankomatów w Brazylii**

Według Banku Światowego Brazylia posiada 118 bankomatów na 100 tysięcy dorosłych mieszkańców i zajmuje pod tym względem dziewiąte miejsce na świecie. To daje oszustom wiele możliwości zainstalowania urządzeń do przechwytywania i przechowywania danych dotyczących kart kredytowych (ang. skimmer), znanych również jako urządzenia „Chupa Cabra”.

**Wskazówki**

Podczas wprowadzania kodu PIN zasłoń ręką klawiaturę – to doskonały sposób, aby przechytrzyć większość skimmerów, którzy zwykle posługują się ukrytymi kamerami.

Jeżeli zauważysz coś podejrzanego, poinformuj o tym bank lub właściciela maszyny i spróbuj wypłacić pieniądze w innym miejscu.

„Zachowaj ostrożność podczas korzystania z bankomatów lub płacenia przy użyciu karty kredytowej. Nie zapominaj, że brazylijscy cyberprzestępcy stosują swoje szkodliwe sztuczki przez cały czas. Nawet w biały dzień, ubrani w klapki i strój plażowy, mogą instalować skimmery w zatłoczonym banku. Pamiętaj również, że będzie o wiele bezpieczniej, jeśli transakcje, których dokonujesz, zostaną przeprowadzone na Twoich oczach. W razie jakichkolwiek wątpliwości natychmiast poinformuj o incydencie swój bank” – radzi **Fabio Assolini**, starszy badacz bezpieczeństwa z Globalnego Zespołu ds. Badań i Analiz (GReAT), Kaspersky Lab.

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>.