TROJAN UKRYTY W APLIKACJACH DLA HUAWEI

Hakerzy za pomocą sklepu z aplikacjami dedykowanymi dla urządzeń Huawei rozpowszechniali złośliwe oprogramowanie, które było ukryte w legalnych produktach. Wirus pozwalał na wykupywanie subskrypcji wersji premium określonych usług bez zgody użytkowników oraz przechwytywanie wiadomości SMS. Trojan został zainstalowany przez ponad pół miliona użytkowników.

Specjaliści firmy Dr. Web, zajmujący się oprogramowaniem antywirusowym, wykryli nowy wariant trojanów Android.Joker w AppGallery, oficjalnym sklepie z aplikacjami na urządzenia Huawei. Wirusy umożliwiają hakerom zdalne wykonywanie poleceń, a w ramach tej konkretnej kampanii pozwalają na subskrybowanie określonych usług premium bez wiedzy i zgody użytkowników.

Jak poinformowała firma w oficjalnym oświadczeniu, jej specjalistom udało się ustalić, że do wirtualnego sklepu dedykowanego produktom chińskiego giganta trafiło 10 zmodyfikowanych trojanów, które zostały zainstalowane na ponad 538 tys. urządzeniach.

Eksperci przypominają, że Android.Joker to względnie stara odmiana złośliwego oprogramowania, która pierwszy raz została wykryta w 2019 roku. Do tej pory było ono powszechnie wykorzystywane przez hakerów podczas kampanii z wykorzystaniem sklepu Google Play. „Atakujący najwyraźniej postanowili rozszerzyć skalę prowadzonych działań i uderzyć w alternatywne platformy dla czołowych graczy branży urządzeń mobilnych” – czytamy na stronie Dr. Web.

Specjaliści ustalili, że wirusy były rozpowszechniane pod przykrywką legalnych i nieszkodliwych aplikacji, które po uruchomieniu pozornie działały zgodnie z oczekiwaniami, nie wzbudzając żadnych wątpliwości użytkowników. W ten sposób hakerzy realizowali swoje zadania przez dłuższy czas, unikając wykrycia. Trojany były ukrywane w m.in. komunikatorach internetowych, grach czy aplikacjach do aparatu.

„Android.Joker to zagrożenie wieloskładnikowe, które jest w stanie zdalnie wykonywać zadania w zależności od tego, czego chcą hakerzy” – tłumaczą specjaliści Dr. Web. W najnowszej kampanii wirusy są wykorzystywane przede wszystkim do subskrybowania wersji premium określonych usług, co odbywa się bez wiedzy i zgody użytkownika. Ponadto, umożliwiają przechwytywanie przychodzących wiadomości SMS.

> *Huawei przeprowadzi dodatkowe dochodzenie, aby zminimalizować ryzyko pojawienia się tego typu szkodliwych aplikacji w przyszłości.*
>
> Rzecznik prasowy AppGallery

W związku z odkryciem firmy Dr. Web rzecznik prasowy AppGallery poinformował, że Huawei podjął działania mające na celu usunięcie złośliwego oprogramowania ze sklepu, aby w ten sposób chronić użytkowników.

Czytaj też: Szukasz Telegrama w wersji desktopowej? Uważaj w co klikasz