安卓恶意app检测现状

赵帅
Zhaoshuai(at)mobeisecurity.com

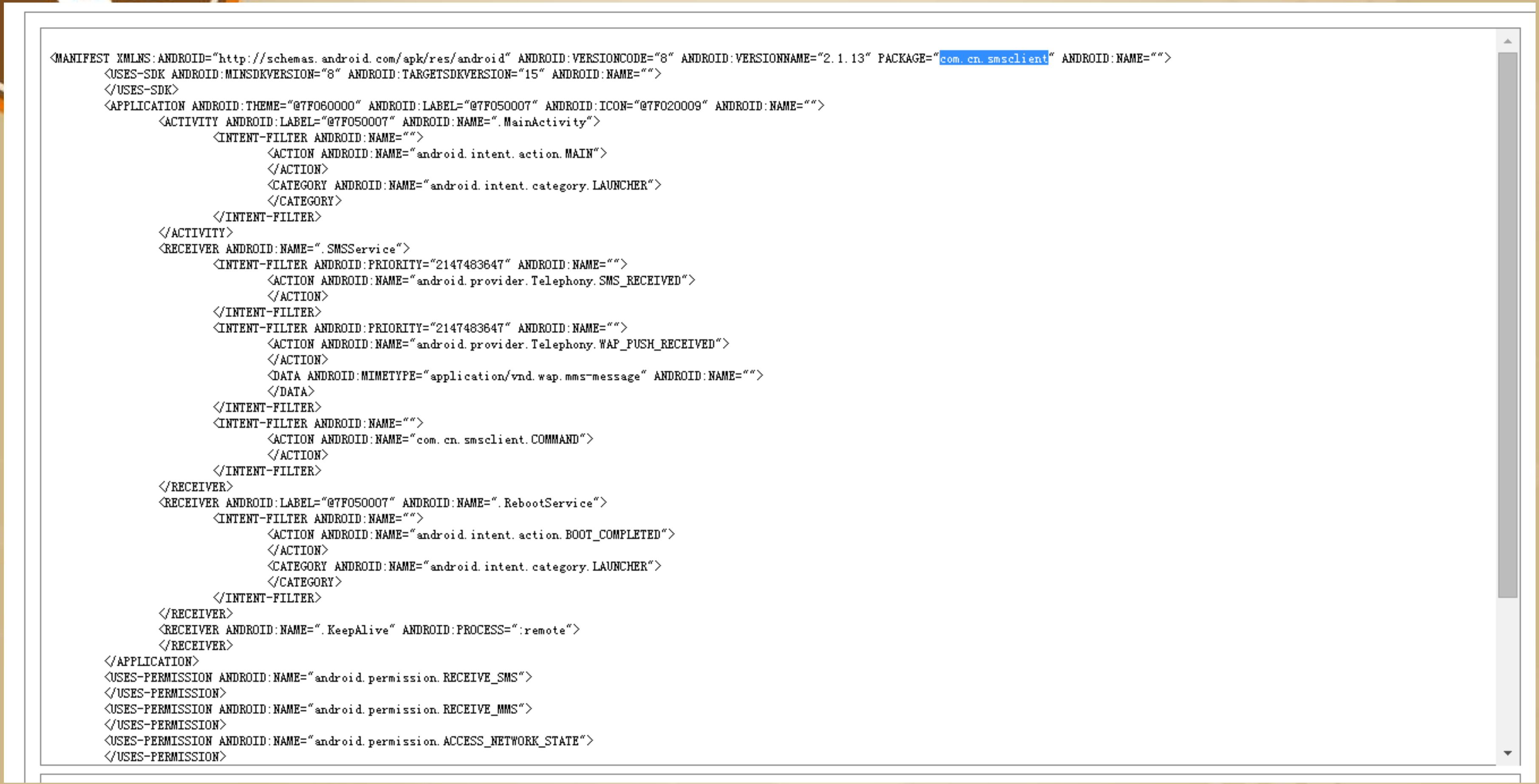
Apr 16,17 2014 Shanghai

{xKungfoo 2014}

Agenda

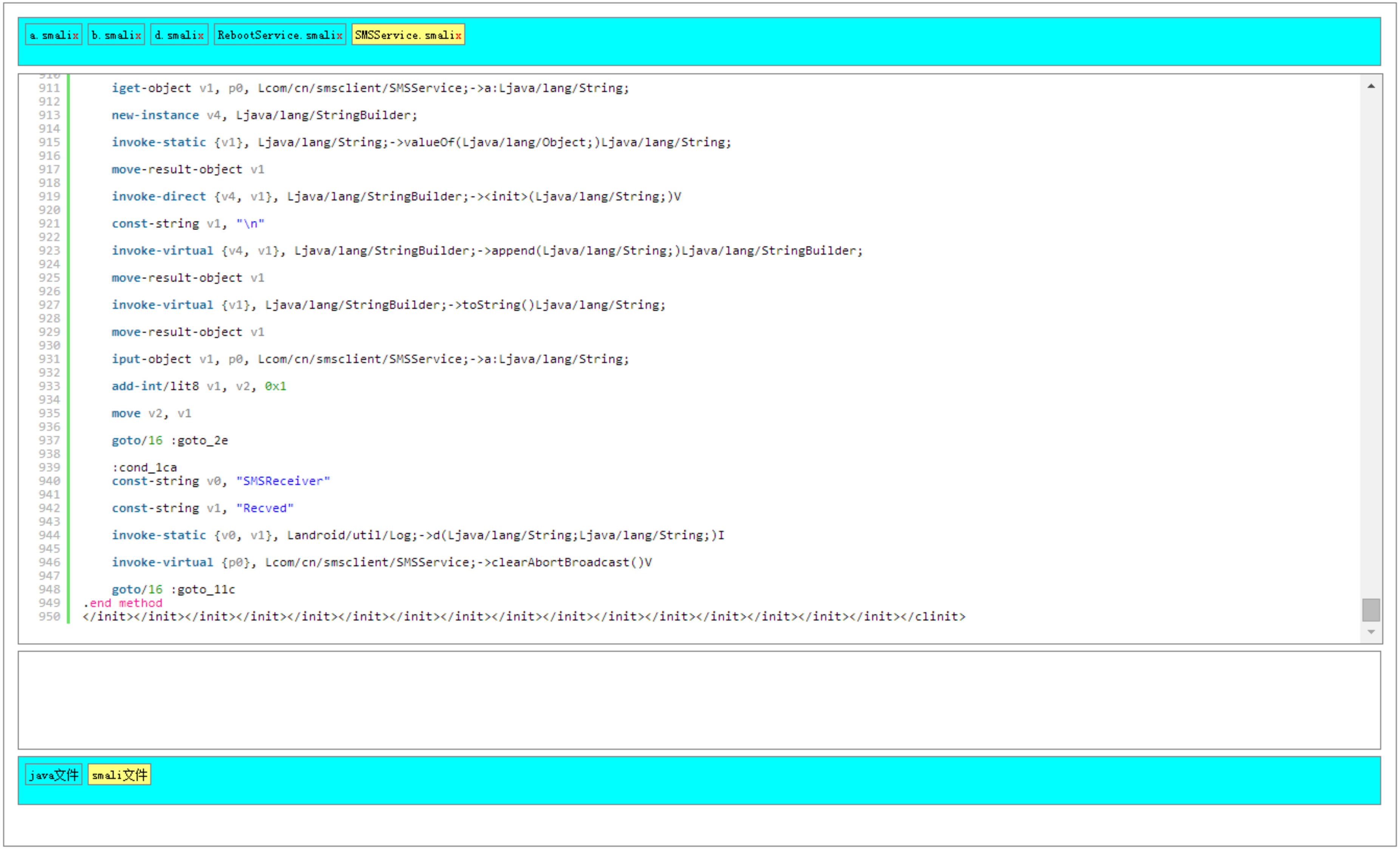
- 静态检测现状
- 动态检测现状
- 检测方法展望

静态特征



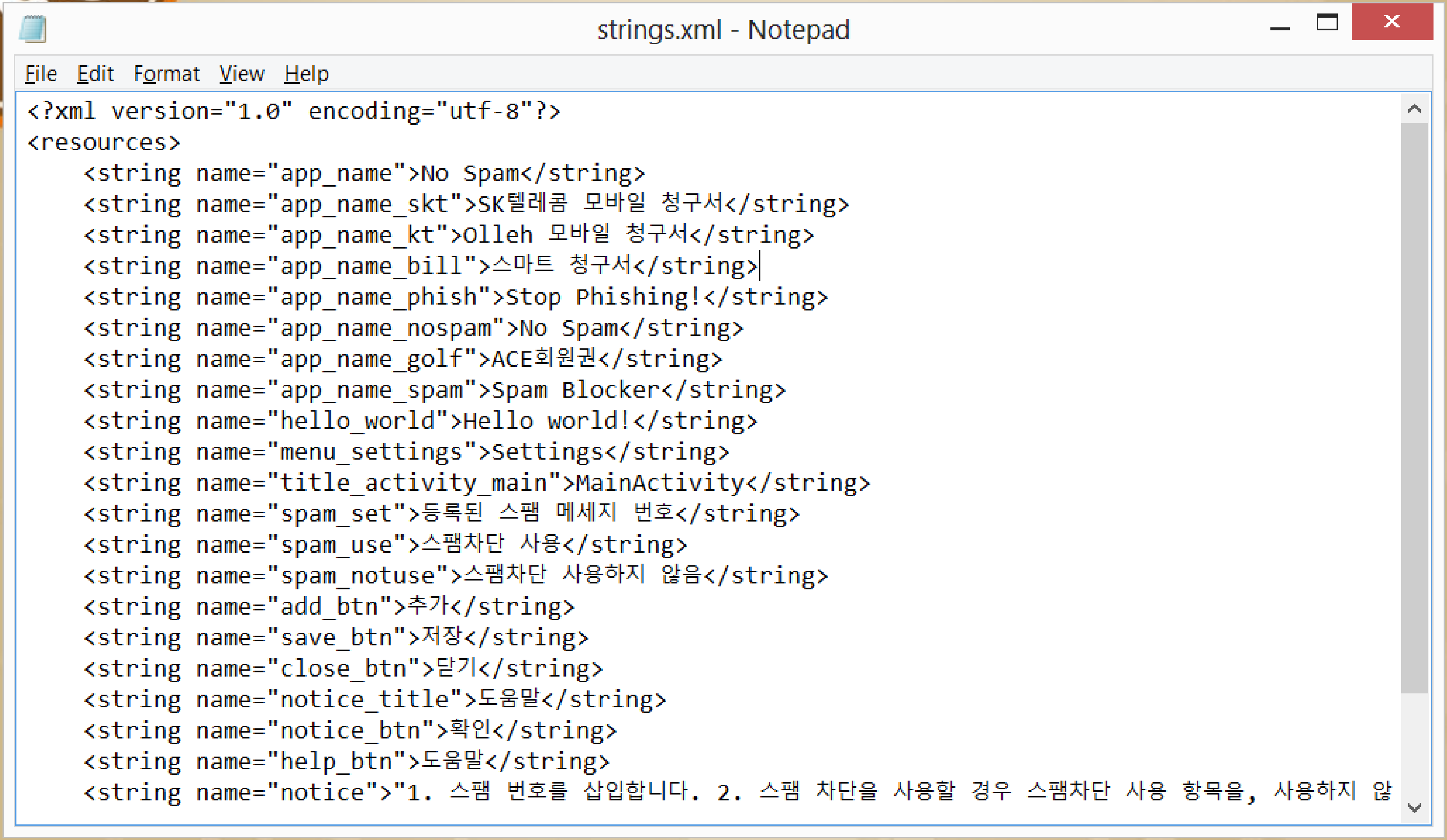
```
<MANIFEST XMLNS:ANDROID=“http://schemas.android.com/apk/res/android” ANDROID:VERSIONCODE=“8” ANDROID:VERSIONNAME=“2.1.13” PACKAGE=“com.cn.smsclient” ANDROID:NAME=“”>
        <USES-SDK ANDROID:MINSDKVERSION=“8” ANDROID:TARGETSDKVERSION=“15” ANDROID:NAME=“”>
        </USES-SDK>
        <APPLICATION ANDROID:THEME=“@7F060000” ANDROID:LABEL=“@7F050007” ANDROID:ICON=“@7F020009” ANDROID:NAME=“”>
                <ACTIVITY ANDROID:LABEL=“@7F050007” ANDROID:NAME=“.MainActivity”>
                        <INTENT-FILTER ANDROID:NAME=“”>
                                <ACTION ANDROID:NAME=“android.intent.action.MAIN”>
                                </ACTION>
                                <CATEGORY ANDROID:NAME=“android.intent.category.LAUNCHER”>
                                </CATEGORY>
                        </INTENT-FILTER>
                </ACTIVITY>
                <RECEIVER ANDROID:NAME=“.SMSService”>
                        <INTENT-FILTER ANDROID:PRIORITY=“2147483647” ANDROID:NAME=“”>
                                <ACTION ANDROID:NAME=“android.provider.Telephony.SMS_RECEIVED”>
                                </ACTION>
                        </INTENT-FILTER>
                        <INTENT-FILTER ANDROID:PRIORITY=“2147483647” ANDROID:NAME=“”>
                                <ACTION ANDROID:NAME=“android.provider.Telephony.WAP_PUSH_RECEIVED”>
                                </ACTION>
                                <DATA ANDROID:MIMETYPE=“application/vnd.wap.mms-message” ANDROID:NAME=“”>
                                </DATA>
                        </INTENT-FILTER>
                        <INTENT-FILTER ANDROID:NAME=“”>
                                <ACTION ANDROID:NAME=“com.cn.smsclient.COMMAND”>
                                </ACTION>
                        </INTENT-FILTER>
                </RECEIVER>
                <RECEIVER ANDROID:LABEL=“@7F050007” ANDROID:NAME=“.RebootService”>
                        <INTENT-FILTER ANDROID:NAME=“”>
                                <ACTION ANDROID:NAME=“android.intent.action.BOOT_COMPLETED”>
                                </ACTION>
                                <CATEGORY ANDROID:NAME=“android.intent.category.LAUNCHER”>
                                </CATEGORY>
                        </INTENT-FILTER>
                </RECEIVER>
                <RECEIVER ANDROID:NAME=“.KeepAlive” ANDROID:PROCESS=“:remote”>
                </RECEIVER>
        </APPLICATION>
        <USES-PERMISSION ANDROID:NAME=“android.permission.RECEIVE_SMS”>
        </USES-PERMISSION>
        <USES-PERMISSION ANDROID:NAME=“android.permission.RECEIVE_MMS”>
        </USES-PERMISSION>
        <USES-PERMISSION ANDROID:NAME=“android.permission.ACCESS_NETWORK_STATE”>
        </USES-PERMISSION>
```

静态特征



```
    iget-object v1, p0, Lcom/cn/smsclient/SMSService;->a:Ljava/lang/String;

    new-instance v4, Ljava/lang/StringBuilder;

    invoke-static {v1}, Ljava/lang/String;->valueOf(Ljava/lang/Object;)Ljava/lang/String;

    move-result-object v1

    invoke-direct {v4, v1}, Ljava/lang/StringBuilder;-><init>(Ljava/lang/String;)V

    const-string v1, "\n"

    invoke-virtual {v4, v1}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;

    move-result-object v1

    invoke-virtual {v1}, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;

    move-result-object v1

    iput-object v1, p0, Lcom/cn/smsclient/SMSService;->a:Ljava/lang/String;

    add-int/lit8 v1, v2, 0x1

    move v2, v1

    goto/16 :goto_2e

    :cond_1ca
    const-string v0, "SMSReceiver"

    const-string v1, "Recved"

    invoke-static {v0, v1}, Landroid/util/Log;->d(Ljava/lang/String;Ljava/lang/String;)I

    invoke-virtual {p0}, Lcom/cn/smsclient/SMSService;->clearAbortBroadcast()V

    goto/16 :goto_11c
.end method
</init></init></init></init></init></init></init></init></init></init></init></init></init></init></init></init></clinit>
```

静态特征



```
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="app_name">No Spam</string>
    <string name="app_name_skt">SK텔레콤 모바일 청구서</string>
    <string name="app_name_kt">Olleh 모바일 청구서</string>
    <string name="app_name_bill">스마트 청구서</string>
    <string name="app_name_phish">Stop Phishing!</string>
    <string name="app_name_nospam">No Spam</string>
    <string name="app_name_golf">ACE회원권</string>
    <string name="app_name_spam">Spam Blocker</string>
    <string name="hello_world">Hello world!</string>
    <string name="menu_settings">Settings</string>
    <string name="title_activity_main">MainActivity</string>
    <string name="spam_set">등록된 스팸 메세지 번호</string>
    <string name="spam_use">스팸차단 사용</string>
    <string name="spam_notuse">스팸차단 사용하지 않음</string>
    <string name="add_btn">추가</string>
    <string name="save_btn">저장</string>
    <string name="close_btn">닫기</string>
    <string name="notice_title">도움말</string>
    <string name="notice_btn">확인</string>
    <string name="help_btn">도움말</string>
    <string name="notice">"1. 스팸 번호를 삽입합니다. 2. 스팸 차단을 사용할 경우 스팸차단 사용 항목을, 사용하지 않
```

静态特征

- MD5
- 指令中的字符串
- 指令
- 方法调用
- AndroidManifest.xml
- 其他配置文件

可测试目标	本次测试
更改MD5	Y
更改代码中的字符串	Y
更改指令	部分
更改方法调用	部分
更改AndroidManifest.xml	Y
更改其他配置文件	N

测试用例

- com.cn.smsclient, MD5: 12cbedc185d82c61150d8c9ee38a9fcb
- VirusTotal：
  - Detection ratio: 35 / 51
  - https://www.virustotal.com/en/file/48e71bfdd6a88594d5b04ccefac6279ab6898b0302ac8c937f4b0c8bb358e6bb/analysis/1397455551/
- andrototal：
  - Detections： 7 / 7
  - http://andrototal.org/sample-analysis/hash/48e71bfdd6a88594d5b04ccefac6279ab6898b0302ac8c937f4b0c8bb358e6bb

静态测试

测试过程
↗更改MD5
更改代码中的字符串
更改指令
更改方法调用
更改AndroidManifest.xml
更改其他配置文件

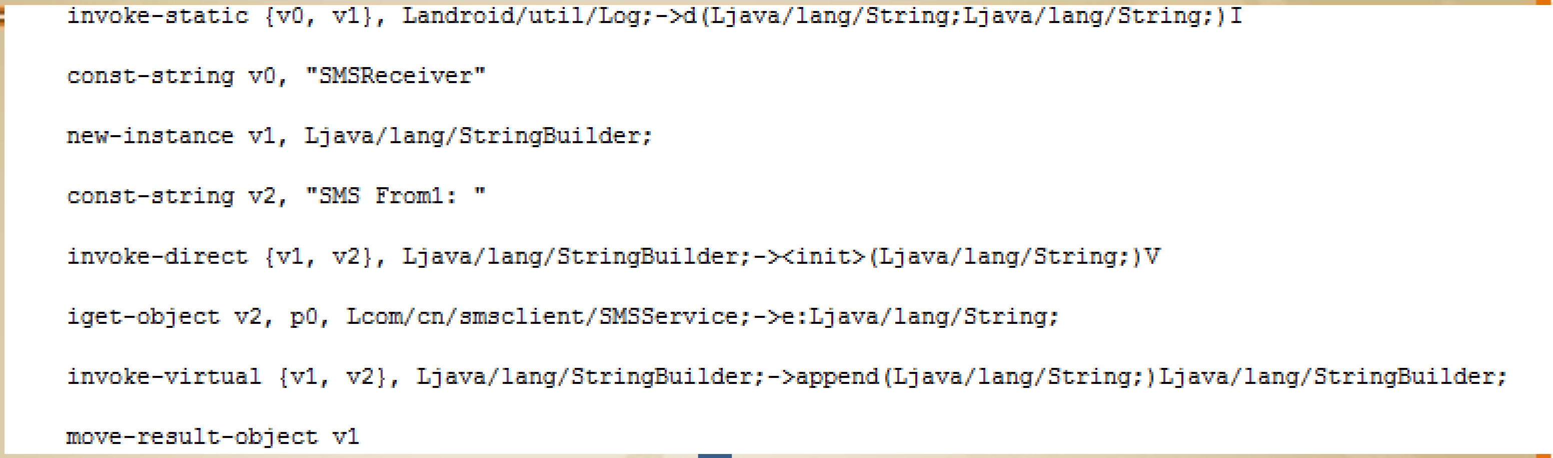
- VirusTotal：
  - Detection ratio: 22 / 51 (减少37%)
  - https://www.virustotal.com/en/file/231c9fbec215adc2cb3eabff802a95f3cd7bea1c606df12ab6b1b44d3afff21d/analysis/1397456348/
- Andrototal：
  - Detections： 0 / 7
  - http://andrototal.org/sample-analysis/hash/231c9fbec215adc2cb3eabff802a95f3cd7bea1c606df12ab6b1b44d3afff21d

静态测试

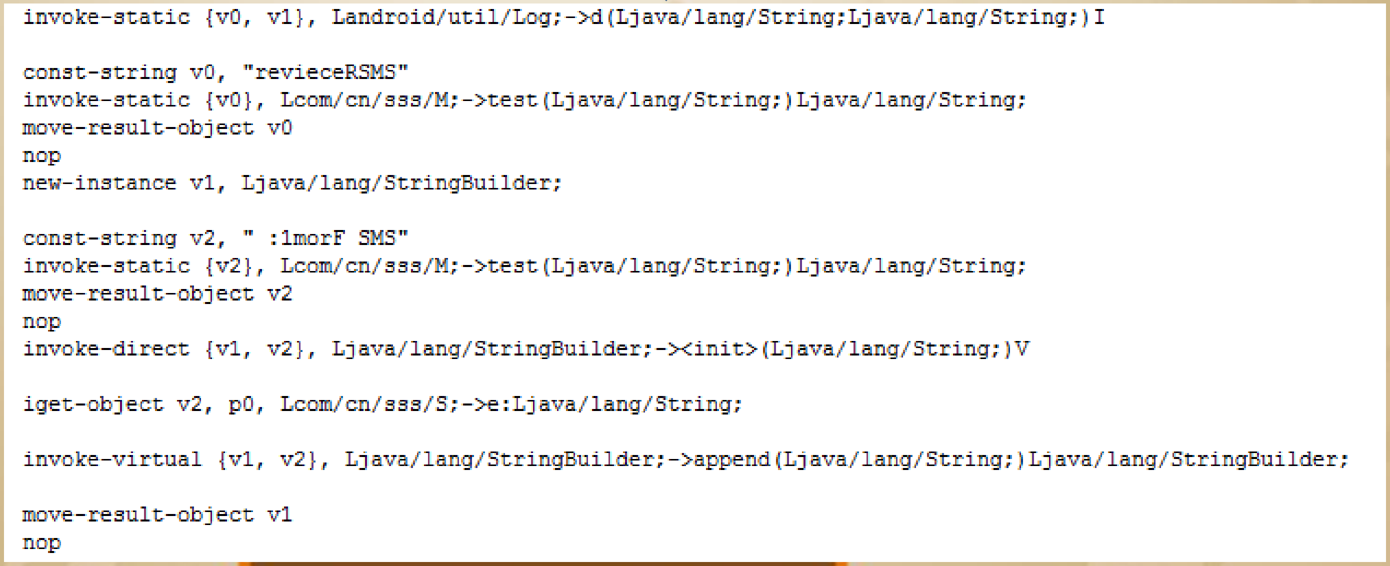
测试过程
↗更改MD5
↗更改代码中的字符串
更改指令
更改方法调用
更改AndroidManifest.xml
更改其他配置文件

- VirusTotal：
  - Detection ratio: 9 / 51 (减少74%)
  - https://www.virustotal.com/en/file/f8fb1cd7492a297e47f2993a6cbab13f3fdce54daaa4bb61ccf8abe0f4879ff6/analysis/1397459819/
- Andrototal：
  - Detections： 0 / 7
  - http://andrototal.org/scan/result/set/42144

静态测试



```
invoke-static {v0, v1}, Landroid/util/Log;->d(Ljava/lang/String;Ljava/lang/String;)I

const-string v0, "SMSReceiver"

new-instance v1, Ljava/lang/StringBuilder;

const-string v2, "SMS From1: "

invoke-direct {v1, v2}, Ljava/lang/StringBuilder;-><init>(Ljava/lang/String;)V

iget-object v2, p0, Lcom/cn/smsclient/SMSService;->e:Ljava/lang/String;

invoke-virtual {v1, v2}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;

move-result-object v1
```



```
invoke-static {v0, v1}, Landroid/util/Log;->d(Ljava/lang/String;Ljava/lang/String;)I

const-string v0, "revieceRSMS"
invoke-static {v0}, Lcom/cn/sss/M;->test(Ljava/lang/String;)Ljava/lang/String;
move-result-object v0
nop
new-instance v1, Ljava/lang/StringBuilder;

const-string v2, " :1morF SMS"
invoke-static {v2}, Lcom/cn/sss/M;->test(Ljava/lang/String;)Ljava/lang/String;
move-result-object v2
nop
invoke-direct {v1, v2}, Ljava/lang/StringBuilder;-><init>(Ljava/lang/String;)V

iget-object v2, p0, Lcom/cn/sss/S;->e:Ljava/lang/String;

invoke-virtual {v1, v2}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;

move-result-object v1
nop
```

静态测试

测试过程
↗更改MD5
更改代码中的字符串
↗更改指令
更改方法调用
更改AndroidManifest.xml
更改其他配置文件

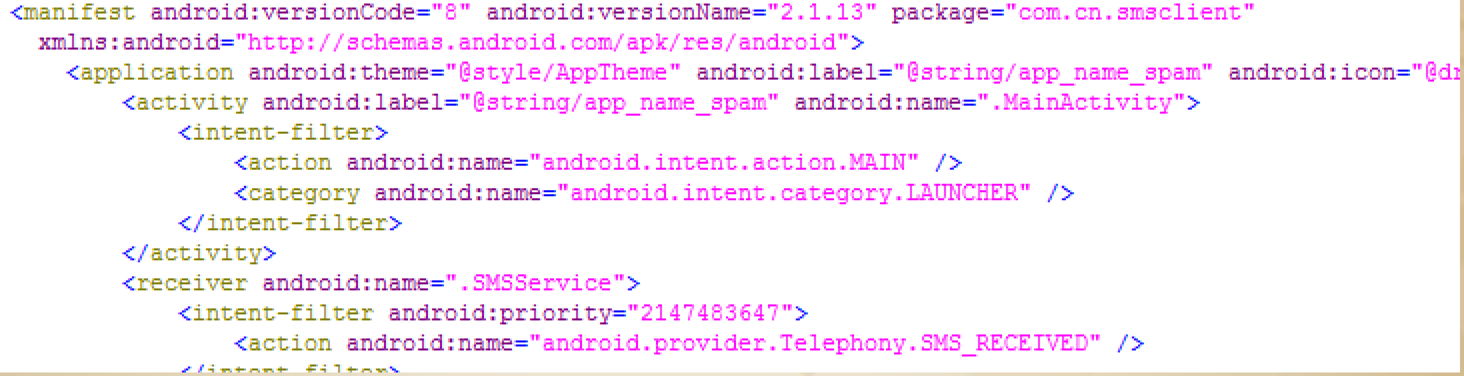
- VirusTotal：
  - Detection ratio: 14 / 51 (减少60%)
  - https://www.virustotal.com/en/file/230e20bdfdef4182625416334328192547a1fb2bb9c118a2ad0ced19af9cd2b6/analysis/1397460218/
- Andrototal：
  - Detections： 0 / 7
  - http://andrototal.org/sample-analysis/43628

静态测试

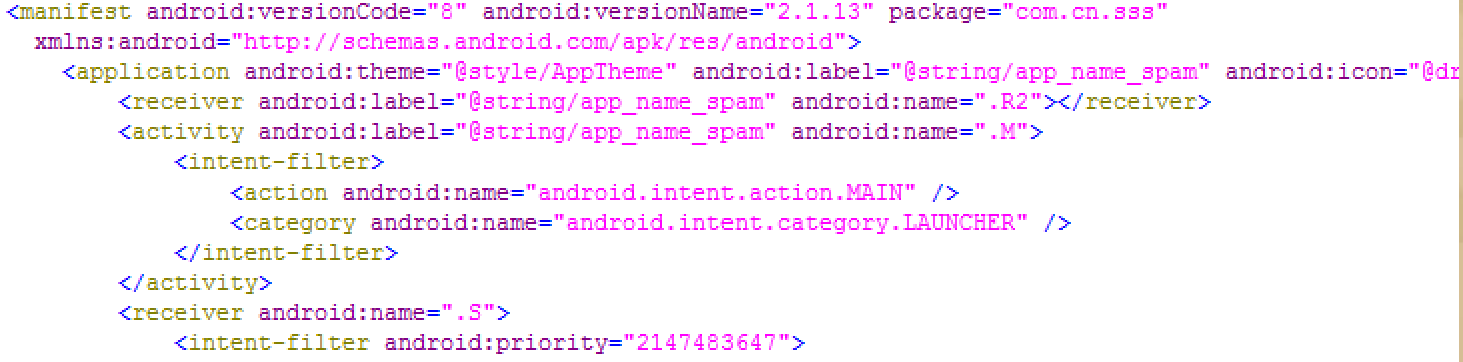
测试过程
↗更改MD5
更改代码中的字符串
更改指令
更改方法调用
↗更改 AndroidManifest.xml
更改其他配置文件

- VirusTotal：
  - Detection ratio: 12 / 51 (减少66%)
  - https://www.virustotal.com/en/file/2aa98231f60e0d9dbf9370c588cb567a4a46165c6786043fd46d92213151f1fa/analysis/1397460722/
- Andrototal：
  - Detections： 0 / 7
  - http://andrototal.org/sample-analysis/hash/2aa98231f60e0d9dbf9370c588cb567a4a46165c6786043fd46d92213151f1fa

静态测试



```
<manifest android:versionCode="8" android:versionName="2.1.13" package="com.cn.smsclient"
  xmlns:android="http://schemas.android.com/apk/res/android">
    <application android:theme="@style/AppTheme" android:label="@string/app_name_spam" android:icon="@dr
        <activity android:label="@string/app_name_spam" android:name=".MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
        <receiver android:name=".SMSService">
            <intent-filter android:priority="2147483647">
                <action android:name="android.provider.Telephony.SMS_RECEIVED" />
            </intent-filter>
```



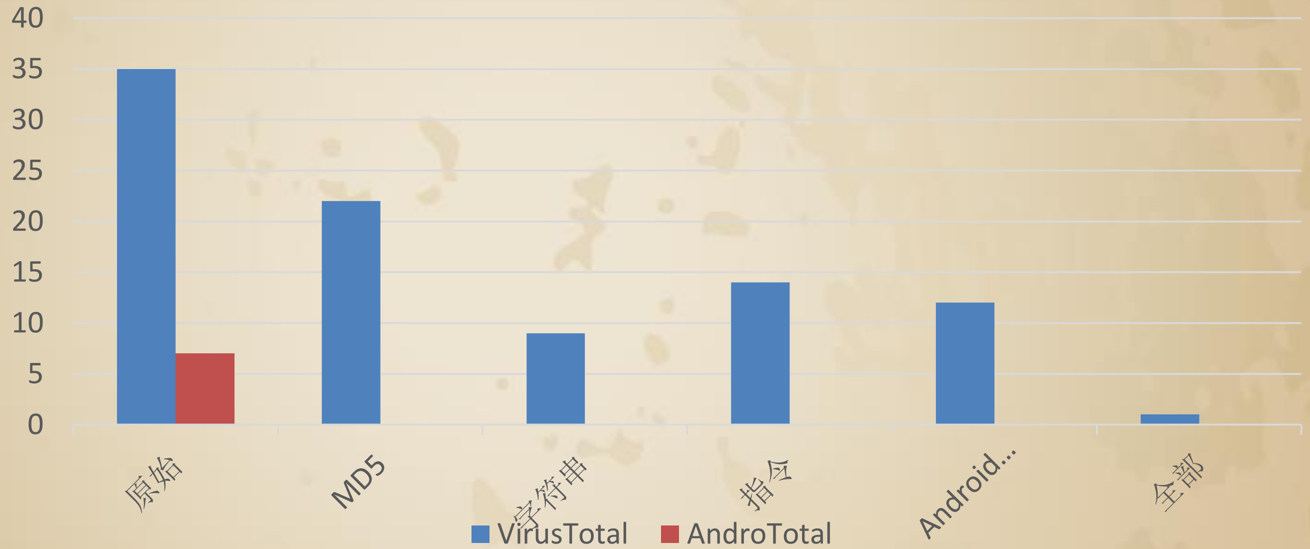
```
<manifest android:versionCode="8" android:versionName="2.1.13" package="com.cn.sss"
  xmlns:android="http://schemas.android.com/apk/res/android">
    <application android:theme="@style/AppTheme" android:label="@string/app_name_spam" android:icon="@dr
        <receiver android:label="@string/app_name_spam" android:name=".R2"></receiver>
        <activity android:label="@string/app_name_spam" android:name=".M">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
        <receiver android:name=".S">
            <intent-filter android:priority="2147483647">
```

静态测试

测试过程
↗更改MD5
↗更改代码中的字符串
↗更改指令
更改方法调用
↗更改AndroidManifest.xml
更改其他配置文件

- VirusTotal：
  - Detection ratio: 1 / 51
  - https://www.virustotal.com/en/file/bb177ede77e2ccdfa906a7ffedbae720d4e036593f61db265bf619a7a0e3adf5/analysis/1397461868/
- Andrototal：
  - Detections： 0 / 7
  - http://andrototal.org/scan/result/set/42147

静态测试



测试工具下载：http://www.mobeisecurity.com/morph.zip

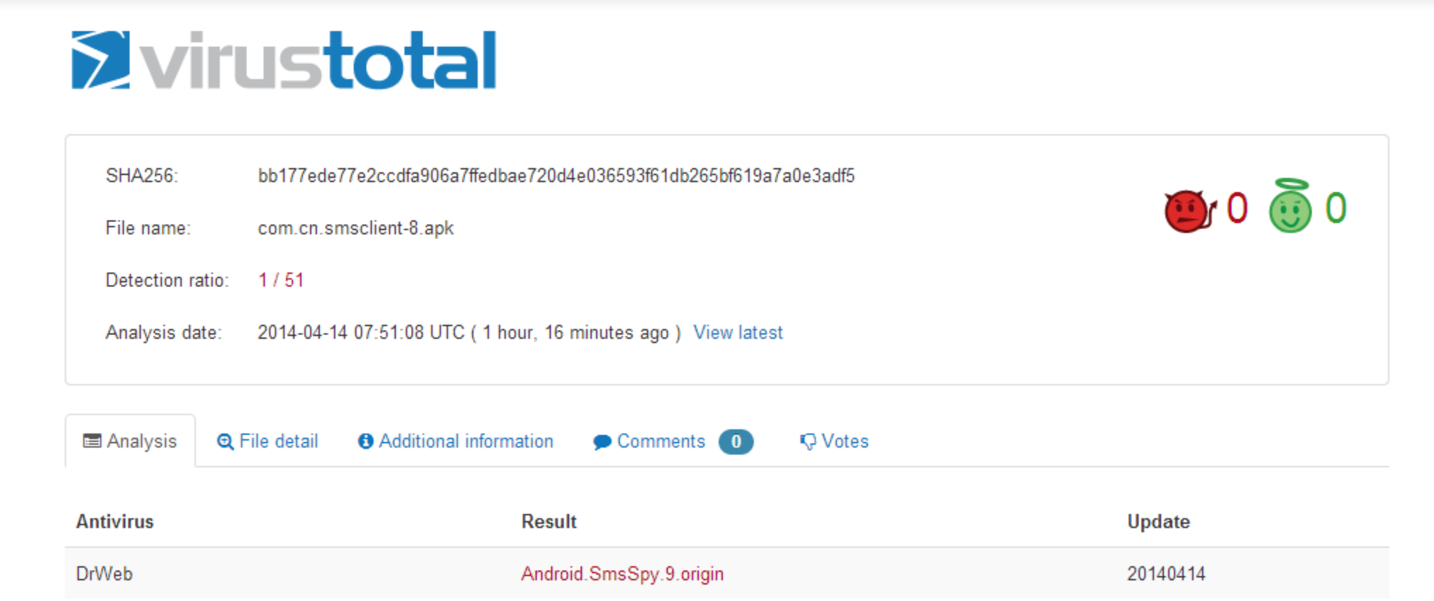
静态测试

测试过程
↗更改MD5
↗更改代码中的字符串
↗更改指令
更改方法调用
↗更改AndroidManifest.xml
更改其他配置文件

- com.tao.bao, MD5: 45dae1ee4ca1980c140cb5c9da2a7ed5
- VirusTotal：
  - Detection ratio: 2 / 51 (减少93%)
  - https://www.virustotal.com/en/file/dad6cfc19eb8423b3e3876c0564764f7060e49326b34e5212fc1bf2a024f47a5/analysis/1397466107/

静态测试

- 思考
  - 静态扫描的提升空间
  - 静态扫描的窘境



SHA256: bb177ede77e2ccdfa906a7ffedbae720d4e036593f61db265bf619a7a0e3adf5

File name: com.cn.smsclient-8.apk

Detection ratio: 1 / 51

Analysis date: 2014-04-14 07:51:08 UTC (1 hour, 16 minutes ago) View latest

Antivirus	Result	Update
DrWeb	Android.SmsSpy.9.origin	20140414

静态测试

- 重打包的难度
  - 修改代码
  - 修改资源
- 案例：
  - 修改QQ
  - 修改taobao

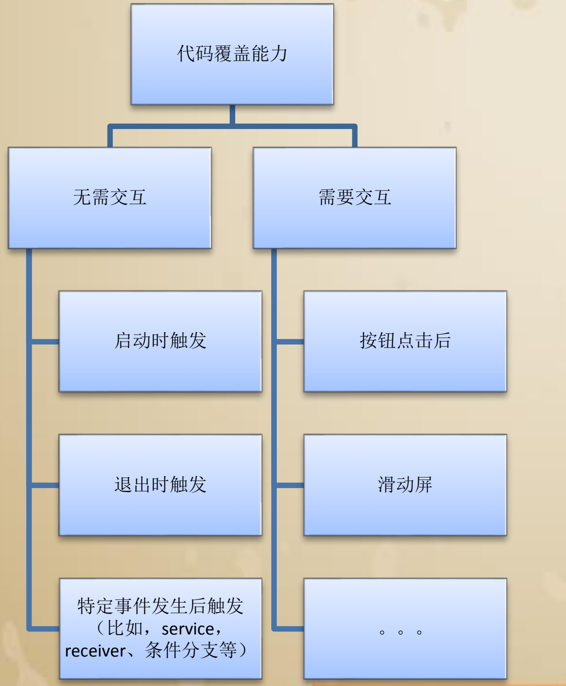
REF: Vaibhav Rastogi, Yan Chen, Xuxian Jiang: DroidChameleon: evaluating Android anti-malware against transformation attacks. ASIACCS 2013:329-334

动态测试

- 基准测试集
- 指纹特征

动态测试

- 基准测试集
  - 检测能力
  - 代码覆盖能力



代码覆盖能力

无需交互

启动时触发

退出时触发

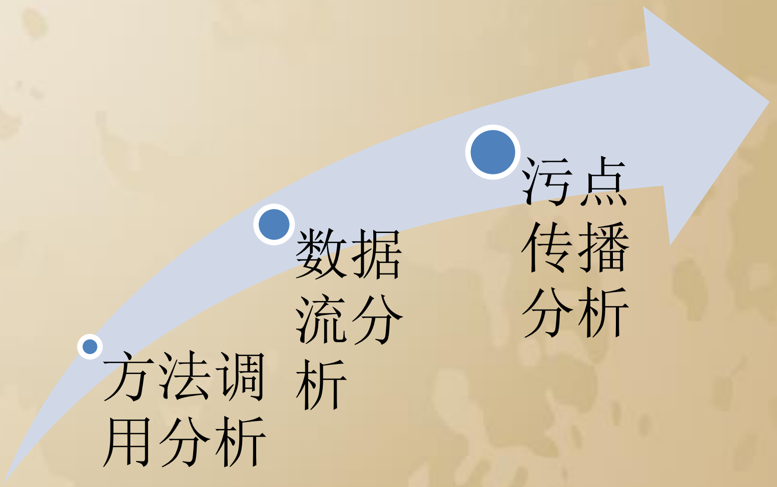
特定事件发生后触发（比如，service，receiver、条件分支等）

需要交互

按钮点击后

滑动屏

。。。



动态测试

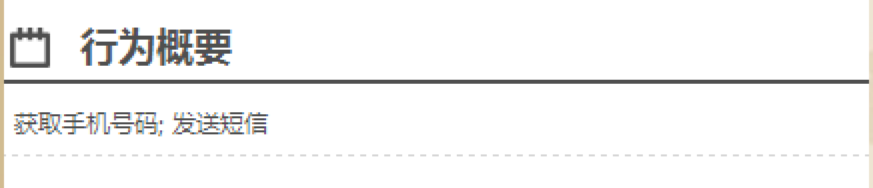
- 基准测试集的设计（发送短信）
  - SMS_send_button_onclick
  - SMS_send_view_ontouch
  - SMS_send_ScrollerView_onTouchEvent
  - SMS_send_ScrollerView_onInterceptTouchEvent
  - SMS_send_Receiver
  - SMS_send_service
  - SMS_send_classLoader
  - SMS_send_reflect
  - SMS_send_onCreate
  - SMS_send_onPause
  - SMS_send_onRestart
  - SMS_send_onResume
  - SMS_send_onDestroy
  - ……

动态测试

- 测试目标
  - Anubis
  - https://anubis.iseclab.org
  - B-chao
  - https://b-chao.com
  - Fireeye
  - http://fireeye.ijinshan.com

动态测试

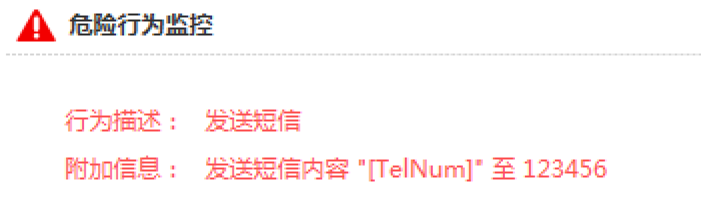
- 检测能力测试



行为概要

获取手机号码; 发送短信

B-chao

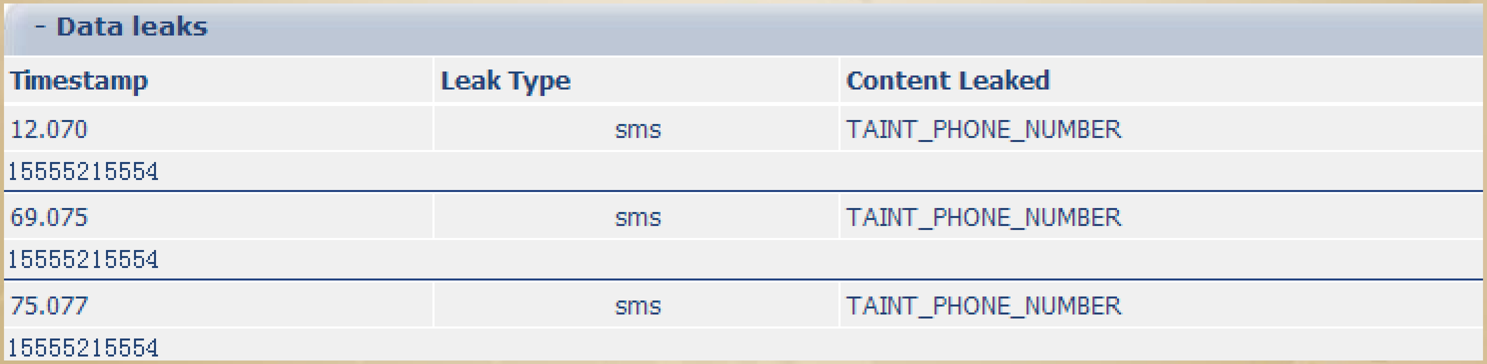


危险行为监控

行为描述： 发送短信

附加信息： 发送短信内容 "[TelNum]" 至 123456

Fireeye



- Data leaks

Timestamp	Leak Type	Content Leaked
12.070	sms	TAINT_PHONE_NUMBER
15555215554		
69.075	sms	TAINT_PHONE_NUMBER
15555215554		
75.077	sms	TAINT_PHONE_NUMBER
15555215554		

Anubis

动态测试

- 代码覆盖能力测试

	SMS_send_onCreate	SMS_send_onDestroy	SMS_send_button_onClick	SMS_send_view_onTouch	SMS_send_with_conditions	SMS_se_receive
Anubis	Y	Y	Y	Y	N	N
B-chao	Y	N	N	N	N	N
Fireeye	Y	N	N	N	N	N

动态测试

- 指纹特征
  - b-chao(https://b-chao.com/)
  - DEVICEID:000000000000000;TEL:15555215554;IMSI:310260000000000
  - fireeye(https://fireeye.ijinshan.com/)
  - name:TaintDroid Notification Service;packageName:org.appanalysis
  - anubis(https://anubis.iseclab.org/)
  - TEL:15555215554;IMEI:89014103211118510720
  - foresafe(http://www.foresafe.com/)
  - DEVICEID:000000000000000;TEL:15555215554;IMEI:890141032111185
    10720;IMSI:310260000000000

REF: DISSECTING THE ANDROID BOUNCER

检测方法展望

- 业界
  - 静态检测 - 启发式的检测方法（代表DrWeb）
  - 动态检测 - 事件驱动，加入更多的测试路径（代表Anubis）
- Android平台的一些特性，使得现有查杀手段失效

检测方法展望

- 恶意程序行为和正常程序行为界限不明显

- 结论：应该提供一个分析的平台，提供尽可能多的信息，来辅助人工分析。

- 谢谢！

更多信息： www.mobeisecurity.com
联系邮箱：zhaoshuai@mobeisecurity.com