Bądźmy czujni... coraz więcej niebezpiecznych aplikacji podszywa się pod popularne programy

Kategoria: Styl życia
Opublikowano: czwartek, 01, luty 2018 10:10
Dawid Kulpa
Odsłony: 1273

Pobierając aplikację trzeba uważać. Szkodliwe aplikacje podszywają się pod popularne programy. By zwieść użytkowników, twórcy fałszywych aplikacji wykorzystują podobieństwo ikon i nazw.

Wiele fałszywych aplikacji jest dostępnych przez krótki czas, od kilku dni do kilku tygodni. Mimo to niektóre z nich potrafią osiągać nawet do kilkuset tysięcy pobrań. Sztuczką stosowaną przez nieuczciwych twórców jest generowanie bądź kupowanie pozytywnych ocen aplikacji. Wysoka ocena podnosi wiarygodność aplikacji w oczach potencjalnego użytkownika.

Jak działają fałszywe aplikacje?

Analitycy z firmy Fortinet sprawdzili trzy aplikacje podszywające się pod znany komunikator.

Pierwsza z nich miała przeźroczystą ikonę, przez co nie można było jej zobaczyć na liście aplikacji w smartfonie. Użytkownik mógł nawet nie mieć świadomości, że jest ona zainstalowana na jego urządzeniu. Program pozoruje pobieranie aktualizacji dla oficjalnej aplikacji. Aplikacja wykorzystuje bibliotekę o nazwie startapp.android.publish, by wyświetlać reklamy przy zmianie ekranu i ostatecznie nie pobiera żadnych danych. Twórca aplikacji najwyraźniej czerpie korzyści za każdą emisję reklamy.

Druga analizowana aplikacja działała w podobny sposób, wyświetlając natrętne reklamy oraz ekrany z linkami, za którymi mogło się kryć dużo groźniejsze oprogramowanie – np. potajemnie wykonujące zrzuty ekranu czy przechwytujące komunikację SMS.

Trzeci program różnił się od poprzednich tym, że rzeczywiście pobierał dane do pamięci urządzenia. Była to zmodyfikowana wersja komunikatora oferująca, przynajmniej według opisu, dodatkowe funkcje niedostępne w oficjalnej wersji aplikacji. Użytkownik otrzymywał nawet instrukcję instalacji aplikacji. Sama aplikacja nie wykazywała groźnego działania, ale również wyświetlała reklamy.

Na co uważać przy instalowaniu aplikacji?

Użytkownicy systemu Android muszą zachować czujność podczas pobierania aplikacji nawet z oficjalnych źródeł. Należy sprawdzać, czy nazwa i ikona aplikacji są dokładnie takie, jak należy. Nawet najmniejsze odstępstwo od oficjalnej identyfikacji powinno wzbudzić podejrzenie.

Warto zwrócić uwagę na liczbę instalacji oraz przejrzeć więcej niż kilka opinii użytkowników – nawet jeżeli większość ocen fałszywej aplikacji jest wygenerowanych, to często ci, którzy dali się nabrać, ostrzegają przed tym pozostałych.

- *Po zainstalowaniu aplikacji trzeba zawsze przyjrzeć się wymaganym przez nią uprawnieniom oraz być szczególnie ostrożnym wobec programów chcących pobierać pliki z nieznanych źródeł* – radzi Robert Dąbrowski, szef zespołu inżynierów Fortinet.

Źródło: newsrm.tv /wypowiedź: Robert Dąbrowski, szef zespołu inżynierów Fortinet.