بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

تحلیل بدافزار اندرویدی ((فیلترشکن آمدنیوز))

تاریخ نگارش ..... ۲۸ دی ۱۳۹۶

شماره نگارش ۱

طبقه‌بندی ..... عادی

مقدمه

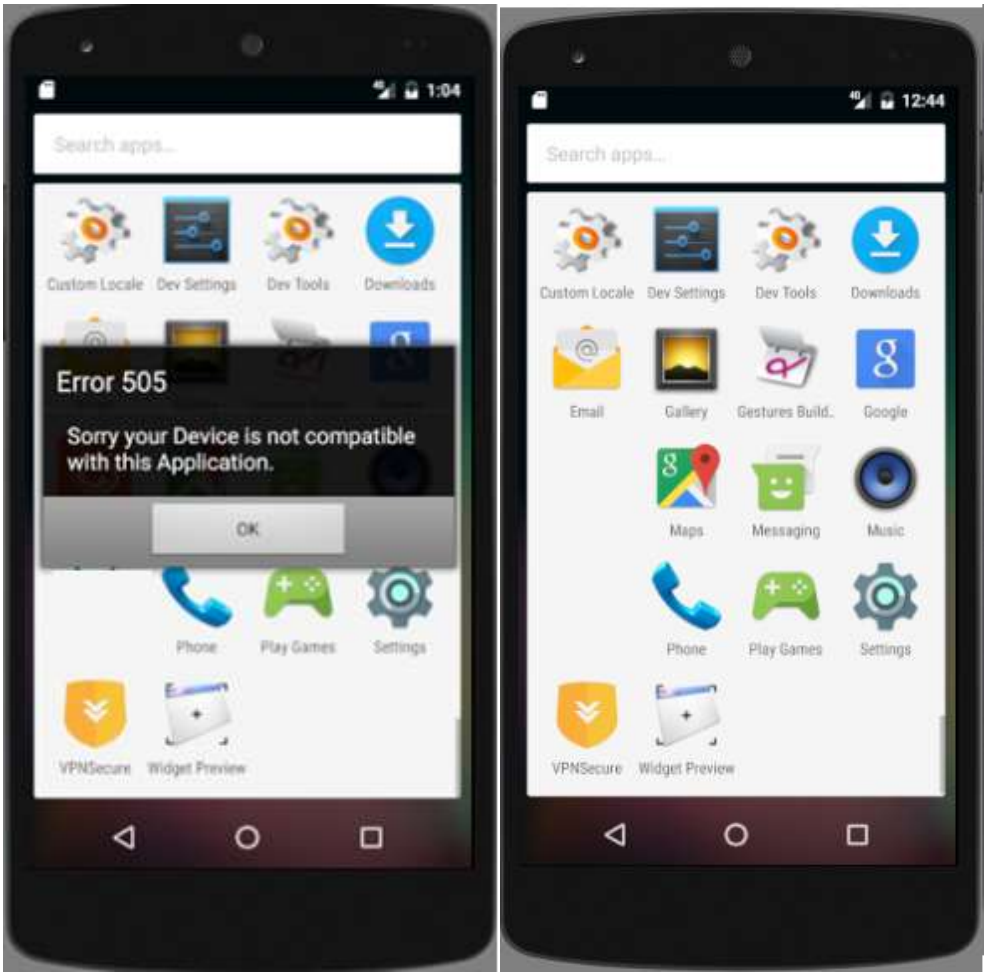
اوایل دی‌ماه ۱۳۹۶، لینک یک برنامه اندرویدی از طریق پیامک در مقیاس وسیع توسط کاربران تلفن همراه کشور دریافت شد. در این مستند به بررسی ماهیت و چگونگی عملکرد این برنامه می‌پردازیم.

مشخصات فایل مورد بررسی عبارتند از:

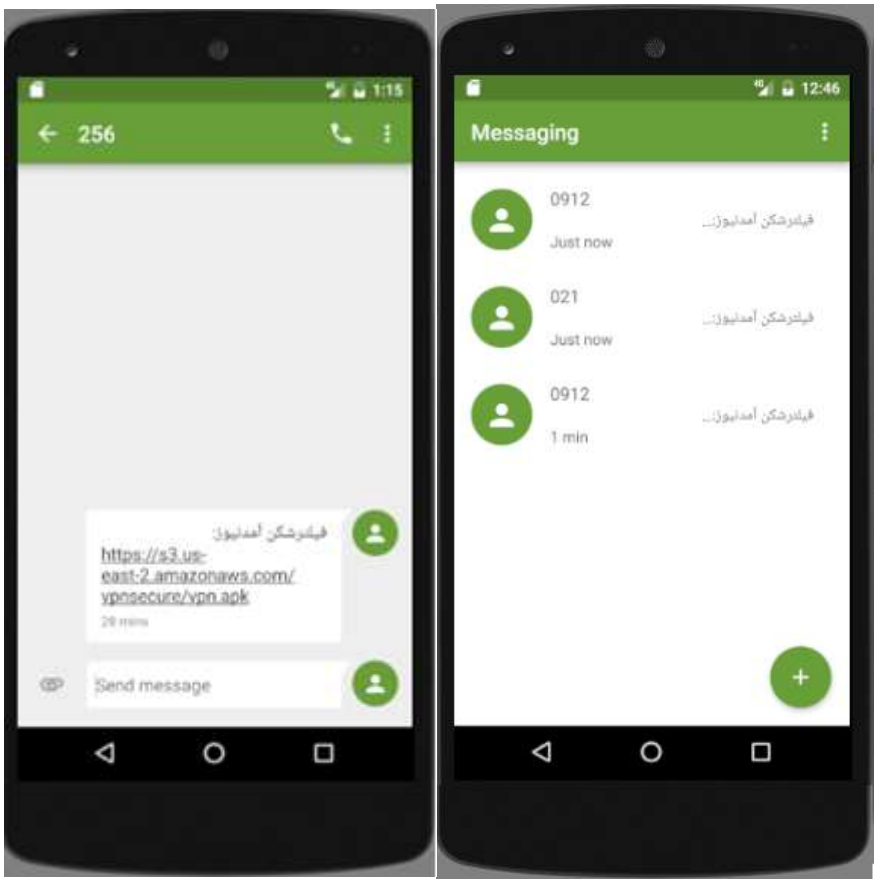
File Name: vpn.apk
Size: 336.0 kB
MD5: 562e02130fcbdea7cc0d2a527aee6c05

اجرای برنامه

اجرای این برنامه در محیط آزمایشگاهی صورت گرفت. پس از نصب، برنامه‌ای با عنوان VPNSecure به فهرست برنامه‌ها اضافه می‌گردد. با اجرای این برنامه پیغام خطایی مبنی بر عدم سازگاری برنامه با این تلفن همراه توسط برنامه نمایش داده می‌شود:

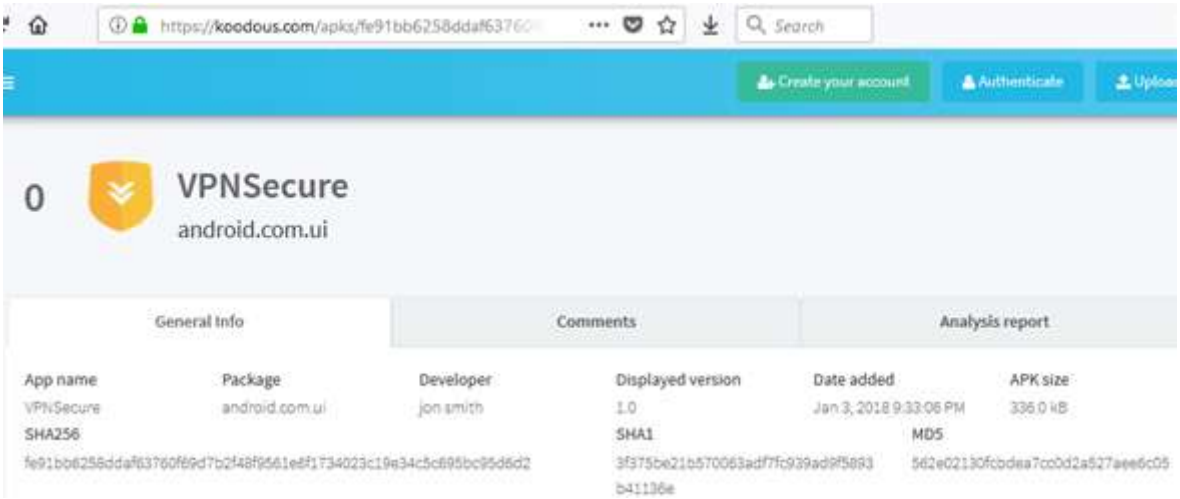


بطور همزمان بدون دخالت کاربر، به تمام مخاطبین کاربر پیامکی حاوی لینک دریافت این فایل ارسال گشته و سپس همه مخاطبین حذف می‌گردند. در همین زمان به مدت ۶۰ ثانیه حالت لرزش تلفن بصورت پیوسته فعال می‌گردد. پس از آن نیز صفحه‌ای حاوی لوگوی آمدنیوز هر چندثانیه یکبار بر روی صفحه نمایش داده می‌شود.



تحلیل داینامیک

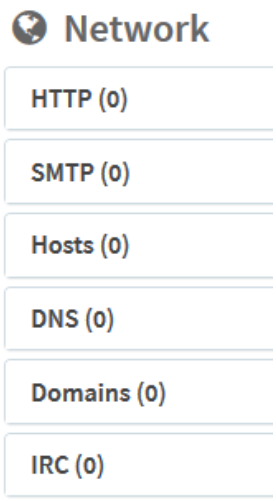
بمنظور بررسی دقیق‌تر برنامه نتایج اجرای آن در یکی از سندباکس‌های آنلاین مشاهده‌شد. جستجو نشان داد این برنامه در تاریخ ۱۵ دی‌ماه بر روی سندباکس آنلاین koodous.com بارگزاری شده است:



مهمترین نکات قابل برداشت در نتایج این تحلیل داینامیک در جدول زیر ارائه شده‌اند:

Activities	• android.com.ui.MainActivity (Main Activity) • android.com.ui.AdActivity
Receivers	• android.com.ui.receiver.MyBroadcastReceiver
Urls	• https://s3.us-east-2.amazonaws.com/vpnsecure/vpn.apk
Services	• android.com.ui.service.MyService
Permissions	• android.permission.WRITE_CONTACTS • android.permission.SEND_SMS • android.permission.RECEIVE_BOOT_COMPLETED • android.permission.INTERNET • android.permission.VIBRATE • android.permission.READ_CONTACTS

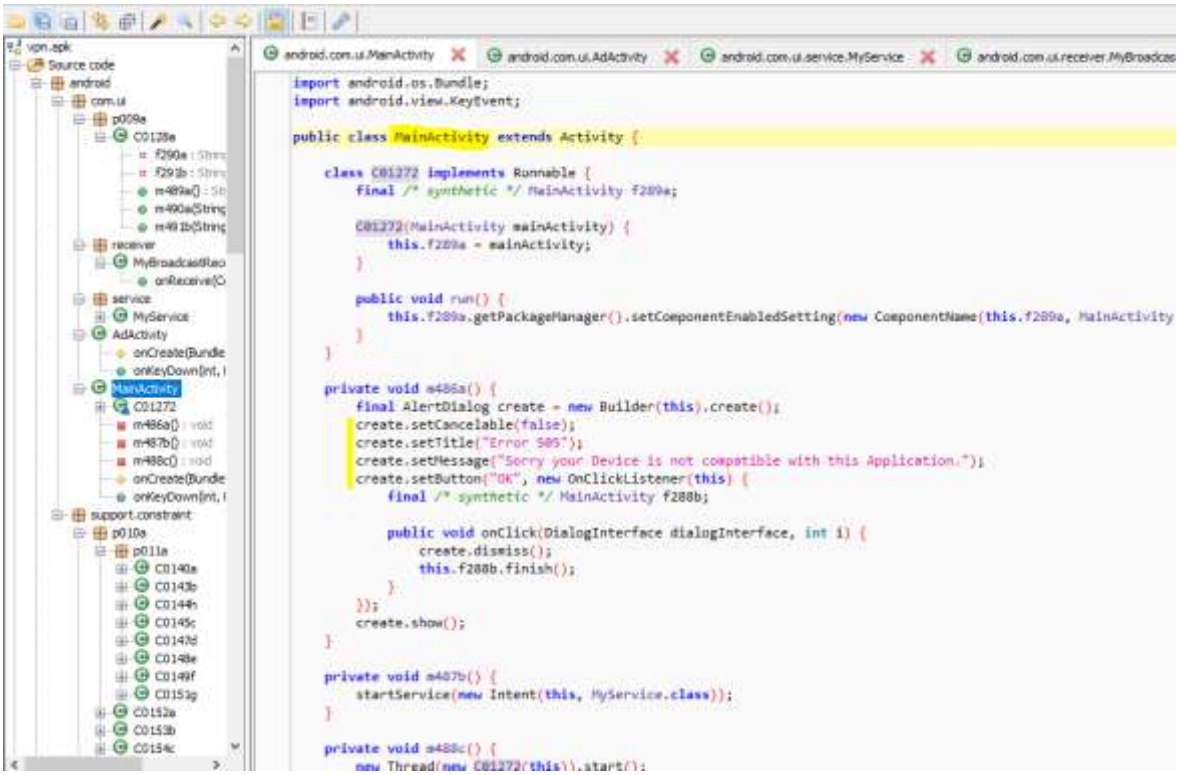
هچنین نتایج تحلیل این سامانه نشان می‌دهد که برنامه تحت بررسی هیچ فعالیت شبکه‌ای ندارد:

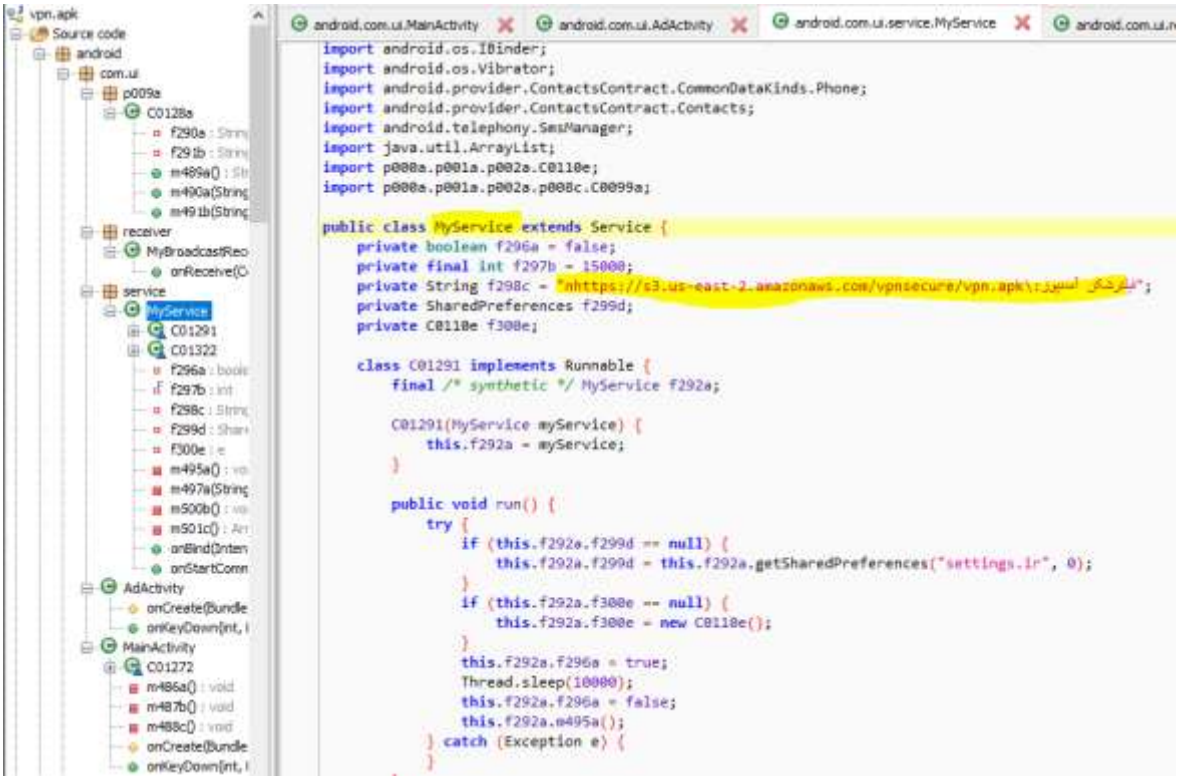


تحلیل استاتیک (تحلیل کد)

مهندسی معکوس برنامه و مطالعه کدهای آن ضمن تایید نتایج تحلیل داینامیک، نتایج زیر را بدست می‌دهد:

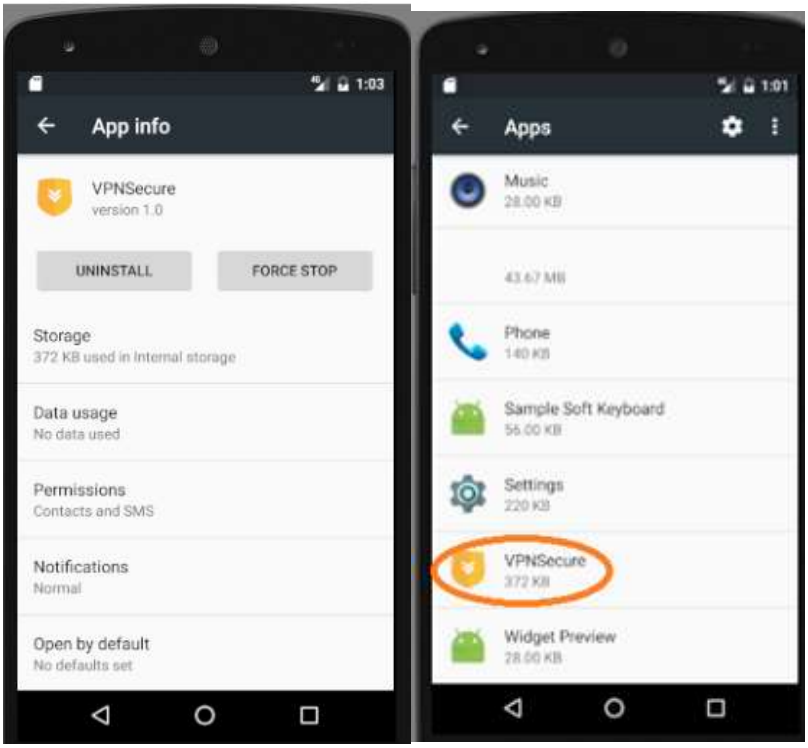
- عملکرد برنامه در یک سرویس و دو صفحه (activity) خلاصه می‌گردد.
- هیچ رفتار و قابلیت دیگری اضافه بر موارد شرح داده شده در برنامه پیاده‌سازی نشده است.
- عملکرد ارسال لینک به مخاطبین از طریق پیامک، فعالسازی لرزش و حذف مخاطبین در سرویس MyService پیاده‌سازی شده است.





نحوه پاکسازی

در صورت آلودگی به این بدافزار، کافی است از طریق Settings قسمت apps، نسبت به متوقف سازی و حذف اپلیکیشن با عنوان VPNsecure افدام نمایید:



خلاصه نتایج

- این اپلیکیشن پس از اجرا، به تمام مخاطبین کاربر، پیامکی حاوی لینک دریافت این فایل را ارسال کرده و سپس همه مخاطبین را حذف می‌کند.
- اپلیکیشن ساختار و طراحی ابتدایی و ساده دارد.
- غیر از عملکرد شرح داده شده، هیچ قابلیت و عملکرد دیگری در این اپلیکیشن وجود ندارد.
- هیچ گونه ارتباط اینترنتی، سرقت اطلاعات و تماس با سرور کنترلی وجود ندارد.
- لینک ارسالی توسط پیامک بر بستر سرویس ابری شرکت آمازون بوده است که در حال حاضر غیرفعال شده است.