

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 دی ماه 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 می پردازیم.

مشخصات فایل مورد بررسی عبارتند از:

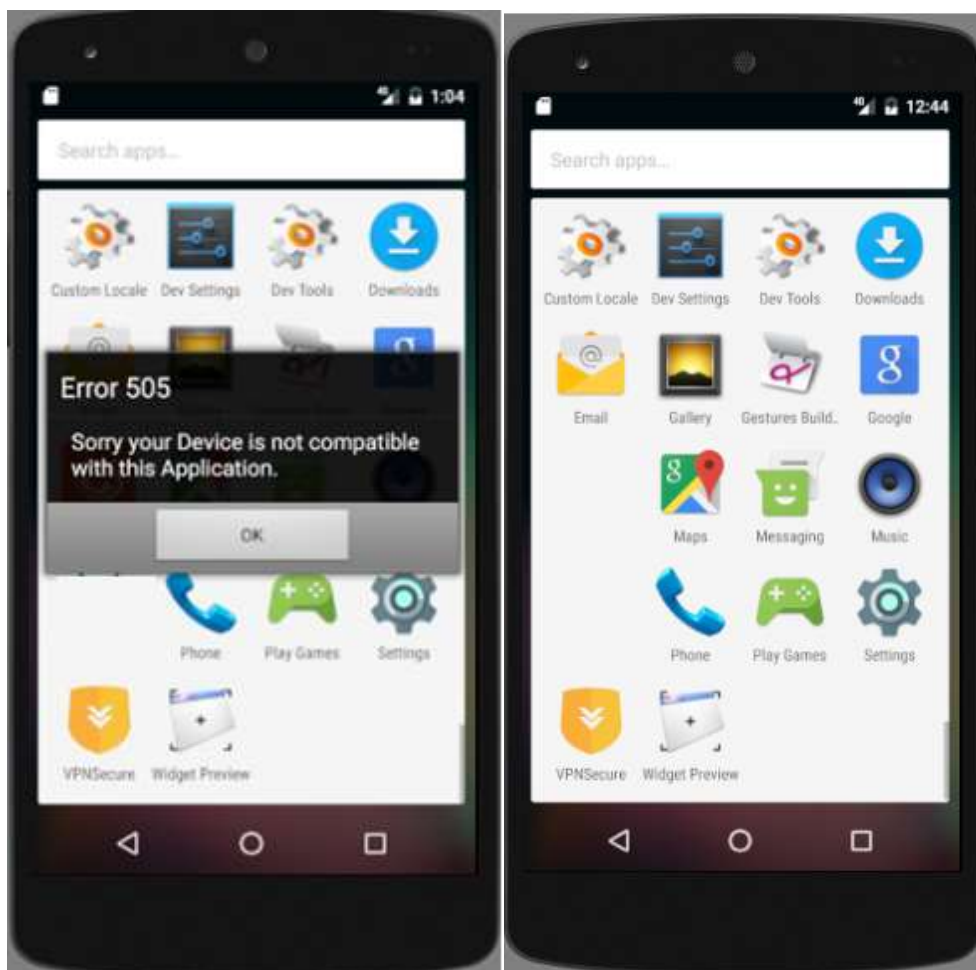
File Name: vpn.apk

Size: 336.0 kB

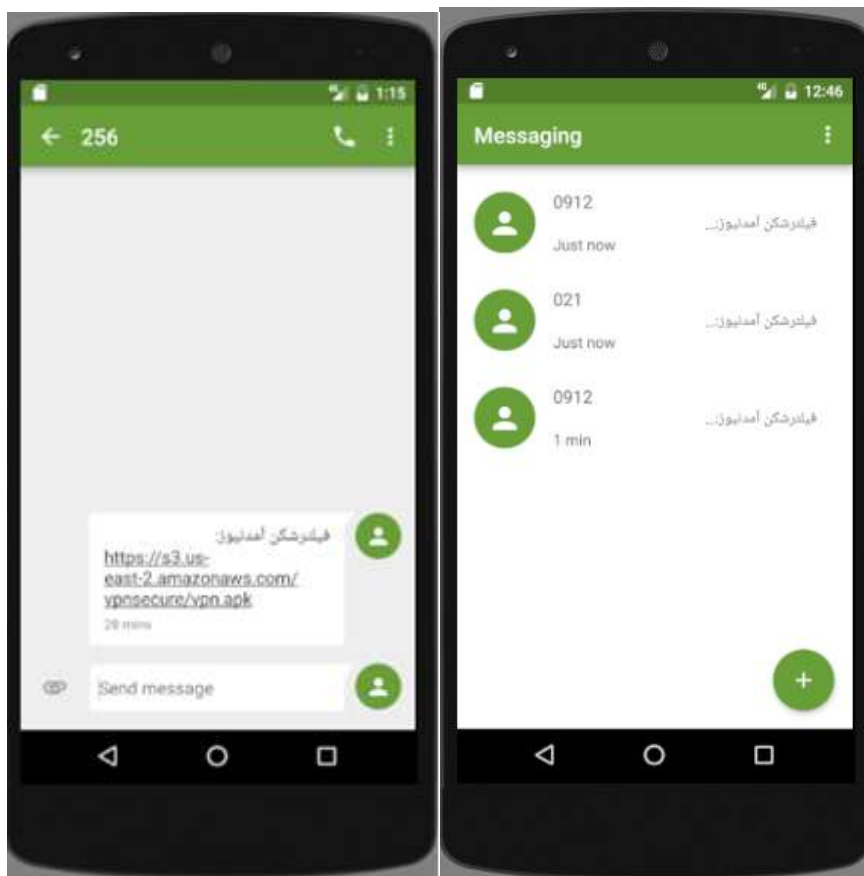
MD5: 562e02130fcbdea7cc0d2a527aee6c05

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 می گردند. در همین زمان به مدت ۶۰ ثانیه حالت لرزش تلفن بصورت پیوسته فعال می گردد. پس از آن نیز صفحه ای حاوی لوگوی آمدنیوز هر چندثانیه یکبار بر روی صفحه نمایش داده می شود.



تحلیل داینامیک

بمنظور بررسی دقیق تر برنامه نتایج اجرای آن در یکی از سندباکس های آنلاین مشاهده شد. جستجو نشان داد این برنامه در تاریخ ۱۵ دی ماه بر روی سندباکس آنلاین koodous.com بارگزاری شده است:

General Info		Comments		Analysis report	
App name	Package	Developer	Displayed version	Date added	APK size
VPNSecure	android.com.ui	jon.smith	1.0	Jan 3, 2018 9:33:06 PM	336.0 kB
SHA256	SHA1	MDS			
fe91bb6258dda63760f69d7bc248f9561e8f1734023c19e34c5c695bc95d6d2	3f375be21b570063adf7fc939ad9f5893b41136e	562e02130fcbdea7cc0d2a527aee6c05			

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

Activities	<ul style="list-style-type: none"> • android.com.ui.MainActivity (Main Activity) • android.com.ui.AdActivity
Receivers	<ul style="list-style-type: none"> • android.com.ui.receiver.MyBroadcastReceiver
Urls	<ul style="list-style-type: none"> • https://s3.us-east-2.amazonaws.com/vpnsecure/vpn.apk
Services	<ul style="list-style-type: none"> • android.com.ui.service.MyService
Permissions	<ul style="list-style-type: none"> • android.permission.WRITE_CONTACTS • android.permission.SEND_SMS • android.permission.RECEIVE_BOOT_COMPLETED • android.permission.INTERNET • android.permission.VIBRATE • android.permission.READ_CONTACTS

همچنین نتایج تحلیل این سامانه نشان می دهد که برنامه تحت بررسی هیچ فعالیت شبکه ای ندارد:

Network

HTTP (0)

SMTP (0)

Hosts (0)

DNS (0)

Domains (0)

IRC (0)

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.

```

import android.os.Bundle;
import android.view.KeyEvent;

public class MainActivity extends Activity {

    class C01272 implements Runnable {
        final /* synthetic */ MainActivity f289a;

        C01272(MainActivity MainActivity) {
            this.f289a = MainActivity;
        }

        public void run() {
            this.f289a.getPackageManager().setComponentEnabledSetting(new ComponentName(this.f289a, MainActivity
        )
    }

    private void m486a() {
        final AlertDialog create = new Builder(this).create();
        create.setCancelable(false);
        create.setTitle("Error 505");
        create.setMessage("Sorry your Device is not compatible with this Application.");
        create.setButton("OK", new OnClickListener(this) {
            final /* synthetic */ MainActivity f288b;

            public void onClick(DialogInterface dialogInterface, int i) {
                create.dismiss();
                this.f288b.finish();
            }
        });
        create.show();
    }

    private void m487b() {
        startService(new Intent(this, MyService.class));
    }

    private void m488c() {
        new Thread(new C01272(this)).start();
    }
}
    
```

```

import android.os.IBinder;
import android.os.Vibrator;
import android.provider.ContactsContract.CommonDataKinds.Phone;
import android.provider.ContactsContract.Contacts;
import android.telephony.SmsManager;
import java.util.ArrayList;
import p008a.p001a.p002a.C0110e;
import p008a.p001a.p002a.p008c.C0099a;

public class MyService extends Service {
    private boolean f296a = false;
    private final int f297b = 15000;
    private String f298c = "https://e3.us-east-2.amazonaws.com/vpnsecure/vpn.apk";
    private SharedPreferences f299d;
    private C0110e f300e;

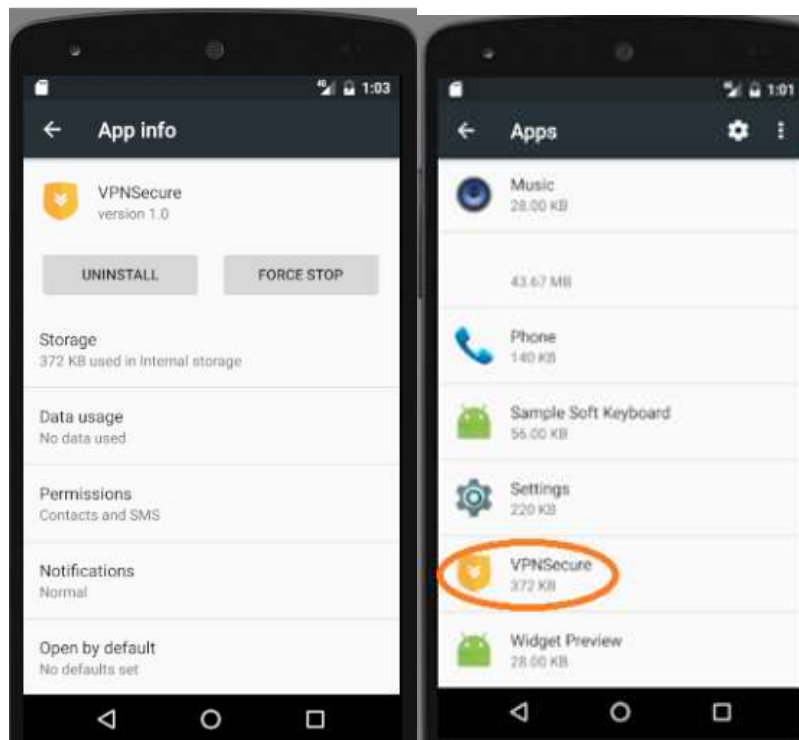
    class C01291 implements Runnable {
        final /* synthetic */ MyService f292a;

        C01291(MyService myService) {
            this.f292a = myService;
        }

        public void run() {
            try {
                if (this.f292a.f299d == null) {
                    this.f292a.f299d = this.f292a.getSharedPreferences("settings.ln", 0);
                }
                if (this.f292a.f300e == null) {
                    this.f292a.f300e = new C0110e();
                }
                this.f292a.f296a = true;
                Thread.sleep(10000);
                this.f292a.f296a = false;
                this.f292a.m495a();
            } catch (Exception e) {}
        }
    }
}
    
```

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 اقدام 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.