

# 浅谈Android重打包技术

---

沈明星

<http://weibo.com/fattestmonkey>

2013.1.12

# 大纲

---

- \* Android应用APK文件结构
- \* 重打包步骤
  - \* Apk unpackaging
  - \* Decompiling
  - \* Resource and code manipulation
  - \* Repackaging and signing
- \* Case study – 基于重打包技术的geinimi木马样本简单分析
- \* 总结

# Android应用开发步骤

Coding

- Java in SDK
- C/CPP in NDK

Compiling

- Compiling to Dalvik (DEX-Files)

packaging

- Packaging as signed APK

# APK文件结构

APK 实际上是个ZIP文件

assets

META-INF

Manifest.mf

Cert.rsa

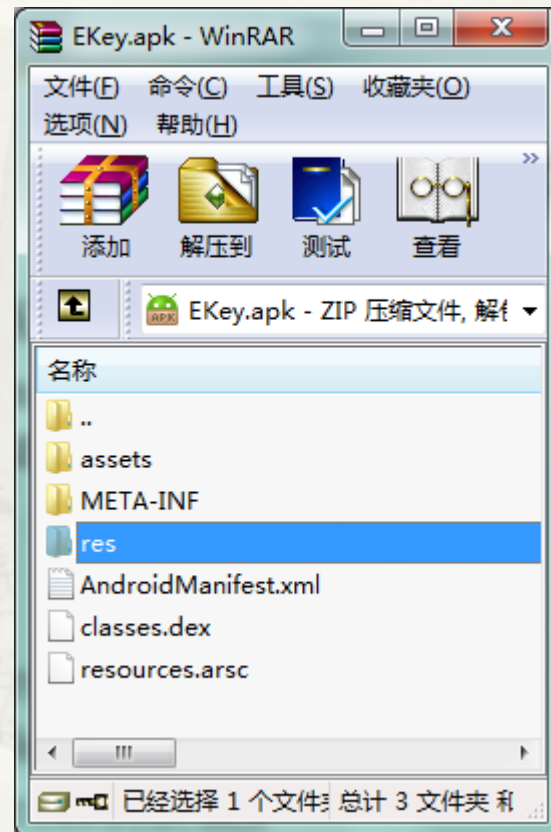
Cert.sf

res

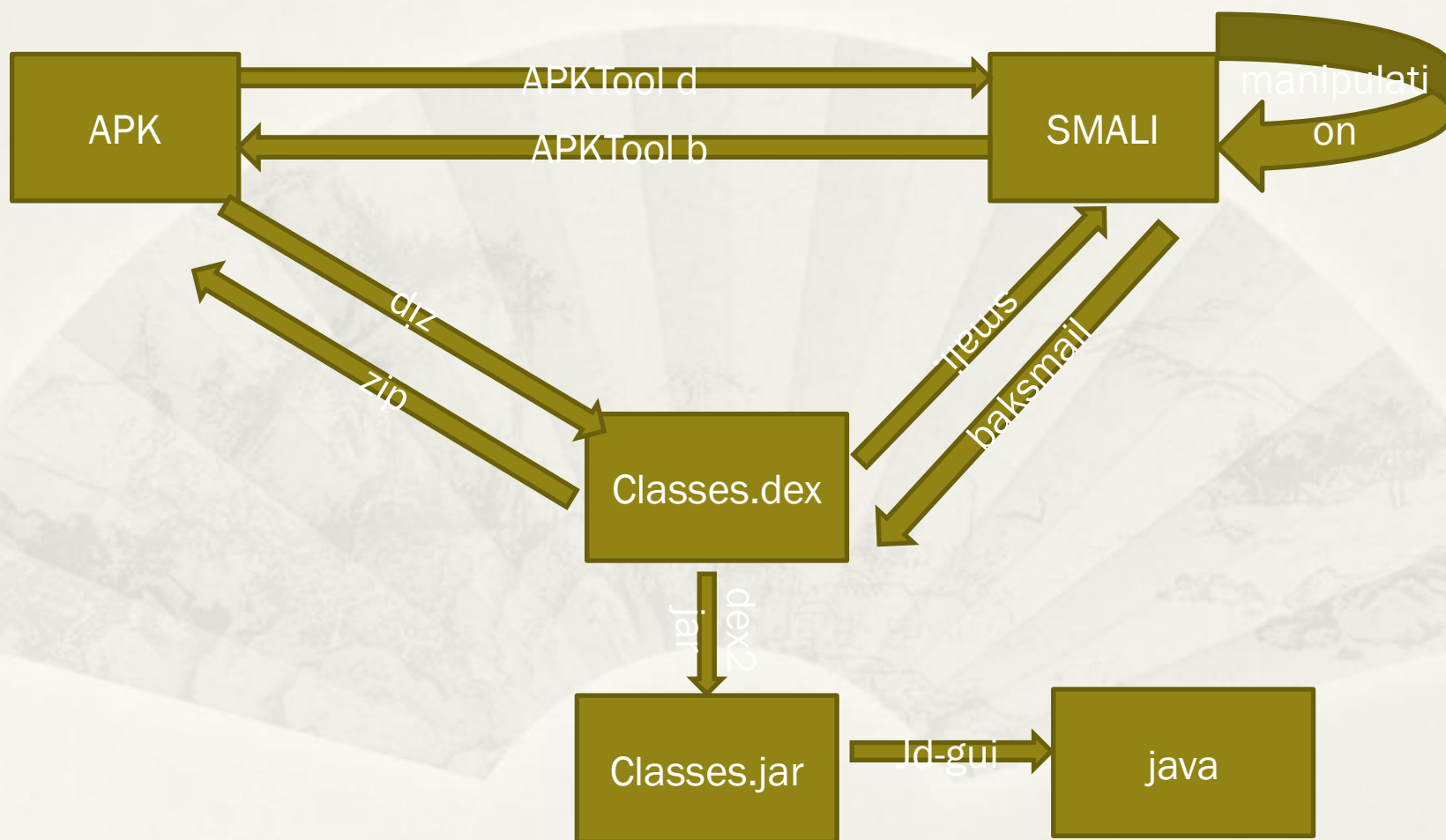
AndroidManifest.xml

classes.dex

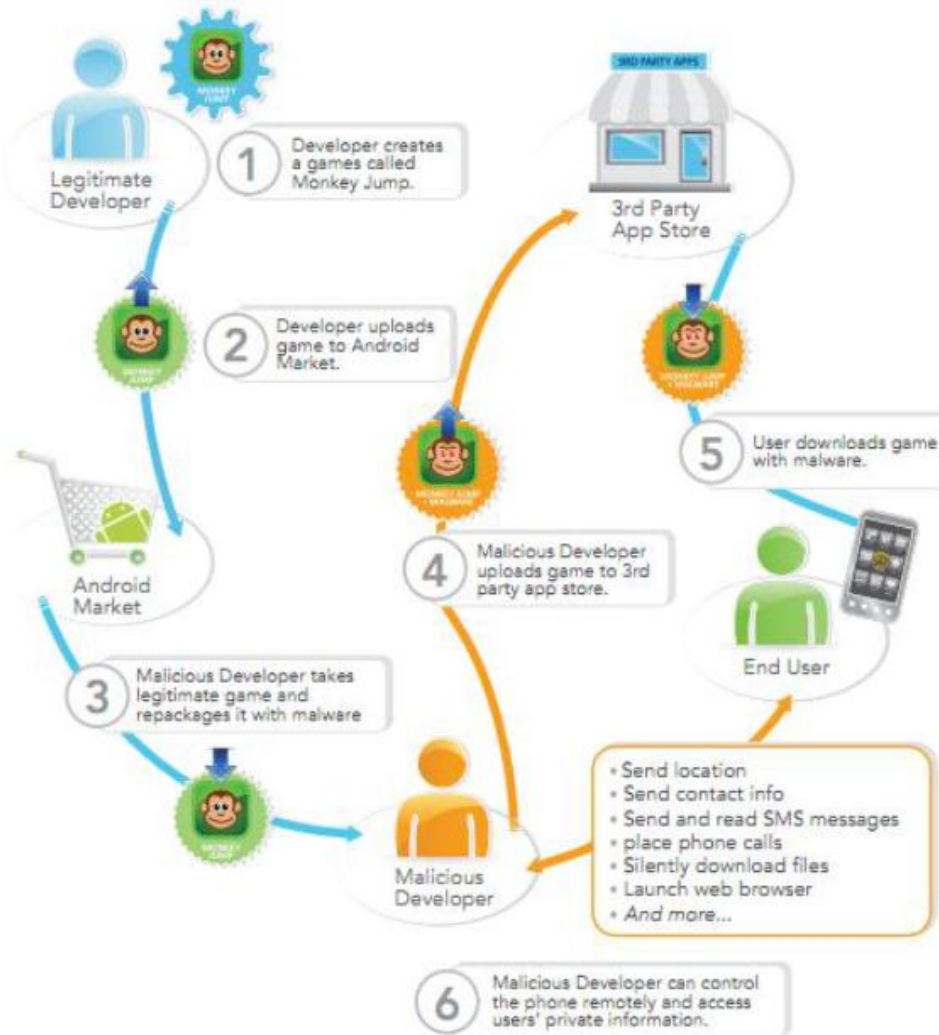
resources.arsc



# 文件转换图



# 重打包过程



# unpackaging

- \* 使用apktool解包
- \* Apktool d <file.apk> [<dstdir>]

```
D:\Android-Tools\apktool>apktool.bat d HelloActivity.apk
I: Baksmaling...
I: Loading resource table...
I: Loaded.
I: Loading resource table from file: C:\Users\hou\apktool\framework\1.apk
I: Loaded.
I: Decoding file-resources...
I: Decoding values*/*.XMLs...
I: Done.
I: Copying assets and libs...
D:\Android-Tools\apktool>
```

# Resource and code manipulation

---

简单	修改配置文件，包括sd卡中和一些xml配置文件
中等	修改apk中的资源文件
较难	修改smali文件内容
难	需要绕开破解一些本地的加密，混淆机制



# 修改smali代码

```
new-instance v5, Ljava/lang/String;
const/4 v6, 0x0
invoke-direct {v5, v3, v6, v4}, Ljava/lang/String;-
><init>([BII)V
v3 = 0x1fa3
v3 = v5.equals(v3);
const-string v3, "hello"->"你好"
invoke-virtual {v5, v3}, Ljava/lang/String;-
>equals(Ljava/lang/Object;)Z
move-result v3
```

# 修改AndroidManifest.xml

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.netease.is.helloandroid"
    android:versionCode="1"
    android:versionName="1.0" >
    <uses-sdk
        android:minSdkVersion="8"
        android:targetSdkVersion="15" />
    <application
        android:icon="@drawable/ic_launcher"
        android:label="@string/app_name"
        android:theme="@style/AppTheme" >
        <activity
            android:name=".MainActivity" -> another activity
            android:label="@string/title_activity_main" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
</manifest>
```

# Repackaging

---

- \* 使用apktool打包
- \* Apktool b <srcdir>

```
D:\Android-Tools\apktool>apktool.bat b HelloActivity
I: Checking whether sources has changed...
I: Smaling...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
```

# signing with certification

## \* 使用keytool和jarsigner来签名

```
D:\Android-Tools\apktool>keytool -genkey -v -keystore android.keystore -alias an
droid -keyalg RSA -validity 20000
输入keystore密码:
再次输入新密码:
您的名字与姓氏是什么?
[Unknown]: smx
您的组织单位名称是什么?
[Unknown]: smx
您的组织名称是什么?
[Unknown]: smx
您所在的城市或区域名称是什么?
[Unknown]: smx
您所在的州或省份名称是什么?
[Unknown]: smx
该单位的两字母国家代码是什么
[Unknown]: smx
CN=smx, OU=smx, O=smx, L=smx, ST=smx, C=smx 正确吗?
[否]:
```

```
D:\Android-Tools\apktool>jarsign -verbose -keystore android.keystore HelloActivi
ty.apk android
半:
```

## \* 或者使用autosign等其他工具签名

# 重打包技术应用

---

- \* 学习别人的代码设计和逻辑
- \* 汉化
- \* 破解
- \* 制作病毒，木马，广告软件
- \* 。 。 。

# Case study - Geinimi 木马

 [新闻](#) [网页](#) [贴吧](#) [知道](#) [音乐](#) [图片](#) [视频](#) [地图](#) [文库](#) [更多»](#)

 您要找的是不是: [给你米](#)

[给你米病毒](#) [百度百科](#)

百度名片: [给你米\(Geinimi\)](#) [给你米\(Geinimi\)](#)后门程序, 基于Android平台, 通过各种伎俩植入到多款流行手机游戏软件中, 生成新的软件安装包后在手机论坛、手机...

[百度名片](#) - [概念释义](#) - [病毒危害](#) - [传播方式](#) - [应对方法](#)

[baike.baidu.com/view/62359...htm](http://baike.baidu.com/view/62359...htm) 2012-9-1 - [百度快照](#)

[“给你米”?给你手机病毒](#) [经济新闻-解放日报](#)

2010年12月7日 - 本报讯 (记者 吴卫群)近日,网秦全球手机安全中心发布手机安全预警:一组名为“给你米”(Geinimi)的手机后门程序,正在大量手机软件下载站、论坛中肆意...

[newspaper.jfdaily.com/jfrb/html/2010...](http://newspaper.jfdaily.com/jfrb/html/2010...) 2010-12-7 - [百度快照](#)

[“给你米”感染手机或超90万部-MSN中国科技频道](#)

[wenku.baidu.com/search?word=geinimi&lm=0&od=0](http://wenku.baidu.com/search?word=geinimi&lm=0&od=0) 该网友中的正是“给你米”后门程序变种

# 分析样本

---

- \* File: MonkeyJump2.apk
- \* Md5:  
e0106a0f1e687834ad3c91e599ace1be
- \* Sha1:  
179e1c69ceaf2a98fdca1817a3f3f1fa2823  
6b13

# AndroidManifest.xml

## 中入口修改

```
<!-- Default activity --> <activity
android:theme="@android:01030009"
android:label="@7F050000"
android:name="com.dseffects.MonkeyJump2.jump2.c.rufCuAtj">
<intent-filter>
<action android:name="android.intent.action.MAIN"></action>
<category android:name="android.intent.category.LAUNCHER"></category>
</intent-filter>
</activity>
<!-- Broadcast receiver -->
<receiver android:name="com.dseffects.MonkeyJump2.jump2.f">
<intent-filter>
<action android:name="android.intent.action.BOOT_COMPLETED"></action>
<category android:name="android.intent.category.LAUNCHER"></category>
</intent-filter>
<intent-filter android:priority="65535">
<action android:name="android.provider.Telephony.SMS_RECEIVED">
</action>
</intent-filter>
</receiver>
```



# AndroidManifest.xml

## 中权限修改

```
android.permission.INTERNET  
android.permission.ACCESS_COARSE_LOCATION  
android.permission.READ_PHONE_STATE  
android.permission.VIBRATE
```

```
android.permission.INTERNET  
android.permission.ACCESS_COARSE_LOCATION  
android.permission.READ_PHONE_STATE  
android.permission.VIBRATE  
com.android.launcher.permission.INSTALL_SHORTCUT  
android.permission.ACCESS_FINE_LOCATION  
android.permission.CALL_PHONE  
android.permission.MOUNT_UNMOUNT_FILESYSTEMS  
android.permission.READ_CONTACTS  
android.permission.READ_SMS  
android.permission.SEND_SMS  
android.permission.SET_WALLPAPER  
android.permission.WRITE_CONTACTS  
android.permission.WRITE_EXTERNAL_STORAGE  
com.android.browser.permission.READ_HISTORY_BOOKMARKS  
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS  
android.permission.ACCESS_GPS  
android.permission.ACCESS_LOCATION  
android.permission.RESTART_PACKAGES  
android.permission.RECEIVE_SMS  
android.permission.WRITE_SMS
```

# 代码分析

---

- \* 客户端代码

- \* [client.smali](#)

- \* 服务端代码

- \* [server.smali](#)

# 通信数据分析

```
07:51:47.551306 52:54:00:12:34:56 > 52:54:00:12:35:02, ethertype IPv4 (0x0800), length
349: 10.0.2.15.47895 > 117.135.134.184.8080: P 241:536(295) ack 1 win 5840
    0x0020: 5018 16d0 ca6a 0000 7061 7261 6d73 3d33 P..??j..params=3
    0x0030: 6666 3864 3235 6334 3337 3030 3935 3339 ff8d25c437009539
    0x0040: 3866 6533 3735 6137 6465 3137 3937 6137 8fe375a7de1797a7
    0x0050: 3564 6137 6661 3336 6235 6365 6534 3166 5da7fa36b5cee41f
    0x0060: 3261 6266 6464 3964 3065 3034 6333 6239 2abfdd9d0e04c3b9
    0x0070: 6161 6639 3362 6630 3665 6430 3439 3065 aaf93bf06ed0490e
    0x0080: 3637 3062 3461 6234 6263 6536 6563 3961 670b4ab4bce6ec9a
    0x0090: 3133 3166 3864 3336 3864 3661 3039 3933 131f8d368d6a0993
    0x00a0: 3235 6461 3237 3432 3637 3733 3838 6535 25da2742677388e5
    0x00b0: 3639 6130 3866 3161 6532 3530 3764 3066 69a08f1ae2507d0f
    0x00c0: 3261 6266 6464 3964 3065 3034 6333 6266 2abfdd9d0e04c3bf
    0x00d0: 3737 6637 3333 3964 3562 3536 3835 3562 77f7339d5b56855b
    0x00e0: 3538 6136 6533 6333 3063 3466 3037 6233 58a6e3c30c4f07b3
    0x00f0: 6637 6330 3334 3765 3261 3439 3861 6238 f7c0347e2a498ab8
    0x0100: 3631 3964 3533 3231 3036 3330 6637 6563 619d53210630f7ec
    0x0110: 3733 3035 3661 6562 6331 6165 3536 6533 73056aebc1ae56e3
    0x0120: 6665 6631 3863 6266 3335 6431 3163 3134 fef18cbf35d11c14
    0x0130: 6333 3732 3835 3933 3631 6336 3238 6462 c372859361c628db
    0x0140: 6563 6630 6630 6364 3562 3231 3632 62 ecf0f0cd5b2162b
```

```
PTID=33120001&IMEI=0000000000000000&sdkver=10.7&SALESID=0006&IMS1=310260
0000000000&longitude=0.0&latitude=0.0&DID=2001&autosdkver=10.7&CPID=3312
```

# 控制命令列表

---

- \* ***dsms***
- \* ***smsrecord***
- \* ***call***
- \* ***showurl***
- \* ***install:// and install*** - Download an APK ; trigger installation
- \* ***updateHost*** – Updates the server list with a new list supplied by the server.
- \* ***changeFrequency*** – Changes the frequency preference for checking into the server.
- \* ***skipTime*** – Controls the delay between command execution.
- \* ***applist*** – Delivers a list of installed applications to the server.
- \* ***contactlist*** – Dumps contact information including display name, last access time, and phone number about all device contacts to the server.

# 总结

- \* 开发 – 如果防止自己开发的被重打包
  - \* 核心代码放到本地库中 .so
  - \* 在线签名校验
  - \* 代码混淆, ProGuard
- \* 用户 – 如何避免成为受害者?
  - \* 安装前仔细检查权限
  - \* 从可信的第三方菜市场下载安装应用
- \* 安全人员 – 如何检测, 如何帮助开发和用户?

# 静态分析

---

- \* 静态分析

- \* 差异分析
- \* 特征匹配
- \* 权限检测
- \* 函数检测
- \* 类别检测


# 静态分析工具

---

- \* Apktool
- \* Smali/baksmali
- \* Dex2jar
- \* jd-gui
- \* sqlitebrowser

# 动态分析

---

- \* 监控文件读写
  - \* 网络连接
  - \* 短信发送
  - \* 自定义行为匹配
- 
- A decorative background graphic of a fan with a landscape painting, featuring a mountain, trees, and a body of water, rendered in a traditional Chinese style. The fan is open and occupies the lower half of the slide.



# 动态分析工具

---

- \* ☐ Dalvik Debug Monitor – Android SDK
- \* ☐ DroidBox – Application sandbox
- \* ☐ TaintDroid – Application sandbox
- \* ☐ Android Reverse Engineering (A.R.E.)  
Virtual Machine
- \* ☐ Network traffic
  - \* ☐ WireShark
  - \* ☐ Tcpdump
  - \* ☐ Shark for Root

# 谢谢！

---

- \* 网易安全中心

- \* <http://aq.163.com>

- \* 网易安全微博

- \* <http://weibo.com/163security>