MobiDash - trojan podszywa się pod popularną aplikację

ID artykułu: 58049 / 2264

URL: http://www.publikuj.org/58049

Aplikacja FaceApp, pozwalająca m.in. na postarzanie twarzy, przeżywa swoją drugą młodość, a wygenerowane nią zdjęcia szturmem zdobywają profile użytkowników na portalach społecznościowych.Tak duża popularność aplikacji nie mogła umknąć uwadze cyberprzestępców. Badacze z firmy Kaspersky wykryli fałszywe narzędzie podszywające się pod FaceApp, które w rzeczywistości infekuje urządzenia mobilne z Androidem trojanem MobiDash.Popularność aplikacji FaceApp nie jest dużym zaskoczeniem użytkownicy instalują ją z ciekawości, widząc efekty jej działania na profilach społecznościowych swoich znajomych i celebrytów. Niestety chęć szybkiego skorzystania z popularnego narzędzia często usypia czujność użytkowników w kontekście uprawnień nadawanych instalowanym aplikacjom. Z badań firmy Kaspersky wynika, że 63% użytkowników nie czyta umów licencyjnych, a niemal połowa (43%) bez zastanowienia wyraża zgodę na wszystkie uprawnienia podczas instalowania nowych aplikacji. Warto dodać, że dokładne zapoznanie się z umową licencyjną jest szczególnie ważne w przypadku aplikacji, które wysyłają nasze dane na serwery producenta. Zanim zdecydujemy się na korzystanie z takiego narzędzia, powinniśmy zrozumieć, co dzieje się z naszymi danymi, a także kto i w jaki sposób je przetwarza.

O ile w samej chęci wypróbowania nowej popularnej aplikacji nie ma nic złego, nie należy robić tego bez zastanowienia na to właśnie liczą cyberprzestępcy, tacy jak ci stojący za nowym mobilnym szkodliwym programem MobiDash podszywającym się aplikację FaceApp.

Po pobraniu fałszywej aplikacji z nieoficjalnego źródła i zainstalowaniu jej na smartfonie użytkownik widzi komunikat o błędzie. Wyświetlane informacje sugerują, że pobrana aplikacja została odinstalowana. Komunikat ten jest sfałszowany w rzeczywistości szkodliwy moduł pozostaje w systemie i wyświetla niechciane reklamy. Według danych badaczy z firmy Kaspersky, w ciągu dwóch ostatnich dni około 500 unikatowych użytkowników zainstalowało omawiany szkodliwy program, a pierwszą infekcję zarejestrowano 7 lipca 2019 r. Badacze wykryli około 800 różnych modyfikacji szkodliwego modułu.

Cyberprzestępcy stojący za szkodnikiem MobiDash często ukrywają swoje narzędzia pod postacią popularnych aplikacji i usług. To oznacza, że ich aktywność związana z fałszywą wersją narzędzia FaceApp może wzrosnąć. Zalecamy użytkownikom, by nie pobierali aplikacji mobilnych z nieoficjalnych źródeł, by uniknąć niepotrzebnego ryzyka powiedział Igor Gołowin, badacz ds. cyberbezpieczeństwa z firmy Kaspersky.

Produkty firmy Kaspersky wykrywają szkodnika MobiDash jako not-a-virus:HEUR:AdWare.AndroidOS.Mobidash.

Porady bezpieczeństwaEksperci z firmy Kaspersky przygotowali kilka porad, które pozwolą użytkownikom urządzeń mobilnych uniknąć problemów związanych z fałszywymi aplikacjami oraz niekontrolowanym przesyłaniem poufnych informacji:

Pobieraj aplikacje wyłącznie z zaufanych źródeł.

Czytaj opinie oraz recenzje i zwracaj uwagę na oceny aplikacji wystawione przez innych użytkowników.

Uważnie czytaj umowy licencyjne instalowanych aplikacji, by dowiedzieć się, kto, jak i w jakim celu przetwarza oraz przechowuje Twoje informacje.

Zwracaj uwagę na listę uprawnień wymaganych przez instalowane aplikacje.

Podczas instalacji nie klikaj bez zastanowienia przycisku Dalej. Zamiast tego zapoznawaj się z informacjami wyświetlanymi w poszczególnych krokach instalacji.

Zainstaluj skuteczne rozwiązanie bezpieczeństwa, które wykryje szkodliwe programy oraz zapobiegnie próbom wyłudzania informacji poprzez ataki phishingowe.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky jako źródła.

Wszystkie informacje prasowe są dostępne na stronie https://www.kaspersky.pl/nowosci.

Piotr Kupczyk
Dyrektor biura komunikacji z mediami, Kaspersky Lab Polska
E-mail: piotr.kup czyk@kaspersky.pl
Tel. 34 390 94 00

Aktywacja: 19/07/19 13:14, odsłony: 80