NASK
CERT.PL

BEZPIECZEŃSTWO UŻYTKOWNIKA APLIKACJI FACEAPP

Analiza Zespołu CERT POLSKA
w Państwowym Instytucie Badawczym NASK

W dniu 19.07.2019 r. zespół ekspertów **CERT Polska**,
działający w Państwowym Instytucie Badawczym NASK,
dokonał analizy aplikacji FaceApp pod kątem cyberbezpieczeństwa.
Poniżej przedstawiono zakres badania i wnioski wynikające
z analizy.

1. Informacje wprowadzające

Analizę wykonał 19.07.2019 Michał Leszczyński (CERT Polska, NASK-PIB)
Platforma: Android
Nazwa aplikacji pobranej ze sklepu Play: FaceApp (io.faceapp)
Wersja aplikacji: 3.4.9.1
Rozmiar: 12.42 MB (13022304 bajtów)
SHA256 aplikacji: b0dcb12d2ea045888e53979b0e8c0e3ee049a7291484730cf6eb559b78b3cd76
SHA1 certyfikatu użytego do podpisania aplikacji:
60a14471b853bf20974e0e2135d78d427b91067e

Regulamin: https://www.faceapp.com/terms
Polityka Prywatności: https://www.faceapp.com/privacy

Metoda badań:
- analiza dynamiczna w przygotowanym środowisku
- statyczna analiza kodu aplikacji

2. Uprawnienia aplikacji - lista systemowa (objaśnienia poniżej):

```
android.permission.READ_EXTERNAL_STORAGE
com.google.android.providers.gsf.permission.READ_GSERVICES
com.google.android.c2dm.permission.RECEIVE
android.permission.CAMERA
android.permission.WAKE_LOCK
android.permission.ACCESS_NETWORK_STATE
android.permission.INTERNET
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE
android.permission.WRITE_EXTERNAL_STORAGE
com.android.vending.BILLING
```

- Aparat: wykonywanie zdjęć i filmów wideo (nie umożliwia aplikacji samowolnego wykonywania fotografii)
- Pamięć: zmodyfikuj lub usuń zawartość karty pamięci
- Pamięć: odczytywanie zawartości karty SD
- Inne: pełny dostęp do sieci (daje możliwość połączenia z Internetem, nie umożliwia jednak wglądu w to, co wysyłają lub odbierają inne aplikacje)
- Inne: wyświetlanie połączeń sieciowych (korzystając z tego uprawnienia, aplikacja może sprawdzić czy smartfon jest połączony z Internetem i w jaki sposób – przez WiFI, czy też sieć komórkową; uprawnienie nie daje wglądu w przesyłane informacje)
- Inne: usługa płatności w Google Play (wyłącznie w zakresie zakupu wersji “Pro” w tej konkretnej aplikacji; nie ma możliwości odczytu np. danych karty płatniczej)
- Inne: odczytywanie konfiguracji usług Google
- Inne: zapobieganie przejściu telefonu w stan uśpienia
- Inne: odbieranie danych z Internetu
- Inne: interfejs API odesłania do instalacji z Play

Z przeprowadzonej analizy CERT Polska wynika, że żadne z wymienionych wyżej uprawnień nie daje aplikacji większego dostępu niż byłby faktycznie wymagany. Aplikacja nie posiada możliwości technicznych i uprawnień do zbierania nadmiarowych danych, w tym historii połączeń, lokalizacji, historii przeglądarki.

3. Zidentyfikowana komunikacja (poniżej objaśnienia zastosowania):

- serwery producenta aplikacji (api-search.faceapp.io, hosts.faceapp.io, tyrion.faceapp.io)
- usługa integracji z portalem Facebook (graph.facebook.com, graph.accountkit.com)
- usługa przesyłania informacji diagnostycznych, np. czy udało się
- zainstalować aplikację, czy telefon wspiera płatności Google Play itp. (app-measurement.com)
- pobieranie ustawień reklam w aplikacji (firebaseremoteconfig.googleapis.com)
- serwery reklamowe Google (googleads.g.doubleclick.net, tpc.googlesyndication.com)
- usługa pobierania czcionek Google (fonts.googleapis.com)
- usługa analizowania błędów aplikacji (settings.crashlytics.com)
- usługa wyszukiwania Bing do wyszukiwania obrazów w zakładce “Celebs” (tseN.mm.bing.net)

Wymienione wyżej serwery producenta aplikacji znajdują się w amerykańskim oddziale chmury Amazon EC2. Pozostałe połączenia prowadzą bezpośrednio do serwerów Google, Microsoft i Facebooka.

Analizie CERT Polska poddane zostały wszystkie z wymienionych wyżej strumieni danych, ale żaden z nich nie wygenerował nieuzasadnionego ruchu sieciowego ani nie był wykorzystywany niezgodnie z przeznaczeniem. Ponadto analiza potwierdziła, że aplikacja nie przesyła samowolnie lokalnych plików lub zdjęć z galerii. Do chmury trafiają wyłącznie zdjęcia, które zostały ręcznie wskazane przez użytkownika aplikacji.

4. Wnioski dodatkowe

Warto zauważyć, że aplikacja ma dostęp nie tylko do samej treści wrzuconego obrazka, ale również do metadanych EXIF, które w niektórych przypadkach mogą zawierać m.in. pozycję GPS z miejsca zrobienia fotografii. To, czy tego typu dane są zapisywane w pliku zdjęcia, zależy od wybranych przez użytkownika ustawień prywatności, które obowiązują globalnie dla całego urządzenia.

Wolumen ruchu sieciowego generowanego przez aplikację podczas obróbki zdjęcia wskazuje na to, że przesyłana jest tylko wybrana fotografia.

Komunikat “Wyszukiwanie selfie...”, który pojawia się zaraz po udzieleniu dostępu do galerii zdjęć oznacza, że aplikacja sprawdza fotografie użytkownika za pomocą algorytmu wyszukiwania twarzy. Czynność ta jest jednak realizowana bezpośrednio na smartfonie i nie powoduje przesyłania skanowanych zdjęć do chmury.

Jeżeli użytkownik zdecyduje się na opcjonalną integrację z Facebookiem, aplikacja uzyska dostęp do galerii z jego profilu, ale również pozna jego imię, nazwisko, adres e-mail oraz zdjęcie profilowe. Dodatkowo aplikacja ma możliwość odczytania listy znajomych, ale tylko tych, którzy również używają FaceAppa.

PODSUMOWANIE

W wyniku przeprowadzonej przez Zespół CERT Polska w NASK PIB analizy stwierdzono z wysokim prawdopodobieństwem, że badana wersja aplikacji (3.4.9.1) nie zawiera złośliwego oprogramowania ani backdoorów. Kolejne wydania aplikacji mogą wprowadzić nowe funkcje, w związku z czym należy w każdym przypadku użytkowania zachować ostrożność, zwłaszcza w sytuacji, gdy aktualizacji użytkownik proszony jest o udzielenie dodatkowych uprawnień.

NASK

CERT.PL