安卓应用程序安全性分析

pLL(at)mobeisecurity.com

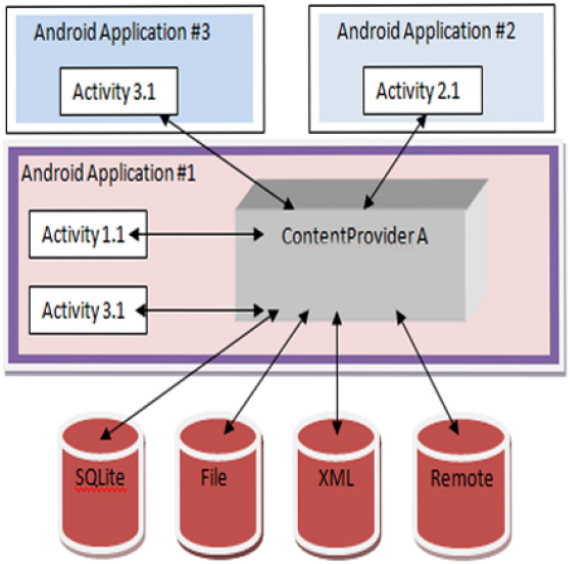
开放 合作 共赢

检查项目很多


安全评估
misc
SharedPreferences问题
SQL注入
WebView漏洞检测
不安全传输
不安全存储
不安全的log
流量检测
组件安全
耗电怎么检测？
组件安全
Activity劫持检测
Activity暴露检测
广播劫持检测
广播伪造检测
广播暴露检测
服务劫持检测
服务暴露检测
Content-provider暴露检测
...
恶意检测
内置代码检测
反射调用检测
字符串扫描
应用程序无图标
敏感方法的识别
检查广告
敏感方法
拨打电话
发送短信息
获取短信息
获取通信录
拦截短信
代码自修改
动态类加载
注册为设备管理器
...
杂项
加固检测
处理odex
模拟执行
特殊apk的处理

检查项目很多

Android Content Provider机制的隐私泄露与数据污染漏洞



Android Content Provider

- Content Provider隐私泄露漏洞
  - 未检查访问者权限：Content Provider接口暴露
  - 接口参数的输入检查不全面导致SQL注入或路径遍历
  - 两者结合使得恶意应用可以窃取用户隐私数据
- Content Provider数据污染漏洞
  - 篡改应用数据或配置

Ref: Android系统安全漏洞检测与利用（诸葛建伟）

检查过程很复杂

- 开发者文档描述有问题
  - 不清晰
  - 有错误
  - 很复杂
- 安全性依赖个人能力
  - 审查很复杂
  - 无现成工具

代码安全分析的几个层面

- 静态分析
  - 配置文件上的安全检测(AndroidManifest.XML、签名、hash)
  - 代码层面上的安全检测
  - 关联分析
  - 代码逻辑上的分析
- 动态分析

安全评估动态检测方法

- Intent-fuzzer
- Content-fuzzer
- Drozer

恶意程序动态测试

- 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_send_receive
Anubis	Y	Y	Y	Y	N	N
B-chao	Y	N	N	N	N	N
Fireeye	Y	N	N	N	N	N

恶意程序动态测试

- 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:890141032111118510720
  - foresafe(http://www.foresafe.com/)
  - DEVICEID:000000000000000;TEL:15555215554;IMEI:890141032111118510720;IMI:310260000000000

REF: DISSECTING THE ANDROID BOUNCER

配置文件上的安全检测

- 广告分析
- **部分**组件安全
- 查杀特征

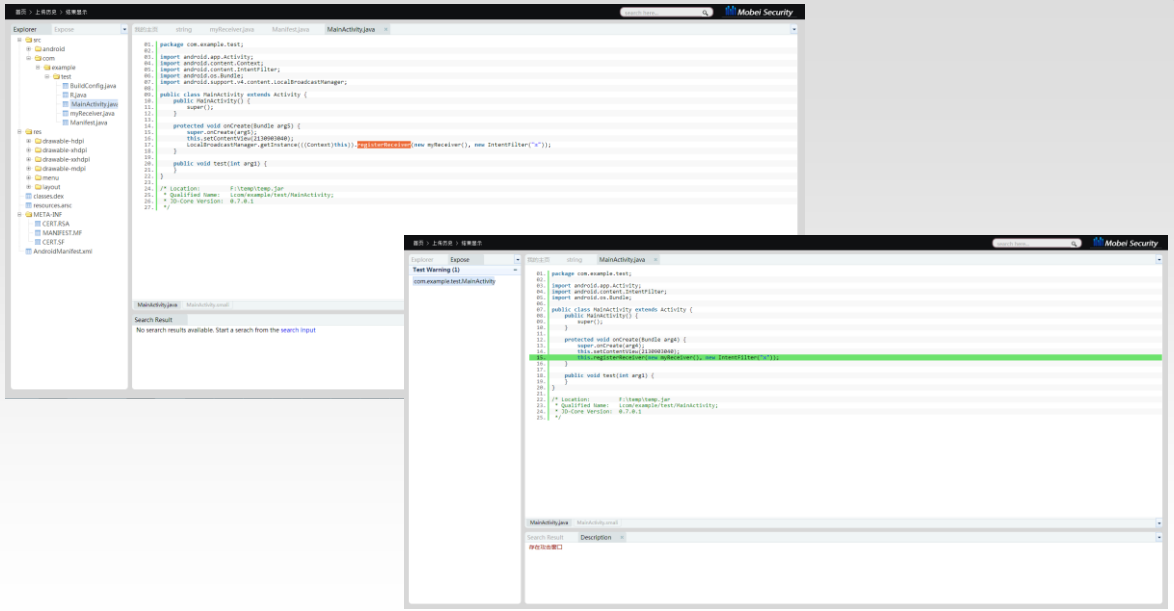
代码层面上的安全检测

- 代码扫描

传统APK分析流程

代码层面上的安全检测

- Dex、apk输入
- 预处理（反编译、代码预处理）
- 抽象语法树
- 控制流与符号表
- 数据流
- 污点传播分析

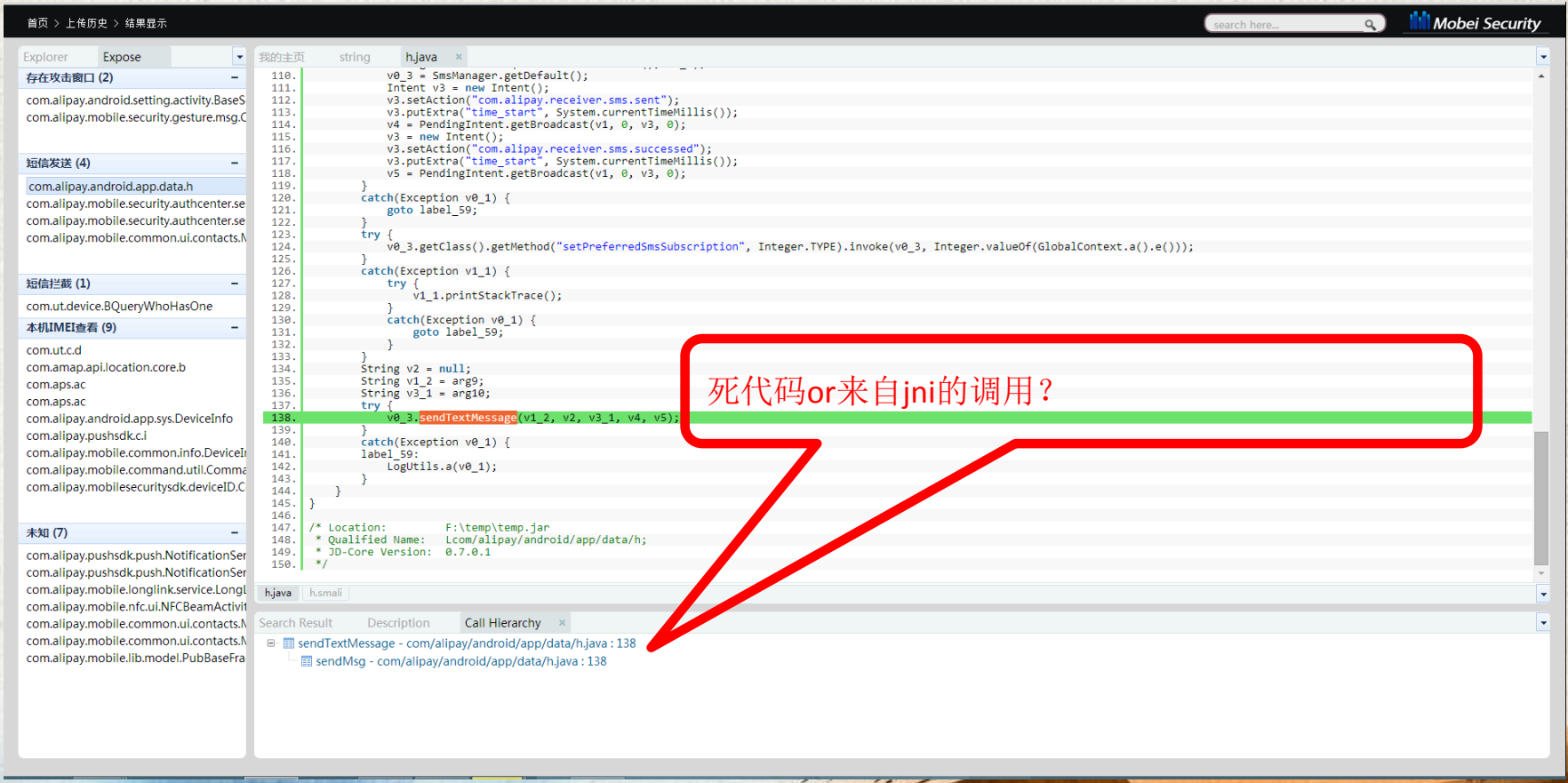


静态分析

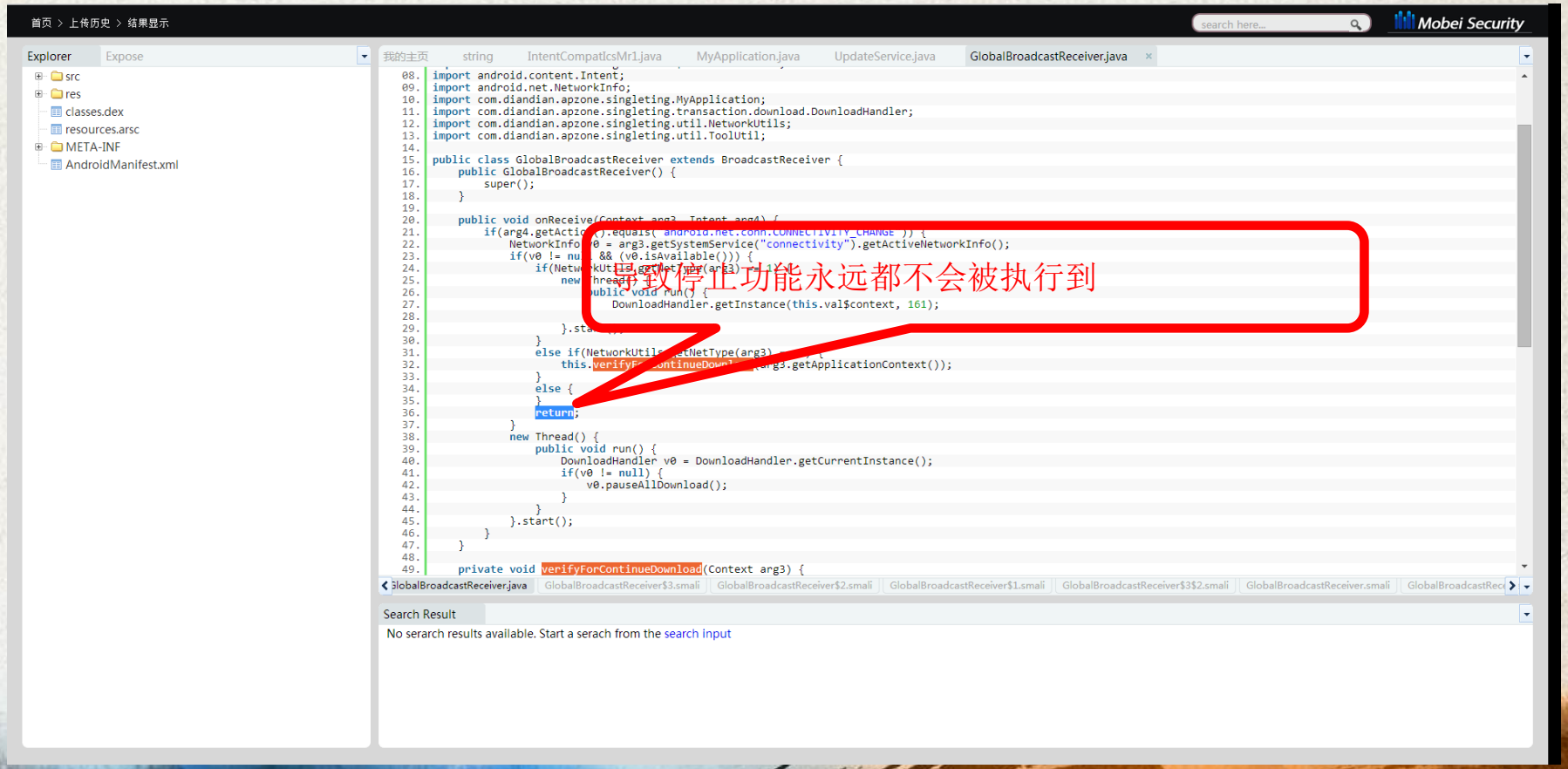
关联分析

- 安全评估
- “恶意”行为是否经过”交互”？
  - 调用序列问题
  - 什么样子的交互？

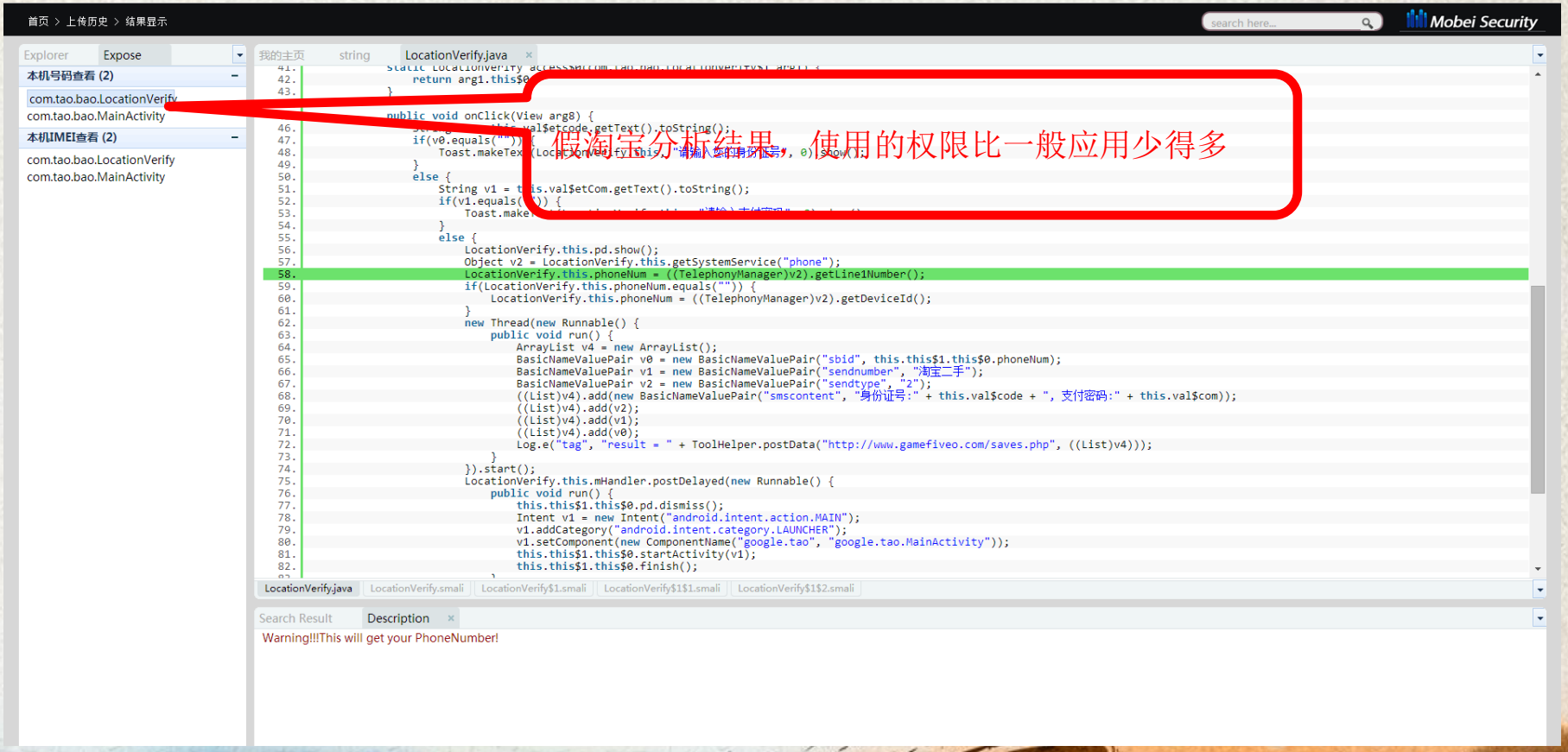
关联分析


首页 > 上传历史 > 结果显示
search here...
Mobei Security
Explorer
Expose
存在攻击窗口 (2)
com.alipay.android.setting.activity.BaseS
com.alipay.mobile.security.gesture.msg.C
短信发送 (4)
com.alipay.android.app.data.h
com.alipay.mobile.security.authcenter.se
com.alipay.mobile.security.authcenter.se
com.alipay.mobile.common.ui.contacts.N
短信拦截 (1)
com.ut.device.BQueryWhoHasOne
本机IMEI查看 (9)
com.ut.c.d
com.amap.api.location.core.b
com.aps.ac
com.aps.ac
com.alipay.android.app.sys.DeviceInfo
com.alipay.pushsdk.c.i
com.alipay.mobile.common.info.DeviceI
com.alipay.mobile.command.util.Comma
com.alipay.mobilesecuritysdk.deviceID.C
未知 (7)
com.alipay.pushsdk.push.NotificationSer
com.alipay.pushsdk.push.NotificationSer
com.alipay.mobile.longlink.service.Longl
com.alipay.mobile.nfc.ui.NFCBeamActivit
com.alipay.mobile.common.ui.contacts.N
com.alipay.mobile.common.ui.contacts.N
com.alipay.mobile.lib.model.PubBaseFra
我的主页
string
h.java
v0_3 = SmsManager.getDefault();
Intent v3 = new Intent();
v3.setAction("com.alipay.receiver.sms.sent");
v3.putExtra("time_start", System.currentTimeMillis());
v4 = PendingIntent.getBroadcast(v1, 0, v3, 0);
v3 = new Intent();
v3.setAction("com.alipay.receiver.sms.successed");
v3.putExtra("time_start", System.currentTimeMillis());
v5 = PendingIntent.getBroadcast(v1, 0, v3, 0);
}
catch(Exception v0_1) {
goto label_59;
}
try {
v0_3.getClass().getMethod("setPreferredSmsSubscription", Integer.TYPE).invoke(v0_3, Integer.valueOf(GlobalContext.a().e()));
}
catch(Exception v1_1) {
try {
v1_1.printStackTrace();
}
catch(Exception v0_1) {
goto label_59;
}
}
String v2 = null;
String v1_2 = arg9;
String v3_1 = arg10;
try {
v0_3.sendTextMessage(v1_2, v2, v3_1, v4, v5);
}
catch(Exception v0_1) {
label_59:
LogUtils.a(v0_1);
}
}
}
/* Location: F:\temp\temp.jar
* Qualified Name: Lcom/alipay/android/app/data/h;
* JD-Core Version: 0.7.0.1
*/
h.java
h.smali
死代码or来自jni的调用？
Search Result
Description
Call Hierarchy
sendTextMessage - com/alipay/android/app/data/h.java : 138
sendMsg - com/alipay/android/app/data/h.java : 138

逻辑上的问题


首页 > 上传历史 > 结果显示
search here...
Mobei Security
Explorer
Expose
src
res
classes.dex
resources.arsc
META-INF
AndroidManifest.xml
我的主页
string
IntentCompatIcsMr1.java
MyApplication.java
UpdateService.java
GlobalBroadcastReceiver.java
import android.content.Intent;
import android.net.NetworkInfo;
import com.diandian.apzone.singleting.MyApplication;
import com.diandian.apzone.singleting.transaction.download.DownloadHandler;
import com.diandian.apzone.singleting.util.NetworkUtils;
import com.diandian.apzone.singleting.util.ToolUtil;
public class GlobalBroadcastReceiver extends BroadcastReceiver {
public GlobalBroadcastReceiver() {
super();
}
public void onReceive(Context arg3, Intent arg4) {
NetworkInfo v0 = arg3.getSystemService("connectivity").getActiveNetworkInfo();
if(v0 != null && (v0.isAvailable())) {
new Thread() {
public void run() {
DownloadHandler.getInstance(this.val$context, 161);
}
}
return;
}
new Thread() {
public void run() {
DownloadHandler v0 = DownloadHandler.getCurrentInstance();
if(v0 != null) {
v0.pauseAllDownload();
}
}
}.start();
}
}
private void verifyForContinueDownload(Context arg3) {
导致停止功能永远都不会被执行到
GlobalBroadcastReceiver.java
GlobalBroadcastReceiver$3.smali
GlobalBroadcastReceiver$2.smali
GlobalBroadcastReceiver$1.smali
GlobalBroadcastReceiver$3$2.smali
GlobalBroadcastReceiver.smali
Search Result
No serarch results available. Start a serach from the search input

识别程序的意图


首页 > 上传历史 > 结果显示
search here...
Mobei Security
Explorer
Expose
本机号码查看 (2)
com.tao.bao.LocationVerify
com.tao.bao.MainActivity
本机IMEI查看 (2)
com.tao.bao.LocationVerify
com.tao.bao.MainActivity
我的主页
string
LocationVerify.java
假淘宝分析结果，使用的权限比一般应用少得多
LocationVerify.java
LocationVerify.smali
LocationVerify$1.smali
LocationVerify$1$1.smali
LocationVerify$1$2.smali
Search Result
Description
Warning!!!This will get your PhoneNumber!

恶意|非恶意界限不明确

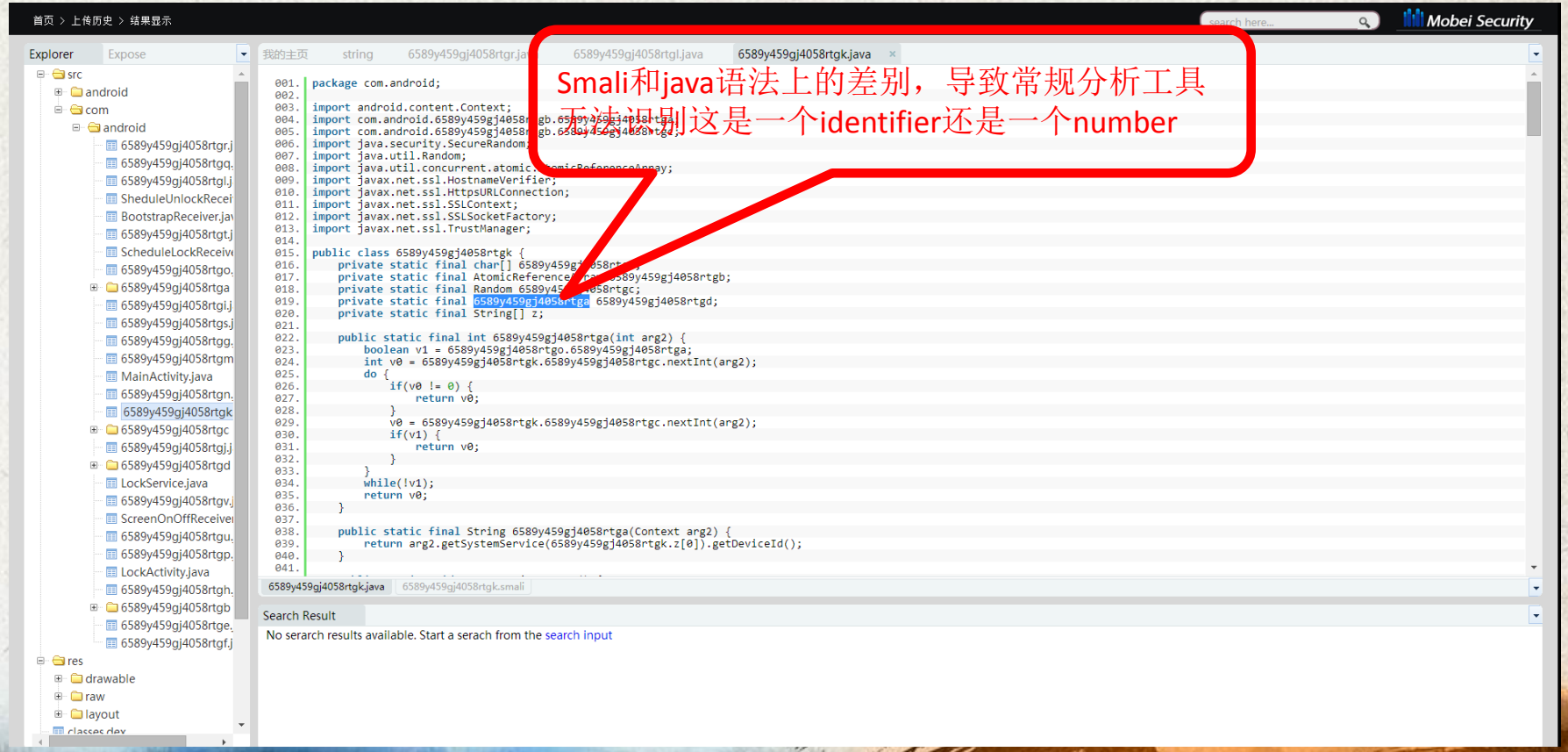
- 支付宝比faketaobao使用的权限还多
- 有些恶意程序没恶意行为

Ref:VisualThreat信息安全公司

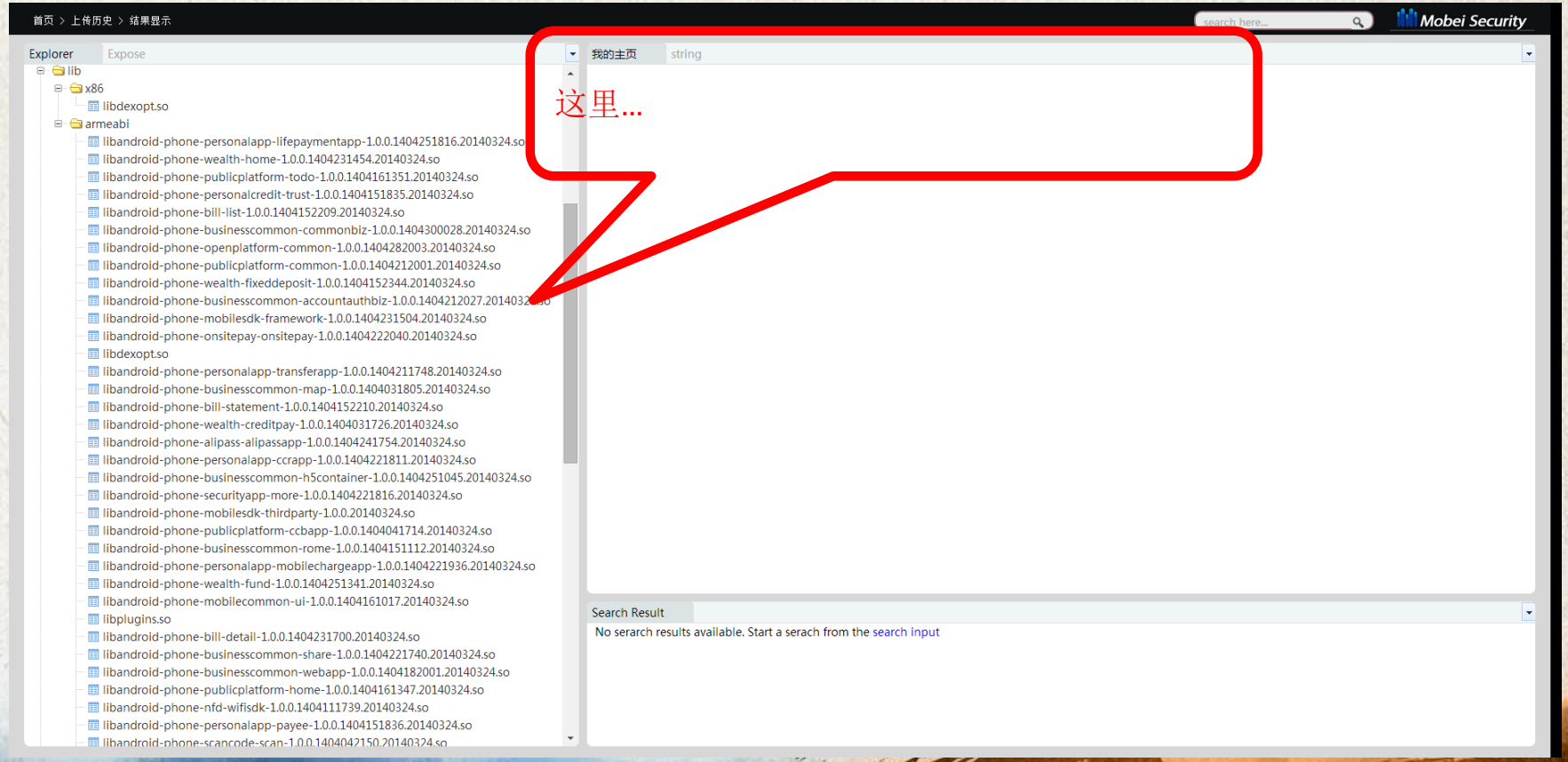
攻击技术走在检测技术前头

- 混淆代码
  - 1000a.1000b = 1000c
  - 1000.1000 = 1000
- reflection
- 加密代码
- 加固
- …

攻击技术走在检测技术前头



还有更多工作要做


首页 > 上传历史 > 结果显示
search here...
Mobei Security
Explorer
Expose
lib
x86
libdexopt.so
armeabi
libandroid-phone-personalapp-lifepaymentapp-1.0.0.1404251816.20140324.so
libandroid-phone-wealth-home-1.0.0.1404231454.20140324.so
libandroid-phone-publicplatform-todo-1.0.0.1404161351.20140324.so
libandroid-phone-personalcredit-trust-1.0.0.1404151835.20140324.so
libandroid-phone-bill-list-1.0.0.1404152209.20140324.so
libandroid-phone-businesscommon-commonbiz-1.0.0.1404300028.20140324.so
libandroid-phone-openplatform-common-1.0.0.1404282003.20140324.so
libandroid-phone-publicplatform-common-1.0.0.1404212001.20140324.so
libandroid-phone-wealth-fixeddeposit-1.0.0.1404152344.20140324.so
libandroid-phone-businesscommon-accountauthbiz-1.0.0.1404212027.20140324.so
libandroid-phone-mobilesdk-framework-1.0.0.1404231504.20140324.so
libandroid-phone-onsitepay-onsitepay-1.0.0.1404222040.20140324.so
libdexopt.so
libandroid-phone-personalapp-transferapp-1.0.0.1404211748.20140324.so
libandroid-phone-businesscommon-map-1.0.0.1404031805.20140324.so
libandroid-phone-bill-statement-1.0.0.1404152210.20140324.so
libandroid-phone-wealth-creditpay-1.0.0.1404031726.20140324.so
libandroid-phone-alipass-alipassapp-1.0.0.1404241754.20140324.so
libandroid-phone-personalapp-ccrapp-1.0.0.1404221811.20140324.so
libandroid-phone-businesscommon-h5container-1.0.0.1404251045.20140324.so
libandroid-phone-securityapp-more-1.0.0.1404221816.20140324.so
libandroid-phone-mobilesdk-thirdparty-1.0.0.20140324.so
libandroid-phone-publicplatform-ccbapp-1.0.0.1404041714.20140324.so
libandroid-phone-businesscommon-rome-1.0.0.1404151112.20140324.so
libandroid-phone-personalapp-mobilechargeapp-1.0.0.1404221936.20140324.so
libandroid-phone-wealth-fund-1.0.0.1404251341.20140324.so
libandroid-phone-mobilecommon-ui-1.0.0.1404161017.20140324.so
libplugins.so
libandroid-phone-bill-detail-1.0.0.1404231700.20140324.so
libandroid-phone-businesscommon-share-1.0.0.1404221740.20140324.so
libandroid-phone-businesscommon-webapp-1.0.0.1404182001.20140324.so
libandroid-phone-publicplatform-home-1.0.0.1404161347.20140324.so
libandroid-phone-nfd-wifisdk-1.0.0.1404111739.20140324.so
libandroid-phone-personalapp-payee-1.0.0.1404151836.20140324.so
libandroid-phone-scancode-scan-1.0.0.1404042150.20140324.so
这里...
我的主页
string
Search Result
No serarch results available. Start a serach from the search input

应用检测

+应用检测

状态	程序名称	MD5值	创建时间	操作
分析结束	CtClientL.apk	43b50e26001d684d532408dd4739f27b	2014-07-05 14:52:49.0	查看结果
分析结束	568d40ccd7b91951715ac4079a860128-des.apk	568d40ccd7b91951715ac4079a860128	2014-07-03 22:58:10.0	查看结果
分析结束	程序分析.apk	9068ba3f7c045cfe0422fb6b3b5d23aa	2014-07-03 22:12:26.0	查看结果
分析结束	Alipay.apk	13ca622f4ca2975fc925843d6fab8a50	2014-07-03 22:11:57.0	查看结果
分析结束	alipay_5637.apk	b15deffed2c88dd72fe8f27993efdad0	2014-07-03 22:08:57.0	查看结果
分析结束	郭德纲相声_com.diandian.apzone.yflgdg_26.apk	d186b20562db03eda1ed67cb4a31bd	2014-07-03 14:33:42.0	查看结果
分析结束	plain.apk	3963009445825b376279fc1a0f92e3f9	2014-07-03 14:06:06.0	查看结果
分析结束	敲诈者安卓病毒1.apk	67bde6039310b4bb9ccd9fcf2a721a45	2014-07-03 14:05:33.0	查看结果
分析结束	fakeAV.apk	16bd4b23b55f0ade6df16d8c6dcf502c	2014-07-03 14:05:08.0	查看结果
分析结束	银行毒手.apk	1df09807170c26dcdf3a7cfde05567d1	2014-07-03 14:04:49.0	查看结果
分析结束	0bad.apk	e1064bfd836e4c895b569b2de4700284	2014-07-03 14:04:12.0	查看结果
分析结束	Faketaobao_45DAE1EE4CA1980C1[illegible]CB5C9DA2A7ED5.apk	45dae1ee4ca1980c140cb5c9da2a7ed5	2014-07-03 14:03:16.0	查看结果
分析结束	qq_4.7.2.2185_and[illegible]id.apk	517d22939844cb696205f4aed953864a	2014-07-03 13:56:28.0	查看结果
分析结束	yixin_2.7.0.189_66113_201[illegible]0527[illegible]66.apk	c9aec954f5cbb7704f25442711749a72	2014-07-03 13:55:25.0	查看结果
分析结束	weixin531android[illegible]60.apk	be8a54c7b87d5d45427fb8f7185d92c4	2014-07-03 13:53:30.0	查看结果
分析结束	Twitter_5.14.0_3000[illegible]10.apk	eda58a48779645c566222da5ce520d45	2014-07-03 13:52:13.0	查看结果
分析结束	Tenpay_V2.4.2.apk	fd0e3e1a8[illegible]	2014-07-03 13:51:19.0	查看结果
分析结束	ctrip_9289.apk	[illegible]6c2c86a62ee4e6973fa5f88ad4afed	2014-07-03 13:50:55.0	查看结果
分析结束	alipay_wap_main.apk	90d7e006ee885d13508c5597ce80d920	2014-07-03 13:33:01.0	查看结果
分析结束	浦发手机银行4.1.apk	758aa68823311c430696f159d33245c1	2014-07-02 23:44:11.0	查看结果
插件分析中	招商银行2.1.2.ap[illegible]	863352d1a198743d9c1bdd8e57c5d46b	2014-07-02 23:34:51.0	----
反编译中	我查查-360加固.apk	c8b5f20e63298ed9dbb51302fdeb7f62	2014-07-02 11:35:33.0	----
分析结束	有解压密码的APK.apk	ad0e40b3136fdddbc221ba8db896aff4	2014-07-02 11:30:25.0	查看结果
分析结束	F7BE25E4F19A3A82D2E206DE8AC979C8.apk	f7be25e4f19a3a82d2e206de8ac979c8	2014-07-02 11:29:36.0	查看结果
分析结束	test.apk	b482083dd30bda3cd26a10970745b033	2014-07-02 11:08:25.0	查看结果

这里...

App的安全不只包含客户端代码安全

END

Q&A 谢 谢！

开放 合作 共赢