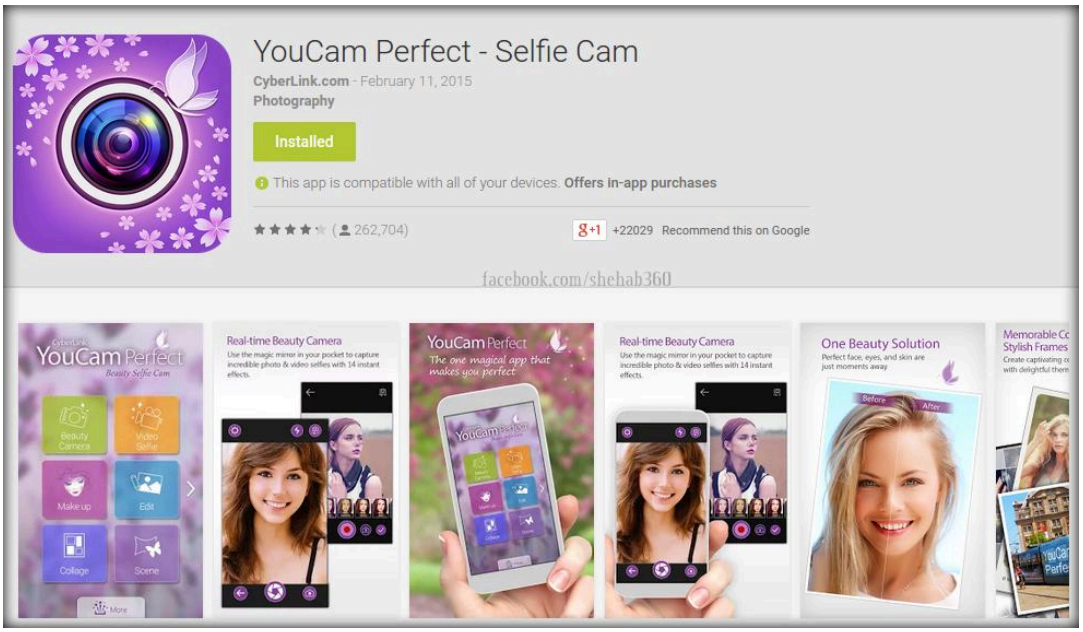
Youcam Perfect هو تطبيق قامت شركة cyberlink بتصميمه ليسمح للمستخدم تعديل والتقاط واضافة التأثيرات على الصور,لكن ما لفت نظري بأن هناك امر غريب في صلاحيات التطبيق,مما دفعني لتحليل اولي للتطبيق مع مجموعة من خبراء امن المعلومات وباستخدام ادوات تحليل اولية بسيطة.

النتيجة النهائية كانت ان التطبيق يقوم بتشغيل خاصية التقاط التسجيلات الصوتية رغم ان التطبيق لا يحتوي اي خاصية تسجيل او التقاط صوت,وهذا ما دفعنا للبحث اكثر,حيث تبين ايضا ان اسلوب اتصال التطبيق بخادم الموقع يحتوي على خلل امني تحفظنا عن نشر تفاصيل هذه المعلومة في التحليل لان الهدف من هذا التحليل التوعية الامنية للافراد لا احداث الاضرار بأي جهة,وبالنسبة للخلل الذي ظهر لنا سنراسل شركة cyberlink لاصلاحه.

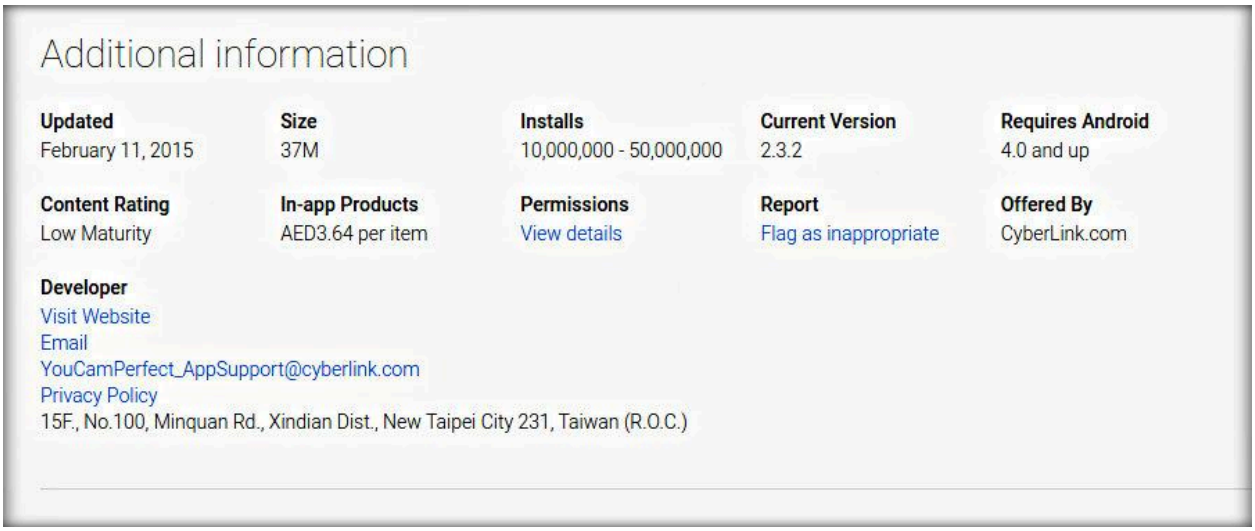
اسم التطبيق : Youcam Perfect

الشركة المصّنعة : cyberlink.com



حجم التطبيق بعد التحميل على الاجهزة : 36.40 MB

رقم النسخة : 2.3.2



اخر تحديث للتطبيق: Feb 11,2015

عدد من قام بتحميل التطبيق : اكثر من 10 مليون مستخدم.

تصرفات التطبيق بعد تحميله:

- يقوم بالتحقق ان كان جهاز الموبايل متصل بالشبكة ام لا
- يقوم بالتحقق في حال كان جهاز الموبايل في وضع الاستعداد ام لا.

ديناميكية استقبال السجل الخاص بالتطبيق:

عند تغيير او تبديل الشبكة تعمل هذه العمليات او الخدمات بشكل الي دون تدخل المستخدم وهي:

com.cyberlink.youperfect.utility.s و com.flurry.sdk.fe

تصرفات التطبيق داخل مسارات ذاكرة الجهاز والذاكرة التخزينية الاضافية SD:

- بعد تحليل التطبيق,يستطيع التطبيق الدخول الى:

/mnt/sdcard/YCP_LOG_2016_10_25_10:21:41:731.txt
/mnt/sdcard/.uma-id هذا المسار يحتوي على ملفات حساسة

ومسارات اخرى متوفرة ايضا كالموضحة بالصورة ادناه :

/mnt/sdcard/YCP_LOG_2014_09_02_10:21:20:884.txt
/mnt/sdcard/YCP_LOG_2016_11_08_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2016_07_17_10:21:41:731.txt
/mnt/sdcard/YouCam Perfect/YouCam Perfect Sampl
e
/mnt/sdcard/YCP_LOG_2017_04_22_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2016_08_08_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2014_09_10_10:21:20:884.txt
/mnt/sdcard/YCP_LOG_2016_10_13_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2016_11_28_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2017_04_14_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2016_07_04_10:21:41:731.txt
/mnt/sdcard/uma-override.txt
/mnt/sdcard/YCP_LOG_2016_04_24_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2016_12_30_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2017_02_24_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2016_09_24_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2017_02_26_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2016_07_10_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2014_08_29_10:21:20:884.txt
/mnt/sdcard/YCP_LOG_2016_10_09_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2016_12_26_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2016_06_06_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2016_07_15_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2016_12_22_10:21:41:731.txt
/mnt/sdcard/YCP_LOG_2017_04_06_10:21:41:731.txt

هذا المسار يحتوي على ملفات حساسة بالمستخدم /mnt/sdcard/Andriod/data ظهر اثناء التحليل

يقوم التطبيق بتحميل الوحدة التالية:

UiimageCodec.so
PicassoProxy.so
Common.so

load the .so module
UIImageCodec.so
PicassoProxy.so
Common.so

معلومات اضافية:

- اسم حزمة التطبيق: com.cyberlink.youperfect
- حجم الحزمة : 36.40
- تاريخ ومعلومات شهادة التسجيل: مجهولة,unknown

- MD5 : 44a968279ecbf81df314f12dd88fb671
- sha-1: e9bcc4b2ec951c7248533aae55df40f4cb60e6d8

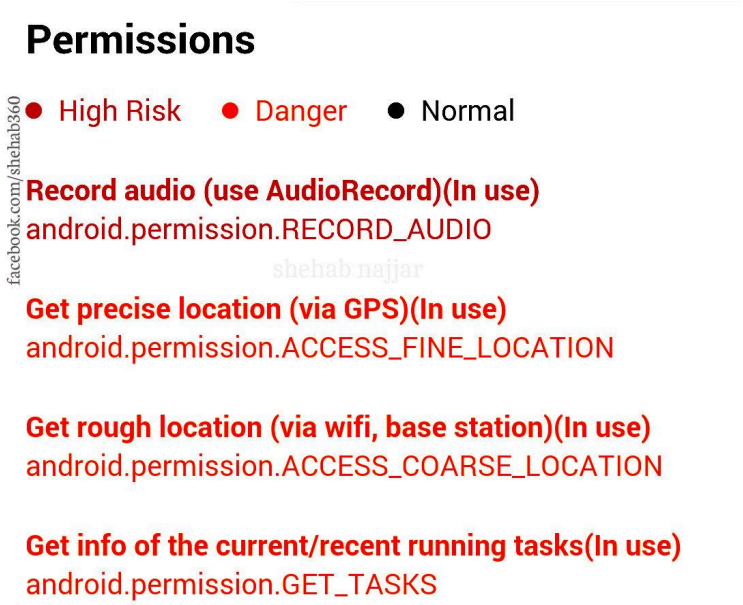
- عند استخدام التطبيق للانترنت,تعمل خاصية مراقبة الشبكة Network monitor هنا ظهرت نقاط ضعف امنية في التطبيق لم يتم كتابتها في هذا التحليل وسيتم مراسلة الشركة المُصنعة للتطبيق بها,علما انني لم اكن اتطلع للبحث عن ثغرات او خلل امني في التطبيق بل كنت ابحث في ديناميكية عمل التطبيق لا اكثر.

صلاحيات التطبيق بعد التحميل على جهاز الموبايل:

- يقوم بتسجيل مباشرة من المايكروفون رغم ان التطبيق للتصوير والتعديل للصور,يلتقط الاصوات من خلال :
andriod.permission.RECORD_AUDIO | Use AudioRecord
ويبقى في حالة عمل طيلة فترة فتح التطبيق !

- يحصل التطبيق على مكانك الجغرافي الفعلي ال GPS وذلك عبر تحليل :
Andriod.permission.Access_fine_location وقد ذكرت الشركة اسباب استخدام المكان الجغرافي قبل تحميل التطبيق,الا ان كل ذلك غير مقنع,فقد ذُكر ان سبب الحصول على صلاحية المكان الجغرافي هي بهدف نشر المكان الجغرافي مع الصور التي يتم نشرها على مواقع التواصل.

- عمليات ونشاطات التطبيق تعمل حتى اثناء اغلاق شاشة جهاز الموبايل وذلك عبر تحليل :
Andriod.permission.WAKE_LOCK



- **الخلاصة:**

- التطبيق يستخدم خاصية التقاط الاصوات او تسجيل الاصوات علما ان التطبيق لا علاقة له مطلقا في تسجيل الاصوات ولا يوجد داخل التطبيق مطلقا ما يتطلب فتح المايكروفون او الالتقاط للاصوات,التطبيق مخصص فقط للتعديل على الصور واضافة التأثيرات على الصور,علما ان خاصية الالتقاط في حالة Active طيلة فترة تشغيل التطبيق.

- ان التطبيق يستخدم خاصية معرفة المكان الجغرافي بالتحديد لمستخدم التطبيق وهو امر لا ارى فيه اي اهمية لتطبيق تعديل صور وتأثيرات على الصور.

- معلومات شهادة الترخيص الخاصة بالتطبيق مجهولة وهو امر غريب على تطبيق من شركة معروفة,اي تطبيق يتم رفعه على متجر جوجل يمتلك شهادة ترخيص خاصة ويجب ان تظهر اثناء التحليل.

النتيجة : "تجنب تحميل او استخدام التطبيق"
