Cyberdefence 24

aut. Szymon Palczewski 14.12.2018

ZŁOŚLIWA APLIKACJA NA ANDROIDA. KRADZIEŻ DANYCH I PIENIĘDZY

W jednym z alternatywnych sklepów dla Google Play pojawiła się nowa aplikacja na urządzenia z system Android, która umożliwia kradzież danych logowania m.in. do WhatsApp oraz Skype, a także informacji dotyczących karty płatniczej lub konta PayPal.

Optimization Android to aplikacja w teorii służąca jako narzędzie do optymalizacji wydajności baterii w urządzeniach mobilnych. Zawiera w sobie mechanizmy umożliwiające obejście dwuskładnikowego uwierzytelniania wielu usług.

Aplikacja odpowiada za kradzież danych wrażliwych dotyczących kart kredytowych, a także kont na WhatsApp'ie, Skype'ie czy Gmail'u. Co więcej, umożliwia ona cyberprzestępcom dokonanie przelewu w postaci tysiąca euro na specjalnie utworzone do tego celu konto. Optimization Android jest narzędziem działania hakerów, a więc w praktyce nie ma nic wspólnego z optymalizacją funkcjonowania akumulatorów w urządzeniach mobilnych.

Aplikacja posiada dwie funkcje w pełni kontrolowane przez cyberprzestępców. Jedną z nich jest bezpośrednia kradzież tysiąca euro z konta PayPal użytkownika. Sposób działania hakerów opiera się na zachęceniu ofiary do pobrania aplikacji. Następnie proponowane jest „włączenie statystyk". W przypadku wyrażenia zgody, użytkownik zostaje odesłany do witryny PayPal, gdzie pojawia się informacja o konieczności wpisania danych w celu weryfikacji. Po uzupełnieniu wymaganych treści poszkodowany otrzymuje kod autoryzacyjny, a w ciągu dalszych 5 sekund z jego konta znika tysiąc euro.

Drugą funkcją kontrolowaną przez hakerów dotyczy wyłudzania od użytkowników informacji na temat kart płatniczych, a także danych logowania do wielu innych aplikacji, m.in. Skype, Gmail, WhatsApp czy Viber. W trakcie korzystania z urządzenia mobilnego Optimization Android uruchamia specjalną nakładkę ekranową, która całkowicie blokuje możliwość posługiwania się aparatem. Wizualnie przypomina okno logowania danej aplikacji. Jedyną różnicą jest dodatkowe pole wymagające podania numeru karty płatniczej.

Specjalistą, który wykrył szkodliwą aplikację jest Lukas Stefanko z firmy ESET. Według jego przypuszczeń hakerzy za pomocą Optimization Android mogli zdobyć dane logowania do poczty Gmail i w ten sposób usuwać wszelkie powiadomienia na temat transakcji PayPal, zanim odczytał je sam właściciel.

Wszyscy użytkownicy, którzy zainstalowali na swoich urządzeniach aplikację Optimization Android powinni niezwłocznie sprawdzić stan konta PayPal, historię transakcji kartą oraz dokonać zmiany haseł do komunikatorów, poczty oraz systemów swojego banku. W przypadku odkrycia naruszenia incydent można zgłosić bezpośrednio PayPal'owi za pośrednictwem specjalistycznego centrum pomocy. Samą aplikację należy usunąć po włączeniu trybu awaryjnego Androida.