بسمه تعالی

سوءاستفاده‌ی فعال از آسیب‌پذیری روزصفرم CVE-2019-2215

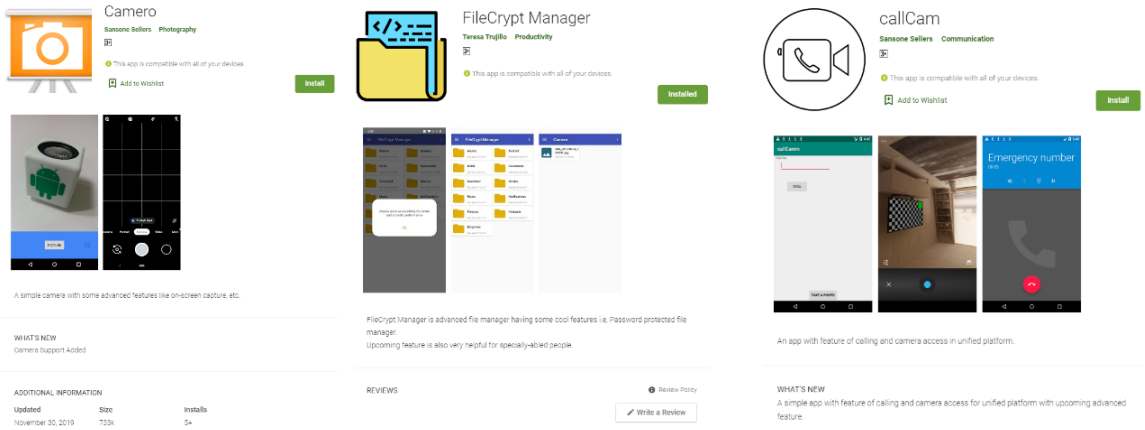
برای اولین بار از یک آسیب‌پذیری استفاده پس از آزادسازی (use-after-free) به‌طور گسترده در حملات استفاده شده است. این آسیب‌پذیری که با شناسه‌ی CVE-2019-2215 ردیابی می‌شود در ماه اکتبر سال ۲۰۱۹ توسط محققان Google Project Zero به عنوان یک آسیب‌پذیری روزصفرم افشا شد. این نقص ابتدا در ماه دسامبر سال ۲۰۱۷ در هسته‌ی Linux 4.14، هسته‌ی 3.18 پروژه‌ی متن‌باز اندروید (AOSP)، هسته‌ی AOSP 4.4 و هسته‌ی AOSP 4.9 برطرف شده بود. دو سال بعد، این آسیب‌پذیری همچنان Pixel 2؛ Pixel 1؛ Huawei P20؛ Xiaomi Redmi 5A؛ Redmi Note 5 و A1؛ Oppo A3؛ گوشی‌های LG دارای اندروید Oreo و گوشی‌های سامسونگ مدل‌های Galaxy S7,S8 و S9 را تحت‌تأثیر قرار می‌داد.

گوگل وصله‌هایی برای این نقص در مجموعه اصلاحات اندرویدی ماه اکتبر سال ۲۰۱۹ منتشر ساخت.

بنا به اطلاعات جمع‌آوری شده توسط کارشناسان، از این آسیب‌پذیری سوءاستفاده شده است. این آسیب‌پذیری توسط شرکت باج‌افزاری اسرائیل، NSO (معروف به ساختن بدافزار iOS مشهور Pegasus) سوءاستفاده شده است و از آن برای نصب یک نسخه از Pegasus سوءاستفاده می‌کند.

اکنون محققان دریافته‌اند سه برنامه‌ی مخرب که از ماه مارس سال ۲۰۱۹ در فروشگاه Google Play در دسترس بوده است، به‌منظور به خطر انداختن دستگاه کاربر و جمع‌آوری اطلاعات با هم کار می‌کنند. یکی از این برنامه‌ها که Camero نامیده می‌شود از آسیب‌پذیری CVE-2019-2215 سوءاستفاده می‌کند. این آسیب‌پذیری در Binder (اصلی‌ترین سیستم ارتباطی درون‌فرایندی اندروید) وجود دارد. بررسی‌های بیشتر نشان می‌دهد که هر سه‌ی این برنامه‌ها مربوط به گروه تهدید SideWinder (فعالیت خود را از سال ۲۰۱۲ آغاز کرده و ماشین‌های ویندوزی موجودیت‌های ارتش را هدف قرار می‌دهد) هستند. این سه برنامه از این جهت به گروه SideWinder نسبت داده شده‌اند که به نظر می‌رسد کارگزارهای C&C استفاده شده مربوط به بخشی از ساختار SideWinder باشند. علاوه‌براین، یک URL که به یکی از صفحات Google Play این برنامه‌ها لینک می‌خورد نیز در یکی از این کارگزارهای C&C یافت شده است.

این سه برنامه‌ی مخرب وانمود می‌کنند ابزارهای عکاسی یا مدیریت فایل هستند (شکل ۱). به نظر می‌رسد این برنامه‌ها بر اساس اطلاعات گواهینامه‌ی یکی از برنامه‌ها فعال شده‌اند (شکل ۲).



شکل ۱ سه برنامه‌ی مخرب مربوط به گروه SideWinder

275d530542315404b20eeacff58948fbcd03c781

Certification0	
signer_CN	Android
signer_C	US
signer_O	Google Inc.
signer_OU	Android
signer_L	Mountain View
owner_O	Google Inc.
validDateTo	2049-03-27 08:32:42
owner_L	Mountain View
validDateFrom	2019-03-27 08:32:42
signer_ST	California
owner_CN	Android
owner_OU	Android
owner_C	US
owner_ST	California
serialNumber	F884DF9405CBAA483D4FB72752C1B6FC5DDC2B37

شکل ۲ اطلاعات گواهینامه‌ی یکی از برنامه‌ها

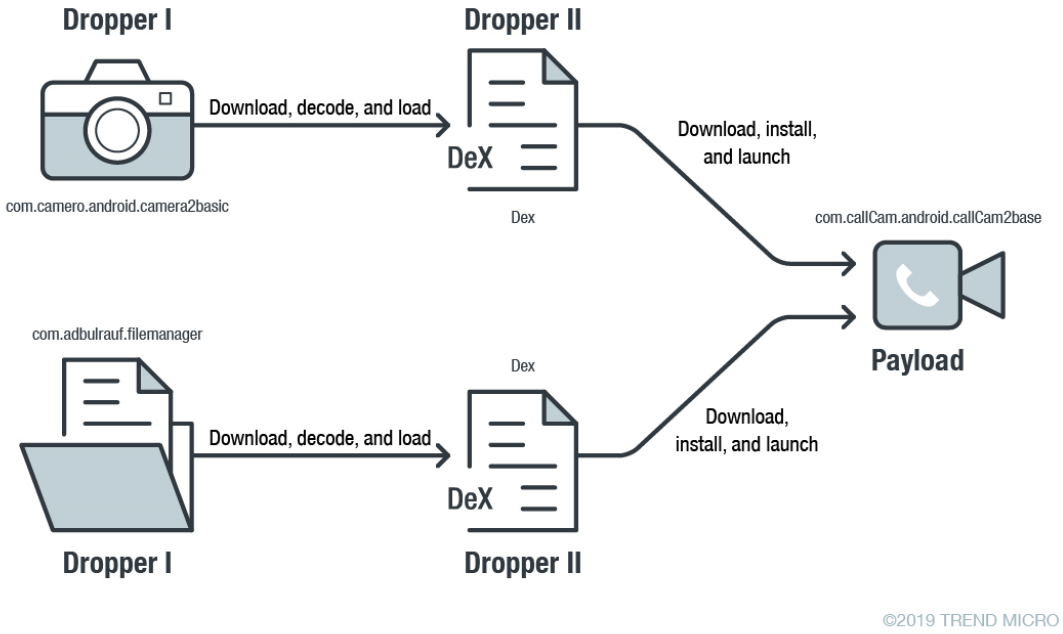
مهاجمان برای سوءاستفاده از این آسیب‌پذیری، برنامه‌ی خرابکار را در دو مرحله نصب می‌کنند. در مرحله‌ی اول، ابتدا یک فایل DEX (یک نوع فرمت فایل اندروید) را از کارگزار کنترل و فرمان (C&C) خود دانلود می‌کنند. آن‌ها برای تنظیم آدرس کارگزار C&C از Apps Conversion Tracking استفاده می‌کنند (شکل ۳). این آدرس توسط Base64 کدگذاری می‌شود و سپس به پارامتر مراجعه‌کننده در URL که در توزیع بدافزار استفاده می‌شود، تنظیم می‌شود.

```
String v10_1 = v10.getString("referrer");
if(v10_1 == null) {
    return;
}

OutputStream v3 = this.b;
StringBuilder v4 = new StringBuilder();
v4.append("refer: ");
v4.append(v10_1);
v4.append(v2);
v3.write(v4.toString().getBytes());
System.out.println("Successfully byte inserted");
this.b.flush();
Log.e("asdffff", v10_1);
a v10_2 = new a(new ByteArrayInputStream(f.a(Base64.decode(URLDecoder.decode(v10_1, "UTF-8"), 0))));
SharedPreferences v9_1 = arg9.getSharedPreferences("MyPref", 0);
SharedPreferences$Editor v3_1 = v9_1.edit();
String v4_1 = v10_2.b();
v10_1 = v10_2.b();
OutputStream v5 = this.b;
StringBuilder v6 = new StringBuilder();
v6.append("url: ");
v6.append(v4_1);
```

شکل ۳ آدرس تجزیه‌شده‌ی کارگزار C&C

پس از این گام، فایل DEX دانلودشده، یک فایل APK دانلود می‌کند و پس از سوءاستفاده از دستگاه یا بکارگیری قابلیت دسترسی، آن را نصب می‌کند. تمامی این اقدامات بدون آگاهی و مداخله کاربر انجام می‌شود. به منظور جلوگیری از شناسایی‌شدن، از تکنیک‌های فراوانی همچون ابهام‌سازی، رمزگذاری داده‌ها و درخواست کد پویا استفاده می‌شود (شکل ۴).

برنامه‌های Camero و FileCrypt Manager به عنوان قطره‌چکان (dropper) عمل می‌کنند. فایل اضافی Extra DEX از کارگزار C&C استخراج می‌شود. سپس قطره‌چکان‌های لایه‌ی دوم، به‌منظور دانلود، نصب و راه‌اندازی برنامه‌ی CallCam بر روی دستگاه، کد اضافی درخواست می‌کنند (شکل ۵).



شکل ۴ به‌کارگیری خرابکاری در دومرحله

```
try {
    String v0 = new String(Base64.decode("ZGFsdmlrLnN5c3R1bS5EZXhDbGFzc0xvYWR1cg==", 0));
    File v1 = new File(a.a(arg9.getFilesDir().getPath(), "fex"), "temp");
    if(!v1.exists()) {
        v1.mkdirs();
    }

    File v4 = new File(v1, a.a(18));
    FileOutputStream v1_1 = new FileOutputStream(v4);
    v1_1.write(arg10);
    v1_1.close();
    Object v8_1 = Class.forName(v0).getConstructor(String.class, String.class, String.class, ClassLoader.class)
    Method v10 = v8_1.getClass().getDeclaredMethod("Init", Context.class);
    v10.setAccessible(true);
    v10.invoke(v8_1, arg9);
```

شکل ۵ کد نشان‌دهنده‌ی چگونگی درخواست کد Extra DEX توسط قطره‌چکان

مهاجمان به‌منظور به‌کارگیری برنامه‌ی خرابکار callCam بر روی دستگاه بدون آگاهی کاربر، اقدامات زیر را انجام می‌دهند:

- روت‌کردن دستگاه:

این کار توسط برنامه‌ی قطره‌چکان Camero انجام می‌شود و تنها بر روی دستگاه‌های Google Pixel (Pixel2، Pixel 2 XL)، Nokia 3 (TA-1032)، LG V20 (LG-H990) و Redmi 6A کار می‌کند. این بدافزار سوءاستفاده‌ی خاصی را از کارگزار C&C مبتنی بر DEX دانلودشده توسط قطره‌چکان، استخراج می‌کند.

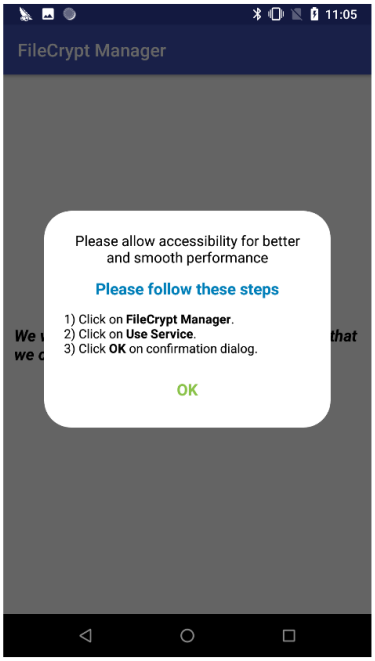
```
if(Build.MODEL.toLowerCase().contains("pixel")) {
    return;
}

if(Build.MODEL.toLowerCase().contains("ta-1032")) {
    return;
}

if(Build.MODEL.toLowerCase().contains("lg-h990")) {
    return;
}

if(Build.MODEL.toLowerCase().contains("cph1881")) {
    return;
}

if(Build.MODEL.toLowerCase().contains("redmi 6a")) {
    return;
}
```

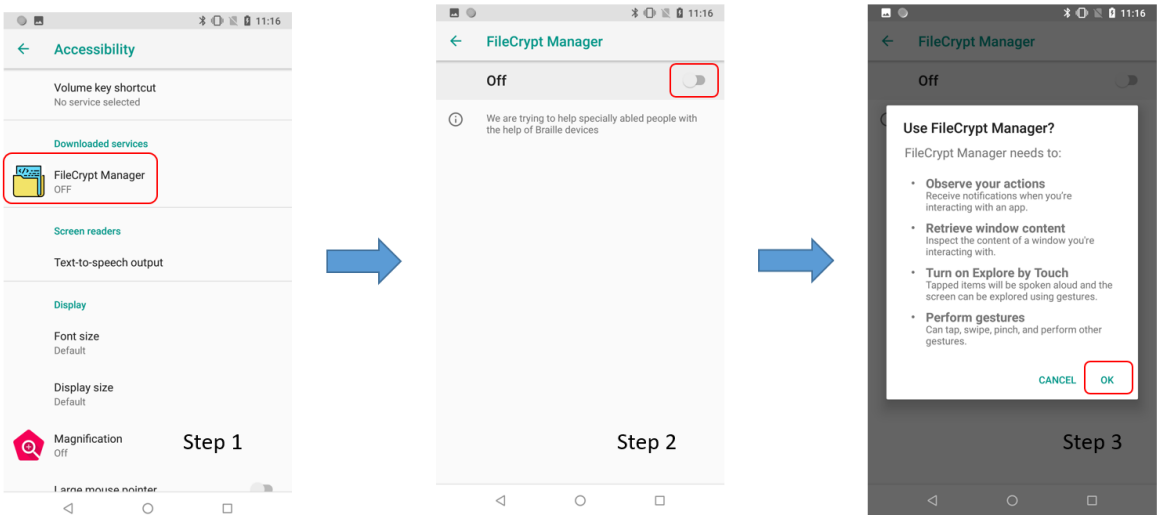
شکل ۶ قطعه کدی از Extra DEX که توسط Camero دانلود شده است

کارشناسان Trend Micro در حین تحقیقات خود، پنج سوءاستفاده از کارگزار C&C دانلود کرده‌اند. این سوءاستفاده‌ها برای به‌دست آوردن دسترسی ریشه‌ای، از آسیب‌پذیری‌های CVE-2019-2215 و MediaTek-SU استفاده می‌کنند. پس از به‌دست آوردن دسترسی ریشه‌ای، این بدافزار برنامه‌ی callCam را دانلود، مجوز دسترسی آن را فعال و سپس آن را راه‌اندازی می‌کند.

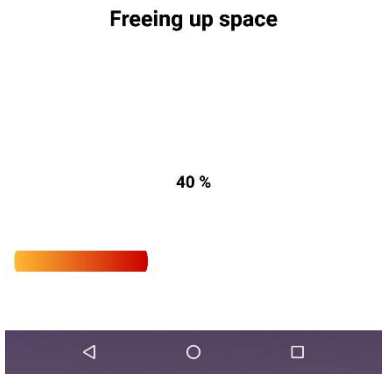
- استفاده از مجوز قابلیت دسترسی:

این کار با استفاده از برنامه‌ی قطره‌چکان FileCrypt Manager انجام می‌شود و روی اکثر گوشی‌های اندرویدی دارای نسخه‌ی بالاتر از Android 1.6 کار می‌کند. پس از راه‌اندازی FileCrypt Manager، از کاربر می‌خواهد قابلیت دسترسی را فعال سازد. پس از اعطای این مجوز، این برنامه یک پنجره‌ی تمام صفحه را نشان می‌دهد که می‌گوید مراحل راه‌اندازی بیشتری لازم دارد (شکل ۷). این پنجره درواقع روکشی روی تمام پنجره‌های فعالیت دستگاه است (شکل ۸). پنجره‌ی روکش، ویژگی‌های خود را به FLAG_NOT_FOCUSABLE و FLAG_NOT_TOUCHABLE تنظیم می‌کند. این ویژگی‌ها به پنجره‌های فعالیت اجازه می‌دهند رویدادهای لمسی کاربران را از طریق صفحه‌ی روکش، شناسایی و دریافت کنند. در همین حال، برنامه برای نصب برنامه‌های ناشناخته و نصب برنامه‌ی خرابکار callCam، از فایل Extra DEX کد درخواست می‌کند. همچنین مجوز قابلیت دسترسی برنامه‌ی خرابکار callCam را فعال و سپس آن را راه‌اندازی می‌کند. تمامی این اتفاقات پشت صفحه‌ی روکش روی می‌دهد و برای کاربر ناشناخته است. تمامی این مراحل بااستفاده از قابلیت دسترسی برنامه انجام می‌شود.





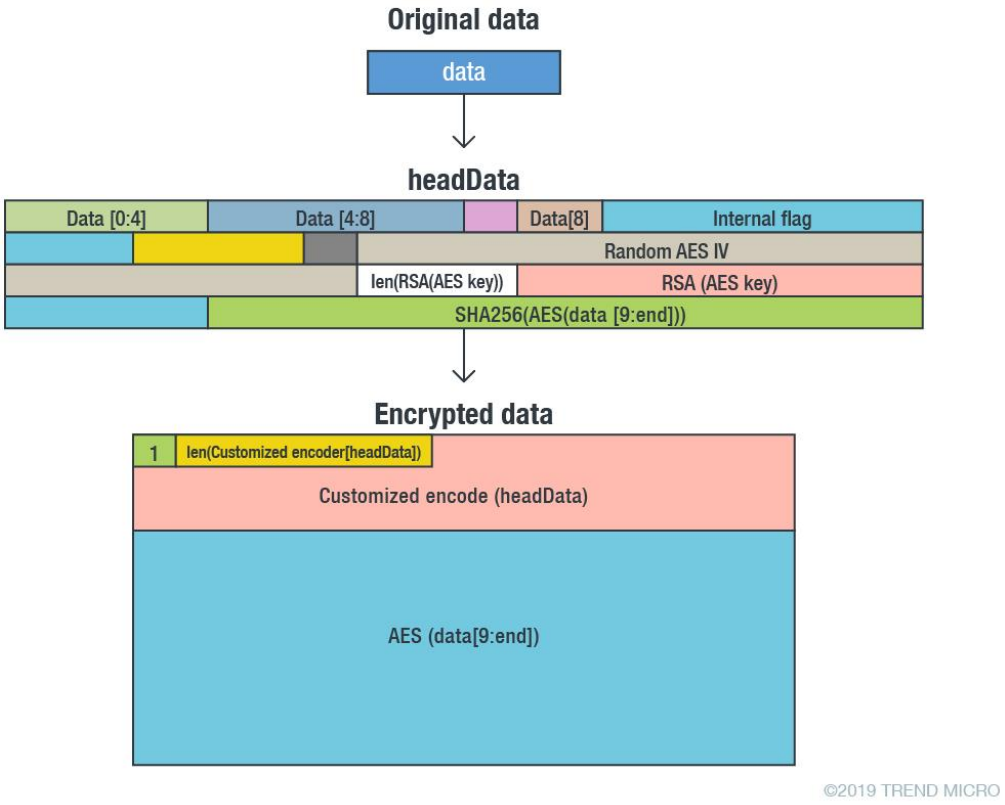
شکل ۷ گام‌هایی که FileCrypt Manager از کاربر می‌خواهد انجام دهد



شکل ۸ صفحه‌ی روکش

برنامه‌ی callCam آیکون خود را پس از راه‌اندازی بر روی دستگاه مخفی می‌کند. اطلاعات موقعیت مکانی، وضعیت باتری، فایل‌های روی دستگاه، لیست برنامه‌های نصب‌شده، اطلاعات دستگاه، اطلاعات سنسور، اطلاعات دوربین، اسکرین‌شات، حساب کاربری، اطلاعات WiFi و داده‌های WeChat، OutLook، Twitter، Yahoo Mail، Facebook، Gmail و Chrome را جمع‌آوری و در پس‌زمینه آن‌ها را به کارگزار C&C می‌فرستد.

این برنامه تمام داده‌های سرقتی را بااستفاده از الگوریتم‌های RSA و AES رمزنگاری می‌کند. از SHA256 برای تأیید صحت داده‌ها و سفارشی‌کردن روال رمزگذاری، استفاده می‌کند. در زمان رمزنگاری، بلوکی از داده‌ها به نام headData ایجاد می‌کند. این بلوک شامل ۹ بایت اول داده‌ی اصلی، طول داده‌ی اصلی، AES IV تصادفی، کلید رمزنگاری AES که با RSA رمزنگاری‌شده و مقدار SHA256 از داده‌ی اصلی رمزنگاری‌شده با AES است. این بلوک، پس از رمزنگاری، بالای فایل نهایی رمزنگاری‌شده و پس از داده‌ی اصلی رمزنگاری‌شده با AES ، ذخیره می‌شود (شکل ۹).



شکل ۹ روند رمزنگاری داده

این سه برنامه در همان تاریخ ماه مارس سال ۲۰۱۹ که مخرب شناسایی شدند، از فروشگاه Google Play حذف شدند.

به منظور مقابله با این آسیب‌پذیری به تمامی کاربران توصیه می‌شود به‌روزرسانی ماه اکتبر سال ۲۰۱۹ گوگل را نصب کنند.

https://blog.trendmicro.com/trendlabs-security-intelligence/first-active-attack-exploiting-cve-2019-2215-found-on-google-play-linked-to-sidewinder-apt-group/

https://www.darkreading.com/application-security/malicious-google-play-apps-linked-to-sidewinder-apt/d/d-id/1336728

https://www.securityweek.com/app-found-google-play-exploits-recent-android-zero-day

https://securityaffairs.co/wordpress/96074/hacking/apps-exploit-cve-2019-2215.html