http://46.248.165.254/dla-konsumentow/bezpieczny-bank/aktualnosci

Aktualności

ZŁOŚLIWE OPROGRAMOWANIE NA SMARTFONY Z SYSTEMEM OPERACYJNYM ANDROID

Komunikat z dnia 12 kwietnia 2016 r.

Szanowni Państwo,

Rada Bankowości Elektronicznej Związku Banków Polskich ostrzega przed nasilającymi się atakami na użytkowników smartfonów z systemem Android. W ostatnim okresie odnotowano nowe kampanie rozsyłania wiadomości SMS mających na celu infekcję smartfona złośliwym oprogramowaniem.

Osoba, która odebrała SMS i kliknęła na link faktycznie instaluje złośliwe oprogramowanie.

Po kliknięciu na link przesłany w wiadomości SMS, otwierana jest strona prezentująca instrukcję instalacji oprogramowania (w szczególności, wykonania w telefonie zmiany opcji umożliwiającej instalację z niezaufanych źródeł). W celu wzbudzenia większego zaufania i uwiarygodnienia oprogramowania, cyberprzestępcy prezentują również producenta smartfona i wyświetlają odpowiednie logo.

Zadaniem trojana zainstalowanego w systemie Android jest jego uaktywnienie w momencie korzystania przez użytkownika telefonu z aplikacji bankowości mobilnej i wygenerowanie specjalnego okna z prośbą o podanie loginu i hasła. Lista aplikacji, na które reaguje trojan została zawarta w jego pliku konfiguracyjnym i obecnie dotyczy 68 aplikacji różnych instytucji finansowych, w tym polskich banków .

Poniżej przykłady działania trojana.

Wyżej widoczne okna pojawiają się nad uruchomioną aplikacją, powodując jej przysłonięcie. Powoduje to, wrażenie, iż to aplikacja bankowa żąda informacji. Nieświadomy użytkownik może odnieść wrażenie, iż komunikat jest efektem działania oryginalnego oprogramowania. Złośliwe oprogramowanie oprócz pozyskiwania danych posiada również funkcjonalność odczytywania i wysyłania SMS, w tym również bankowych kodów SMS. Trojan wyłudza również numery kart płatniczych poprzez generowanie w odpowiednim czasie specjalnych komunikatów proszących o podanie wrażliwych informacji.

Inną funkcją jest również wykradanie danych personalnych, w tym zdjęć dokumentów tożsamości, jak również zdjęcia użytkownika wraz z dokumentem tożsamości trzymanym przy twarzy.

Prawdopodobnie dane mogą być wykorzystywane do otwierania różnego rodzaju dostępów do serwisów z wykorzystaniem skradzionej tożsamości.

Rada Bankowości Elektronicznej Związku Banków Polskich przestrzega użytkowników smartfonów z systemów Android przed pobieraniem i uruchamianiem aplikacji pochodzących z niezaufanego źródła.

Należy mieć na uwadze, że treści SMS pochodzących od nieznanych nadawców mogą nakłaniać do podejmowania określonych działań takich jak klikanie na linki w nich zawarte, a otwarcie odnośnika prowadzącego do niebezpiecznej treści może skutkować zainfekowaniem smartfona i w konsekwencji utratą nad nim kontroli.

Użytkowników bankowych aplikacji mobilnych uczula się na wszystkie nietypowe komunikaty i prośby generowane w telefonie komórkowym. W przypadku jakichkolwiek wątpliwości należy skontaktować się z infolinią danego banku.

Rada Bankowości Elektronicznej

Związek Banków Polskich