腾讯移动安全实验室
Tencent Mobile Security Labs

腾讯手机管家
手机安全管理先锋

腾讯移动安全实验室

2013年
手机安全报告
Mobile Security Report of 2013

目录

2013 年手机安全报告

报告提要

2013 年，基于腾讯手机管家服务的腾讯移动安全实验室共检测截获 Android、Symbian 手机病毒包总数共 793400 个,其中,截获 Android 手机病毒达到 763351 个，占比 96.21%，Symbian 手机病毒占比 3.79%。

2013 年全年，腾讯手机管家用户累计举报垃圾短信达到 11.01 亿条。2013 年全年，腾讯手机管家用户举报垃圾短信达到 7.39 亿，是 2012 年全年总量的 2.4 倍，在 1 月和 10 月用户垃圾短信举报量最多，均达到 0.73 亿。2013 年诈骗类短信举报量超过 2141 万。

2013 年新增手机病毒包数是 2012 年的 4.47 倍 ,Android 系统新增病毒包是 Symbian 系统的 25.4 倍。

2013 年腾讯手机管家查杀病毒次数 1.82 亿次，是 2012 年 3.2 倍。2013 年全年，手机中毒用户总数达到 1.08 亿，相当于广东省人口总数，约为北京市人口的 5 倍。全球仅有 11 个国家的人口总数高于 2013 年国内染毒用户数。2013 年的手机染毒用户是 2012 年的 3.12 倍。

2013 年，在用户举报垃圾短信、诈骗短信、诈骗电话的最高十大省份之中，广东分别以占全国 15.02%、15.35%、15.26%的比例高居第一。

2013 年全年，腾讯手机管家针对骚扰电话进行标记的总次数为 1.02 亿 ,电话标记总数量为 2796.4 万个。

2013 年,大批知名游戏软件遭遇二次打包篡改，游戏成为染毒“毒害”的重灾区。战神 OL、格斗之王 III、魔兽世纪、3D 狂暴赛车、3D 飞车、植物大战僵尸 OL、Talking Tom、地铁跑酷等知名游戏被纷纷被病毒感染。

2013 年，安卓签名漏洞爆发成为重大行业事件。

2013 年来，腾讯移动安全实验室针对 APP 读取隐私权限进行了研究. 腾讯移动安全实验室抽取了近 470 万个软件包，统计发现有读取用户隐私权限相关操作的软件比例达到 71%。

2013 年底，山寨手机购票类 APP 大肆泛滥，含 12306 的山寨软件包达到 744 个，占 12306 软件包的 99.6%。

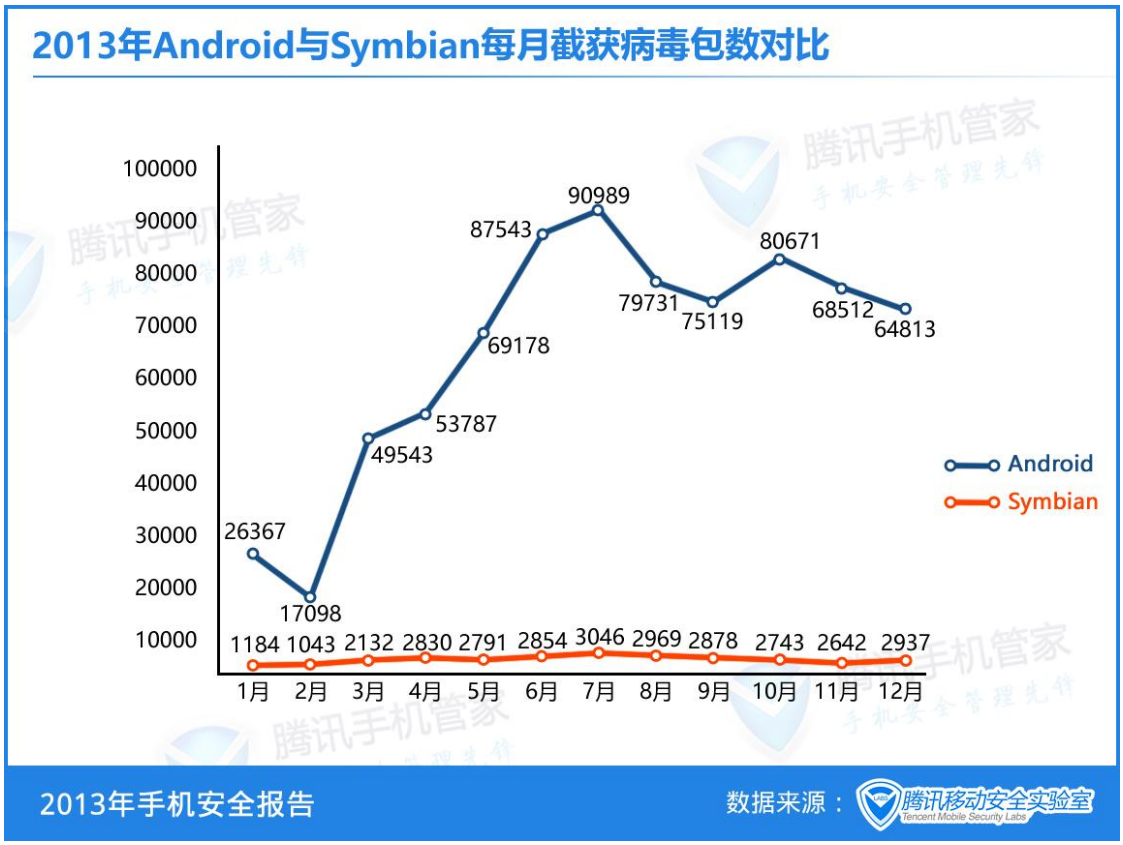
2013 年感染用户最多的十大手机病毒分别是：a.expense.newginger、a.expense.dpn、a.privacy.fakeandroid.a、a.privacy.counterclank（广告偷窥者）、a.expense.letang.a、a.payment.MMarketPay.b.[伪画皮 2]、a.payment.MMarketPay.c a.expense.mdk.f、a.expense.check.a、a.expense.if2boyplayer.e。这十大病毒感染用户达到 2056.75 万 ,与北京市人口相当。是 2012 年感染用户最多的十大病毒感染用户的 11.42 倍。

第一章　2013 年手机安全状况分析

2013 年，基于腾讯手机管家服务的腾讯移动安全实验室共检测截获 Android、Symbian 手机病毒包总数共 793400 个,其中,截获 Android 手机病毒达到 763351 个，占比 96.21%，Symbian 手机病毒包总数为 30049 个，占比 3.79%。

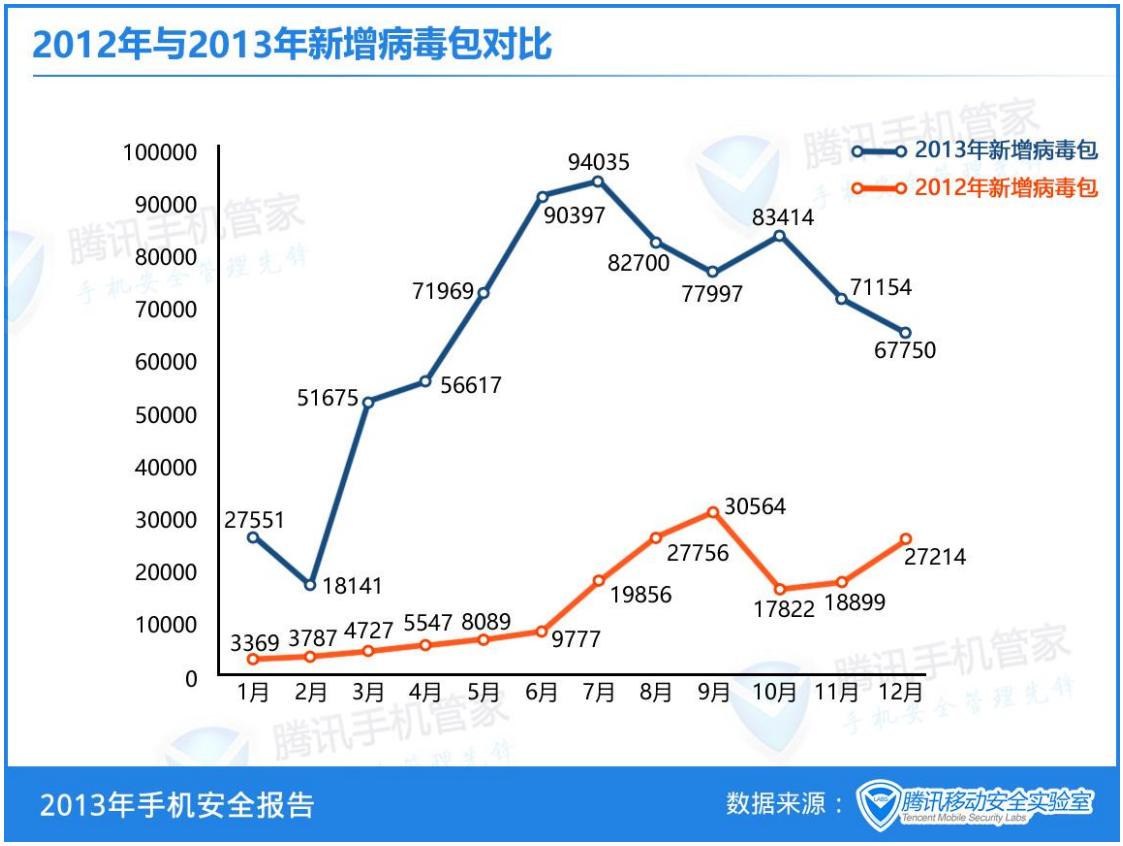
2013 年新增手机病毒包数是 2012 年的 4.47 倍

2013 年，Android 系统新增病毒包是 Symbian 系统的 25.4 倍。2013 年 1 月~7 月，Android 系统检测截获病毒样本在 2013 年上半年呈现激增暴涨之势 ,7 月~12 月呈现缓慢下降。



在 Symbian 系统 ,2013 年病毒包在 1000~3000 的低位区间内平稳增长。从 Symbian 系统与 Android 系统病毒包增量的强烈对比可以看出，Android 系统已经成为手机木马、恶意软件的绝对主战场。

与 2012 年相比,2013 年截获的病毒包总数是 2012 的 4.47 倍。从 2013 年 2 月到 2013 年 7 月，手机病毒呈现几何式疯狂增长态势。



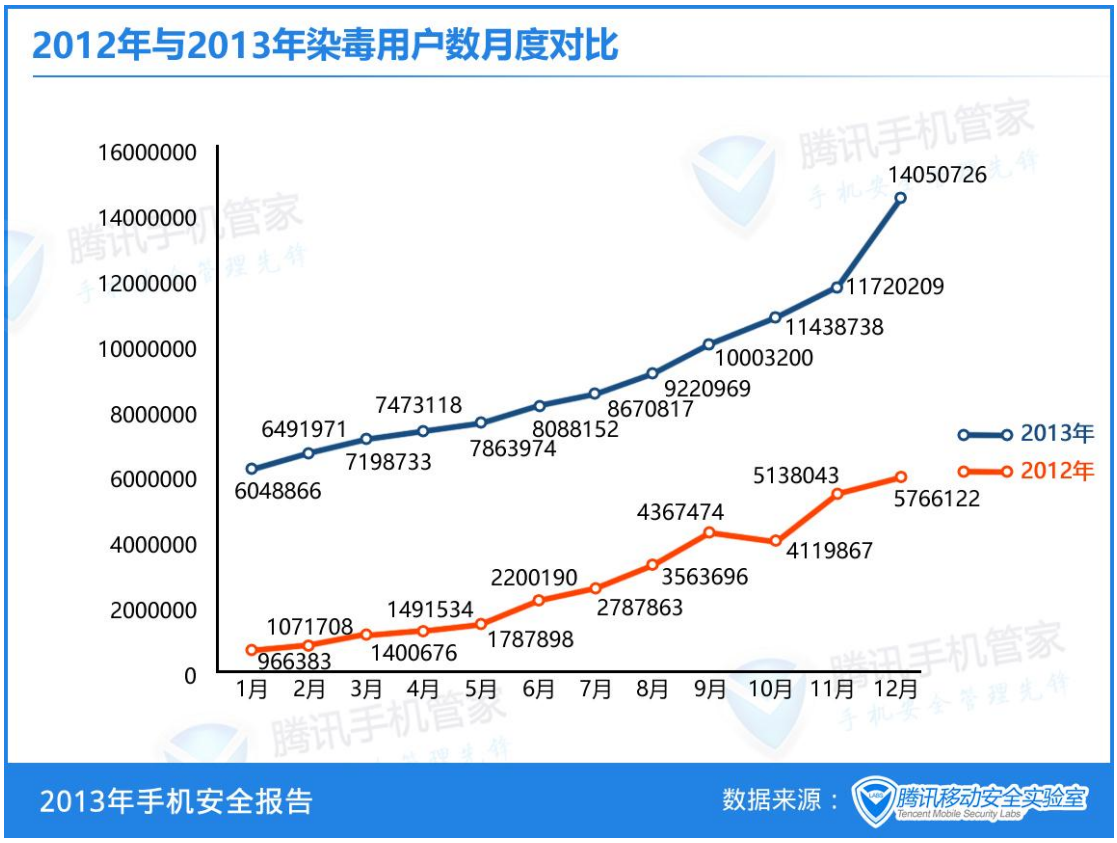
2013 年 7 月是腾讯手机管家 2013 年截获病毒包数最高月份，当月截获病毒包达到 94035 个，同比增长 374%。2 月则是截获病毒包最低月。2013 年 7 月新增病毒包是 2013 年 2 月的 5.18 倍。从 2013 年 2 月到 7 月，新增病毒包每月平均增长率达到 36%。从 2013 年 7 月到 12 月，新增病毒包呈现缓慢下降的趋势，但尽管如此，依然处于高位，2013 年下半年新增病毒包最低值在 12 月，依然达到 67750 个。

总体看，2013 年每月新增病毒包数呈现突增缓降的趋势，2012 年则相对呈现平稳增长，总体来说，2013 年每月新增病毒包的基数大大高于 2012 年，这是手机安全风险激增的直接反映。

1.2 2013 年手机染毒用户数相当于广东省人口总数

2013 年全年，手机中毒用户总数达到 1.08 亿，相当于广东省人口总数，约为北京市人口的 5 倍。全球仅有 11 个国家的人口总数高于 2013 年国内染毒用户数。2013 年的手

机染毒用户是 2012 年的 3.12 倍。

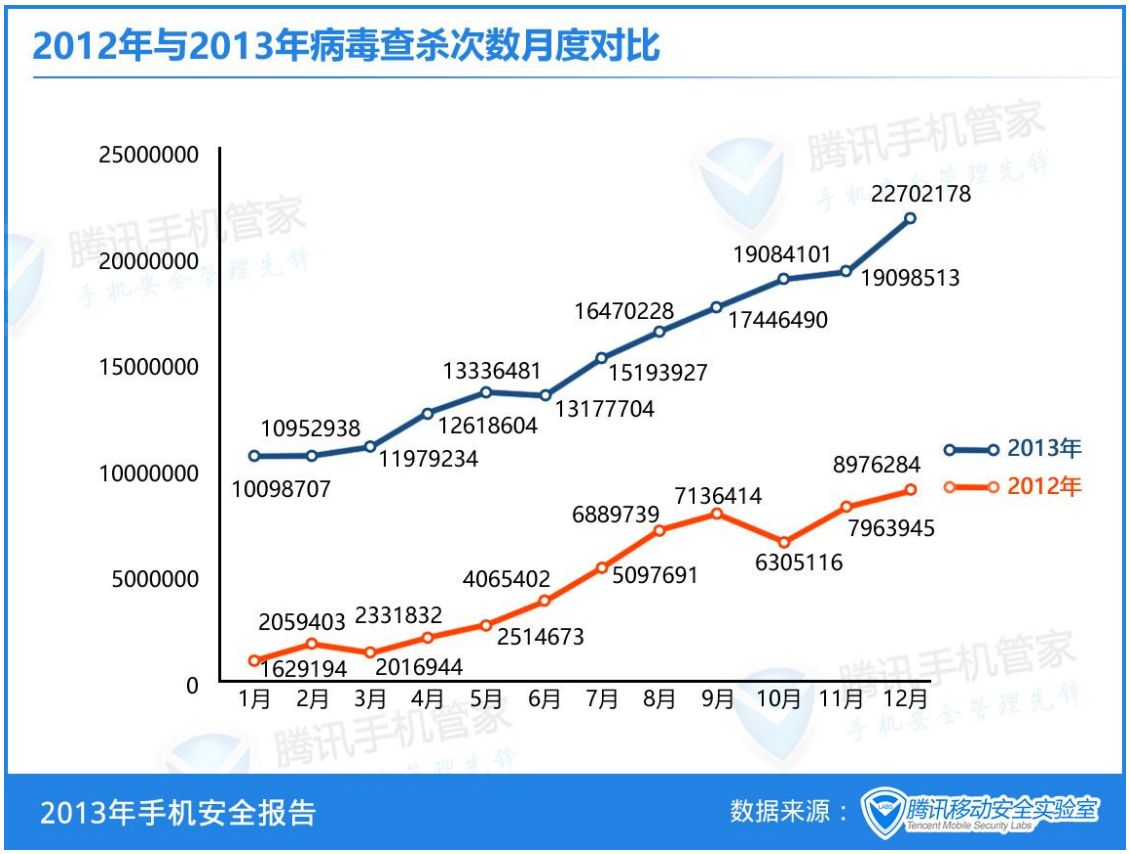


从 2012 年到 2013 年，是截至目前手机染毒用户数激增暴涨的 2 年。2012 年 1 月~2013 年 12 月，手机染毒总用户数突破 1.4 亿，接近俄罗斯总人口。

从 2012 年与 2013 年手机染毒用户数的月度对比值可以看出，两年来的手机染毒用户数均呈现几何式增长态势。2013 年全年，从 1 月到 12 月，手机染毒用户数均呈现出全年平稳快速增长趋势，仅在 10 月有小幅下降，之后再次疯涨。在 2013 年全年，1 月的手机染毒用户处于最低值：604.9 万。12 月达到手机染毒用户最高值：1405 万。即 2013 年 12 月的手机染毒用户人次就已超过 2012 年全年手机染毒用户的三分之一。2013 年第四季度的手机染毒用户均已超过 1100 万。可以看出，2013 年第四季度染毒用户人次已经超过 2012 年全年手机染毒总数。

1.3 2013 年腾讯手机管家查杀病毒次数 1.82 亿次，是 2012 年 3.2 倍

2013 年腾讯手机管家查杀病毒次数为 1.82 亿次，是 2012 年 3.2 倍。2013 年 1~12 月，腾讯手机管家病毒查杀次数呈现逐月上升趋势。1 月，腾讯手机管家为用户查杀病毒次数为 1009.9 万次，为 2013 年查杀病毒次数最低点。12 月查杀病毒次数达到年度顶峰，为 2270 万次。



从 2012~2013 年中毒用户数与病毒查杀次数月度对比可以看出，病毒感染用户与病毒查杀次数大致呈现同样的平稳增长趋势。而 2013 年的感染用户数与病毒查杀次数每月数量都远高于 2012 年。2013 年的感染用户、病毒查杀次数最低月数量均高于 2012 年的中毒用户、病毒查杀次数最高月数量。这是 Android 安全风险激增的一个侧面。

第二章　2013 年垃圾短信状况分析

2.1 2013 年用户举报垃圾短信达到 7.39 亿

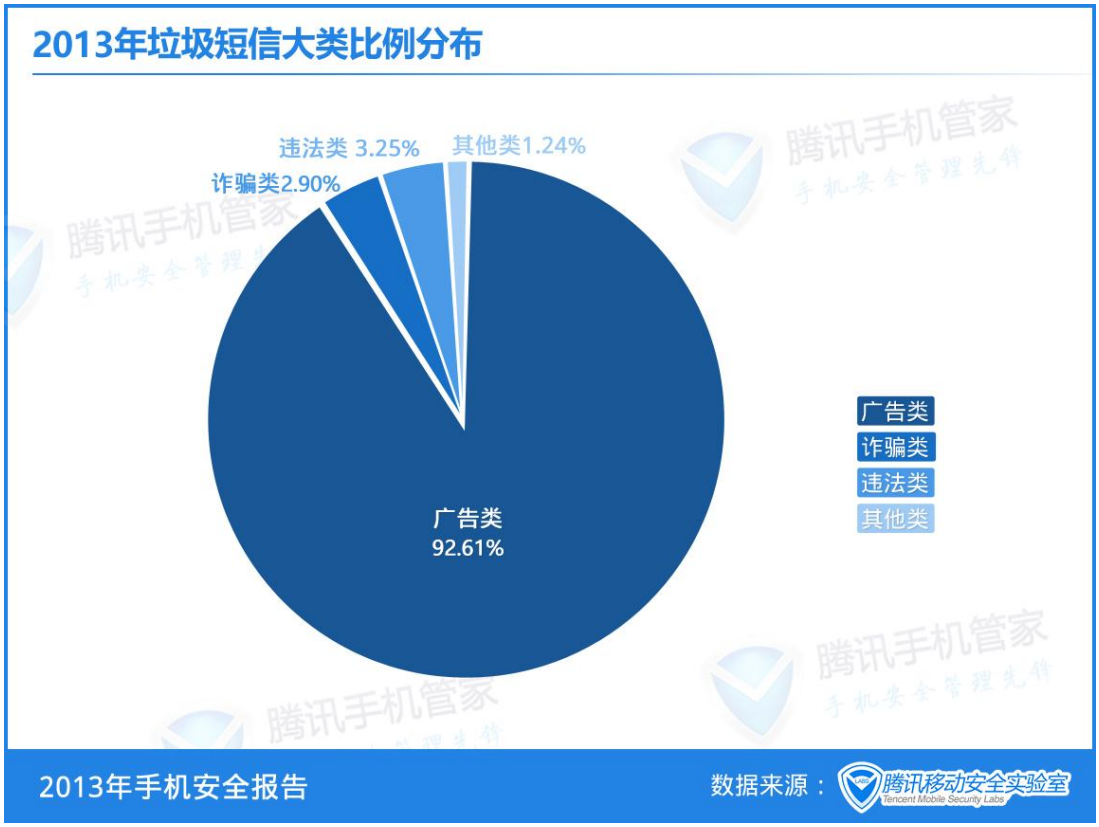
2013 年全年，腾讯手机管家用户举报垃圾短信达到 7.39 亿，在 1 月和 10 月用户垃圾短信举报量最多，均达到 0.73 亿。2013 年 4 月，是垃圾短信举报最低月，举报量为 0.43 亿。

可以看出，从 2013 年 1 月到 2013 年 12 月，用户举报垃圾短信数量全年处于平稳增长状态，相对而言，下半年用户举报垃圾短信量略高于上半年，全年手机用户针对垃圾短信举报呈现比较平稳的状态。

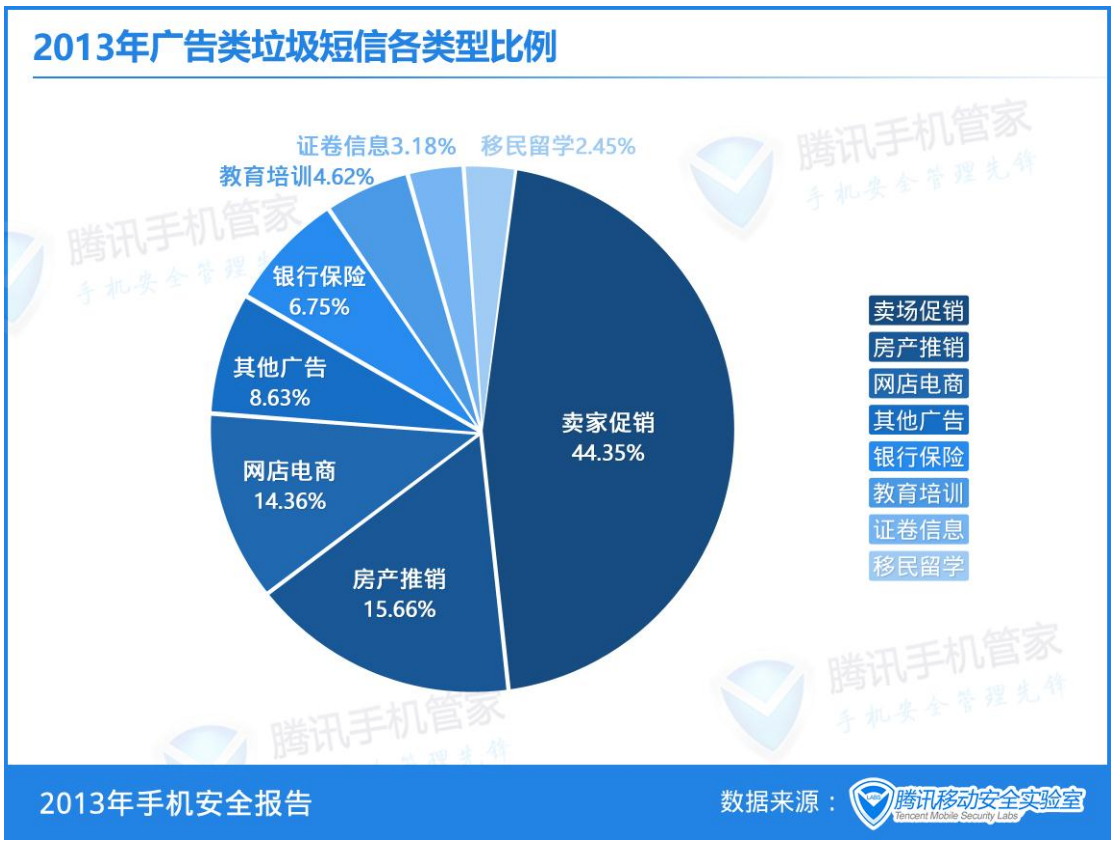
2013 年全年，腾讯手机管家用户举报垃圾短信总量是 2012 年的 2.43 倍，累计垃圾短信举报量达到 11.01 亿。2013 年诈骗类短信举报超过 2141 万。

2.2 垃圾短信各类型比例

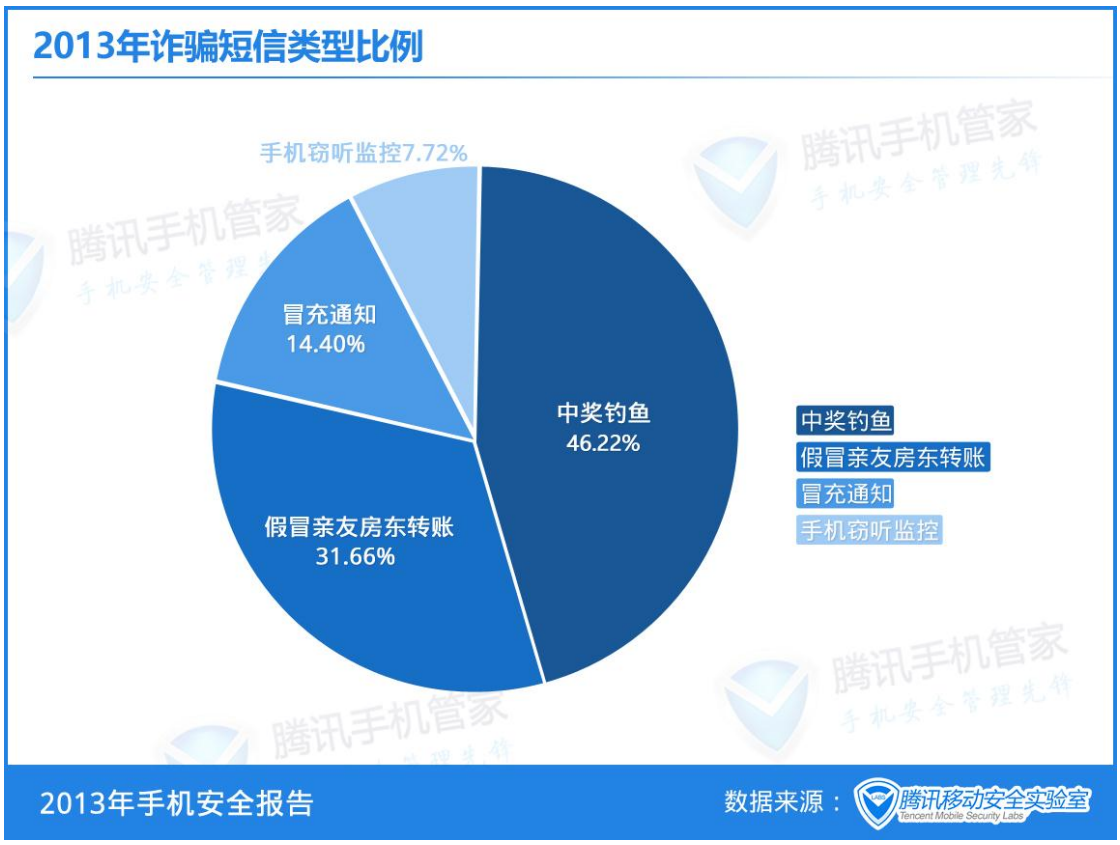
2013 年，在腾讯手机管家用户举报的垃圾短信类型中，广告类短信依然占据最大比例，占比达到 92.61%。违法类占比 3.25%，诈骗类占比 2.9%，其他类占比 1.24%。



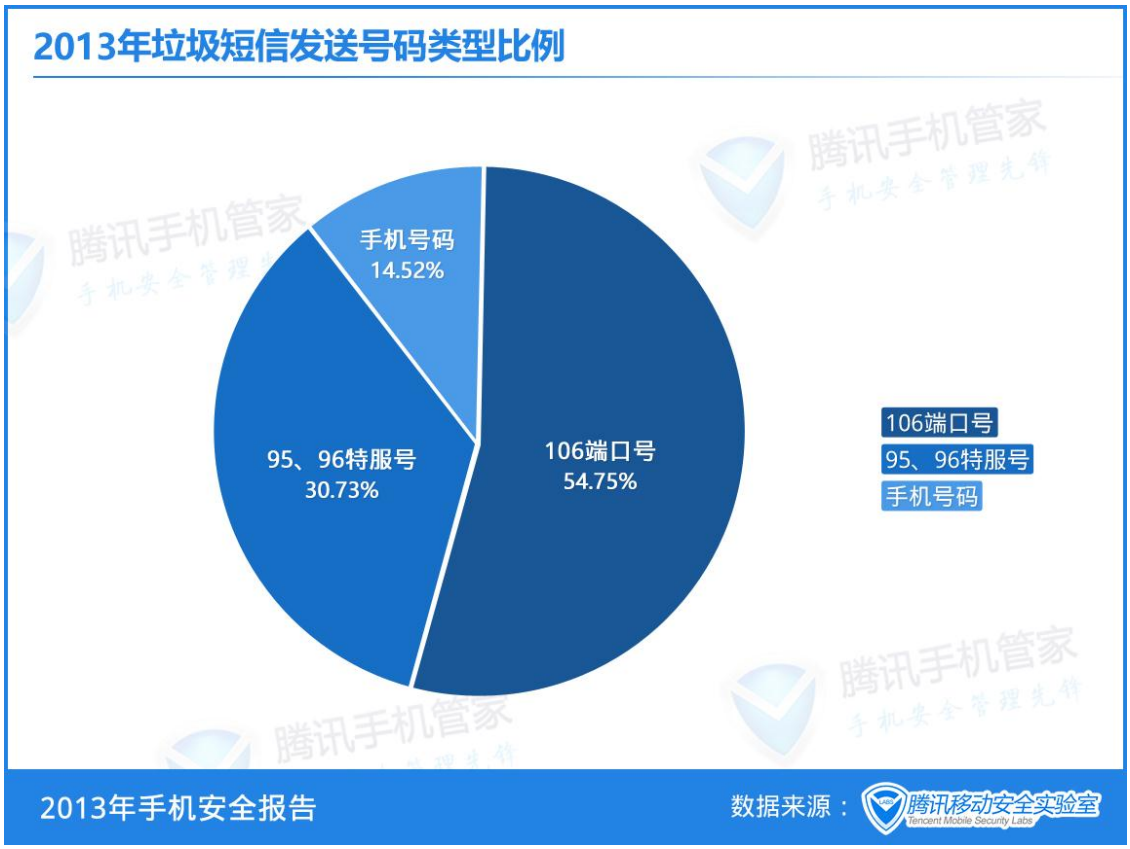
相对 2012 年,2013 年广告类垃圾短信年增长率达到 184.7%。在广告类垃圾短信中，卖场促销、房产推销、网店电商类垃圾短信分别占据前三。卖场促销占广告类比例最大，达到 44.35%，房产推销占比 15.66%，网店电商占比 14.36%。另外，银行保险类与教育培训类垃圾短信也在快速增长，分别占据广告类垃圾短信的 6.75%与 4.62%。



2013 年全年，诈骗类垃圾短信年增长率达到 21.49%。在诈骗短信类型中，中奖钓鱼类诈骗短信占据诈骗短信最大的类型比例，占比达 46.22%。《我是歌手》、《中国好声音》、《爸爸去哪儿》等中奖钓鱼诈骗、网银升级等银行支付类钓鱼诈骗在 2013 年大肆泛滥，中奖钓鱼诈骗也因此成为诈骗类垃圾短信的主流。其次是假冒亲友房东转账类诈骗，占比达 31.66%，冒充通知类占比 14.4%，手机窃听监控占比 7.72%。



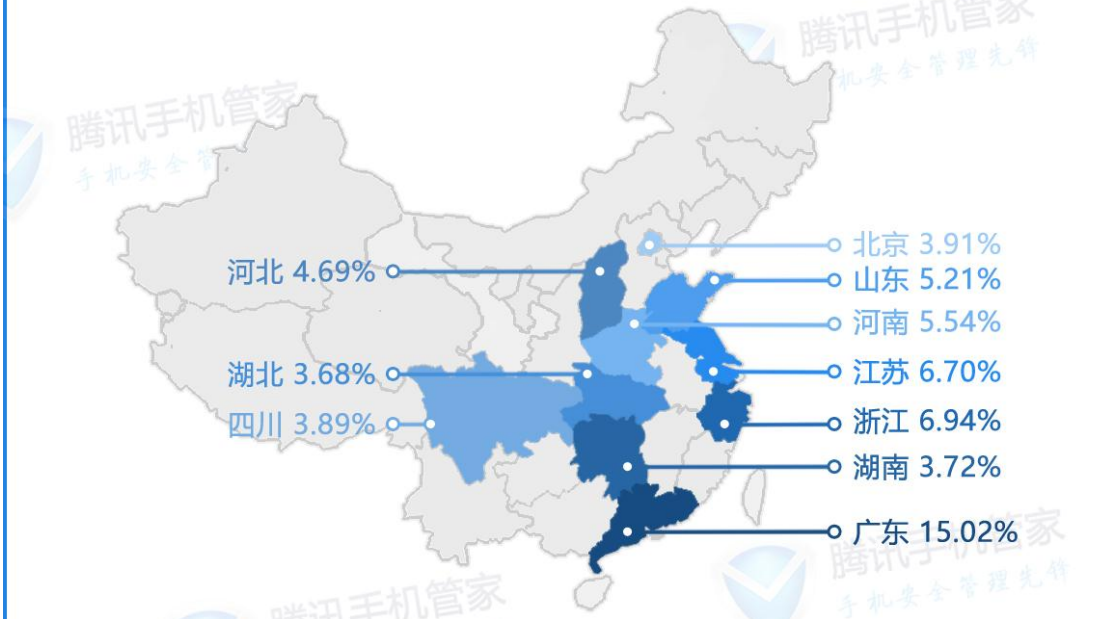
在 2013 年垃圾短信发送号码类型中，106 端口号占比 54.75%，95、96 特服号占比 30.73%，手机号码占比 14.52%。



2.3 2013 年用户举报垃圾短信比例最高十大省份

2013 年全年 ,用户举报垃圾短信各省分布排名前十的省份比例依次分别为:广东、浙江、江苏、河南、山东、河北、北京、四川、湖南、湖北。

2013年用户举报垃圾短信比例最高十大省份



2013年手机安全报告　　数据来源：腾讯移动安全实验室 Tencent Mobile Security Labs

广东以 15.02%的比例位居用户举报垃圾短信第一省份。广东省也成为各种垃圾短信的集中地，其中，在广东省，房东转账、节目中奖、网店电商、房产广告、卖场促销的用户举报比例分别达到 14.11%，14.53%、17.09%、12.36%、8.65%。均位于全国比例第一。广东省作为南方经济大省，城市流动人口众多，房屋中介市场、电子商务、第三产业、小商品市场、移动互联网均比较繁荣，智能手机保有量与出货量高，垃圾短信发送者基于盈利需要，可通过各种渠道获知各类手机号码，集中针对该省份大肆群发垃圾短信。

浙江、江苏、河南、山东垃圾短信举报量分别占比 6.94%、6.70%、5.54%、5.21%。分别位居第二、第三、第四、第五。可以看出，垃圾短信举报占比前五的省份都是人口大省和沿海省份，在这些省份，用户举报垃圾短信积极性在增长，防骚扰意识更加强烈，而用户举报垃圾短信的比例与该省份的垃圾短信总量比例也呈现正相关。沿海经济发达省份市场经济活跃，商场会员消费、电子商务购物、买房租房、求职、各种网站实名注册甚至非法信息交易等各种途径均会使得手机号隐私被泄漏，在人口众多、经济发达的省份也更容易成为垃

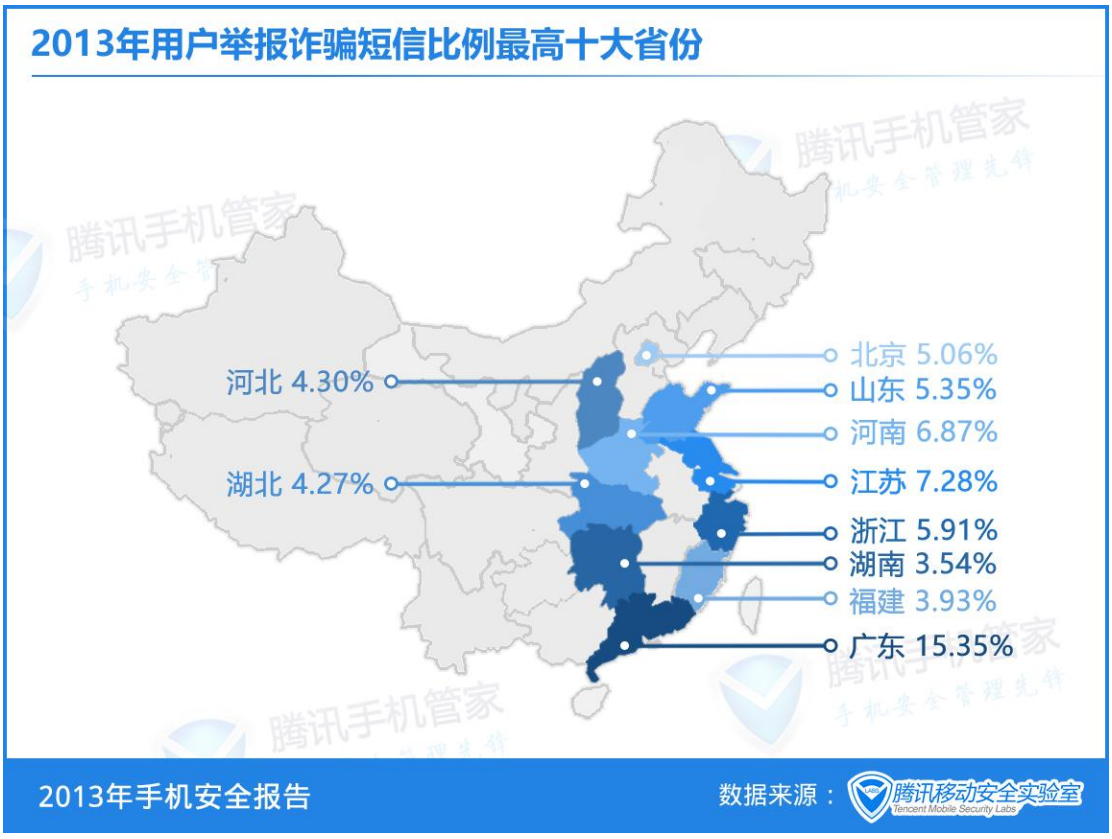
圾短信发送的目标省份。

另外，在四川、湖南、湖北，垃圾短信的举报比例分别达到了 3.89%，3.72%、3.68%。举报比例分别位居全国第八、第九、第十。中西部经济发展省份用户主动防骚扰意识也在持续提升。

江苏省在节目中奖、房东转账、网店电商、卖场促销各类垃圾短信方面的用户举报比例仅次于广东省，该省各类型垃圾短信呈现全面泛滥的趋势。

2.4 2013 年用户举报诈骗短信比例最高十大省份

腾讯移动安全实验室监测，用户主动举报诈骗短信最多的十大省份分别为：广东（15.35%）、江苏（7.28%）、河南（6.87%）、浙江（5.91%）、山东（5.35%）、北京（5.06%）、河北（4.30%）、湖北（4.27%）、福建（3.93%）、湖南（3.54%）。



在用户举报诈骗短信的最高十大省份之中，广东以 15.35%的比例高居第一。其次是江苏与河南，分别以占全国 7.28%、6.87%的比例位居第二、第三。

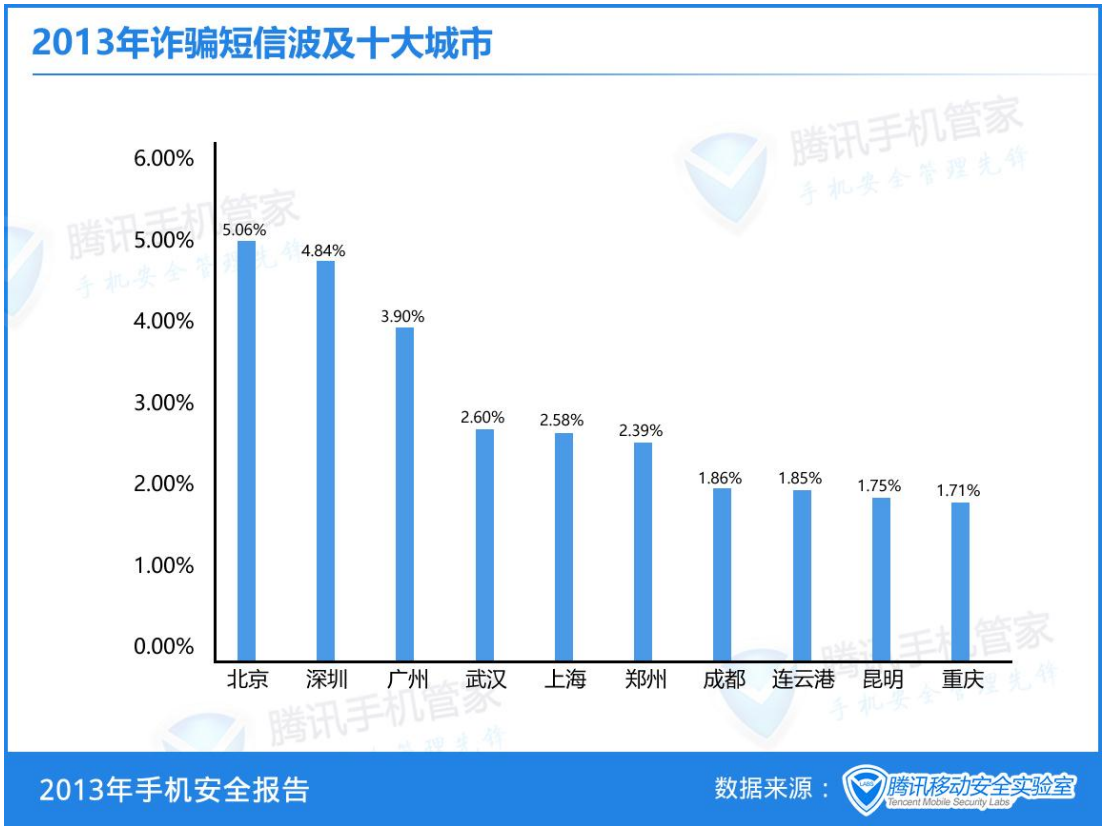
广东省经济相对比较发达，各类务工人员分布广泛，智能机用户量众多，在利益驱使下，大批广告商、诈骗分子针对大批量广东手机用户大批量群发广告类垃圾短信，与此同时，广东省众多“伪基站”窝点的存在也是诈骗短信暴涨的原因之一。

江苏与河南省分别是经济大省与人口大省，河南省人口众多，2013 年随着智能手机用户增长，诈骗短信进一步泛滥。江苏省的娱乐热门电视节目繁荣，导致大量诈骗分子基于地域与用户心理接近性原则，针对该省推送大量节目中奖类诈骗短信。

从总体上分布来看，十大诈骗短信集中于东部沿海、中部经济发展省份。诈骗分子目前正大肆针对山东，湖北、湖南、河北等具有一定经济收入的人群目标人群有针对性的群发大量诈骗短信。由于诈骗短信在各省普遍撒网，参与犯罪人数多，打击取证难度大，这导致短信诈骗在沿海、中部省份大规模存在。

2.5 2013 年诈骗短信波及十大城市

2013 年全年，用户举报诈骗短信最多的十大城市分别为：北京、深圳、广州、武汉、上海、郑州、成都、连云港、昆明、重庆。



北京市是用户举报诈骗短信比例最高的城市，占全国比例达到 5.06%。其次是深圳和广州，分别达到 4.84%、3.9%。武汉和上海分别排名第四和第五，这两个城市的用户举报诈骗短信占全国比例分别达到 2.6%、2.58%。

在全国排名前十大诈骗短信波及城市中，基本是国内一二线城市与省会或区域中心城市。在这些中心城市就业人口多，各种电子商务快递业发达、小商品市场、打折促销品类繁多，流行节目受众广泛，因此在北上广深、武汉、郑州、成都等区域中心城市发送流行节目中奖、网购快递、银行支付类等诈骗短信更加容易定位到相关目标人群。

东、中、西各大省会或区域中心城市人群聚集，经济收入相对较高，诈骗分子倾向于针对市场经济发达城市中有一定经济收入人群定向发送诈骗短信 ,其集中目标城市发送诈骗短信的目的性非常明显：有针对性针对目标人群精准批量发送诈骗短信可以有效提升命中率，导致诈骗短信在这些地区大肆泛滥。

在用户举报诈骗短信占全国比例排名中，连云港、昆明市、重庆市分别位居第七、第

八、第九。比例分别为：1.85%、1.75%、1.71%。而重庆、昆明等城市，随着航空旅游业、电子商务等产业发展，各种诈骗分子也盯上了这些区域城市，在 2013 年第四季度，航班改签、网购支付等诈骗短信一度在重庆、昆明等城市批量出现。

2.6 2013 年十大诈骗短信

2013 年,腾讯移动安全实验室从社会危害、流行程度等方面进行考量,节选出危害最大,数量与公众反响最大的十类典型诈骗短信，提醒手机用户切莫上当受骗。

2013 年,冒充亲友房东转账诈骗是贯穿 2013 年全年的诈骗短信，热门节目中奖类诈骗引起了广泛的用户和媒体关注；冒充政府司法机关诈骗猖獗，网购支付类诈骗短信在第四季度大肆泛滥，航空改签诈骗波及广大航班乘客。

2013 年十大热门典型诈骗短信分别为:冒充亲友房东转账，热门节目中奖、冒充银行支付、航班改签、色情代孕诈骗、赌博诈骗、邮包快递诈骗、网购支付诈骗、冒充政府司法机关诈骗、窃听诈骗。

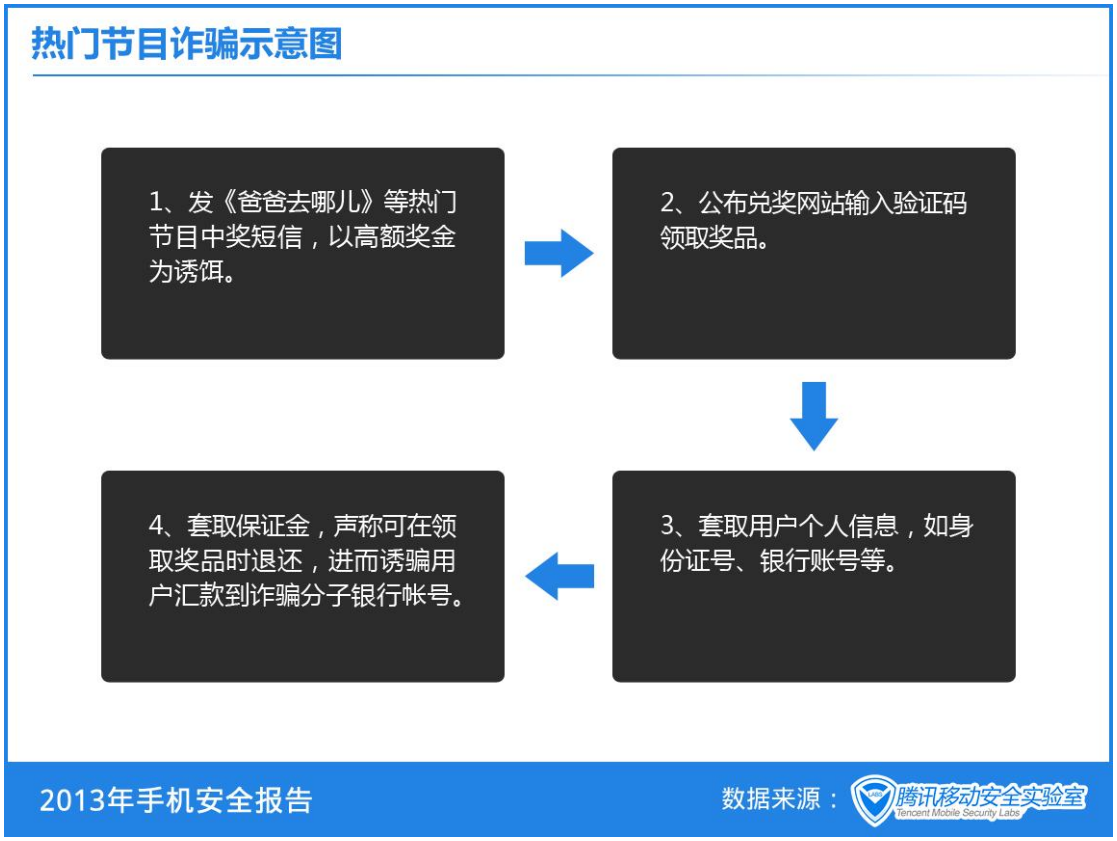
2013年度十大热门诈骗短信	
冒充亲友房东转账	我是房东，换号码了你记一下，以后找我就打这个。另外，这次房租就汇我爱人卡上，工行621226.120900.059***9石娅玲，谢谢。
热门节目中奖（好声音、爸爸去哪儿）	您好，您已被湖南卫视《爸爸去哪儿》抽中为幸运星；获得9.8万元及苹果电脑一台。请用电脑登:bbqne5.com 验证码【5198】
冒充银行支付	尊敬的用户：您的工银电子密码器于次日失效‘请尽快进入我行手机维护网站Wap.icbczh.com进行校准！由此给您带来不便！【工 行】
航班改签	**旅客您好，您所乘坐的***航班因故取消，收到短信后请与我公司联系为您办理退改签手续(退票全额退款，另外多退100元，改签需要缴纳20元手续费)，客服电话******
色情代孕诈骗	张洁30岁，联系电话:18370368***夫港商，因失去生育能力，找健康男士与我怀孕，通话满意速汇定金50万，有孕重酬100万。
赌博诈骗	澳门金沙国际娱乐城宝马等你开回家www.8343.com首存多少送多少！线上游戏有足球，香港乐透，百家乐，时时彩，股票等，3分钟提款到帐。
邮包快递	您好,您有一份包裹已到，因地址不详派送不成功。请速与工作人员联系；130674728**
网购支付	关于您的订单在付款过程中出现系统卡单问题，导致您的资金已被冻结请您及时与淘宝客服联系4009902***退款，否则24小时内资金全部冻结
冒充政府司法机关诈骗	最后通告:您有一张法院传票尚未领取,请于下午4点前领取；过期将冻结其个人账户资产；电询31551**【中级人民法院】
窃听诈骗	18925096***:只要你有他号，就能知道他跟谁说什么，给谁发什么。也可知道他在哪:如需/请找183322079**小安子
数据来源：腾讯移动安全实验室 Tencent Mobile Security Labs	

1.房东转账：这类诈骗短信内容一般是: “我是房东，换号码了你记一下，以后找我就打这个。另外，这次房租就汇我爱人卡上，工行 621226.120900.0593***石娅玲，谢谢”。通过这种简单直接的方式诱导手机用户将房租汇到诈骗分子的帐号上。而这类诈骗短信波及用户广泛,令人防不胜防。

2.热门节目中奖：其中，《我是歌手》、《中国好声音》、《爸爸去哪儿》是被诈骗分子冒充次数和频率最多的三大热门节目。典型的诈骗短信为：“尊敬的用户，恭喜您手机被湖南卫视《爸爸去哪儿》抽选为幸运嘉宾，请登陆活动网 hunanvy.com 获取万元现金大奖和苹果电脑，验证码:6558”。

这类诈骗短信的诈骗流程一般是，首先发中奖短信高额奖金为诱饵；进而公布兑奖网站

输入验证码领取奖品。然后套取用户个人信息，如身份证号、银行账号等，最后套取保证金，声称可在领取奖品时退还，进而诱骗用户汇款到诈骗分子银行帐号。

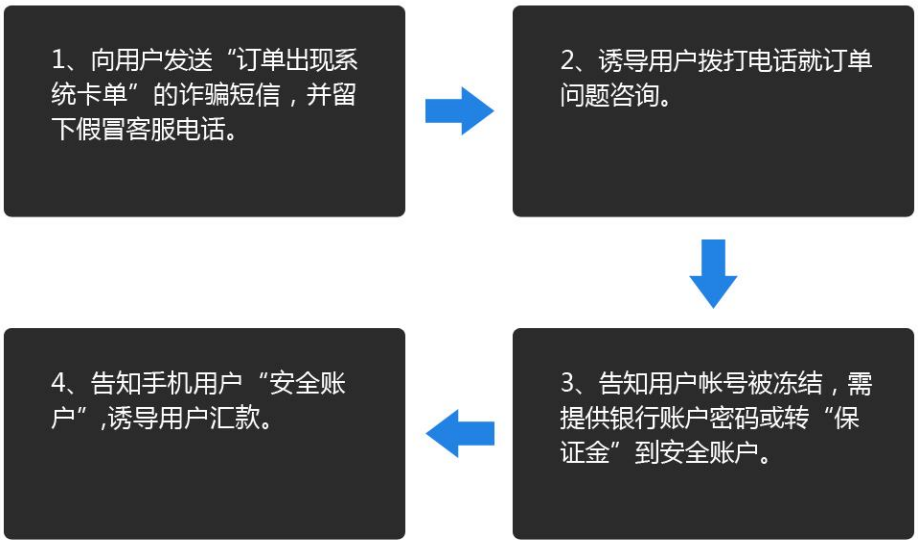


3.网购支付诈骗：2013 年第四季度以来，国庆节、光棍节、双十二、圣诞节等各大节日纷纷来临，全民网购也让诈骗分子嗅到商机，网购支付类诈骗纷纷涌现。

该类典型诈骗短信是："关于您的订单在付款过程中出现系统卡单问题，导致您的资金已被冻结请您及时与淘宝客服联系 4009902***退款，否则 24 小时内资金全部冻结。"

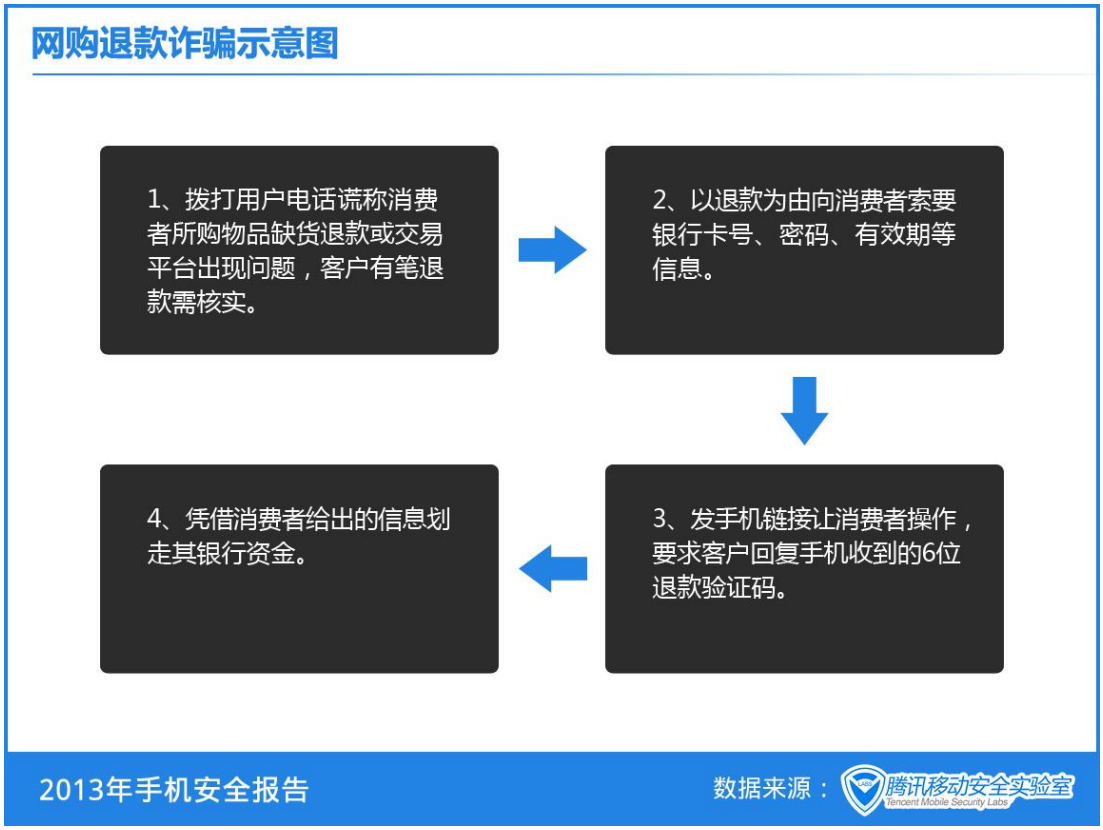
该类诈骗短信的一般流程是：首先向广大用户发送"订单出现系统卡单"的诈骗短信，通过上述订单问题诱导用户回电话咨询，之后告知用户账号被冻结，最后要求用户提供银行账户密码信息，或转账保证金到"安全账号"。

网购支付诈骗示意图



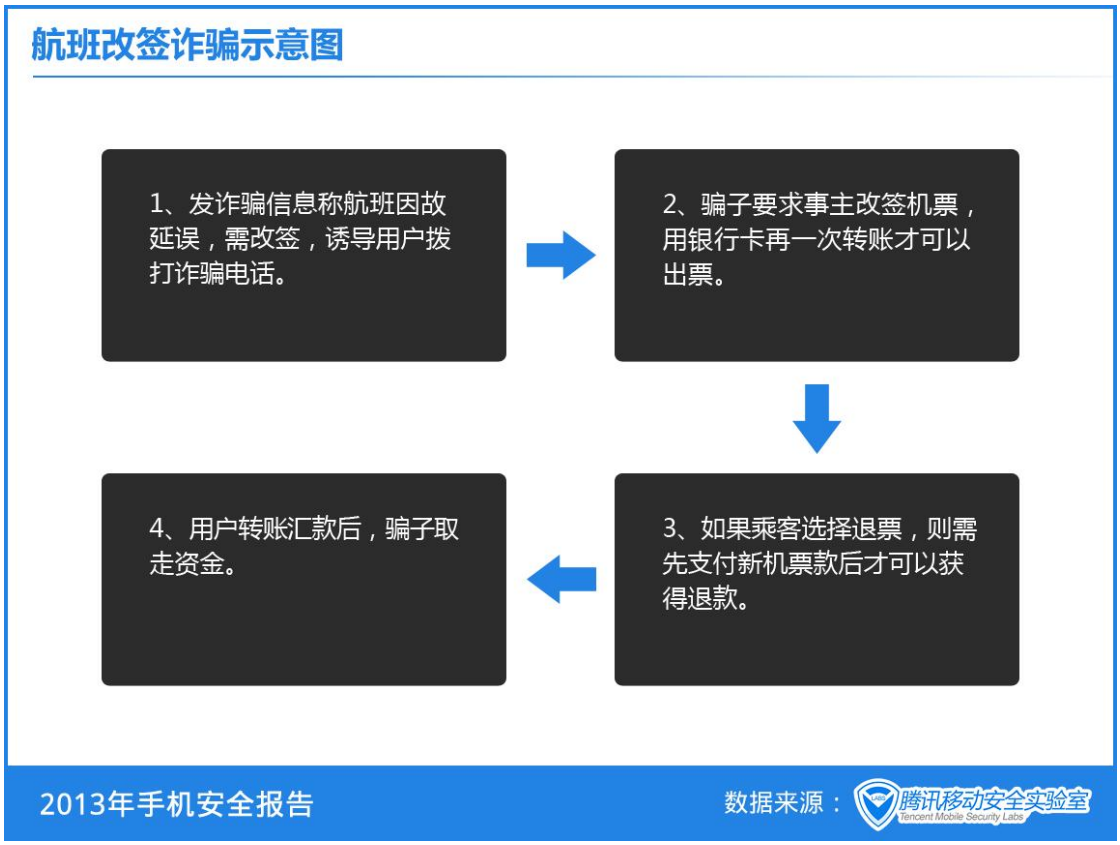
2013年手机安全报告　　数据来源：腾讯移动安全实验室 Tencent Mobile Security Labs

另一类网购退款诈骗是：打电话自称天猫或淘宝客服，并报出用户的订单详细信息与收货地址，称商品没买上需要退款重拍，并给出链接，进而引导用户申请退款、重拍、发送卡号和验证码，要求用户填写支付宝账号、密码等信息。而诈骗分子会利用用户泄露的银行支付信息划走用户的款项。



4.航空改签诈骗：“***旅客您好，您所乘坐的***航班因故取消，收到短信后请与我公司联系为您办理退改签手续(退票全额退款，另外多退 100 元，改签需要缴纳 20 元手续费)，客服电话******* “

2013 年年尾，众多手机用户向腾讯手机管家反馈：航班改签与退票类诈骗短信猖獗，导致众多航班乘客中招。而腾讯手机管家用户也在年尾举报了大量新型的航空改签退票类诈骗短信。

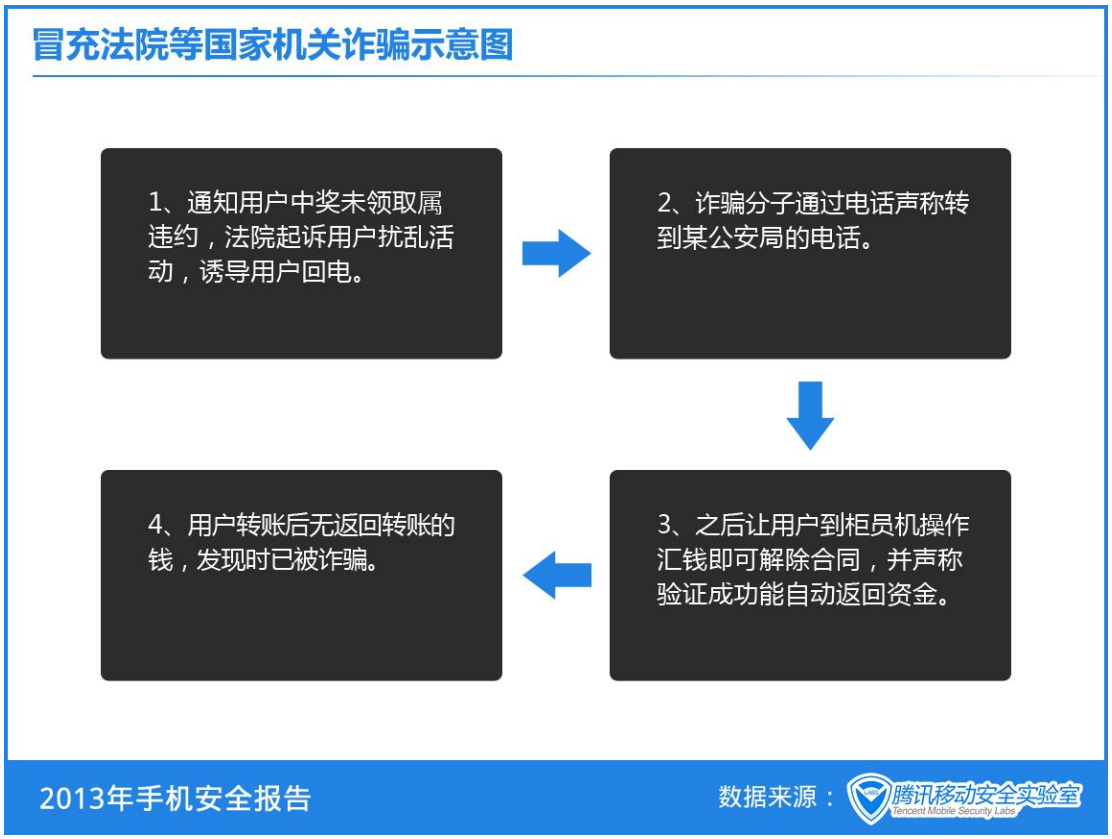


腾讯移动安全实验室监测，航班取消类诈骗短信由于仿真度高，并且准确知道事主的身份证号和航班信息，导致众多航班乘客不幸上当。航班诈骗分子通过要求事主改签机票，诱导用户进而用银行卡再一次转账，事主在按照骗子的指示一步步走进陷阱。手机用户应引起足够的警惕。

5.冒充政府司法机关诈骗：“您好！北京法院通知您！《北京卫视最美和声》把您一份全年 09 日的违约资料传来本法院，要向本法院起诉您违约，起诉您故意扰乱本次活动，请您与本法院联系解除合同。司法部：9501316909555 否则本法院 24 小时后发送您的传票，48 小时通知您当地的公安局出动警力对你强制性的进行逮捕拘留审判。”

这类冒充法院等国家机关的诈骗短信一般流程是：告知用户中奖未领取属违约，法院将起诉用户扰乱活动，诱导用户回电，然后声称转到某公安局的电话；之后让用户到柜员机操作，将钱转到指定的“验证账号”，便可解除合同，并声称验证成功能自动返回短信。用户

转账后无返回转账的钱，发现时已被骗。



6.赌博诈骗：“顶级信誉葡京国际娱乐城官网：www.12771277.com 首存赠送 30%线上游戏有足彩、港彩、时时彩、百家乐、股票等，让您玩转澳门！”这类诈骗短信开始给用户一些甜头，让用户赢一些小额的钱；之后诱导用户多充值，待用户充值后，输多赢少；最后将用户的钱“输”光。这类诈骗短信针对那些有赌博方面偏好的用户，往往十分见效。

7.邮包快递诈骗：“您好,您有一份包裹已到，因地址不详派送不成功。请速与工作人员联系；13067472839。”随着电子商务的进一步繁荣，邮包快递诈骗在 2013 年度成为一个突出的诈骗现象。这类诈骗短信基本都会涉及到“地址不详、无法派送“等关键词，并留下联系电话。诈骗分子其目的就是诱骗事主打电话，告知用户邮包藏毒，通过各种手段套取手机用户的银行账号、家庭住址等信息，进而要求用户转账保证金。用户一旦转账，便落入陷阱。

8.窃听诈骗：“18925096437:只要你有他号，就能知道他跟谁说什么，给谁发什么。也可知道他在哪:如需请找 18332207922 小安子”。

这类诈骗的一般流程是：1、告诉用户可以实现各种窃听、克隆电话卡的功能，加钱可以增加定位等功能，要用户转账 500~上千块的订金，转账后人间蒸发。

9.年费诈骗：腾讯移动安全实验室监测，2013 年年底，大量手机用户通过腾讯手机管家举报年费诈骗短信，典型的诈骗短信内容为：短信通提醒，于全年 28 日将从你的银行卡上扣除年费 1200 元 ,疑问请咨询 0532—66635***。不知情的手机用户会迅速回电咨询，对方会以“资金不安全”、“账目需要重新清理”等借口诱骗手机用户缴纳相关费用或者输入网银密码核对等，让手机用户前往 ATM 柜员机上操作，继而将受害人资金转移至诈骗分子指定帐号。

这类诈骗短信有如下特征：1、短信内容上看，一般没有提及尾号、尾数以及具体卡号信息的。2、一般声称信用卡年费上千的或者牵涉到需要用户银行帐号、密码信息的基本都

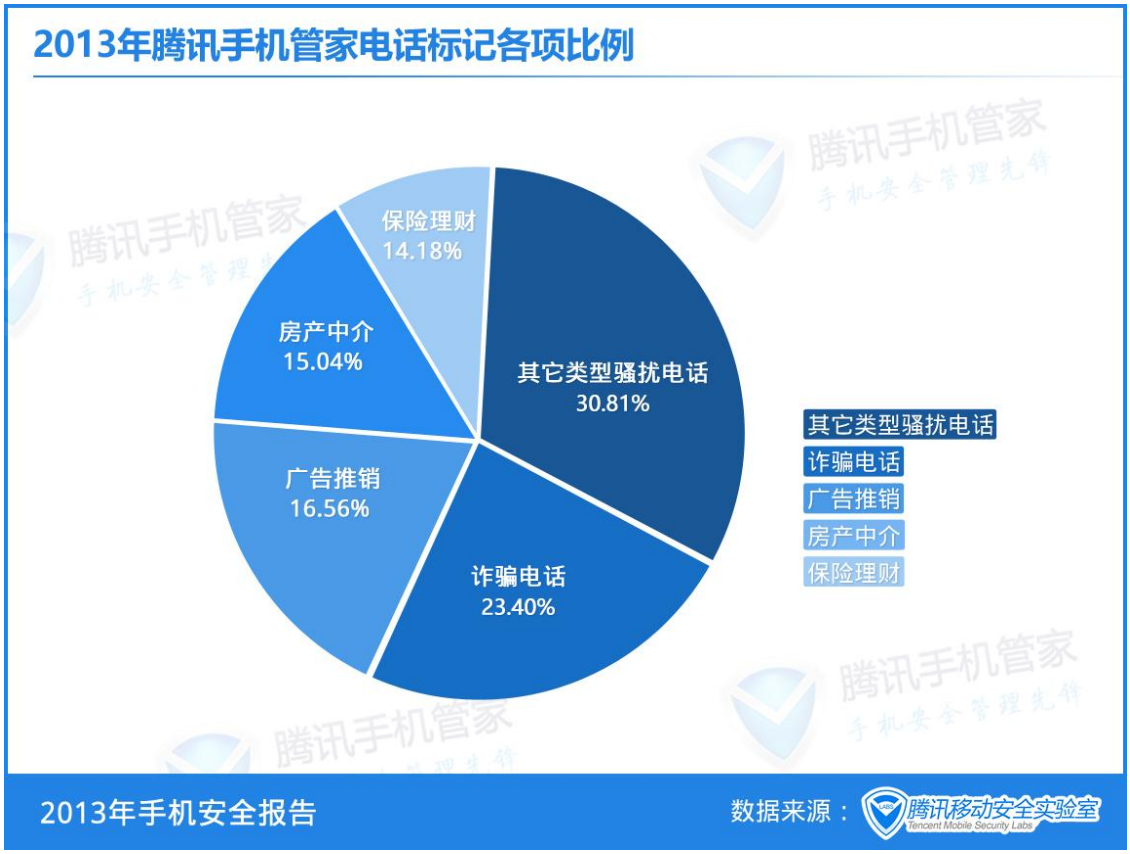
是诈骗。

10.色情代孕诈骗：典型诈骗短信案例为：“张洁 30 岁，联系电话:18370368677 夫港商，因失去生育能力，找健康男士与我怀孕，通话满意速汇定金 50 万，有孕重酬 100 万。”

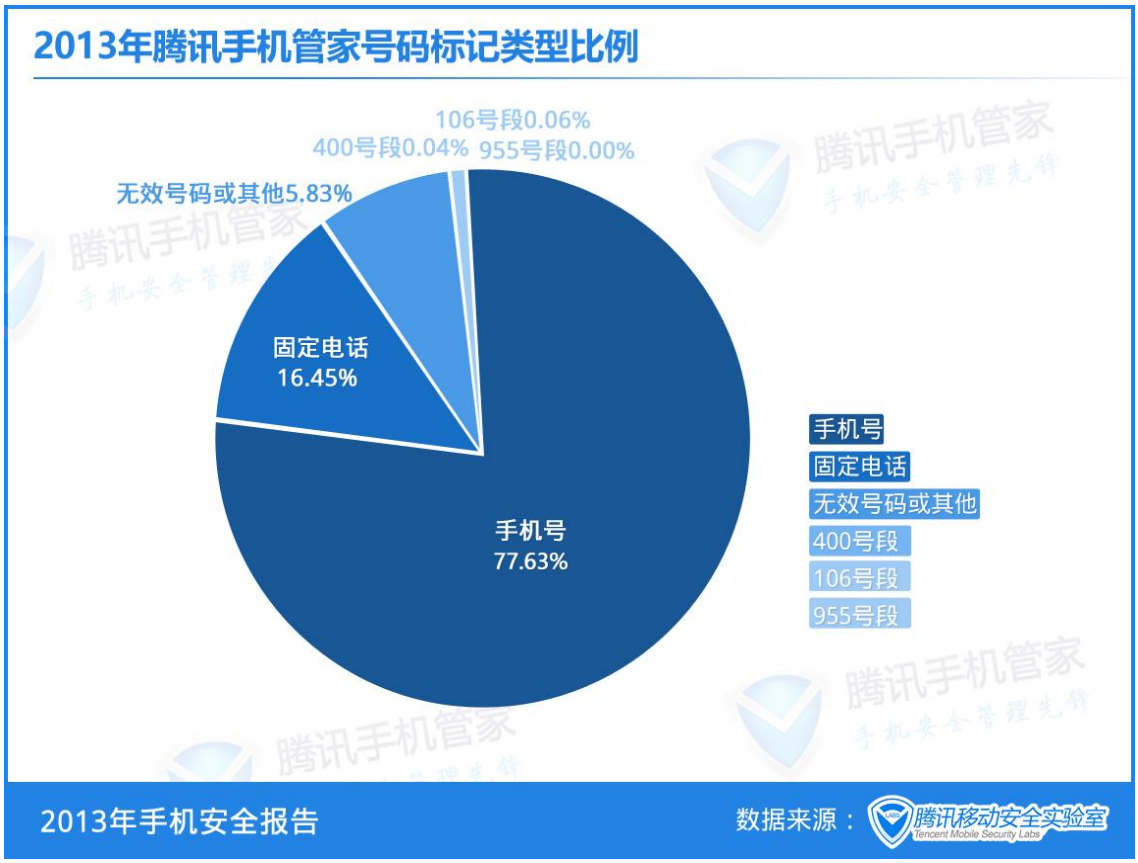
腾讯移动安全实验室提醒手机用户：手机用户若收到”幸运号用户”、“系统卡单“、”安全帐号“、”验证码“、“中奖“、“法院通知”“年费“、”网银升级“、”包裹地址不详“、航班退款（改签）等关键词的短信即可确定为诈骗短信，最好开启腾讯手机管家等安全软件有效拦截此类诈骗短信，避免不必要的利益损失。

2.7 2013 年腾讯手机管家用户针对骚扰电话标记总次数为 1.02 亿

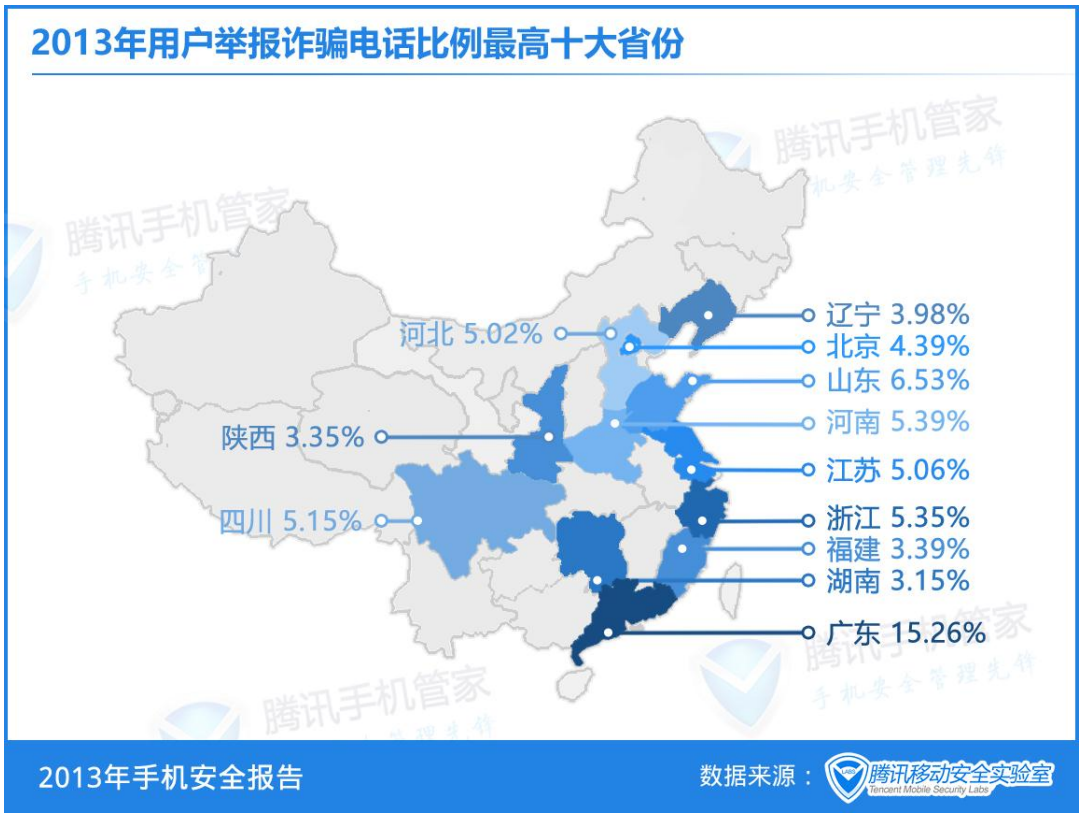
截至 2013 年底，腾讯手机管家针对骚扰电话进行标记的总次数为 1.02 亿，电话标记总数量为 2796.4 万个。腾讯手机管家用户标记各种骚扰电话的类型比例分别为：诈骗电话为 23.4%，广告推销为 16.56%，房产中介为 15.04%，保险理财为 14.18%，其他类型骚扰电话为 30.81%。



2013 年全年，腾讯手机管家号码标记类型中，手机号占据最大的比例，达 77.63%。固话占比 16.45%,无效号码或其他占比 5.83% ,106 号段占比 0.06% ,400 号码占比 0.04%。



2013 年全年，用户举报诈骗电话比例最高十大省份为：广东、山东、河南、浙江、江苏、四川、河北、北京、辽宁、湖南、陕西、福建。



广东省以 15.26%的高比例占据用户举报诈骗电话第一的位置。

而山东、河南、浙江、江苏分别以 6.53%、5.39%、5.35%、5.06%的比例位居第二、第三、第四、第五。可以看出，这四个省份的比例非常接近。在地理位置上，四省位于中东部、东部沿海。四省份经济发展迅速，智能机出货量大增，成为各种诈骗电话的目标省份。

诈骗电话往往是诈骗短信的衍生后续手段。因此，诈骗电话最高的十大省份往往与诈骗短信分布的规律相似。在经济发达省份与沿海地区的手机用户收到诈骗电话的机率更高。电话诈骗手法多样，不断衍生出新的变种。由于诈骗电话往往骗取的金额非常高，同时取证难，因此诈骗电话近年来呈现多发趋势。在广东、北京、江苏、浙江等地，由于市场经济发达，诈骗分子往往通过刷卡消费、虚假中奖、高薪招聘诈骗等手段为诱饵，致使大量不明真的手机用户上当受骗。

在山东、河南两省，诈骗电话举报比例分别达到 6.53%，5.39%。在这些地区，经济发展，市民收入正在进一步提高，退税退款、低价购物等诈骗手段比较常见。

四川、陕西两省的诈骗电话举报比例也分别占据了 3.35%、5.15%。分别占全国举报诈骗短信比例的第六与第九。诈骗短信正逐渐有针对性中西部发展省份迁移。

第三章　2013 年垃圾短信特征分析与解决之道

2013 年以来，垃圾短信呈现大规模泛滥的态势，并引发了社会各界、政府部门、运营商、手机安全厂商等各方关注。2013 年垃圾短信的总体增量远超 2012 年，覆盖全国各省份，影响社会各界与各个行业，影响恶劣。

3.1　垃圾短信地下产业链形成，社会呼吁联盟力量反制

垃圾短信尤其是诈骗类短信的发送者开始利用先进技术来牟利，伪基站窝点迅速发展。各种卖场促销、医疗美容广告商通过伪基站群发广告类垃圾短信，可提升精准度与节约成本。目前，派传单与区域硬广的方式正逐步往伪基站迁移。

诈骗短信是目前对民众的经济生活造成严重干扰和威胁的垃圾短信类型。2013 年以来，各种诈骗短信层出不穷，花样翻新，涨势迅猛，诈骗金额巨大，给民众的经济生活造成了巨大的威胁。

垃圾短信正在广泛的侵扰市民的正常通信和私人空间生活，许多短信群发公司通过聚敛客户，业务遍及房地产、汽车、并形成地下垃圾短信产业链。

与此同时，垃圾短信到达率高、限制少、取证难、难以管理和监督。单靠政府或企业的一家力量已很难彻底打击。因此社会各界携手达成共识，建立制度规范、整合产业链和动员社会各界与政府的力量来反信息诈骗成为当务之急，也是社会各界的共同心声。

2013 年全年，中国电信发布《关于进一步从严治理垃圾短信的通知》，严格落实平台及端口短信的责任制，并出台系列从严问责办法。2013 年 12 月 26 日，腾讯手机管家协同社会各界、政府组织成立了反信息诈骗联盟。

3.2　反信息诈骗联盟成立改变反诈骗单兵作战的现状

2013 年 12 月 26 日，腾讯公司联合广东省公安厅、中国互联网协会、银监局、银行协会、三大运用商、世纪佳缘、去哪网等政府组织、企业共同发起了国内首个反信息诈骗联盟，旨在动员全社会力量，通过标记诈骗电话和短信、数据共享、案件侦破受理及安全防范教育等深度合作，向日益猖獗的信息诈骗产业链发起全面反击。

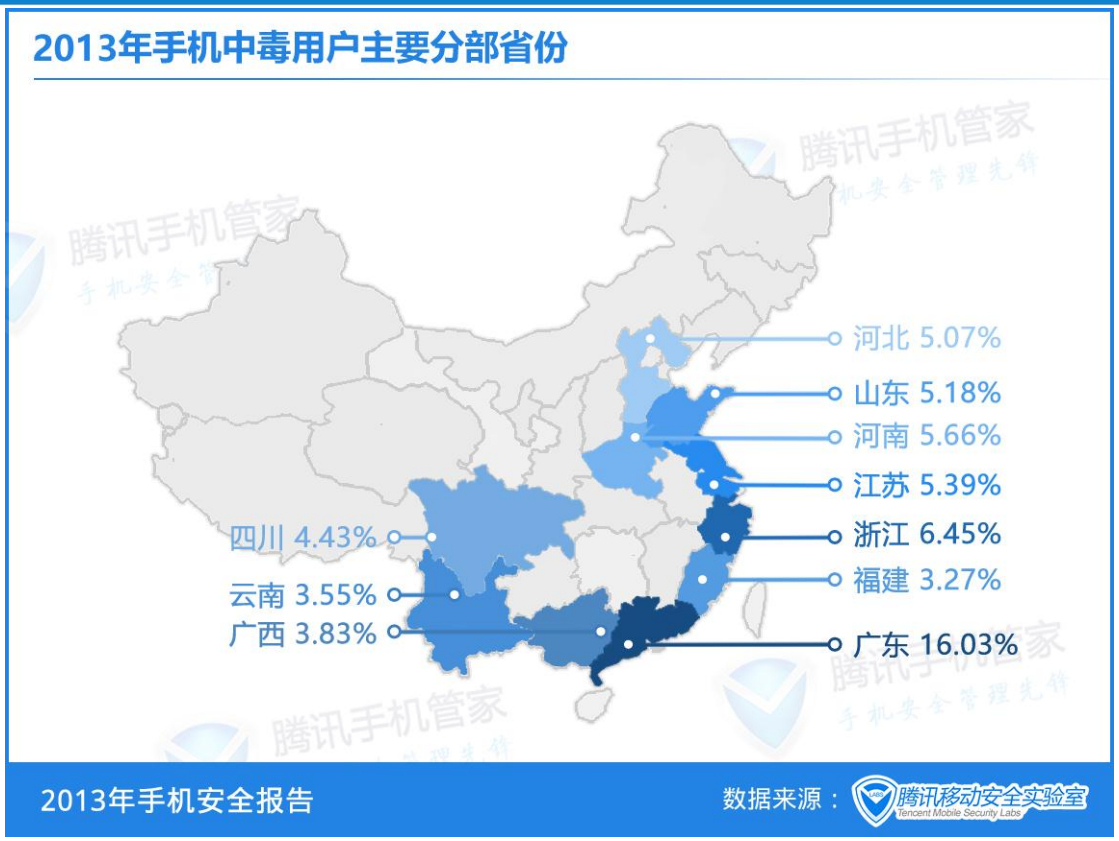
反信息诈骗联盟的成立，对手机用户而言也利好消息，基于腾讯公司的庞大用户和数据基础，建设一个由政府、警方、银行、企业、运营商等全面协同的反信息诈骗联盟，致力于打造一个“网络+社交”的反诈骗信息网络，改变了过往打击信息诈骗单兵作战、各自为政的现状。

3.3 各链条联动提升打击诈骗短信效率

目前，反信息诈骗联盟的成立作为整合产业链的力量共同打击诈骗短信的试水案例，基于腾讯手机管家的诈骗举报功能，可以将诈骗线索及数据与警方共享，极大提升侦破骗局的机率。与此同时，针对诈骗中“资金转移”这一核心环节，警方联合银行系统可以做到及时帮助民众冻结操作，避免或减少被骗损失，未来还将针对骗子建立银行账号黑名单机会。通过各链条联动极大提升了打击诈骗团伙的有效性，该联盟可对诈骗产业链形成极大的威慑力，也将极大的降低诈骗短信对民众的经济与感情伤害，随着法律法规进一步健全，各方合作的进一步深入，整合产业链的力量共同打击诈骗短信的效果将会更加显著。

第四章 2013 年手机染毒用户各省分布

在 2013 年全年，全国手机染毒人次达到 1.05 亿，与整个广东省人口相当。手机染毒省份区域分布上，广东省以 16.03%的比例占据全国手机染毒第一，整个 2013 年，广东感染手机用户人次达到 1694.19 万，是 2012 年的 3.32 倍，即 2013 年广东省染毒人次同比增长 232%。广东省作为华南地区各种 Android 智能机的集散地，水货手机出货量大，手机用户众多，刷机用户与 APP 下载量增势明显，导致广东省长期居于手机染毒第一省份。



在 2013 年，国内手机染毒人次最多的十大省份与占据全国比例依次分别为广东（16.03%）、浙江（6.45%）、河南（5.66%）、江苏（5.39%）、山东（5.18%）、河北（5.07%）、四川（4.43%）、广西（3.83%）、云南（3.55%）、福建（3.27%）。可以看出，排名前十大省份手机染毒占全国比例达到 58.84%，这十大省份染毒手机用户总数达到 6178.2 万,排名前十省的手机染毒总人次超过安徽省全省人口。

2013年全年手机病毒主要分布省份			
广东	16.03%	江西	2.57%
浙江	6.45%	甘肃	2.04%
河南	5.66%	内蒙	2.04%
江苏	5.39%	黑龙江	1.99%
山东	5.18%	重庆	1.88%
河北	5.07%	吉林	1.79%
四川	4.43%	新疆	1.69%
广西	3.83%	上海	1.56%
云南	3.55%	天津	1.17%
福建	3.27%	海南	0.64%
湖南	3.16%	宁夏	0.60%
北京	3.11%	青海	0.44%
辽宁	2.82%	西藏	0.20%
安徽	2.71%	香港	0.12%
陕西	2.67%	台湾	0.06%
贵州	2.63%	内蒙古	0.02%
湖北	2.61%	澳门	0.02%
山西	2.60%		
数据来源：腾讯移动安全实验室 Tencent Mobile Security Labs			

在手机染毒的地域分布上，东南沿海与西南重省成为手机用户染毒的聚集省份。手机染毒区域在环渤海、环长三角、珠三角与西南三省聚集，整体呈现“U 状”弧形分布。江浙两省由于市场经济发达，水货手机、刷机用户与 APP 下载用户活跃增长，山寨机等出货量众多，造成智能机染毒用户居高不下，两省手机染毒总量超过 1243 万。

另外，在河南、山东两省，智能机消费者增长迅速，达到 5.66%与 5.18%。在河南省，

智能手机产业的上下游产业链正在逐步完善，各种以手机整机研发、生产制造于一体的产业基地与代工厂正在快速发展，新兴智能机用户大幅增长，但与此同时，用户手机安全意识不强，许多用户在 APP 下载中对渠道的选择缺乏谨慎态度，许多内置恶意软件的水货手机也在市场大量流通，导致手机用户染毒占比进一步提高。

在四川、广西、云南这西南三省，随着经济增长，各种品牌厂商抢滩登陆，智能机新兴用户增长，染毒手机用户也在持续增长。

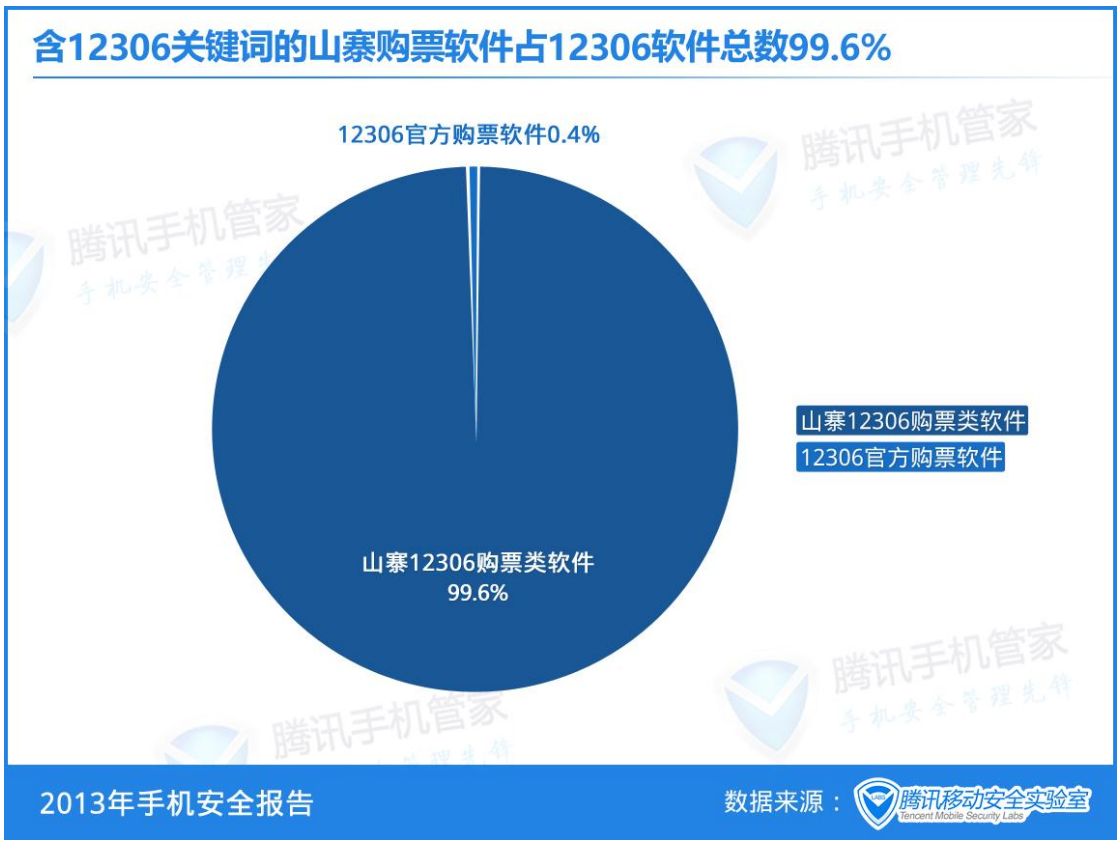
第五章　山寨手机购票类 APP 抽样分析

2013 年 12 月,随着春运临近,各种抢票软件应运而生,含病毒或恶意插件的山寨抢票软件迅速增长。2013 年 12 月，腾讯移动安全实验室针对含有“火车票、订票、购票、机票、抢票、列车时刻表、抢线、抢票攻略”等 17 类关键词分类，随机抽取包含上述关键词的手机购票类软件包共 8423 个进行检测统计，统计发现，在 8423 个手机购票类软件中，有官方版本的购票类软件包为 2778 个,而被二次打包的非官方山寨购票软件包达到 6940 个。山寨购票软件包占比高达 82.4%。

在 8423 个手机软件软件包中，含病毒包数达到 142 个，占比 1.69%；含恶意广告插件的包数达到 2855 个，占比达到 33.9%。

腾讯移动安全实验室统计发现，在 8423 个手机购票软件包中，含“12306”软件包共 778 个 ,官方包仅为 34 个 ,占比为 0.4% ;而含 12306 的山寨软件包达到 744 个 ,占 12306 软件包的 99.6%。

含“12306”关键词的病毒包有 30 个，官方包与病毒包几乎一样多。含“12306”关键词的病毒软件占手机购票类病毒包总数的 21%。



5.1 打包党年底紧盯购票类 APP 大肆打包吸金

在取样统计的手机购票类 APP 中，其中，山寨购票软件包达到 6940 个，其中含“火车票“、”订票“、”12306”、“机票”四类关键词的 APP 数量在山寨购票软件包数量中排名前四，分别含有 2605、747、744、706 个山寨软件包。其中各类别典型恶意软件分别为：伪“实时火车票”、伪”呼呼火车订票电话“、伪“春运购票全攻略秘籍”、伪“12306订票大师”、伪“机票酒店”、伪“抢票大师”。

在“火车票”类的山寨购票软件中，病毒软件包达到 32 个，其中“实时火车票“被病毒 a.expense.g3app.a 感染，该病毒在“实时火车票”中植入恶意推广广告，私自下载推广软件，给用户造成资费消耗。

而“抢票大师”被病毒 a.payment.geinimi.a 感染，该病毒以游戏名义诱导用户下载安装，激活后自动删除通话记录，并添加联系人，获取手机中的短信，泄露用户隐私，并在

后台发送短信等恶意行为，可以看出，该病毒已对手机用户的支付确认类短信隐私构成重大威胁。

在被感染的手机购票 APP 中，“12306 订票助手”是被病毒打包感染用户最多的“12306”类软件。感染“12306 订票助手”的典型病毒为 a.expense.kbanner。该病毒运行后下载恶意代码，同时获取用户的手机信息。

另外，在火车票余票查询这款软件中，被二次打包植入了扣费类病毒 a.payment.paojapp.b，该病毒会订购一个名为"**业务 支付*元/月"的业务，同时会屏蔽运营商订购回复短信,在用户毫不知情的情况下被恶意扣取资费。可以看出，打包党在年底紧盯“购票类”APP 吸金已渐成趋势，而窃取隐私与扣费是打包党主要的目的。

5.2 2013 年 12 月染毒手机购票软件 TOP10 统计

2013 年 12 月，感染用最多的十大染毒手机购票软件分别是伪“12306 订票助手”、伪“实况模拟列车”、伪“火车订票抢线”、伪“实时火车票”、伪“机票酒店”、伪“春运火车票购买”、伪“铁友火车票”、伪“火车票抢票”、伪“火车票验证器”、伪“掌上机票”。这十款染毒山寨购票软件目前共感染手机用户已达到 13.92 万。

2013年12月感染用户最多的十大染毒购票软件			
软件名称	感染病毒	病毒描述	感染用户
12306订票助手	a.expense.kbanner	该病毒恶意嵌入其他软件，运行后下载恶意代码，同时获取用户的手机信息，可能会给用户的手机安全造成一定的威胁。	62408
实况模拟列车	a.expense.if2boyplayer.e	该病毒启动后，未经用户允许自动联网下载推广安装包，给用户造成资费消耗。	40412
火车订票抢线	a.expense.mdk.f	该病毒安装后，开机强制启动，从远端服务器私自下载恶意脚本代码，为盗版软件，给用户造成资费消耗和存在恶意传播的行为。	13435
实时火车票	a.expense.g3app.a	该病毒捆绑在热门应用中，植入恶意推广广告，无提示私自建立推广快捷方式，修改浏览器书签，同时存在无提示私自下载推广软件的行为，给用户造成资费消耗。	6877
机票酒店	a.privacy.enginewings	该病毒非官方版本，启动后会私自窃取系统信息、手机号码等隐私信息，并会私自发送短信，可能会给您的手机造成一定的威胁。	5089
春运火车票购买	a.system.facade	该恶意软件运行后，可后台私自静默安装其他软件，对用户手机带来危害。	3262
铁友火车票	a.expense.googla.a.[银行毒手]	该病毒伪装成正常软件，检测是否安装安全软件决定是否运行恶意程序，后台私自发送短信，屏蔽回馈信息，上传手机信息等，给用户造成自费消耗和隐私泄露。	2207
火车票抢票	a.expense.kbanner	该病毒恶意嵌入其他软件，运行后下载恶意代码，同时获取用户的手机信息，可能会给用户的手机安全造成一定的威胁。	2231
火车票验证器	a.expense.delivery	该病毒安装后，未经用户允许私自发送短信，上传用户手机号码，给用户造成资费消耗和隐私泄露。	2012
掌上机票	a.expense.apkquq.b	该病毒安装后，未经用户允许私自下载未知安装包，消耗用户流量，给用户造成资费消耗。	1288
数据来源：腾讯移动安全实验室 Tencent Mobile Security Labs			

2013 年 12 月底，随着春运铁路临客车票预售期来临，大量山寨购票类软件涌现。而被植入 a.expense.kbanner 、a.payment.googla.b(“银行扒手”)病毒代码的山寨 “12306 订票助手” 成为感染用户最多恶意软件，感染用户量达到 6.02 万。该病毒恶意嵌入其他软件，运行后下载恶意代码，同时获取用户的手机信息。

实况模拟列车、火车票订票抢线两款软件分别被 2013 年感染用户最多十大病毒之二的 a.expense.if2boyplayer.e、a.expense.mdk.f（“僵尸网络”）感染，感染用户分别达到 4.04 万、1.34 万。

可以看出，黑客在 2013 年的年尾阶段大肆针对购票类 APP 打包病毒，窃取用户手机敏感隐私的目的性非常明显。排名第五、第八、第九的三款山寨购票软件：伪“机票酒店”、伪“火车票抢票”、伪“火车票验证器”分别被植入了病毒 a.privacy.enginewings、a.expense.kbanner、a.expense.delivery，a.privacy.enginewings。这三款恶意软件分别会私自窃取手机号码等隐私信息，未经用户允许私自发送短信，上传用户手机号码，由于手机购票软件会涉及手机用户关联的网银支付信息，也因此对手机用户网银帐号造成巨大威胁。

另一方面，许多植入恶意代码的山寨购票软件也通过消耗用户流量资费或者通过恶意推

广来盈利。“实时火车票”被恶意打包了病毒代码 a.expense.g3app.a，该病毒植入恶意推广广告，可私自下载推广软件，用户不知不觉被消耗资费。

腾讯移动安全实验室提醒 :许多手机购票类软件需要用户输入金额与关联网银或第三方支付帐号，这给打包党与黑客有了可乘之机，随着 2013 年春节日渐临近，山寨购票软件将越来越多，手机用户应引起足够的警惕，用户最好去腾讯手机管家软件游戏中心、应用宝或者 12306 官方网站下载正版 12306 购票 APP。

第六章　2013 年各类型 TOP10 手机病毒

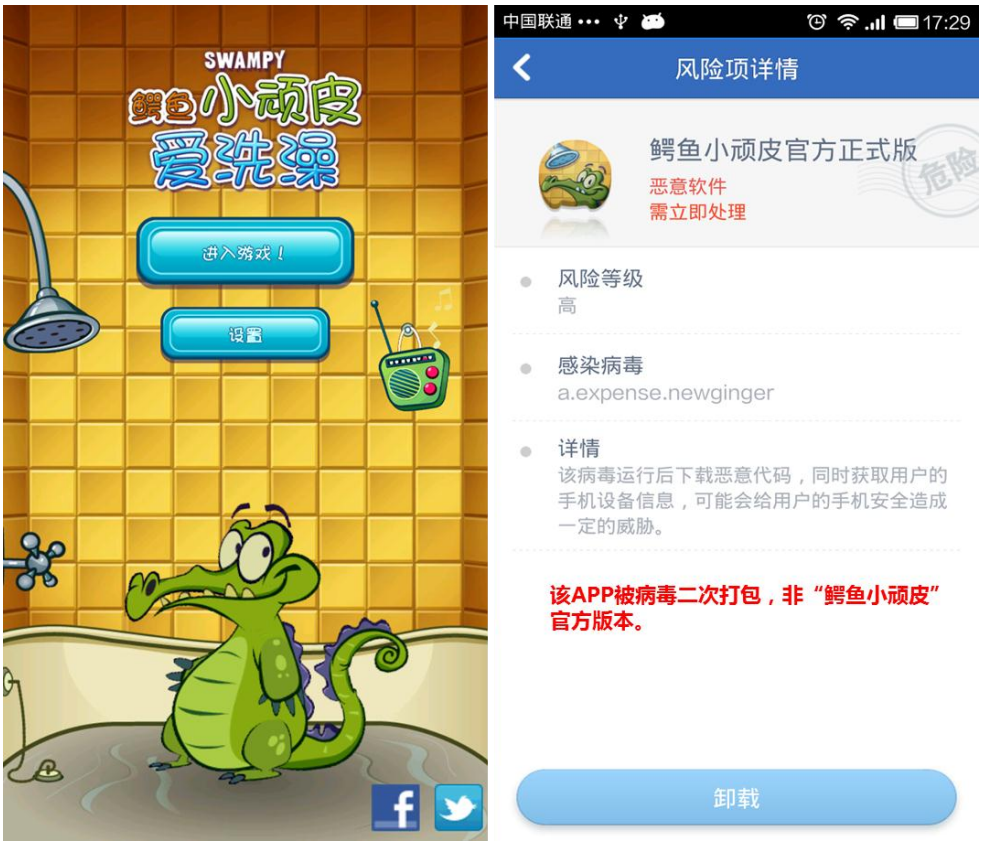
2013 年，手机病毒席卷广告用户，隐私窃取类病毒大肆泛滥，扣费病毒猖獗，新型高危漏洞病毒层出不穷，腾讯移动安全实验室通过监测，从不同类型和维度分别统计出了感染用户最多的十大手机病毒、感染用户最多的十大隐私窃取病毒和十大扣费病毒以及十大高危病毒。

6.1　2013 年感染用户最多的十大手机病毒

2013 年感染用户最多的十大手机病毒分别是：a.expense.newginger、a.expense.dpn、a.privacy.fakeandroid.a、a.privacy.counterclank（广告偷窥者）、a.expense.letang.a、a.payment.MMarketPay.b.[伪画皮 2]、a.payment.MMarketPay.c a.expense.mdk.f、a.expense.check.a、a.expense.if2boyplayer.e。这十大病毒感染用户达到 2056.75 万 ,与北京市人口相当,是 2012 年感染用户最多的十大病毒感染用户的 11.42 倍。

2013年感染用户最多的十大手机病毒			
病毒名称	危害描述	感染用户数	感染知名软件
a.expense.newginger	恶意嵌入其他软件，运行后下载恶意代码，获取用户的手机信息	3874571	手电筒 鳄鱼小顽皮爱洗澡 会说话的汤姆猫
a.privacy.fakeandroid.a	该病毒伪装成系统软件，窃取用户隐私。	2547530	Device Service Device Statistics
a.privacy.counterclank	传用户浏览器书签，同时收集手机固件信息，给用户隐私造成安全威胁。	1908950	Romantic Kiss GoLocker Theme
a.expense.dpn	该病毒启动后私自联网下载软件，静默安装推广软件。	3505664	天气通 UpdateService
a.expense.letang.a	后台私自下载推广软件，给用户造成资费消耗。	1842806	战神OL 格斗之王III 魔兽世纪
a.expense.mdk.f	开机强制启动，从远端服务器私自下载恶意脚本代码，给用户造成资费消耗和存在恶意传播的行为。	1324380	3D狂暴赛车 3D飞车 植物大战僵尸OL
a.expense.if2boyplayer.e	该病毒启动后，未经用户允许自动联网下载推广安装包，给用户造成资费消耗。	1118387	消灭星星 神庙逃亡 Subway Surf
a.expense.check.a	该病毒安装后无图标，会在后台发送短信，窃取用户手机的通讯录等隐私信息。	1153853	Goomer 功夫熊猫3 DeviceManager
a.payment.MMarketPay.b.[伪画皮2]	该病毒能通过偷偷切换APN为CMWAP，然后后台模拟访问运营商扣费接口扣费，并拦截扣费的回执短信，让用户不知不觉被扣费。	1605992	清理大师 陌陌 百度地图
a.payment.MMarketPay.c	该病毒能通过偷偷切换APN为CMWAP，然后后台模拟访问运营商扣费接口扣费，拦截扣费的回执短信，让用户不知不觉被扣费。	1685389	一键锁屏 美女报时 恶搞小电影
数据来源：腾讯移动安全实验室 Tencent Mobile Security Labs			

在 2013 年感染用户最多的十大病毒中 ,a.expense.newginger 病毒感染用户近 387.5 万。是 2013 年感染用户最多的手机病毒。该病毒恶意嵌入其他软件 ,运行后下载恶意代码，获取用户的手机信息，感染鳄鱼小顽皮等知名软件，隐私窃取类病毒正猖獗发展。



在 2013 年感染用户最多的十大手机病毒当中，资费消耗类木马占据 6 个，即达到 60%，隐私窃取类与扣费类病毒均占 20%。在感染用户最多的十大病毒中，依然是以资费消耗类病毒占主导。

在上述的十大手机病毒中，部分病毒曾在 2012 年就已经被腾讯手机管家查杀并多次曝光，“伪画皮”系列病毒家族也曾在 2012 年感染用户最多的十大病毒榜单之列。

“广告偷窥者”系列 a.privacy.Counterclank 也在 2012 年就已经猖獗爆发，2013 年，该病毒感染用户 190.8 万，感染用户量排名第四。这是一种捆绑在各类壁纸、主题等小应用里的恶意广告插件，其感染的软件数量众多，安装后会获取手机 IMEI、IMSI、SIM 卡序列号、设备序号等手机硬件信息，同时会有修改书签地址、修改浏览器主页、访问指定网址等行为。感染了 Romantic Kiss GoLocker Theme、Blue Heart GoLocker theme 等多款手机主题软件。爱好安装壁纸主题类手机用户应留意并查杀 a.privacy.Counterclank 病毒。

a.expense.dpn（“K 歌毒器”）病毒在 2012 年就感染了唱吧等知名 K 歌软件。在 2013 年，该病毒感染用户达 350.57 万，并持续感染了天气通、UpdateService、Maxthon Browser（遨游浏览器）、海豚浏览器、新浪游戏中心等多款软件，作为一款典型的资费消耗病毒，a.expense.dpn 被海量打包植入到各种软件与渠道中，导致众多手机用户持续被感染。

资费消耗类病毒捆绑知名游戏成为一种趋势。感染用户达到 184.2 万，排名第五的病毒 a.expense.letang.a 席卷二次打包了战神 OL、格斗之王 III、魔兽世纪等热门流行游戏，导致众多玩家被感染而并不自知。排名第六的病毒 a.expense.mdk.f（僵尸网络）感染了用户 132.4 万， 3D 狂暴赛车、3D 飞车、植物大战僵尸 OL、Talking Tom 等知名高下载率的游戏纷纷被感染；排名第七的病毒 a.expense.if2boyplayer.e 也感染了消灭星星、神庙逃亡、Subway Surf、实况模拟列车等流行度超高的游戏。可以看出，用户在玩游戏对于资费消耗缺乏感知，而排名前十的这三个资费消耗类病毒无疑是该类型木马的典型与代表，通过捆绑流行游戏寄生并传播，悄无声息大肆吸取用户资费。

捆绑必备软件、热门游戏进行海量二次打包，席卷海量用户成为感染用户前十大手机病毒的惯用手段，随着手机用户下载 APP 进一步分散化，制毒者或制毒机构通过针对特定知名软件海量打包，可以更快的席卷感染海量用户，这也是 2013 年十大病毒感染用户数远超 2012 年的重要因素。因此，在 APP 下载渠道与应用分发入口日渐多元化的今天，手机用户选择安全的 APP 下载渠道尤其重要。

6.2 2013 年十大高危手机病毒

2013 年，涌现了许多高危的木马漏洞，对手机用户的资金、流量、隐私等造成了全方位的安全威胁。腾讯移动安全实验室针对危害指数排名 ,列出了如下年度十大高危手机病毒。

2013年十大高危病毒			
病毒名称	病毒描述	感染用户	感染知名软件
a.rogue.kuaidian360.[推荐密贼]	执行云端指令，私自占用第三方知名应用界面，强行显示推广广告信息，严重影响用户体验和存在流氓行为。	1632352	铁拳3D
a.rogue.centero.[鬼推墙]	后台监控某些知名软件的运行，并在这些知名软件界面中强行显示广告，消耗用户流量，影响知名软件的用户体验。	944392	宜搜+ 搜狗号码通 安卓市场
a.system.masterkey(“冒牌天煞”)	自动检测确认用户未安装杀毒软件后，便私自订购SP业务，同时拦截用户短信，替用户回复扣费确认信息，并向用户联系人发送恶意软件下载推荐短信。	329778	找你妹、导航犬、百合网
a.fraud.actehc.[广告毒株]	该病毒内含恶意广告插件，启动后伪造短信推送垃圾广告，向用户频繁发送垃圾短信，伪造欺诈短信，监听用户短信息，未经用户允许私自删除指定短信，存在流氓行为。	232432	斗地主 PDF阅读器 明星麻将
a.expense.g3app.g.[无间推鬼]	该病毒捆绑在热门应用中，植入恶意推广广告，无提示私自建立推广快捷方式，修改浏览器书签，同时存在无提示私自下载推广软件的行为，给用户造成资费消耗。	219398	速度与激情6 美图秀秀
a.expense.afoynq.[游戏杀手]	该病毒安装后，从远端服务器私自下载其他软件，本身为盗版软件，给用户造成资费消耗和存在恶意传播的行为。	202392	跑酷功夫熊猫 疯狂斗地主
a.system.RomSu.A.[权限杀手]	该病毒内置在系统里，安装后无图标，会接受服务器指令静默安装推广软件并上传手机固件信息到服务器，同时阻止第三方软件获取root权限，给手机的安全带来严重的威胁。	131481	高德地图 欧朋浏览器 梦回西游
a.system.apkbox.[复活爬虫]	该病毒包含病毒子包，获取手机Root权限静默安装病毒子包，可能会给您的手机安全造成一定的威胁。	124432	APKBox GoogleRi
a.expense.lockpush.[洛克蠕虫]	该病毒安装后，未经用户允许私自下载软件并安装，可能会造成一定的流量消耗。	109305	豆瓣小组 R.E.管理器 蜻蜓.fm
a.rogue.bankrobber.[银行悍匪]	该病毒可读取淘宝以及十余家银行手机客户端软件账号密码信息，还可后台卸载安全软件，窃取用户手机短信、通话记录，并可后台私自发短信控制手机。	65728	农业银行、招商银行、广发银行
数据来源：腾讯移动安全实验室 Tencent Mobile Security Labs			

- **类型一：“影子广告”类病毒泛滥**

- **典型两大高危木马：a.rogue.kuaidian360.[推荐密贼]、a.rogue.centero.[鬼推墙]**

“推荐密贼”在今年出现以来，引发巨大的行业震动。该病毒可针对知名软件投放精品推荐字样的“浮窗广告”、BANNER 广告、弹窗广告等。通过模拟这种貌似“官方内置广告 ”“嫁祸”给这些被病毒入侵的知名应用，消耗用户流量并赚取广告分成。铁拳 3D、安卓优

化大师、百度新闻、腾讯新闻、新浪微博、人人网、YouTube、经典俄罗斯方块等众多知名软件都纷纷被感染。感染用户超过 163 万。

“鬼推墙”病毒则是“推荐密贼”的变种，同样感染了搜狗号码通、安卓市场、人人网、YouTube、天涯社区等知名软件，通过云指令控制针对知名应用强行投放恶意广告，不仅对手机用户造成用户体验上的伤害，更对知名软件造成品牌伤害，这也是云端指令类“影子广告”病毒智能化程度正快速提升的一个重要危险信号。

➢ 类型二：安卓“签名”漏洞爆发

● 典型高危漏洞木马—冒牌天煞

2013 年，安卓连续曝出 3 个高危级别的系统“签名”漏洞，黑客可在不破坏数字签名的情况下，将木马植入正常应用，实现窃取账号和用户隐私、甚至包括窃听、打电话或发短信等多种恶意行为。

➢ **类型三：短信欺诈和恶意推广类手机病毒迅速泛滥**

● **典型高危木马：a.fraud.actehc.[广告毒株]、a.expense.g3app.g.[无间推鬼]**

通过在热门应用或游戏中内置病毒和恶意代码进行广告推广获利的手机木马在 2013 年成为手机安全威胁的重要类型。这类典型木马包括“广告毒株”和“无间推鬼”两大年度高危病毒。

“广告毒株”病毒内含恶意广告插件，启动后伪造短信推送垃圾广告，向用户频繁发送垃圾短信，同时该插件存在伪造欺诈短信风险，该恶意广告插件还监听用户短信息，未经用户允许私自删除指定短信。可以看出，“广告毒株”不仅可推广告、还监听隐私、伪造欺诈信息，智能化程度大大提升，该木马成为短信欺诈类病毒的一个重要危险信号。

而“无间推鬼”病毒捆绑在热门应用中，植入恶意推广广告，私自下载推广软件，感染用户 21.9 万，该病毒的特征是“打包党”最热衷利用的恶意推广的手段。

- **类型三：嗜游类病毒猖獗爆发**

- **典型高危病毒：游戏杀手**

2013 年，众多手游遭遇木马洗劫，打包党针对手游打包吸金非常普遍。“游戏杀手“是最为突出的高危游戏病毒之一。2013 年，“游戏杀手”病毒瞬间感染 641 款手游。该病毒可私自下载其他软件，共有 20.2 万用户被该病毒感染，未来很可能会有更多新兴手游被高危游戏木马感染。

- **类型四：反卸载并获取 root 权限的高危病毒出现**

- **典型高危病毒：a.system.RomSu.A.[权限杀手]、a.system.apkbox.[复活爬虫]**

“权限杀手”通过刷机包植入用户手机中，将 Bluekey、Sndconsole 、Xinitd 三个文件

分别隐藏在系统目录下。这三个病毒程序各有明确的分工，分别负责防卸载、启动恶意程序、实施恶意行为，构成了严密的防查杀逻辑，具有很强的反卸载能力。

“复活爬虫“包含病毒子包，可获取手机 Root 权限静默安装病毒子包。这两大病毒的特征是入侵手机 ROM，获取手机 root 权限，具备强大的反卸载能力。2013 年来，手机木马智能化程度在进一步提升。

- **类型五：手机支付高危病毒威胁互联网金融**

- **典型高危木马：a.expense.lockpush.【洛克蠕虫】、a.rogue.bankrobber.[银行悍匪]**

2013 年，腾讯手机管家分别查杀了“洛克蠕虫”、“银行悍匪”这类高危的银行支付类病毒，洛克蠕虫可通过二次打包的方式把恶意代码嵌入银行 APP，“银行悍匪”（a.rogue.bankrobber.）病毒则被二次打包到知名应用和游戏中，目前已感染超过 6 万用

户，该病毒会启动监听短信，窃取通话记录，屏蔽回执短信，删除所有短信，还会读取手机中安装的购物客户端（淘宝）、银行客户端（包括农业银行、招商银行、广发银行、兴业银行、邮储银行等 20 余家手机银行）的帐号密码。

这两个高危木马的出现，是手机支付安全威胁进一步加剧的表现，未来，手机支付类病毒更可对互联网金融行业造成威胁。

6.3 2013 年十大扣费手机病毒

2013 年，手机恶意扣费类手机病毒呈现出猖獗上升的趋势。据腾讯移动安全实验室监测，2013 年感染用户最多的十大扣费手机病毒感染用户总数达到 688.18 万。

2013年感染用户最多的十大扣费病毒			
病毒名称	病毒描述	感染用户	感染知名软件
a.payment.MMarketPay.c	该病毒能通过偷偷切换APN为CMWAP，然后后台模拟访问运营商扣费接口扣费，并拦截扣费的回执短信，让用户不知不觉被扣费。	1685389	一键锁屏 美女报时 恶搞小电影
a.payment.MMarketPay.b.[伪画皮2]	该病毒能通过偷偷切换APN为CMWAP，然后后台模拟访问运营商扣费接口扣费，并拦截扣费的回执短信，让用户不知不觉被扣费。	1605992	清理大师 陌陌 百度地图
a.payment.moonplayer	该病毒以情色内容引诱用户安装，启动后私自下载其他安装包，并发送短信订阅服务，存在恶意扣费行为。	1019745	美眉热播 播影先锋 媚女影院
a.payment.ms.b	该病毒自动激活后在后台随机向指定的SP端口号发送扣费短信，同时屏蔽SP商的确认短信；另外，病毒会把云端指令的操作记录发送到指定的手机号，泄漏用户隐私。	855857	91助手 云雨商城 飞聊
a.payment.MMarketPay.d	该病毒能通过偷偷切换APN为CMWAP，然后后台模拟访问运营商扣费接口扣费，并拦截扣费的回执短信，让用户不知不觉被扣费。	625525	可爱脑筋急转弯 超级信号增强器 音乐猎手
a.payment.letu	该病毒安装后，私自发送短信，同时拦截用户短信，存在恶意扣费和流氓行为。	462090	墨香书客 乐图壁纸 麦可漫画
a.payment.daemon	该病毒以游戏名义诱导用户下载安装，一旦激活便后台向某SP号码发送订购信息，订购高额的SP业务，并且删除相应的反馈信息，让用户在不知情的情况下被扣除高额的话费	460954	乐媒 酷盾 五子棋
a.payment.cc	该软件启动后自动向指定号码发送短信，给用户造成资费消耗。	364871	CC来电炫图
a.payment.kituri.[隐私飓风]	私自发送短信，开机自启动后会启动一个定时任务，上传用户隐私信息到指定服务器上，并且恶意拦截回执短信	338538	魔兽大富翁 愤怒的小鸟
a.payment.pman	该病毒启动后，诱骗用户点击发送短信恶意扣费，擅自下载未知安装包并静默安装，并且收集用户手机信息上传到指定服务器，造成用户资费消耗和隐私泄露。	318745	智库市场 DD世界 DDLord
数据来源：腾讯移动安全实验室 Tencent Mobile Security Labs			

感染用户最多的扣费病毒木马为：a.payment.MMarketPay.c（“伪画皮”家族）病毒，感染用户达到 168.5 万，该病毒病毒能通过偷偷切换 APN 为 CMWAP，然后后台模拟访问运营商扣费接口扣费，并拦截扣费的回执短信，让用户不知不觉被扣费。该病毒感染了清理大师、陌陌、百度地图、导航犬等知名软件。排名第二的是 a.payment.MMarketPay.b（“伪画皮”2）。感染病毒达到 160 万，一键锁屏、美女报时、恶搞小电影、3G 信号增强器等手

机常用软件遭感染。“伪画皮”家族系列的两个病毒及变种分别在 2013 年扣费类病毒排行榜单排名第一、第二。

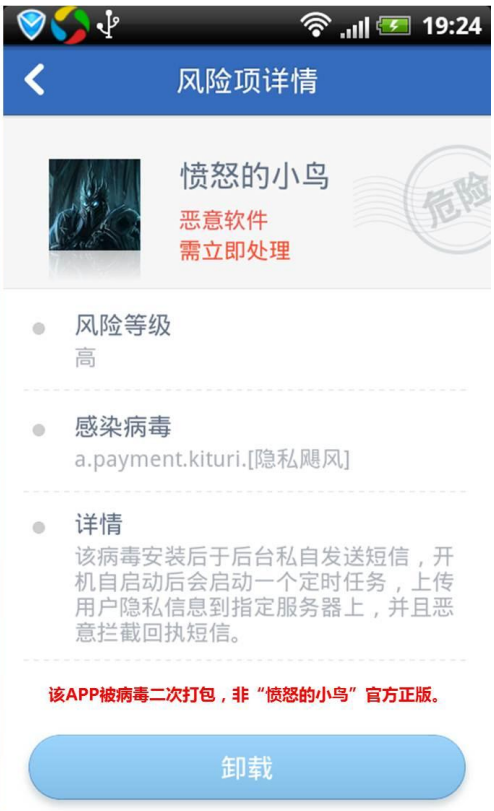
而“伪画皮”的另一个变种 a.payment.MMarketPay.d 排名第五，感染用户 62.55 万。“可爱脑筋急转弯”、“超级信号增强器”、“音乐猎手”、“天天影视”等软件均被感染。“伪画皮”病毒家族曾在 2012 年席卷大量知名软件，该病毒由于特征显著，扣费隐秘，黑客基于非法盈利需求，将该病毒海量二次打包到各种知名和常用软件中，通过电子市场和手机论坛等渠道发布，导致海量用户感染该病毒，“伪画皮”家族病毒顽固性强，成为风险性非常高的扣费类木马。

值得一提的是 a.payment.staservice 扣费手机病毒，该病毒安装后，开机强制启动，上传手机固件信息，访问指定网址从云端获取恶意短信内容、恶意应用程序列表等，通过用户手机设置定时服务私自发送未知短信、拨打未知号码、下载未知应用程序，同时拦截指定

内容短信和删除指定通话记录。

可以看出，该病毒形成立体化的隐私窃取攻势，对手机用户的短信、通讯录等隐私全面拦截与窃取，私自拨打电话、发送短信进而扣取资费而用户毫不知情，这是扣费类病毒危险度正在提升的反映。

排名第八、第九、第十的扣费病毒分别为 a.payment.cc、a.payment.kituri.[隐私飓风]、a.payment.pman，这三个病毒是典型的扣费类木马。后台私自发送短信、屏蔽运营商发回来的确认短信，无形中吸取用户话费是三个扣费病毒的共同特征，也是扣费类木马病毒的典型特征。



可以看出，2013 年十大扣费病毒多半会集中目标紧盯美女壁纸、热门游戏、棋牌类游戏，而这些游戏由于牵涉到金币道具等方面的输赢，往往可以扣费于无形，而用户也毫不知情。

6.4 2013 年十大隐私窃取类病毒

2013 年，感染用户最多的十大隐私窃取类病毒感染用户总数达到 873 万，排名第一的病毒为 a.privacy.fakeandroid.a，该病毒通过伪装成系统软件，窃取用户隐私，感染手机用户达到 254.7 万。排名第二、第三的病毒分别为 a.privacy.counterclank、a.privacy.dlwx，感染用户分别达到 190.9 万、95.7 万。a.privacy.counterclank 窃取手机固件信息、a.privacy.dlwx 窃取用户短信和位置信息。可以看出，隐私窃取类病毒针对用户各种隐私的窃取具有明显的针对性，隐私贩卖与获取地理位置进行商业广告精准推送是手机病毒窃取隐私非常明显的目的。

2013年感染手机用户最多十大隐私窃取类病毒			
病毒名称	病毒描述	感染用户数	感染知名软件
a.privacy.fakeandroid.a	该病毒伪装成系统软件，窃取用户隐私，造成用户隐私泄露。	2547530	Android更新 Device Service
a.privacy.counterclank	在桌面创建快捷方式，并且上传用户浏览器书签，收集手机固件信息，给用户隐私造成威胁。	1908950	Romantic Kiss GoLocker Theme Blue Heart
a.privacy.dlwx	该病毒安装后会私自发送短信，窃取你的短信信息以及位置信息，给您的个人隐私造成一定的威胁。	957341	内存卡清理 优化大师 七彩祖玛
a.privacy.kkpush.[盗Q密探]	该病毒安装后，会尝试盗取用户好友的QQ号码，以及用户使用QQ音乐听过的音乐名称，并上传到指定服务器，同时还会窃取用户手机联系人，通话记录，浏览器书签等隐私信息。	751937	Temple Run 互动电视 安卓市场 星座日历
a.privacy.kkpush.a	该病毒安装后，会尝试盗取用户好友的QQ号码，以及用户使用QQ音乐听过的音乐名称，并窃取用户手机联系人，通话记录，浏览器书签等隐私信息。	542448	动物波普星 经典泡泡龙 大家来找茬高级版
a.privacy.fakeandroid.b	该病毒安装后，上传用户通话记录，造成用户隐私泄露。	491597	Memroy Manager
a.privacy.fakelight	该病毒安装后，随着系统启动，监听短信接收并上传到远端服务器，给用户造成隐私泄露。	464995	精品小说 appexplorer 阳光手电筒
a.privacy.FrozenBubble	该病毒启动后会私自发送短信、修改浏览器书签、拦截短信、窃取用户的短信信息，并会在后台私自下载软件静默安装，给手机造成威胁。	407133	AndroidSMSPatch 世界杯老虎机
a.privacy.fakelight.b	该病毒安装后，随着系统启动，监听短信接收并上传到远端服务器，给用户造成隐私泄露。	349601	哇呗来电 音乐小榜单 com.android.shared
a.privacy.fakelight.a	该病毒安装后，随着系统启动，监听短信接收并上传到远端服务器，给用户造成隐私泄露。	308465	阳光手电筒 精品小说 诱惑美女拼图
数据来源：腾讯移动安全实验室 Tencent Mobile Security Lab			

2013 年，感染用户最多的十大隐私窃取类病毒感染用户近 873 万。从该十大隐私窃取类病毒可以看出，手机短信信息、通话记录、浏览器书签、位置信息、固件信息等隐私是十大隐私窃取类病毒的获取的目标隐私。

隐私排名第四的病毒是“盗 Q 密探”,该病毒会尝试盗取用户好友的 QQ 号码,以及用户使用 QQ 音乐听过的音乐名称,并上传到指定服务器,同时还会窃取用户手机联系人、通话记录等隐私。

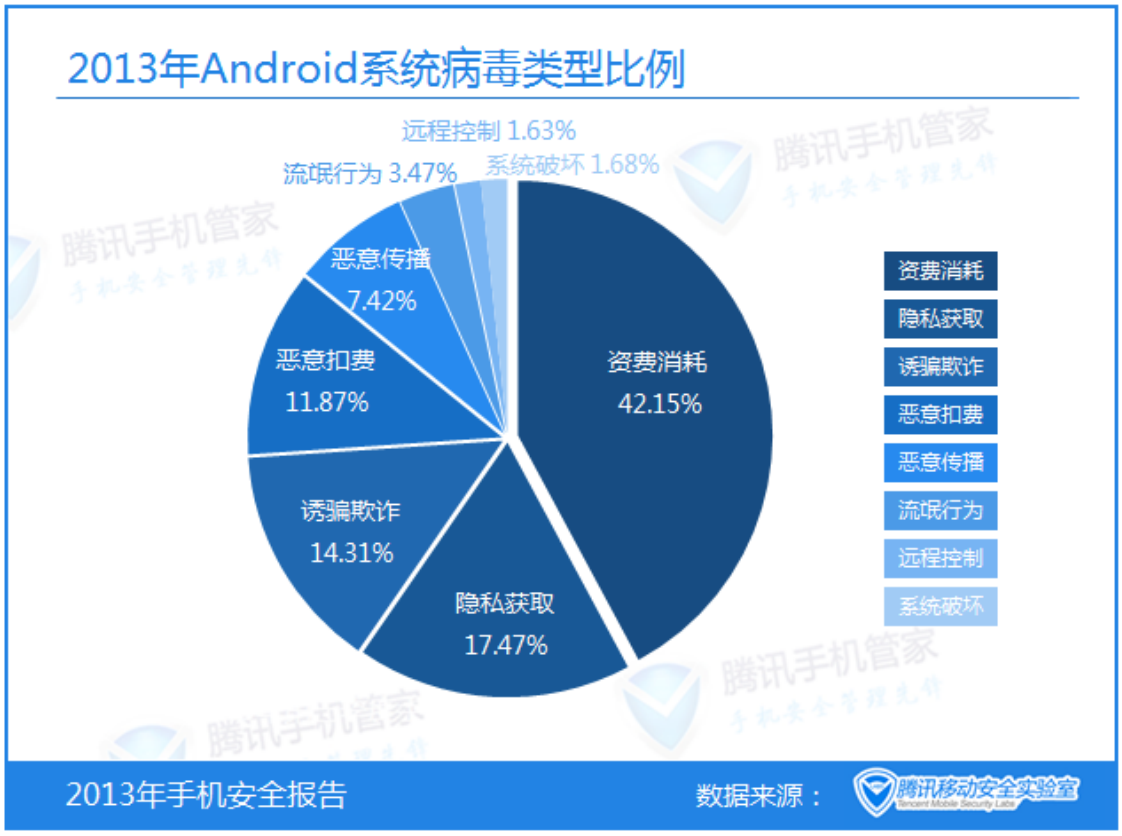
而另一方面，监听短信类隐私窃取病毒正快速发展，比如排名第七的 a.privacy.fakelight、排名第九、第十的 a.privacy.fakelight.b、a.privacy.fakelight.a 病毒均具备监听短信接收并上传到远端服务器的特征。这三个病毒分别感染用户达到 46.5 万、35 万、30.8 万。而这一特征的出现，病毒极可能窃取用户敏感隐私，包括监听到银行支付等敏感信息等，对用户的银行帐号、资金造成极大威胁。

第七章　2013 年 Android 系统病毒类型比例

2013 年全年的 Android 病毒行为类型比例统计中，相较 2012 年，资费消耗类占据 42.15%的比例，排名第一；隐私获取类病毒蹿升到第二的位置，占比达 17.47%；而诱骗

欺诈类病毒多并行于其它几种病毒行为中，占比一直居高不下，达到 14.31%；恶意扣费类占比达 11.87%；恶意传播类占比达 7.42%；流氓行为、系统破坏、远程控制类行为分别占比 3.47%、1.68%、1.63%。

资费消耗类病毒依然是最为普遍的病毒类型。隐私窃取类病毒发展迅速，此类病毒通常会通过后台上传用户短信、通讯录、照片、甚至网银密码等强隐私信息。2013 年，腾讯移动安全实验室截获的一个名为短信盗贼 a.remote.eneity 的手机病毒，该病毒伪装成热门软



件，后台接收短信指令静默安装、卸载用户手机软件，同时转发用户短信到指定号码、拦截用户短信，可能威胁到用户的手机联系人私密、商业类机密短信以及各种支付、电商网购验证确认短信等，严重危害到用户手机以及支付安全，隐私窃取病毒的隐蔽性和危害性在进一步彰显。

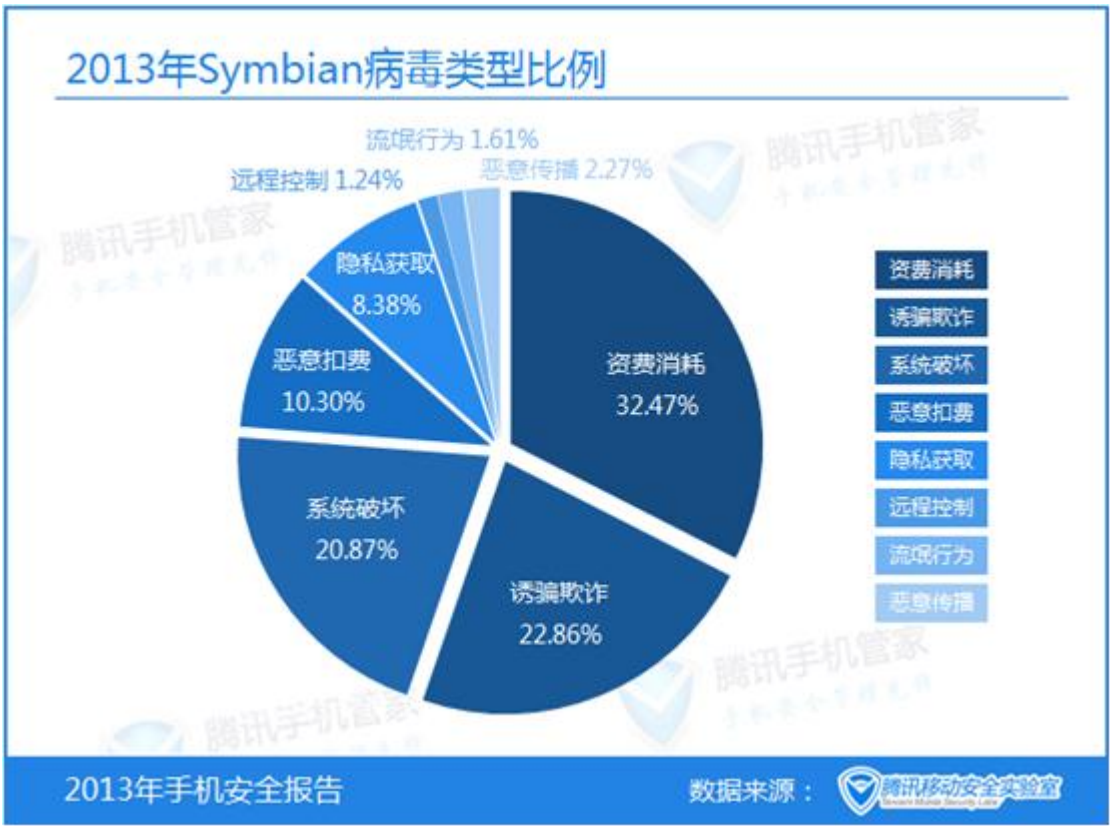
11.87%的恶意扣费类病毒行为大多会私自联网，通过后台私自发送短信，同时恶意拦截指定号码短信，诱骗开通 SP 扣费业务，偷偷吸取用户的手机话费。典型扣费病毒

a.payment.MMark 伪画皮在 2013 年当中演变出多个子病毒活跃在安卓平台，整个病毒家族均能通过偷偷切换 APN 为 CMWAP ,然后后台模拟访问运营商的 MobileMarket 的扣费接口并验证，并拦截扣费的回执短信，让用户不知不觉被扣费。

2013 年，手机病毒已进一步转向资费消耗、隐私窃取类病毒行为，尤其是资费消耗类病毒。与 2012 年相比，资费消耗类病毒占比增长了 7%。Android 平台手机病毒类型正在进一步朝多元化方向发展。

第八章　2013 年 Symbian 系统病毒类型比例

2013 年，Symbian 系统持续衰落。在 2013 年全年中，资费消耗类、诱骗欺诈类以及系统破坏类病毒行为占据 Symbian 病毒类型的重要位置，分别占比 32.47%、22.86%以及 20.87%；恶意扣费类占比 10.30%，隐私获取类占比 8.38%，恶意传播、流氓行为和远程控制类分别 占比 2.27%、1.61%和 1.24%。



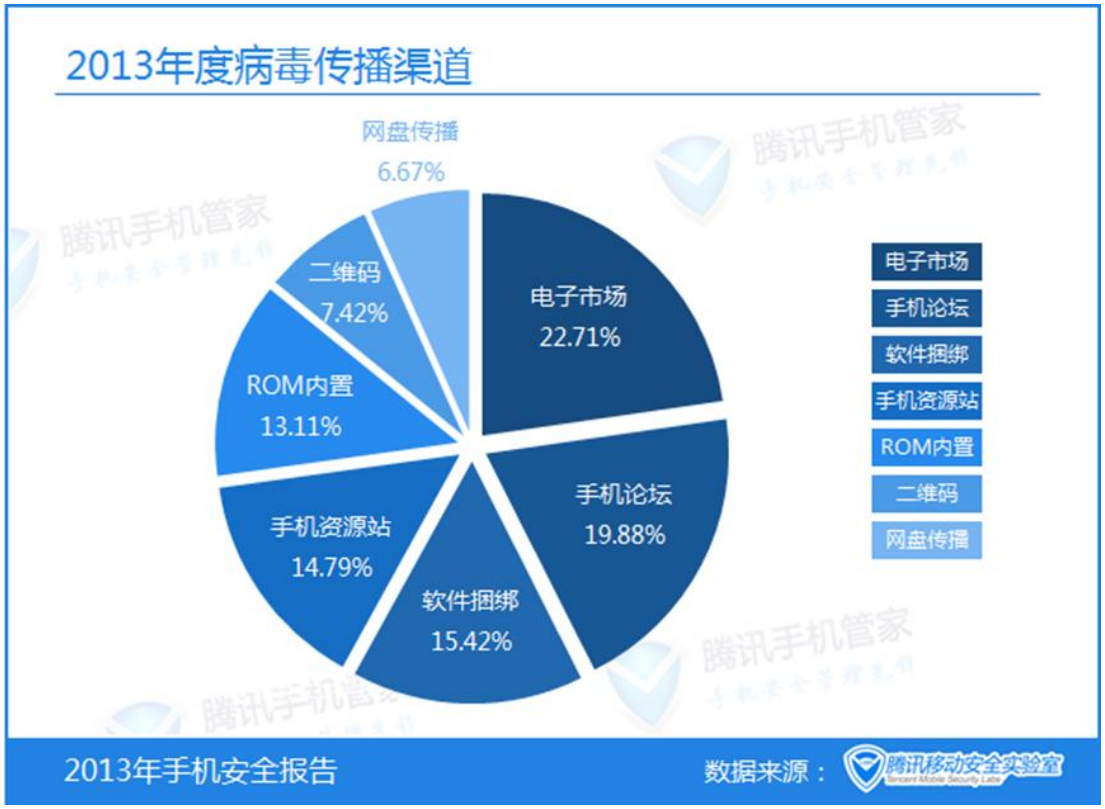
资费消耗类病毒同样是 Symbian 平台最主要的病毒行为类型。在 Symbian 平台，资费消耗类病毒通常会表现出无提示私自联网消耗流量的特征，如典型病毒 kernel.c，常伪装成系统组件驻留于用户手机中，自激活后常驻后台且私自联网并下载安装其他恶意插件，以此影响用户手机的正常使用。

与 Android 系统相比有所不同的是，系统破坏类病毒始终占据着 Symbian 系统相当高的比例，此类病毒通常会开机自启动后常驻后台运行，无法手动将其卸载。从整体上来看，Symbian 系统处于持续衰落之中，智能机保有量与新增病毒、恶意软件在进一步降低。病毒制作者或制毒机构对 Symbian 病毒投放的权重持续降低。

Symbian 系统的病毒持续呈现平稳缓慢增长的趋势。但衰落的大趋势已经无法避免，未来 Symbian 平台将有可能逐渐淡出舞台。

第九章　2013 年手机病毒传播渠道分析

在 2013 年，手机病毒的来源渠道分布中，手机论坛和电子市场依然占据了绝对的主导地位，分别占据了 22.71%和 19.88%的来源比例，软件捆绑以 15.42%的比例位居第三。



2013 年，电子市场的手机病毒来源与感染比例呈现稳定与稍微下降的趋势。这是因为电子市场是手机用户下载手机应用最主要的渠道，电子市场的安全性也因此日益得到重视，越来越多的安全软件厂商为电子市场提供底层病毒查杀引擎，建立病毒查杀合作，一定程度上控制了电子市场上的病毒传播。2013 年，电子市场病毒传播比例为 22.71%。另外，手机论坛占比 19.88%，占据第二。

Rom 内置渠道染毒达到 13.11%。Android 用户刷机盛行，不良水货商以及部分互联恶意 rom 开发者通过对 ROM 内置恶意软件，牟取灰色利益。用户一旦刷入病毒 ROM 即中招，危害性较大。如典型的 ROM 内置病毒“权限杀手”，具有严密的反查杀逻辑，能阻止其他软件获取 root 权限，对其进行查杀，给手机带来严重的安全威胁。随着刷机用户增多，部分刷机平台没有解决 ROM 的安全检测机制问题，ROM 中毒比例还在继续攀升。

二维码在 2013 年则得到一个相对快速的发展。二维码的流行，使得制毒者和制毒机构也盯紧该渠道，逐渐加大在二维码渠道的病毒投放，二维码的病毒传播比例已达到 7.42%。

越来越多的制毒者通过该渠道内置恶意软件或恶意链接进而盗取网银资金，二维码的安全性已经受到越来越多人的关注。

第十章　2013 年手机安全状况解读与趋势分析

2013 年病毒呈现多层次、多类型发展。2013 年全年，手机病毒呈现多层次多类型的发展。扣费类、隐私类、投影广告类、ROM 病毒、手机支付类病毒多向发展，特征向复杂性与高危性迈进。

10.1　安全趋势一：大批手游被“血洗”，成为吸金诱饵

2013 年以来，大批游戏软件遭遇打包篡改，游戏成为手机病毒“毒害”的重灾区。战神 OL、格斗之王 III、魔兽世纪、3D 狂暴赛车、3D 飞车、植物大战僵尸 OL、Talking Tom 等知名游戏纷纷被病毒感染。腾讯手机管家 2013 年 3 月查杀的“游戏杀手”感染 641 款手游；腾讯移动安全实验室在 2013 年 5 月截获了一款名为“嗜血扣费(a.payment.gpay)”的手机病毒，该病毒感染了德州扑克、塔防战争、泡泡龙等 500 余款热门安卓手机游戏，2013 年 10 月，腾讯手机管家查杀了一款短时间感染 13000 款 APP 的病毒“嗜游恶魔”(a.expense.igameplay.b)，该病毒恶意打包了植物大战僵尸 2 等热门游戏；流行游戏《我叫 MT》在 2013 年 7 月遭病毒 a.expense.tgapp 入侵；地铁跑酷、黄金矿工等知名游戏均遭遇“恶推毒手”入侵。Master key 漏洞木马“冒牌天煞”感染了“找你妹”等知名手游。可以看出，各类型病毒紧盯游戏二次打包已成为趋势，知名游戏几乎都沦为手机木马吸金诱饵，手游在某种程度上成为的黑客批量打包植入恶意代码的目标类型 APP。

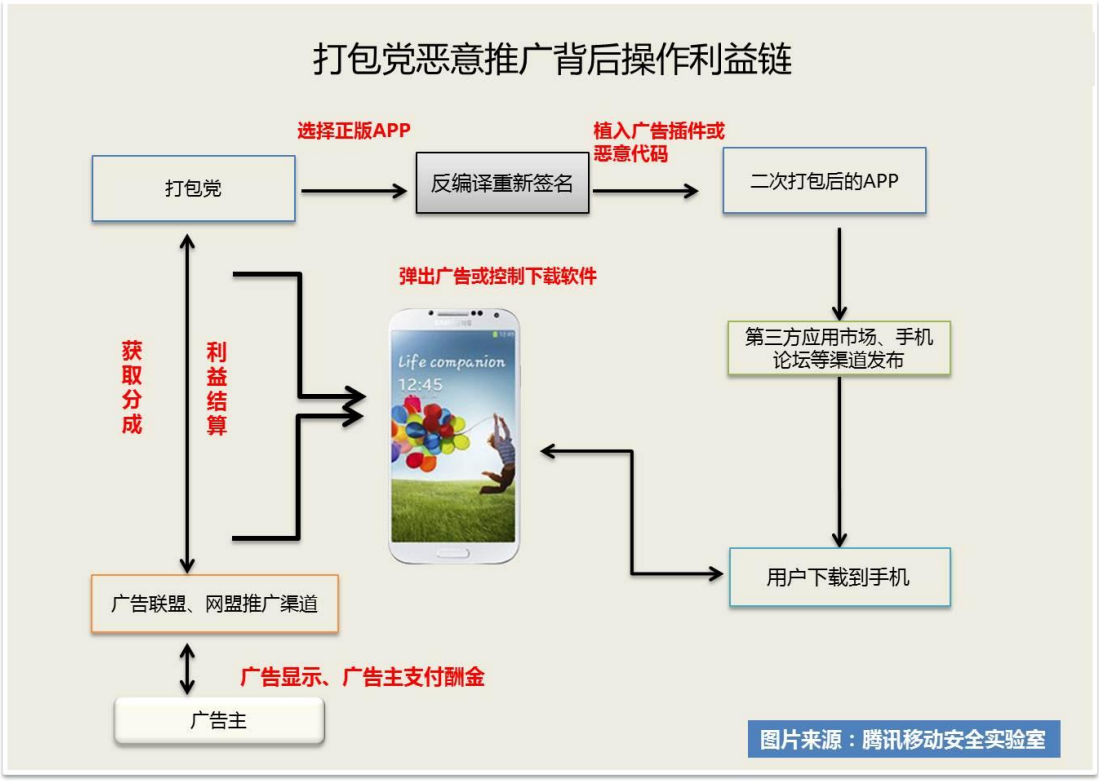
10.2　发展趋势二：恶意推广泛滥，黑色产业链成型

2013 年 7 月，带恶意推广传播特征的恶意扣费病毒在感染篡改情色类壁纸方面显得十分突出。a.rogue.smszombie.[短信巫毒]再次浮出水面，感染了泷泽萝拉动态壁纸等系列

美女色情类壁纸软件。许多恶意扣费类病毒也包含恶意推广的动作行为，这往往给用户造成连锁伤害。

2013 年以来，恶意推广类病毒消耗用户流量的方式已经变得十分的智能化与多元化。“免费的 APP+植入广告”已经成病毒开发者惯用敛财手段 。

2013 年以来，病毒制作者加速变相利用了广告联盟的软件推广、广告点击的分成利益机制，病毒制作者通过针对知名 APP 二次打包篡改，植入恶意广告插件或恶意推广类病毒代码，偷偷在后台私自下载恶意推广软件包或者强行显示广告，通过这种方式，按照每个用户被推广的软件来计费，从广告联盟平台非法获取推广费用。通过这种违背用户意愿、侵犯用户的知情权和选择权的病毒行为，对用户造成了巨大经济损失。



部分不法广告商也会与手机病毒制作者或者打包党合作，通过在正版软件中植入广告插件或者恶意代码，通过重新打包、上传，通过各种形式弹出广告，消耗流量来攫取利益。另外，盗版 APP（打包党）通过针对正常 APP 二次打包非法内嵌广告插件恶意强推下载，影

响了正版 APP 的品牌形象和产品美誉度，极大伤害了正版 APP 开发者的利益。

目前，随着移动互联网的发展，APP 开发者对用户的争夺日趋激烈，盈利方式却依旧单一，加之目前移动 APP 行业缺乏监管，推广模式和管理机制依旧不太健全，在这种情况下，便有了制毒者或制毒机构的生存空间和土壤。

为保护手机用户的经济利益以及对流量资费的知情权，产业链各方应携手对手机恶意广告进行治理并携手共同设定防御方案，共同创建和维护良好的手机安全环境。

10.3 发展趋势三：电商支付、高危漏洞病毒成用户的重大威胁

2013 年以来，黑客逐利性进一步显现，洗劫用户钱袋更成为一种趋势。2013 年，由于手机支付已经开始形成规模，2014 年将会是手机支付类病毒爆发的一年。继 2013 年 3 月份腾讯手机管家截获首个感染手机银行客户端手机病毒“洛克蠕虫”之后，手机支付危机一直如影随形。2013 年，腾讯截获一款 a.privacy.bankun 病毒，该病毒专盯韩国银行 App，只要发现手机中有指定的韩国银行 App 软件，就会将这些 App 替换成病毒自带的恶意软件，然后偷偷上传用户手机通信录、监听手机短信息并上传，窃取用户的隐私。

可伪装成淘宝客户端，盗取手机支付帐号的“伪淘宝”病毒在 2013 年 7 月被腾讯手机管家查杀，该病毒可通过模拟淘宝官方的用户登录页面收集用户输入的淘宝帐号密码以及支付密码。给用户支付风险带来巨大风险。

一款可以监听“手机输入法”的 Android 恶意程序惊现海外，病毒制作者可以通过病毒感染输入法软件，记录用户的信用卡、网银以及各种账户密码信息，拥有海量用户的国际知名输入法软件 SwiftKey KeyBoard 不幸被感染。腾讯手机管家首家查杀这些支付类病毒之后便通过各途径向广大用户预警。

2013 年，Android 签名漏洞爆发，利用该签名漏洞的扣费手机病毒可寄生于正常 APP 中， 进而针对捆绑手机用户进行恶意扣费，并向用户联系人发送恶意软件下载推荐短信，

一系列扣费操作十分智能化。该漏洞引发了各界关注，该漏洞成为手机用户的重要安全威胁。目前，腾讯手机管家已针对利用该漏洞的扣费手机病毒 a.system.masterkey 实现了全面查杀。

10.4 发展趋势四："影子广告"病毒猖獗

2013 年 5 月末，"投影广告"类病毒大肆来袭。在 2013 年 4 月，感染"铁拳 3D"等热门游戏的"推荐密贼"病毒可针对微信等知名软件强制推送广告，在 5 月，云端控制指令病毒"鬼推墙"疯狂来袭，该病毒针对微信、手机 QQ、人人网、YouTube 等知名软件大肆强制推送广告，目前已有超过 160 万用户被感染。

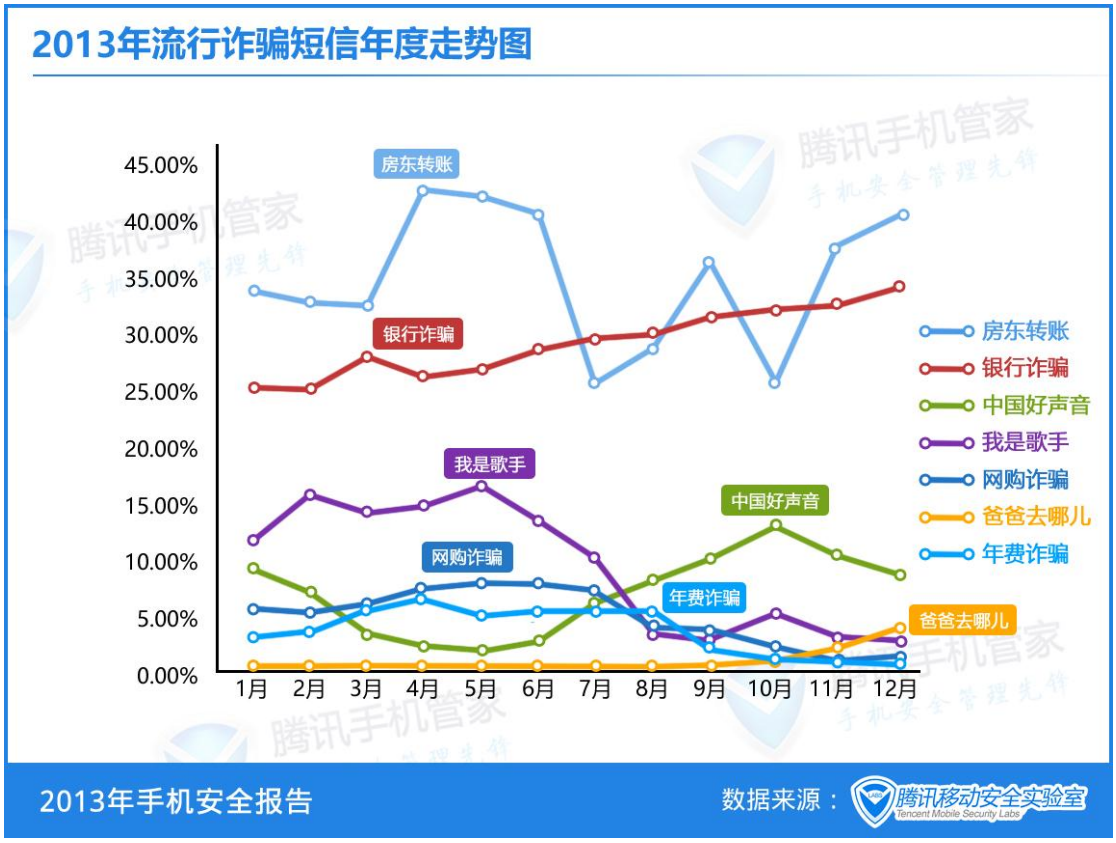
"推荐密贼"体现出"投影广告"类病毒更强的隐蔽性与伪装性，该病毒通过以模拟官方内置广告的形式"嫁祸"给这些被病毒入侵的知名应用，消耗用户流量并赚取广告分成，这也是云端指令类病毒智能化程度正快速提升的一个重要危险信号。

该病毒对于整个国内移动互联网行业造成严重品牌伤害。由于该病毒通过云指令控制针对知名应用强行投放恶意广告，不仅对手机用户造成用户体验上的伤害，而且会让用户误认为该"精品推荐"的浮窗广告是出自该知名应用自家投放的广告。制毒者基于这种病毒触发广告获取利益分成，为自身牟取非法利润，更对微博、百度搜索、安卓优化大师、腾讯新闻等品牌造成伤害，以"移花接木"的手段进行行业攻击的目的性非常明显。

近年来，移动互联网快速发展，但盈利模式相对缺失，对于 APP 开发者而言，广告几乎成了唯一的获利渠道。某些不法开发者基于快速盈利的功利需求，与第三方手机广告行业建立合作，往往通过强制嵌入广告插件与恶意推送广告等手段，建立分成模式来获取利润。"推荐密贼"病毒彰显出制毒者或制毒机构与某些 APP 从业者等建立黑色产业链和利益联盟来盈利的本质。

10.5 发展趋势五：手机诈骗电话、欺诈短信持续大规模涌现

2013 年以来，涌现出众多新型诈骗短信，另一方面，诈骗内容不断变化，紧随流行娱乐、经济热点趋势非常明显。银行诈骗、房东转账、中国好声音诈骗全年泛滥，10 月份，在好声音话题最热时期，该类诈骗短信数量达到最高峰。2013 第四季度，网购诈骗、网银升级、爸爸去哪儿电视节目中奖的诈骗持续快速增长，全年，网购诈骗骤增，快递诈骗伴随网购诈骗应运而生。诈骗短信的爆发高潮验证了节目的流行度。



而热门综艺节目的共同点在于收视率高，节目覆盖群体广泛，观众认可率高，因而当被骗者收到此类短信时，从心理层面会有一定的品牌认知度与信任度。2013 年，流行娱乐节目诈骗短信的数量随节目播出时间节点与流行时间段呈现出发展、快速上升、高潮、缓慢降低等波动曲线。可以预见，热门节目诈骗将持续大规模出现。

技术的开放性、存量用户规模巨大、利益的巨大诱惑，吸引了不少的技术高手进入手机的黑色、灰色产业链，而在 2014 年将往集团化运营转变，也有传统诈骗集团往手机诈骗

转移的倾向，另一方面，诈骗分析利用先进技术手段群发诈骗短信手法进一步成熟，伪基站诈骗日益猖獗，由于非法利润巨大而正在快速繁殖，派传单与区域硬广的方式正逐步往伪基站迁移。众多省份均在严打伪基站诈骗。

另一方面，诈骗分子都是团伙作案，诈骗短信背后伴随着众多对接的诈骗电话，诈骗电话花样手段方式不断翻新，正呈现持续增长态势，诈骗分子正在进一步向智能手机用户和电信业务集中的省份区域。另一方面，诈骗短信、电话诈骗涉及金额巨大。根据深圳网监数据显示：深圳网监自 2013 年 6 月 6 日至 2013 年全年 11 日，接受用户对于电信诈骗的案例举报达到 27371 次，劝阻 7687 人受骗，涉及金额达到 8640.6 万元，在这 7687 人中，平均每人涉及被诈骗的金额高达 1.12 万。2013 年，腾讯手机管家用户举报诈骗类短信就超过 2141 万。因此，2014 年需要特别防范各种电信诈骗。手机用户可安装腾讯手机管家，有效精准识别并拦截各种诈骗短信、诈骗电话。

10.6 移动安全趋势一：风险多样化,产业链合作成为必然

随着移动互联网的进一步发展,移动安全的风险日趋多样化.手机病毒二次打包，大量 APP 越权读取用户隐私权限，手机隐私信息安全风险大增；目前,病毒的伪装性和逐利性加强,针对手机支付软件、手机银行 APP 的病毒正在逐渐涌现，手机帐号风险增大。用户刷机,可能会导致恶意软件入侵。另外，诈骗短信、诈骗电话正给手机用户带来巨大的资金安全隐患等，移动安全风险正逐步多样化，用户下载 APP 和下载渠道都趋向于分散化，这就要求移动安全企业与产业链各链条和渠道进行打通，而目前，腾讯移动安全联盟与腾讯 ROM 安全联盟则是移动产业链合作的典型案例，这也将促使手机安全的防御生态体系更为健全。

10.7 移动安全趋势二：安全厂商从提供技术到提供标准

2013 年，腾讯手机管家用户针对垃圾短信、诈骗短信的举报、针对骚扰电话的举报大幅提升，针对手机病毒的查杀次数也正在迅速增长，可以看出，手机用户更加关注手机各方

面的安全。而用户安全意识进一步高涨也将推动手机安全行业的发展进程加速。而手机安全厂商也从用户需求与用户利益角度进行对手机用户安全因素做全方位的考量，并由此开始树立行业安全标准。

2013 年 7 月，腾讯手机管家首家发起成立腾讯 ROM 安全联盟，甜椒刷机、刷机精灵、深度安卓门户等刷机厂商纷纷加入，腾讯手机管家针对加入 ROM 安全联盟的商家的 ROM 资源下渠道入口，均实施了“腾讯 ROM 安全联盟”的检测和认证,并建立了相应的防御机制。

而建立腾讯 ROM 安全联盟认证机制也意味着建立了手机 ROM 的安全标准。从提供病毒查杀引擎检测 ROM 安全，到贴上腾讯 ROM 安全联盟的认证标签，腾讯手机管家逐步深耕 ROM 渠道，将影响力逐步铺开逐渐释放到整个行业。

在此之前，腾讯手机管家仅仅为合作电子市场提供检测工具，而目前基于用户安全需求，进一步建立了行业标准。“腾讯 ROM 安全联盟认证”的意义在于，为整个刷机行业树立了标准和安全认证机制，这也从另一方面驱动用户对手机安全的全面关注。

10.8 移动安全趋势三：行业深耕产业链细分领域，差异化竞争态势明显

在 2012 年初，腾讯移动安全联盟的布局就已经闪电式铺开，截至 2013 年，腾讯手机管家联合运营商、终端厂商、40 大应用商店、15 大安全厂商等共同宣布建立了“腾讯移动安全联盟。”通过携手产业链各链条端口，从渠道来源提供安全检测，把控安全入口。

另外，基于垃圾短信、诈骗短信和诈骗电话的进一步泛滥，腾讯携手 12321 建立 12321 垃圾短信举报中心的合作，同时联手顺丰速运、宅急送、圆通、中通等多家物流速运公司推出“来去电提醒”服务,减少冒充快递诈骗案的发生概率。

另外，2013 年以来，腾讯手机管家也携手陕西西安等公安共防电话诈骗。2013 年 12

月 26 日，腾讯手机管家更联合广东省公安厅、中国互联网协会、银监局、银行协会、三大运用商、世纪佳缘、去哪网等政府组织、企业共同发起了国内首个反信息诈骗联盟，这一系列合作，通过整合作产业链上的资源来促成了资源优化组合，反诈骗效果大幅提升，并促使自身软件功能的优化，并形成了有效的差异化竞争优势。

腾讯手机管家还与三星、华为等手机厂商也建立进行深度合作，为其手机产品提供 SDK 或内置“安全模块”。腾讯手机管家在移动安全产业链的系列布局，也从侧面反映出与产业链携手合作并服务于产业链的思路，同时也是移动安全行业的未来发展趋势。

专家建议

目前，Android 手机安全形势变得更加复杂，手机用户应逐步提升手机安全意识，腾讯移动安全实验室专家对手机用户做出如下建议：

1.手机用户应通过正规安全的渠道下载官方版支付、工具、游戏等各类手机 APP，比如可在腾讯手机管家“软件游戏”下载应用，可确保绿色安全。目前,各种网络购物、流行节目中奖等诈骗猖獗，手机用户可开启腾讯手机管家骚扰拦截，有效拦截诈骗类垃圾短信。

2.刷机用户应注重 ROM 安全。许多水货手机出货前就已经刷机或者内置了各种流氓软件，而这些刷入或内置入 ROM 的恶意软件包一般很难用常规手段卸载或清除，新买的手机应及时下载腾讯手机管家，获取 Root 权限，并在安全渠道刷 ROM 包。目前在国内，腾讯手机管家首家发起成立了腾讯 ROM 安全联盟，凡是加入该 ROM 联盟内的刷机厂商上线的 ROM 包，均已通过“腾讯 ROM 安全联盟”检测并可确保绝对安全。有刷机需求的用户可选择已加入腾讯 ROM 联盟内的厂商甜椒刷机、刷机精灵下载安全纯净的 ROM。

3.随着二维码的流行，目前已成为增长最快的染毒渠道，风险增大，手机用户不要见码就扫，最好安装具备二维码恶意网址拦截的手机安全软件进行防护，或者安装带有安全识别

的二维码工具进行二维码扫描，如此可降低二维码染毒风险。

4. 各种新型诈骗短信和电话在今年持续泛滥，对于收到“我是歌手”、“爸爸去哪儿中奖”、“年费”、“密码器过期”类、“网购支付货款被冻结”、“快递地址不详”等以及网银支付、网络购物等系列的诈骗短信与关键词应果断举报并开启腾讯手机管家骚扰拦截，有效拦截诈骗类垃圾短信。

5.综合而言，手机用户应养成使用安全软件来保护手机安全的良好习惯。手机用户可下载安装如腾讯手机管家一类的手机安全软件定期给手机进行体检和病毒查杀，并及时更新病毒库。针对最新流行肆虐危害较大并且难以清除的病毒或者漏洞可下载专杀工具及时查杀或修复。

6.目前而言，用户还可以关注@腾讯移动安全实验室、@腾讯手机管家的官方微博以及相关的“恶意软件曝光”行动，对手机安全资讯做到全面把握和掌控，安享移动互联网生活。

腾讯手机管家官方网站：http://m.qq.com

腾讯手机管家腾讯微博：http://t.qq.com/qqsecure

腾讯手机管家新浪微博：http://weibo.com/txmanager

腾讯移动安全实验室官方微博：http://t.qq.com/QQSecurityLab

2014 年 1 月 9 日

腾讯出品 值得信赖