بسمه تعالی

تحلیل برنامه‌ی گوگل سرویس

فهرست مطالب

۱ مقدمه

با گسترش تلگرام و استفاده روزافزون همه اقشار جامعه از این شبکه اجتماعی، بازار جدیدی برای کلاه‌برداران و هکرها به وجود آمده است. ازآنجاکه عموم مردم از دانش فنی و امنیتی کمی برخوردار هستند، احتمال آلوده شدن آن‌ها بسیار زیاد است. ازاین‌رو مهاجمین با استفاده از مهندسی اجتماعی می‌توانند به‌راحتی به دستگاه قربانی نفوذ و از آن سوءاستفاده نمایند.

وجود قابلیت ارسال فایل و برنامه‌های کاربردی نظیر فایل‌های اجرایی اندروید (apk)، بر این مشکل دامن زده است. مهاجمین با بهره‌گیری از این قابلیت، به‌سادگی برنامه‌های مخرب را روی دستگاه قربانی نصب می‌کنند.

ازجمله حقه‌های مهندسی اجتماعی، برنامه‌ها و ربات‌هایی است که ادعا می‌کنند می‌توانند کسانی که از پروفایل کاربر بازدید کرده‌اند را نشان دهند. طیف فراوانی از بدافزارها تحت همین عنوان منتشر و قربانیان بسیاری داشته است. نکته جالب اینجاست که پیاده‌سازی چنین قابلیتی امکان‌پذیر نیست و API ای برای این عملکرد در تلگرام وجود ندارد و هرگونه ادعایی در این مورد منجر به سوءاستفاده از کاربر می‌شود.

در این گزارش یکی از برنامه‌هایی که تحت این عنوان (″کی پروفایلت رو دیده″) منتشر و از کاربر سوءاستفاده می‌کند، بررسی شده است.

۲ تحلیل برنامه‌ی گوگل سرویس

در حال حاضر تبلیغات زیادی در کانال‌ها و گروه‌های تلگرامی برای برنامه‌های مختلف اندرویدی صورت می‌گیرد. در یکی از این تبلیغ‌ها که در آن برنامه‌ی ″کی پروفایلت رو دیده″ تبلیغ شده است، برنامه‌ای وجود دارد که پس از دریافت و نصب، آیکون خود را از صفحه پاک می‌کند و در پس‌زمینه مشغول به کار می‌شود. ازآنجایی‌که این برنامه از سرویس پوشه استفاده می‌کند، می‌تواند بدون آنکه کاربر متوجه شود که منبع اعلانات از کدام برنامه است، در بازه‌های مختلف زمانی، برای آن اعلان‌هایی مبنی بر دعوت به پیوستن به کانال تلگرامی یا دانلود برنامه‌های مختلف ارسال کند. از طرفی به دلیل پنهان شدن آیکون برنامه، نمی‌توان آن را حذف کرد و از مزاحمت‌های آن خلاص شد.

در این مورد خاص، برنامه‌ای که در اصل روی دستگاه کاربر نصب شده است، Google Service نام دارد. در ادامه به تحلیل این برنامه پرداخته شده است.

۲-۱ اطلاعات اولیه برنامه

نام برنامه:

Google Service

نام بسته:

com.google.gms.android

توسعه‌دهنده:

ehsan

نسخه:

1.0

سایز فایل:

1.7 MB

مقدار SHA256:

9522349ebdb92f70f90d9d7aeb65d0dedde0dd36ea4534756188cd32a48

مقدار SHA1:

9f909f406ab86841f2eb37e55e615d56d64acb38

مقدار MD5:

12816a1ee6fb6faedb72b6a25fc14306

این فایل توسط ۱۲ ضدویروس به‌عنوان برنامه‌ی مخفی شناسایی‌شده است.

۲-۲ تحلیل ایستای گوگل سرویس

مجوزهای این برنامه به شرح زیر است:

```
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
```

- دریافت و ارسال پیامک.

```
<uses-permission android:name="android.permission.WRITE_INTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_INTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
```

```
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission
android:name="com.google.android.gms.permission.ACTIVITY_RECOGNITION"/>
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
```

- پنجره هشدار سیستم برای نشان دادن اعلان.

```
<permission android:name="com.google.gms.android.permission.C2D_MESSAGE"
android:protectionLevel="signature"/>
<uses-permission
android:name="com.google.gms.android.permission.C2D_MESSAGE"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
```

- دریافت مجوز بوت شدن سیستم برای دوباره فعال شدن خودکار برنامه پس از بوت شدن.

```
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
```

- دسترسی برنامه به موقعیت مکانی کاربر که معمولاً توسط پوشه استفاده می‌شود تا بتوان با استفاده از آن تبلیغات را هدفمند ارسال کرد. توکن مورداستفاده این برنامه در پوشه به صورت زیر است:

```
<meta-data android:name="co.ronash.pushe.token"
android:value="PUSHE_318063720839"/>
```

برخی از سرویس‌ها و دریافت‌کنندگان موجود در این برنامه به شرح زیر است:

- قابلیت دریافت به‌روزرسانی برنامه توسط سرویس پوشه:

```
<receiver android:name="co.ronash.pushe.receiver.UpdateReceiver">
   <intent-filter>
       <action android:name="android.intent.action.PACKAGE_REPLACED"/>
       <data android:path="com.google.gms.android" android:scheme="package"/>
   </intent-filter>
</receiver>
```

با استفاده از این سرویس مهاجم می‌تواند بدافزار خود را به‌روزرسانی کرده، قابلیت‌های بیشتری به آن اضافه کند و به‌راحتی نیز بسته‌ی جدید را جایگزین برنامه‌ی قبلی کند.

- قابلیت ارسال اعلان‌های مختلف به کاربران که باز هم توسط پوشه قابل انجام است:

```
<service android:exported="false"
android:name="com.google.gms.android.NotificationServicePushe">
```

```
    <intent-filter>
        <action android:name="co.ronash.pushe.RECEIVE"/>
    </intent-filter>
</service>
```

اعلان‌های ارسالی می‌تواند حاوی دانلود برنامه‌های مخرب، لینک صفحات آلوده، دعوت به کانال تلگرام و غیره باشند.

- قابلیت شنود پیامک:

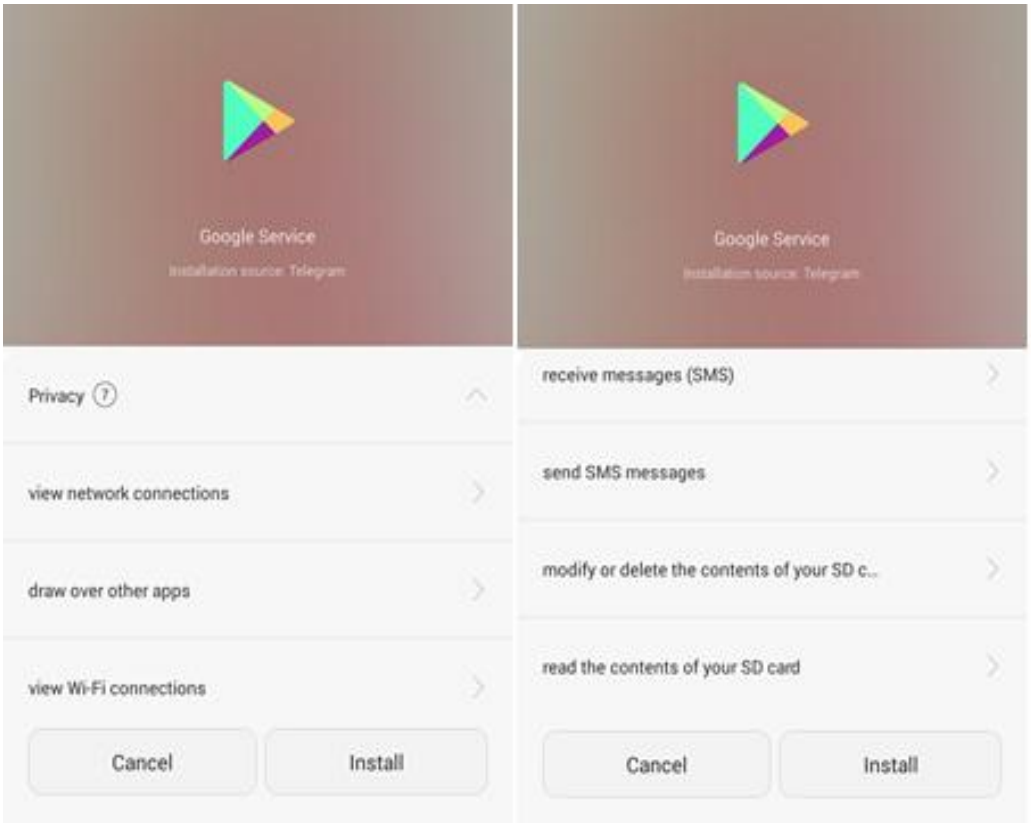
```
<receiver android:name="com.store.pop.SmsListener">
   <intent-filter>
       <action android:name="android.provider.Telephony.SMS_RECEIVED"/>
   </intent-filter>
</receiver>
```

- با استفاده از سرویس پوشه می‌توان کد json را نیز روی دستگاه قربانی اجرا کرد. نمونه‌ای از این کدها که می‌تواند اطلاعاتی راجع به آی پی، شهر، اپراتور و دیگر اطلاعات کاربر استخراج کند، به شرح زیر است:

```
a.add(new AbstractMap.SimpleEntry("http://4.ifcfg.me/json", "ip"));
a.add(new AbstractMap.SimpleEntry("http://ifcfg.me/json", "ip"));
a.add(new AbstractMap.SimpleEntry("https://wtfismyip.com/json",
"YourFuckingIPAddress"));
a.add(new AbstractMap.SimpleEntry("http://ipinfo.io/json", "ip"));
a.add(new AbstractMap.SimpleEntry("http://ip-
api.com/json/?callback=yourfunction", "query"));
a.add(new AbstractMap.SimpleEntry("https://api.ipify.org?format=json", "ip"));
a.add(new AbstractMap.SimpleEntry("http://icanhazip.com/", ""));
a.add(new AbstractMap.SimpleEntry("http://ip.ronash.co/geoip", "ip"));
```

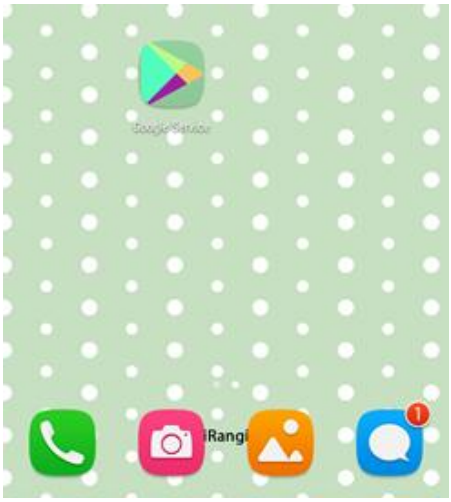
۳-۲ تحلیل پویای گوگل سرویس

هنگام نصب برنامه تصویر شکل ۱ نشان داده می‌شود.



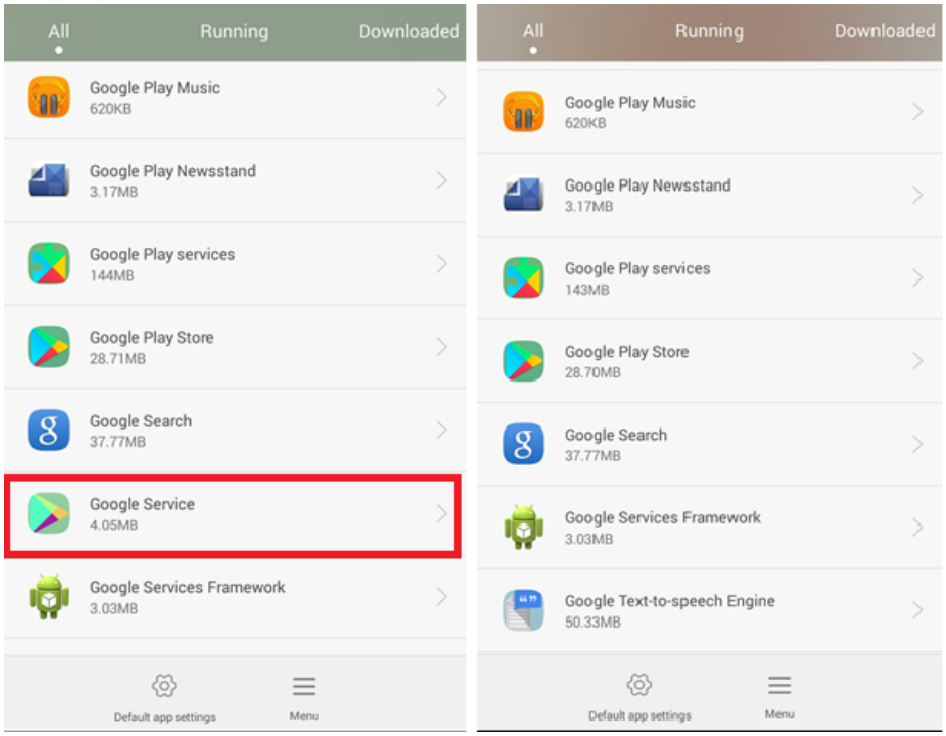
شکل ۱: تصویر نمایش داده شده در زمان نصب

اگر پس از نصب دکمه‌ی done زده شود، آیکون آن مانند شکل ۲ در صفحه نشان داده می‌شود. پس از باز کردن برنامه آیکون آن از صفحه حذف می‌شود.



شکل ۲: نمایش آیکون برنامه در صفحه

همان‌طور که در شکل ۳ دیده می‌شود، برنامه‌ای به نام Google Service به برنامه‌ها اضافه شده است که تشخیص آن برای حذف مشکل است.



شکل ۳: اضافه شدن برنامه‌ی گوگل سرویس به لیست برنامه‌ها

۳ نتیجه‌گیری

کاربران باید مراقب باشند و از دریافت و نصب هرگونه برنامه از کانال‌های غیررسمی مانند تلگرام خودداری کنند. تمامی این برنامه‌ها، با عناوین مختلف، مخرب هستند و سوءاستفاده‌های مختلفی از کاربر می‌نمایند.