FAŁSZYWE EKRANY LOGOWANIA. OSTRZEŻENIE DLA KLIENTÓW BANKÓW

Wykryta luka umożliwia podszywanie się pod ekran logowania i wykradanie informacji bankowych. Ofiarą złośliwego oprogramowania wykorzystującego błąd mogli paść klienci ponad 60 instytucji finansowych - podało w poniedziałek BBC.

Błąd umożliwiający wprowadzenia fałszywego ekranu logowania do certyfikowanych aplikacji bankowych na system Android wykryła firma cyberbezpieczeństwa Promon.

"Programy brały na cel użytkowników z różnych krajów i z sukcesem kradły im pieniądze" - przekazał przedstawiciel norweskiej firmy Promon Tom Hansen, który jako pierwszy znalazł wrażliwość bezpieczeństwa. "Nigdy nie widzieliśmy podobnego zachowania upodabniającego" - dodał.

"W miarę rozrastania się Androida trudniejsze staje się również śledzenie wszystkich interakcji różnorodnych części systemu. (Strandhogg) wygląda na lukę, która powstała przez nadmierną złożoność" - ocenił ekspert.

Promon we współpracy z amerykańską firmą bezpieczeństwa Lookout zeskanował aplikacje dostępne na oficjalnej platformie z oprogramowaniem Play Store, które mogły zostać dotknięte przez techniki ataku wykorzysujące podatność Strandhogg. W wyniku badanie wykryto 60 różnych instytucji finansowych, których programy były zagrożone. Cyberprzestępcy do oszustw najczęściej wykorzystywać mieli bankbota - szeroko rozpowszechniony złośliwy program kradnący pieniądze.

Za Androida i platformę Play Store, na której rozpowszechnianie były zainfekowane aplikacje, odpowiada firma Google. Spółka wskazała, że podjęła już działania w celu wyeliminowania błędu w kodzie systemu.

"Doceniamy pracę ekspertów bezpieczeństwa i wstrzymaliśmy dystrybucję aplikacji, które nam wskazali" - podał w oświadczeniu koncern z Mountain View.

Hansen ostrzegł, że błędem w kodzie umożliwiającym tzw. spoofing zagrożonych może być znacznie więcej aplikacji. Ekspert wskazał, że nadal możliwe jest tworzenie fałszywych ekranów w programach na Androida 10 i wcześniejsze wersje systemu.

Czytaj też: Bezpieczne wyprzedaże czyli jak nie dać się okraść...z własnych danych i pieniędzy