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

腾讯手机管家
安自心 简随行

腾讯移动安全实验室

2012年
手机安全报告

Mobile Security Report of 2012

目 录

腾讯移动安全实验室 2012 年手机安全报告

第一章 手机安全报告摘要

2012 年，随着 Android 智能手机的大热与普及，手机病毒也发展迅猛。在 Android 平台，2012 年的手机病毒增长呈现直线上升的趋势，安全形势堪忧。

2012 年，腾讯移动安全实验室共检测截获手机病毒总量达到 177407 个，超过 90%的病毒包集中在 Android 平台，Android 已经成为手机病毒肆虐的主战场。

2012 年，在被病毒感染最多的前十款软件中，神庙逃亡、水果忍者、植物大战僵尸 OL 和捕鱼达人这四款最热门游戏无一幸免。

2012 年，腾讯手机管家共为手机用户查出了 5699 万次手机病毒。

广东省 2012 年连续 12 个月手机中毒用户数均位居第一位，全年手机中毒用户比例达到 14.7%，广东、江苏、浙江、北京市、辽宁四省一市位居前五，中毒手机用户比例分别为：14.7%、7.53%、6.5%、6.25%、5.23%。感染比例共占据了全国的 40.21%的比例。

2012 年，腾讯手机管家用户主动举报垃圾短信总量达到 3.04 亿条，其中，广告类垃圾短信占据 79.1% 的比例，位居所有垃圾短信类型之首。

2012 年，各种恶意广告进一步泛滥，截至 2012 年 12 月，腾讯手机管家已检测出含恶意广告的软件包共 467026 个，占已发现所有软件包比例 13.31%。自 2012 年 9 月份腾讯手机管家上线广告拦截功能以来，截至 12 月底，在客户端已经为用户一共拦截了 2404 万次恶意广告。

2012 年二维码大热的背后，安全风险暗藏。据腾讯移动安全实验室监测，腾讯手机管家从 2012 年 7 月为灵动快拍提供二维码安全检测以来，7 月~12 月共为灵动快拍检测网址达 956 万条以上，拦截恶意网址达 20.6 万条。

报告正文

第二章 2012 年全年手机安全现状

2012 年，随着国内 Android 系统的设备的持续大幅增长，Android 系统市场占有率占据主流地位，而 Android 系统的手机病毒包也呈现爆发式增长态势，手机病毒的技术日渐成熟，在 2012 年，手机病毒包全年呈现前所未有的高速增长。而 Symbian 系统逐渐走向没落，手机病毒的发展缓慢平稳，衰落趋势已经非常明显。因此，2012 年，Android 与 Symbian 的病毒增长对比显得非常强烈。

2.1 2012 年全年手机病毒包高速增长

2012 年全年，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手机病毒总量达到 177407 个，其中 Android 平台为 159333 个，占据病毒包总量 90%以上。腾讯手机管家 2012 年全年截获的病毒样本包总量是 2011 年全年 6.98 倍。

在 Android 平台，2012 年腾讯手机管家平均每月检测截获超过 1.3 万个病毒样本，在 9 月检测出全年最高 30564 个病毒样本。2012 年 8、9、12 三个月单月的 Android 病毒样本包数均已超过 2011 年全年的手机病毒样本包总量。

在 Android 平台，据腾讯移动安全实验室监测，2012 年手机病毒包全年持续增长，相对上半年，第三、四季度呈现突增暴涨的趋势，第三、四季度病毒样本包之和是第一、二季度的 5.2 倍。在 Symbian 系统，全年发现病毒总量 18047 个，最高 7 月截获 1789 个病毒包，最低在 11 月仅截获 1127 个病毒包，2012 年，Symbian 系统的病毒包呈现全面平稳缓慢下降的趋势，这与 Symbian 系统的持续衰落的大趋势密切相关。

2.2 2012 年众多热门游戏被病毒感染

在 2012 年，被病毒感染最多的前十款软件中，游戏软件占据了 4 款，分别是 RagingThunder、水果忍者、植物大战僵尸 OL 和捕鱼达人。工具类软件 3 款，分别为 FlashPlayer 和 Batterry SuperCharge、Advanced Task Killer Free；1 款系统软件 Install、1 款主题类软件 KMhome 以及 1 款通讯类软件 Skype。

据腾讯移动安全实验室监测，由于植物大战僵尸自推出以来就备受用户喜爱，在各大电子市场下载次数都已经超过 2000 万，病毒作者也看中了其强大的品牌影响力，纷纷将病毒打包在植物大战僵尸游戏中，普通用户无法做出判断，仅 2012 年 11 月腾讯手机管家就

检测查杀了 14 个病毒入侵植物大战僵尸，总共感染的安装包高达了 583 个，因此染毒的 Android 手机用户规模极其庞大，预计影响人群在百万之众。

除 2012 年感染病毒最多的十大软件之外，许多手机用户耳熟能详的热门软件均被病毒感染。2012 年 7 月，腾讯移动安全实验室就截获了一款 Android 病毒：反动联盟 2（a.fraud.eyu），该病毒将恶意代码注入十余个版本的《鳄鱼爱洗澡》游戏，预计整个 Android 市场已造成上 100 万 Android 用户感染；同月，知名游戏“割绳子”被注入功夫系列病毒恶意代码然后进行二次打包。2012 年 5 月，游戏幽灵（a.fraud.fakeapp）病毒入侵愤怒的小鸟。与此同时，唱吧、捣蛋猪等 2012 年热门软件和游戏都纷纷中招被感染病毒。

可以看出，2012 年，手机病毒打包热门游戏或软件捆绑传播感染成为非常明显的趋势，手机病毒制作者或制毒机构通过一个病毒多次打包捆绑海量应用程序，快速发布快速感染海量用户群，随着制毒者或制毒机构投毒相关技术的提升，手机病毒的伪装性与隐蔽性越来越强，而手机用户选择官方网站与正规渠道下载软件是规避病毒入侵的有效办法。

2.3 2012 年全年用户感染量高速增长

2012 年全年手机病毒感染用户数呈几何式高速增长的态势，在腾讯手机管家上亿的用户数中，其中手机中毒用户就达 3466 万人次，与人口大省贵州省人口总量接近。据腾讯移动安全实验室监测，2012 年 12 月已达 577 万手机用户感染病毒，是 1 月份 97 万感染病毒用户的 5.9 倍。其中 Android 平台在第三季度感染用户数出现剧增，第四季度呈现高速增长态势。而 Symbian 平台感染用户数在第三季度出现增长顶峰后，在第四季度开始逐渐回落。

2012 年，腾讯手机管家共为手机用户查出了近 5699 万次手机病毒。2012 年 12 月查杀次数达到 898 万，病毒查杀次数为全年最高月，是 1 月份 163 万病毒查杀次数的 5.5 倍。其中 Android 平台查出病毒次数 3856 万次，Symbian 平台查出病毒次数 1842 万次，其中 Android 平台在第三季度查出病毒次数开始剧增，第四季度呈现高速增长。而 Symbian 平台查出病毒次数在第三季度出现增长顶峰后，在第四季度开始逐渐回

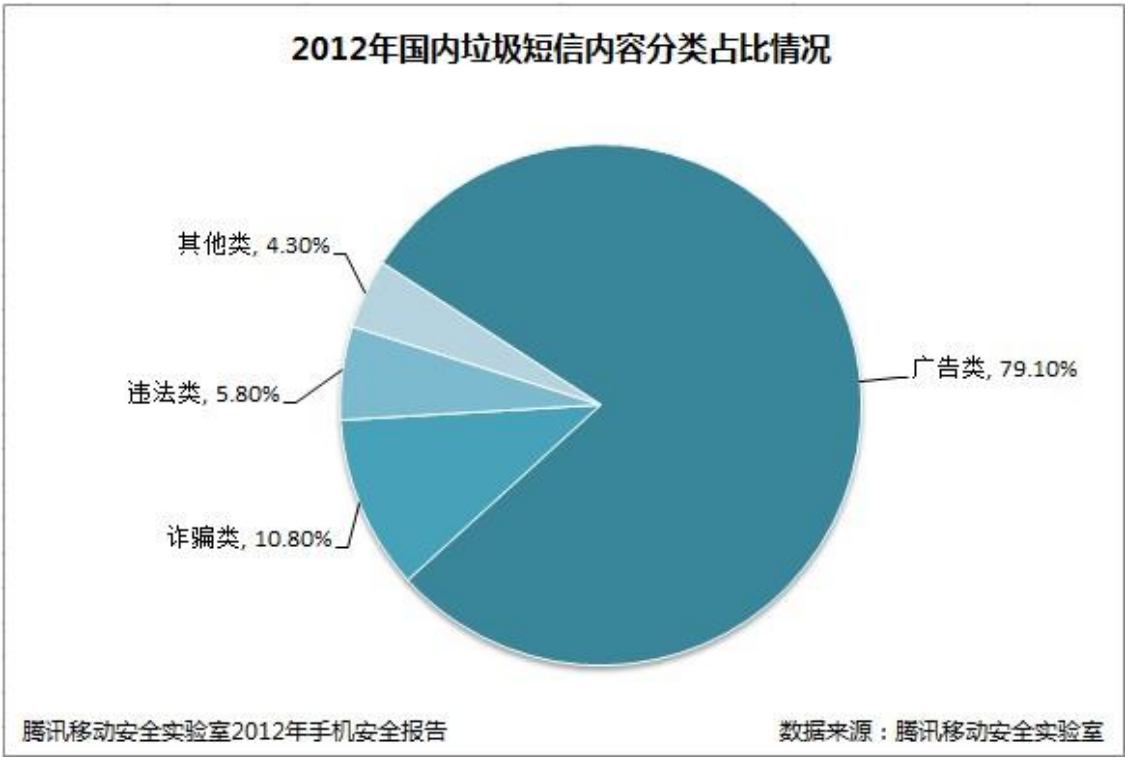
基于手机病毒疯狂增长的趋势，腾讯移动安全实验室总结了 2012 年感染用户最多的十大手机病毒。腾讯移动安全实验室后台监控到，2012 年感染用户排名前十的手机病毒分别为：a.expense.apkquq.[流量凶煞]、a.remote.i22hk.[云指令推手]、a.expense.mdk.[僵尸网络]、a.expense.cc.[暗推神器]、a.payment.lemei.[彩信魅影]、a.expense.dpn.[K 歌毒器]、 a.expense.forge.c.[暗战行者]、a.propagation.rootsmart.[隐私间谍]、a.expense.jxkj.[暗影恶魔]、a.system.deviceadmin.[伪谷歌服务]。感染用户总数已超过 780 万，单个病毒平均感染 78 万用户。其中“流量凶煞“感染用户数已经超过 108 万，为全年感染用户最多的手机病毒。

2012年感染用户最多的十大手机病毒		
病毒名称	感染人数	病毒特征
a.expense.apkquq.[流量凶煞]	1080000	该病毒未经用户允许私自下载未知安装包，且不能正常退出，给用户带来流量消耗与未知风险。
a.remote.i22hk.[云指令推手]	949118	该病毒一旦激活便自动后台上传IMEI、IMSI等信息到http://www.***.hk，并获取云端指令控制用户手机，屏蔽特定号码发送过来的短信，同时会修改浏览器书签以及联网下载未知程序，给用户手机安全造成严重威胁。
a.expense.mdk.[僵尸网络]	908092	该病毒安装后，开机强制启动，从远端服务器自动下载恶意脚本代码，私自下载未知应用程序安装包，消耗用户流量，给用户带来未知的风险。
a.expense.cc.[暗推神器]	851346	该病毒开机后私自下载软件并安装，可能会造成了一定的流量消耗，给用户的手机安全带来未知的风险。
a.payment.lemei.[彩信魅影]	783160	该病毒启动后会私自发送扣费短信，定制SP业务，可能会给用户的手机安全带来一定的威胁。
a.expense.dpn.[K歌毒器]	773986	该病毒启动后私自联网下载软件，静默安装推广软件，给用户带来流量消耗与未知风险。
a.expense.forge.[暗战行者]	648842	该病毒植入恶意推广广告，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。
a.expense.rootsmart.[隐私谍影]	633170	该病毒伪装成系统关键程序，启动后申请授予root权限，并在后台私自下载并静默安装其它恶意应用，同时会收集短信、通话记录等隐私信息，给手机用户的安全造成较大威胁。
a.expense.jxkj.[暗影恶魔]	614694	该病毒安装后无图标，开机自启动，在后台自动下载程序并静默安装，给用户的手机安全造成一定威胁。
a.system.deviceadmin.[伪google服务]	593964	该病毒伪装成系统关键程序，安装后会误导用户授予其系统高级权限，在后台定期发送扣费短信，而且无法通过正常流程卸载，影响系统的正常运行。
数据来源：腾讯移动安全实验室		

2.4 2012 年垃圾短信迅猛增长

垃圾短信的数量在全年呈现大幅上涨的趋势。2012 年，腾讯手机管家用户主动举报垃

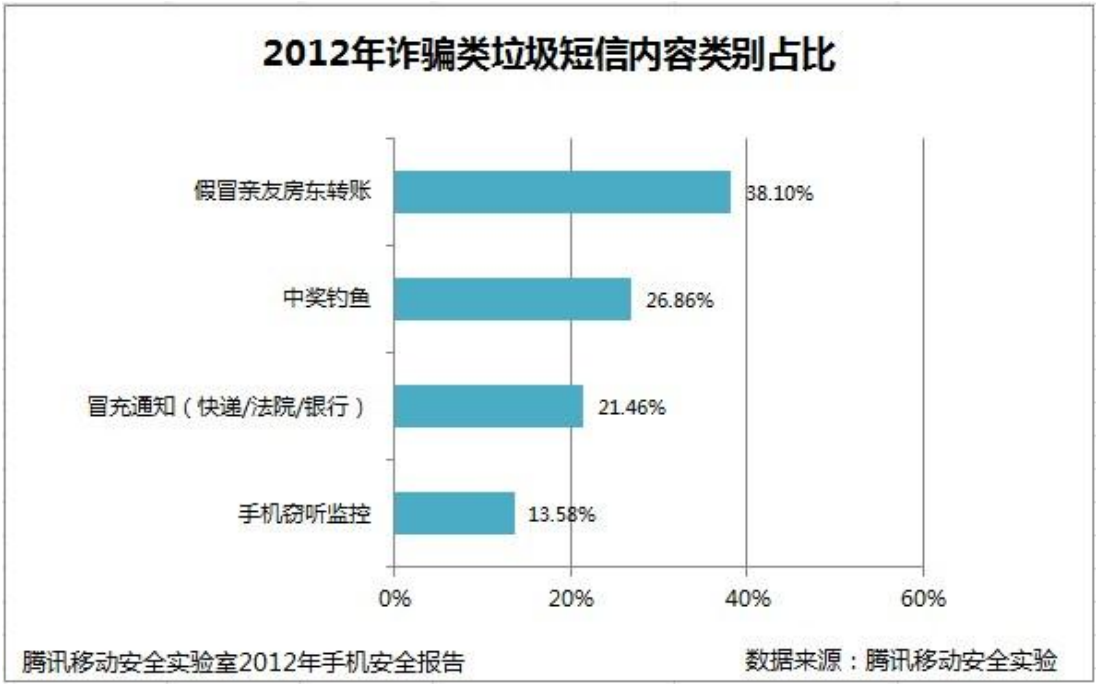
圾短信总量达到 3.04 亿条，其中，广告类垃圾短信占据 79.1% 的比例，位居所有垃圾短信类型之首。诈骗类垃圾短信占总量 10.8%，违法类短信占据垃圾短信总量的 5.8%，其他类别的占比 4.3%。



而在广告类短信中，卖场促销、房产推销、网店电商类为主，分别占据 49.68%、14.10%、8.72%的比例。广告类垃圾短信成为骚扰用户频率最高也最为常见的垃圾短信类型。

在违法类短信中，频率最高的是高利贷、违禁物品、学历买卖这三类，分别占据了违法类短信 39.01%、18.96%、14.22%的比例。

在诈骗类短信中，冒充亲友房东转账类占诈骗类短信的 38.1%，中奖钓鱼类与冒充通知（快递、法院、银行）分别占据 26.86%、21.46%。这三类短信位居诈骗类短信的前三位。



2012 年以来，随着运营商与国家监管部门的大力整治，违法类与诈骗类垃圾短信相对往年的比例正在逐步减少。但与此同时，广告促销类垃圾短信则呈现大幅上扬的趋势。

腾讯手机管家总结了 2012 年垃圾短信中出现频率最高的十大关键词组：订购预约、秒杀回馈、男女公关、促销现金券、资金周转、抵押借贷、星光大道、中国好声音、中奖验证码、传票取票。

腾讯手机管家提醒手机用户，年关在即，手机用户对诈骗类垃圾短信应保持高度警惕，并提醒身边的亲朋好友不要上当受骗。安装腾讯手机管家并开启智能拦截，可对垃圾短信进行一键拦截举报。

2.5 2012 年恶意广告泛滥成灾

2012 年，由于移动应用开发商与移动广告商都急于获取利润，而各种入侵式的恶意弹

出广告则成为他们最快捷的盈利方式。2012 年，捆绑恶意广告插件的手机应用开始大幅增长，比如腾讯手机管家在 2012 年 6 月查杀的的暗战行者病毒，就暗含恶意推广广告插件，感染的软件高达 3700 多款。病毒制作者或制毒机构擅长针对《愤怒的小鸟》、《割绳子》、《捣蛋猪》、《植物大战僵尸》、《鳄鱼爱洗澡》、《水果忍者》、《神庙逃亡》等热门游戏或应用进行恶意篡改、植入恶意广告并进行二次打包推广，进而感染海量用户。

各种内嵌式或通知栏广告弹窗疯狂增长，不仅影响了产品体验，还阻碍移动广告业和移动互联网的健康发展。与此同时，国内众多安全厂商也开始上线广告拦截功能，确保手机用户获得良好的用户体验，避免因恶意广告而带来流量消耗、隐私泄漏等损失。

2012 年 9 月，腾讯手机管家在“实用工具”栏中上线了“广告拦截”功能，只要用户手机已经获取 Root 权限便可以开启该功能。开启广告拦截后，收到恶意广告，会提示用户处理，选择“以后拦截”，这些恶意广告将被精准拦截，不会继续在通知栏弹出骚扰用户。

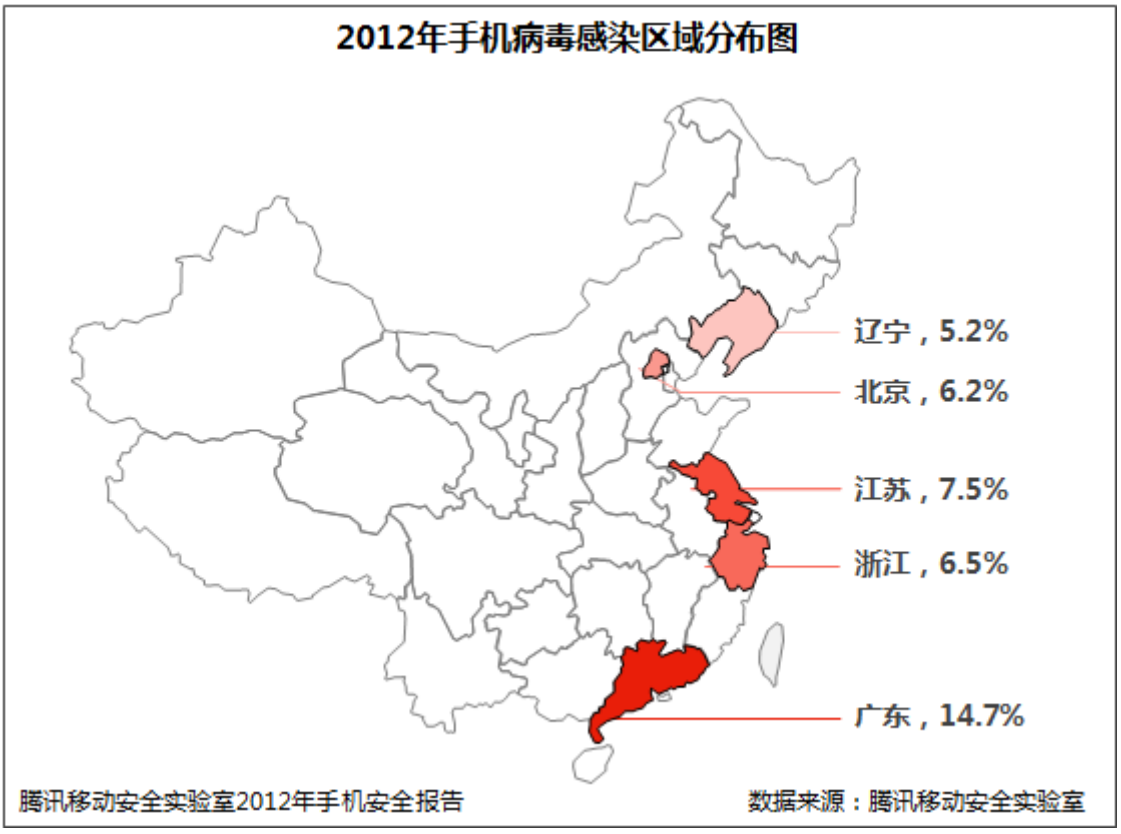
腾讯移动安全实验室在 2012 年的监测数据显示，截至 2012 年 12 月，腾讯手机管家已检测出含恶意广告的软件包共 467026 个，占已发现所有软件包比例 13.31%。从 2012 年 9 月份腾讯手机管家上线广告拦截功能以来，截至 12 月底，在客户端为用户拦截了 2404 万次恶意广告。

第三章　2012 年各区域省份手机中毒情况分析

在 2012 年中，十大中毒手机用户最多的省份依次为广东、江苏、浙江、北京、辽宁、四川、福建、河南、山东、湖北。广东省 2012 年连续 12 个月手机中毒用户数均位居第一位。广东全年手机中毒用户比例达到 14.7%，感染用户人次接近 509 万，接近广州市人口总量 40%。排名前十的中毒省份占据了全国 61.52%的感染用户比例，感染用户超过 2129.8 万人次。

其中，广东、江苏、浙江、北京市、辽宁四省一市位居前五，中毒手机用户人次比例分

别为：14.7%、7.53%、6.5%、6.25%、5.23%。感染比例占据了全国 40.21%的比例。



可以看出，北上广地区是手机中毒用户大规模集聚地区，经济发达程度与中毒手机用户数量基本呈现正相关的发展趋势。制毒机构针对沿海经济发达地区定向投毒渠道已趋于稳定。在这些地区，智能机用户大量集聚、也是线上电子市场、手机论坛用户群分布活跃区域。在线下，刷机产业、水货手机、电子行业市场的繁荣以及恶意软件利益链进一步形成是北上广地区手机中毒居高不下的重要原因。

辽宁省是除北上广地区之外的第一个中毒手机用户大省，全年中毒手机人次比例达到 5.2%.而据腾讯移动安全实验室监测，辽宁在 2012 年第二、三、四季度的 Symbian 平台中毒用户人次比例均排名第三，超过 6%。在 Android 平台，辽宁在 2012 年第二、三、四季度的中毒用户人次比例均进入全国前五。辽宁省处于北京辐射经济区，快速发展的经济推动智能机市场进一步繁荣，加之之前辽宁省 Symbian 平台用户广泛存在，在 2012 年的换机大潮中的表现尤其抢眼。另一方面，众多 Android 系统千元智能机与水货手机也纷纷进入

辽宁市场，Android 用户的大量增加也客观上抬高了内置恶意软件的比例，也使得辽宁省成为手机中毒的高发区。

另一方面，手机中毒省份疫情进一步向中部经济快速发展省份推进，四川（4.96%）、河南（4.34%）、山东（3.88%）、湖北（3.63%）进入前十，这些地区 Android 新兴智能机用户正快速增长，新兴用户缺乏手机病毒防御意识和应对措施，手机中毒的几率较高。加之中部地区手机病毒监管机制的薄弱，制毒机构开始盯紧新增的手机用户，有意识的扩大手机病毒投放区域与提升病毒投放技术，资深黑客正在进一步优化各省份的病毒传播渠道，最大限度的从手机用户身上攫取非法利润，中部经济快速发展省份的手机中毒比例正持续增长。

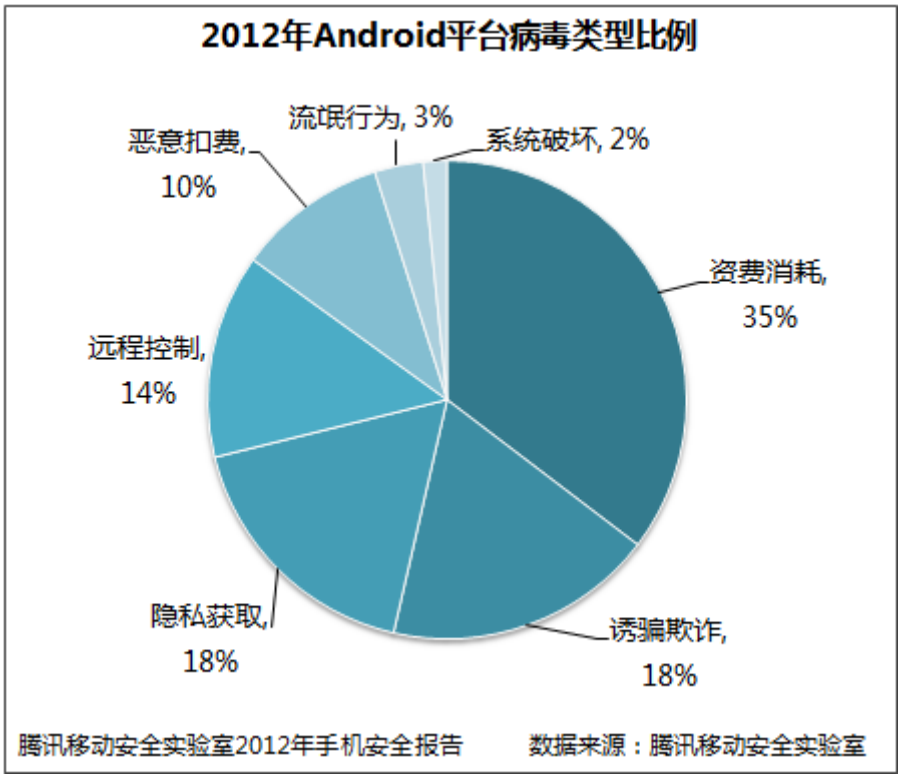
第四章　2012 年各平台手机病毒行为类型比例

4.1　Android 系统病毒行为类型比例

腾讯移动安全实验室监测：在 2012 年全年的 Android 病毒行为类型比例统计中，资费消耗类病毒行为一直是主流，占据 35.33%的比例；诱骗欺诈类病毒行为占据 18.23%；而资费消耗类行为往往并行于其它几种病毒行为中，这也造成了资费消耗类行为一直居高不下的重要原因。

17.53%的隐私窃取类病毒行为可以通过后台上传用户短信、通讯录、照片、甚至网银密码等关键强隐私信息，通过联网或者短信外发到指定号码，导致用户隐私大规模泄露；而比如在 2012 年 11 月，腾讯手机管家查杀的“隐私飓风”病毒，会在后台启动定时任务，收集用户手机里的隐私信息并上传到指定位置，窃取用户隐私，并偷偷发送扣费短信，拦截运营商扣费回执短信，使得用户不知不觉被扣费。同时具备吸费与窃隐私双重特征。

在 Android 平台，13.81%的恶意扣费类病毒行为往往会私自联网下载软件、私自发送、拦截指定号码短信，诱骗开通 SP 扣费业务或者通过连接指定的恶意扣费链接的方式，无声无息“吸取”用户的手机话费。2012 年 7 月与 9 月腾讯手机管家查杀的“伪 MM 画皮”及其变种感染用户超 40 万，可以通过感染并模拟运营商电子市场的扣费接口来诱导用户联网下载，进而间接扣取用户资费。另外，随着黑客远程控制技术的进一步增强，远程控制类行为占据了 10.15%；流氓行为、系统破坏、恶意传播类行为占据比例则极低，分别为 3.28%、1.6%、0.06%。



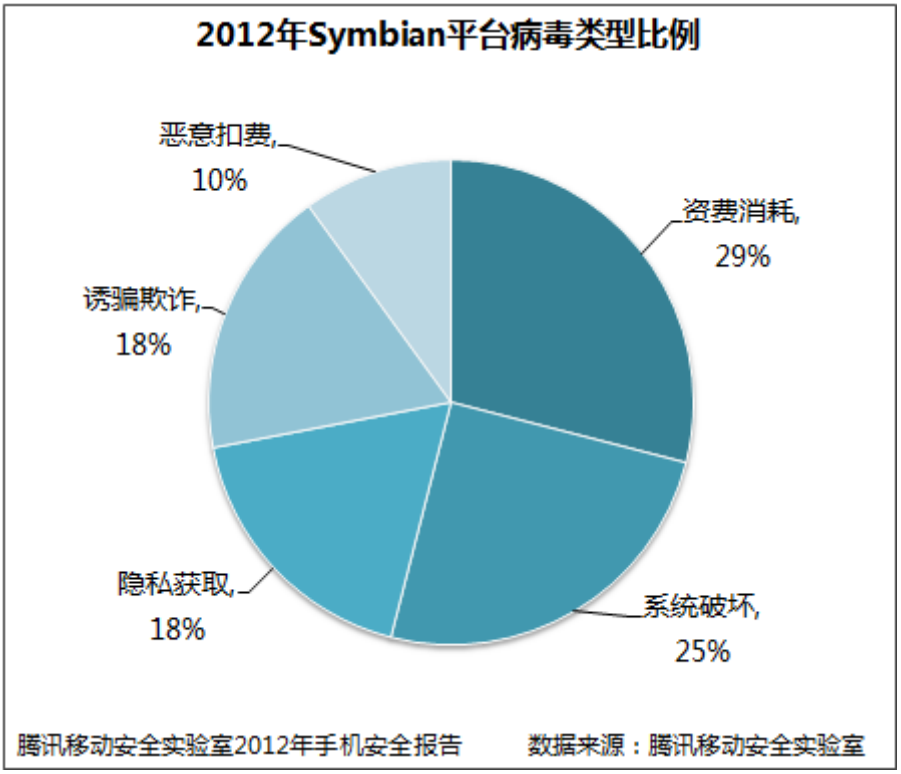
腾讯移动安全实验室预：2012 年，手机病毒大幅转向恶意扣费、隐私窃取与资费消耗类病毒行为，病毒制作者或制作机构追求短平快的盈利模式的倾向性加强。随着病毒制毒者或制毒机构逐利性进一步加强，预计 2013 年 Android 平台手机病毒将继续保持连续高速增长态势，病毒类型进一步朝多元化方向发展。

4.2 2012 年 Symbian 系统病毒类型比例

Symbian 系统的衰落趋势非常明显。在 2012 年全年中，资费消耗类病毒行为与系统破坏类病毒行为占据病毒类型的主流，分别达 29%与 25%的比例；诱骗欺诈与隐私保护类行为均占 18%。恶意扣费类行为占据 10%。2012 年，Symbian 平台病毒类型经历了资费消耗、诱骗欺诈、系统破坏三类病毒行为三分天下的格局之后，隐私保护与恶意扣费类行为开始呈缓慢上升趋势。破坏安全软件进程、诱骗安装、私自联网、消耗流量同时私发短信订购 SP 业务成为 Symbian 病毒 2012 年明显的特征。

总体上，Symbian 系统一直处于持续衰落之中，智能机保有量与新增病毒或恶意软件

都在进一步降低。病毒制作者或制毒机构投放病毒类型将更加多元化，隐私获取与恶意扣费类行为比例还将持续扩大。而手机病毒制作者与制毒机构对 Symbian 病毒投放的权重将会降低。



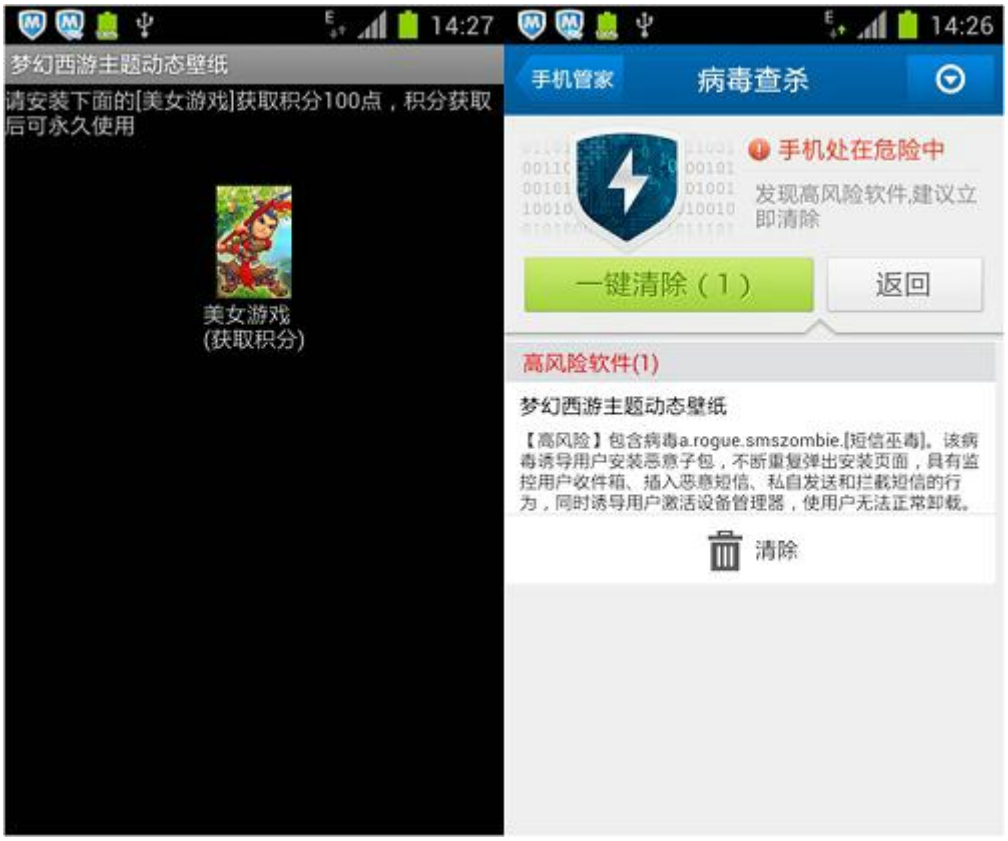
腾讯移动安全实验室预测：在 2013 年，Symbian 系统的病毒发展将保持平稳缓慢增长的趋势。但衰落的大趋势已经无法避免，未来 Symbian 平台将有可能逐渐淡出舞台。

第五章　2012 年最受关注 3 大手机安全事件

5.1　安全事件之一：“短信巫毒”（又称“短信僵尸”）爆发

“短信巫毒”（又称“短信僵尸”）手机病毒在 2012 年 8 月下旬大规模爆发，该病毒可通过监控用户收件箱、插入恶意短信、私自发送和拦截银行卡帐号信息，黑客通过远程控制指令，可将帐号信息发送到黑客指定的号码上，用户的短信内容、银行卡、信用卡帐号以及账单支付等个人网银数据都在黑客监控之下。“短信巫毒”还会捆绑在美女动态壁

纸等热门 Android 应用中，诱骗用户下载。一旦安装激活后，病毒自带恶意安装包会不停弹出提醒用户下载，让用户手机成为病毒“集中营”。短信巫毒（又称“短信僵尸”)大规模爆发之后又呈现多个变种，预测整个市场感染手机用户超过 100 万，引发手机安全行业的集体预警以及手机用户和相关专家的持续关注，成为 2012 年最受关注的手机安全事件之一。



5.2 安全事件之二：Android 系统曝出“短信欺诈”漏洞

2012年11月,美国北卡罗来纳州州立大学发现Android平台“短信欺诈”(Smishing)漏洞之后，研究员当即发现，在对多款流行的 Android 设备，其中包括谷歌 Galaxy Nexus、Nexus S、HTC One X、HTC Inspire、小米 MI-One 和三星 Galaxy S3 等机型测试后，这一漏洞已被证实在上述机型中存在。谷歌之后承认该漏洞可以允许应用在 Android 平台上进行短信伪装，且在所有版本的 Android 软件中都存在这一漏洞。腾讯手机管家迅速反应，于 2012 年 11 月中旬推出了腾讯手机管家新版修补了该漏洞，并推出

“短信欺诈漏洞”专杀工具精准查杀。短信欺诈漏洞病毒不需要获取发送短信的权限就可以直接给本机发送欺诈短信，导致个人财产的巨额损失，成为 2012 年度重大手机安全事件之一。

5.3 安全事件之三：欺诈僵尸网络大规模袭击

2012 年 12 月，美国主要网络又出现了新型的 Android 欺诈僵尸网络。据手机安全工程师分析，该病毒安装后，会私自联网获取大量未知手机号码和恶意短信内容，未经用户允许大量转发恶意短信内容到未知手机号码，形成了一个以恶意传播为目的的欺诈僵尸网络。12 月 18 日，腾讯移动安全实验室在国内也率先截获了造成欺诈僵尸网络的始作俑者——Android 病毒 a.spread.l0rdzs0ldierz。欺诈僵尸网络的的传播非常智能化，病毒激活后，会联网到云端获取大量的手机号码和短信内容并偷偷转发，在用户不知道的情况下发送上千条欺骗短信，消耗手机大量资费，一旦中了该 Android 病毒，手机就会陷入欺诈僵尸网络的死循环，不仅会收到了其他感染手机发来的恶意短信，还会成为传播源，发布大量的恶意短信。一不小心，就成了病毒传播的帮凶。病毒会在这种裂变传播效应中快速扩散传播范围与人群。由于欺诈僵尸网络的传播感染非常智能化，手机用户也在一环扣一环的感染中成为黑客手中的肉鸡，该病毒也因此引起了手机安全行业的预警，成为 2012 年度重大安全事件之一。

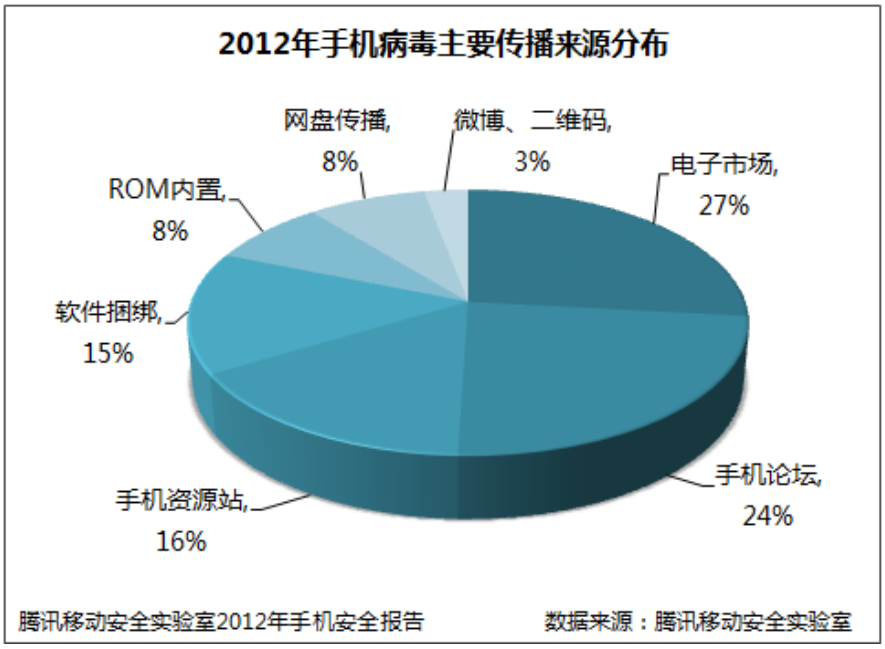
第六章　病毒传播渠道来源分析

在 2012 年全年，恶意软件或手机病毒的来源渠道分布中，手机论坛和电子市场占据了绝对的主导地位，分别占据了27%和24%的来源比例。手机资源站以16%的比例位居第三。在目前，国内许多中小型的电子市场审核机制并不完善，许多电子市场还具有一定的网友自助上传即发布、论坛内搜索等功能，这无疑大大增加了病毒入侵的几率与用户中招的可能性。另一方面，由于许多中小型厂商内置电子市场的安全检测率低，感染手机病毒的情况正在加剧。

2012 年，手机病毒家族在成群增长，通过一个病毒因子多次打包捆绑海量应用程序批量制毒成为突出特点，全年软件捆绑占据了 15%的比例，已成为手机病毒的主流传播渠道。手机病毒制作者快速发布快速感染海量用户群的特征也推动网盘捆绑论坛提供下载链接的传播比重加大，加之在手机论坛相对宽松的审核机制下就越有其有利的生存土壤。

随着刷机用户急剧增长与水货手机内置软件的大规模泛滥，水货手机、山寨手机泛滥推动这内置 ROM 病毒的水涨船高，也为盗版山寨应用潜入各种渠道提供了便利，Rom 内置渠道占据 8%的比例。但另一方面，2012 年下半年腾讯移动官方正版联盟成立之后，各大合作的电子市场的山寨软件识别与查杀功能正在逐步优化，众多电子市场不断加入正版安全联盟，山寨软件在一定程度上被遏制。

2012 年以来，随着二维码的快速流行，使得手机病毒制作者迅速盯上了这个盈利渠道，二维码渠道来源从无到有，并迅速占据了所有病毒传播渠道 3%的比例。2012 年，制毒者或制毒机构利用该渠道内置恶意链接或网址盗取网银资金、恶意扣费等现象已经进一步引起媒体与行业关注，“不要见码就刷”已成为 2012 年二维码火爆的一个关键词。



第七章　2012 年手机病毒、恶意软件发展特征分析

7.1　恶意扣费类木马肆虐

2012 年以来，恶意扣费类木马频频肆虐。据腾讯移动安全实验室监测，2012 年感染用户最多的十大扣费病毒感染用户已经超过 256 万。

感染用户达 78 万的扣费类病毒 a.payment.lemei.[彩信魅影]排名第一，该病毒最为厉害的地方 ,在于可以屏蔽扣费业务反馈给用户的确认或扣费短信 ,无形中吸取用户大量话费。

而腾讯手机管家在 2012 年 7 月与 9 月查杀的“伪 MM 画皮”扣费病毒以及变种，伪装能力进一步加强，该病毒可以通过感染运营商电子市场的扣费接口、执行扣费操作并自行验证、拦截扣费的回执短信，扣取用户资费。目前该病毒已经感染用户超过 40 万。

扣费类病毒在 2012 年表现出来的特征趋向多元化。以腾讯手机管家查杀的“a.payment.kituri.[隐私飓风]”与 a.payment.pmx.[刷机吸费大盗]两个扣费病毒为例，这两个的病毒共同点在于，通过后台私自联网获取扣费配置，偷偷发送扣费短信，并拦截运营商扣费回执短信，并在后台启动定时任务，上传其中用户手机 IMEI、IMSI 号等隐私，其中“隐私飓风”在 2012 年感染用户已达到 44.5 万。

由于扣费类病毒可以直接盗取用户流量资费和隐私，盈利迅速快捷，在 2012 年，扣费类病毒快速发展，并逐步衍生新的变种和技术，值得手机安全行业与手机用户警惕。

2012年十大扣费类病毒		
病毒名称	**感染人数**	**病毒特征**
a.payment.lemei.[彩信魅影]	**783160**	该病毒启动后会私自发送扣费短信，定制SP业务，可能会给用户的手机安全带来一定的威胁。
a.payment.kituri.[隐私飓风]	**445532**	该病毒安装后于后台私自发送短信，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。
a.payment.kituri.a	**326894**	该病毒安装后于后台私自发送短信，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。
a.payment.MMarketPay.b.[伪画皮2]	**232816**	该病毒能通过偷偷切换APN为CMWAP，然后后台模拟点击中国移动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。
a.payment.fakekoogame.a	**226622**	该病毒安装后，恶意拦截SP业务订购短信，同时未经用户允许私自发送短信确认SP订购业务，存在恶意扣费和流氓行为。
a.payment.daemon	**200848**	该病毒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，并且删除相应的回执信息；同时该病毒还尝试联网，获取最新扣费指令，可能给用户带来进一步的经济损失。
a.payment.MMarketPay.a	**154142**	该病毒能通过偷偷切换APN为CMWAP，然后后台模拟点击中国移动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。
a.payment.ms.[黑暗骑士]	**76018**	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，具有严重的安全隐患。
a.payment.req	**69882**	该病毒启动后私自发送扣费短信，并屏蔽指定号码的回馈短信，给用户的手机造成一定的威胁。
a.payment.pmx.[刷机吸费大盗]	**45758**	该病毒安装后没有启动图标，安装后伪装为系统进程常驻内存，病毒一旦激活便在特定的时间向某SP号码发送扣费信息，还会屏蔽回执短信，让用户在不知情的情况下被扣除高额的话费；同时该病毒还会在后台自动联网，读取并且上传用户手机IMEI、IMSI和手机号码等信息，造成用户个人隐私的泄露。
数据来源：腾讯移动安全实验室		

7.2 二维码成手机用户感染病毒新渠道

2012 年，随着二维码的普及与快速流行，该入口也成为一个巨大的病毒传播渠道。黑客利用二维码的兴起，把病毒下载的链接、钓鱼网址等转换为二维码发布在户外、微博、论坛等各种途径开始大规模传播。

二维码病毒一般可以在刷码之后跳转到恶意钓鱼网站，骗取话费或流量，但发展到 2012 年年底，也进入了多元化时代。据腾讯手机管家 12 月底查杀的“扫码巫毒”(a.expense.aiplay)的病毒开始盯上了二维码源头二维码生成器进行传播，用户还未刷码就已经感染。

目前而言，多数二维码厂商欠缺手机安全检测技术，二维码病毒制作者利用二维码、微博短链接技术，将恶意代码内置其中，而真实的网址跳转地址可以被屏蔽，点击含病毒的下载链接地址时，就会自动下载病毒到手机上。

2012 年下半年，灵动快拍、我查查等二维码商家与腾讯手机管家建立了二维码安全检测合作，通过腾讯手机管家的安全认证免费检测是否包含恶意代码等风险，这样可避免用户感染病毒。据腾讯移动安全实验室监测，腾讯手机管家从 2012 年 7 月为灵动快拍提供二维

码安全检测以来，7 月~12 月共为灵动快拍检测网址达 956 万条以上，恶意网址拦截率为 2.1%，拦截恶意网址达 20.6 万条。

7.3 手机支付与手机电商相关病毒爆发式增长，安全支付成重心

整个 2012 年，全球智能机用户已经超过 10 亿。国内 Android 用户已经接近 2 亿，移动电子商务、移动支付的巨大发展前景致使制毒者或制毒机构盯上了这块诱人的蛋糕。

据腾讯移动安全实验室监测，在 2012 年 8 月大规模爆发感染预计超过 100 万用户的“短信巫毒”（又称“短信僵尸”）病毒可通过监控用户收件箱、插入恶意短信、私自发送和拦截银行卡帐户信息，黑客通过远程控制指令，可将信息发送到黑客指定的号码上。而臭名昭彰的网银大盗宙斯木马在 2012 年又推出了新版本，迄今已给银行客户造成 470 万美元的损失。目前，这两种网银窃取类病毒已经被腾讯手机管家精准查杀。而随着移动支付的进一步普及，中国的手机支付业务量与前景均相当可观。手机银行、手机支付、手机一卡通以及移动互联网支付在内的多种应用迅速发展与普及，2013 年，移动支付或将大行其道，而包括金融机构、运营商、设备厂商、安全软件厂商在内的产业链各方将进一步加速布局，与此同时，2012 年攻击用户网银或窃取用户手机支付类账号密码的病毒正逐步增多，“钓鱼式攻击”将更多的从互联网转向了移动互联网，安全支付将成为 2013 年移动互联网发展的重心。而另一方面，通过技术创新，2013 年市场上将出现更多针对移动支付产业的解决方案。

7.4 Android 短信欺诈漏洞的曝光，短信欺诈类病毒大批量涌现

2012 年 11 月 ,美国北卡罗来纳州州立大学发现 Android 平台“短信欺诈” (Smishing) 漏洞之后，央视东方时空也针对 Android “短信欺诈” 漏洞进行了大规模的报道，恶意软件可利用短信“欺诈漏洞”伪装成手机里面通讯录熟人，进行诈骗，令人防不胜防。更让人震惊的是，利用这个漏洞的恶意软件，在手机未联网的情况下，黑客可以通过该漏洞轻松破解并模拟手机中任意号码给用户发送欺诈短信，骗取手机用户的金钱。短信欺诈漏洞病毒同

时会导致用户隐私权限被不正当获取。由于该漏洞可以轻易致使用户“中招”，腾讯手机管家迅速反应，早于 2012 年 11 月中旬便推出新版修复了漏洞，同时还推出“短信欺诈漏洞”专杀工具，以双重解决方案有效成功查杀病毒并修复漏洞。另外，腾讯手机管家还可以通过“权限监控”功能可以监控到病毒或恶意软件利用“短信欺诈”漏洞，并有效阻止病毒或恶意软件利用该漏洞向用户发送欺诈短信。央视对该漏洞进行了大规模报道后，腾讯手机管家又曝光了查杀的 550 款“短信欺诈”漏洞病毒。在制毒者逐利性的驱使下，短信欺诈类病毒还在大规模涌现。

第八章　2013 年手机安全发展趋势预测

8.1　安全趋势之一：利用漏洞、嵌入系统层的病毒将进一步成熟

2012 年 11 月，谷歌被曝光 Android 平台存在短信欺诈漏洞后，通过该漏洞的病毒在 2013 年仍在不断演化变种升级。预测在 2013 年，依然有大量短信欺诈类手机病毒代码被内置到正常游戏、工具类软件中提供给用户下载，然后伺机利用短信欺诈漏洞骗钱。

2012 年 12 月 18 日，腾讯移动安全实验室在国内也率先截获了造成欺诈僵尸网络的始作俑者——Android 病毒 a.spread.l0rdzs0ldierz。该病毒安装后会私自联网获取大量未知手机号码和恶意短信内容，再转发到未知手机号码，形成了一个以恶意传播为目的的欺诈僵尸网络。

截至目前，僵尸网络病毒已感染众多手机用户与热门软件，短信欺诈漏洞病毒已经超过 550 款，预测整个市场被感染用户超 100 万。可以预测的是，在 2013 年，以利用漏洞以及以僵尸网络为基础的病毒传播将进一步成熟。

8.2　安全趋势之二：恶意广告类木马将进一步泛滥，技术更高更隐蔽

2012 年以来，恶意推广类病毒进一步肆虐。以腾讯手机管家 2012 年 10 月截获的

a.expense.fakeKernel.[暗箭射手]为例，此病毒当时已经感染了 2 万用户，107 款软件被感染，共计 19259 个 APK 包。按照一个用户被推广 2-4 个软件来算，每个软件的推广费从 1-1.5 元不等，病毒制造者最高可获利 14 万左右。高盈利、低成本、快速批量感染使得恶意推广类病毒进一步泛滥。

2012 年 10 月，腾讯手机管家查杀的 a.system.gmeil.a.[毒胶囊] 病毒代表着恶意广告类病毒的发展的新阶段，该病毒内嵌了恶意代码，病毒发作后会提醒用户有更新并提醒用户安装 当用户安装了这些软件后继续通过获取 Root 授权的方式静默安装其他软件牟取暴利。该病毒存在自动获取 Root 权限、恶意扣费、推广软件等恶意行为。

2012 年 6 月，腾讯手机管家查杀了命名为暗战行者（a.expense.forge）的恶意推广类病毒，预计整个 Android 市场该病毒感染了超过 100 万用户，一旦下载安装后，会在用户手机通知栏弹出广告，并可能在后台私自下载推广软件。感染软件的款数达到了 1800 款，其中包括斗地主、三国杀、连连看、疯狂摩托、当空接龙等热门游戏。而截至目前，Android

应用开发者的主流盈利模式依然是“免费的 APP+植入广告”，迫于盈利需求，恶意推广类木马在 2013 年将会进一步大幅增长。

8.3 安全趋势之三：资深黑客“拜金主义”倾向将更加强烈

2012 年，大批制毒者从 Symbian 系统平台转移到 Android 平台掘金。也进一步推动资费消耗、网银窃取、恶意扣费类病毒大幅上涨。

腾讯移动安全实验室监测分析预测：2013 年跟金钱相关如短信吸费、手机支付、手机电商等病毒仍将是主流；2012 年下半年以来，网银窃取类病毒呈现爆发式增长趋势，短信巫毒（又称“短信僵尸”）感染上百万用户。同时，许多“山寨网银”不时现身，让许多手机用户饱受账户资金被窃之害；截至到 2012 年 12 月，新宙斯木马病毒又给银行客户造成 470 万美元的损失。腾讯手机管家首家查杀新宙斯木马病毒之后，发现该病毒可通过拦截银行确认短信、绕开银行双因子验证悄无声息地盗走账户余额。

2012 年 12 月末僵尸网络病毒大规模爆发，该病毒会联网到云端获取大量的手机号码和短信内容并偷偷转发，在用户不知道的情况下发送上千条欺骗短信，消耗手机大量资费，形成一个覆盖广阔的欺诈网络，制毒者以此攫取黑色产业链灰色收入。

随着移动支付在 2013 年进一步发展普及，预测病毒制作者或制毒机构将进一步投放更多资源放入 Android 平台，制度者或制毒机构针对读取用户银行卡、信用卡以及账单支付信息的病毒研发投入会加大，将“黑手“直接伸进用户的钱袋已成为黑客最为青睐的非法盈利途径。移动支付涉及到产业链的各个环节，包括银行、银联、手机厂商、运营商、手机安全厂商等多种主体，因次，要最大化破除安全瓶颈，2013 年整个移动支付安全领域所涉及的环节，需要全方位打通壁垒进行全产业链的合作。

8.4 安全趋势之四：隐私窃取类病毒危害进一步扩大

隐私窃取类病毒发展迅速，窃取用户网银和照片、通讯录成为重要的病毒特征引发各方的关注。比如在今年 9 月大规模爆发的病毒“隐私蛔虫”短短 5 天就感染 20 万用户，该

病毒可以通过获取 GPS 地理位置、偷偷录音、上传用户通话记录、手机录音、视频和照片等强隐私信息，成为大面积的个人、商业等机密隐私泄露的重要威胁。

2012 年中秋，腾讯手机管家首家截获了两款命名为“2012，你幸福了吗？”以及“新白发之恶搞你幸福吗？”的视频软件，植入恶意代码，窃取用户手机号码与 IMEI 号等隐私。由于两款恶意软件的共同特征是借助热门话题传播，众多手机用户遭到袭击。

2012 年，腾讯手机管家截获一款 a.spread.rootsmart.[隐私谍影]病毒，预计整个市场感染用户数已超过 63 万，为 2012 年感染用户最多的隐私窃取类病毒，该病毒在启动后申请授予 root 权限，并在后台私自下载并静默安装其它恶意应用，同时会收集短信、通话记录等隐私信息。而今年，整个 Android 市场预测已感染用户上百万的短信巫毒（又称短信僵尸）甚至可以窃取用户网银账号，个人财产安全岌岌可危。

2012 年，隐私窃取类病毒可以将用户照片、账号关键隐私全方位掌控，而用户一旦遭受这类病毒的攻击，往往毫不知情， 2012 年，腾讯移动安全实验室检测出了十大典型与高危隐私窃取类病毒，目前感染用户总数达到了 169 万。由下图所示，2012 年十大隐私窃取类病毒，平均单个病毒感染人数接近 17 万，从 IMEI、IMSI 号到手机通讯录、短信、地理位置，全方位窃取用户隐私，预测在 2013 年，随着隐私信息的价值彰显，隐私窃取类病毒将进一步疯狂席卷手机。

2012年十大隐私窃取病毒		
病毒名称	感染人数	病毒特征
a.privacy.counterclank	566650	该病毒启动后在用户未授权的情况下，在桌面创建快捷方式，并且上传用户浏览器书签，同时收集手机固件信息，给用户隐私造成安全威胁。
a.privacy.fakeNetworkSupport	353948	该病毒伪装成Android系统网络组件骗取用户安装，安装后无图标，启动后会私自读取、删除、拦截手机短信信息，并私自下载软件等，给用户的手机安全造成较大的威胁。
a.privacy.jwtime	321392	该病毒伪装成系统软件，安装后无图标显示，强制开机启动并在后台收集用户短信等私人信息上传到远程服务器，给用户的隐私安全带来严重威胁。
a.privacy.strategy	122372	该病毒激活便会驻后台收集联系人、短信、通话记录等用户信息并上传，还会尝试破解系统获取root权限，静默安装其它恶意程序或者卸载指定的安全杀毒类软件。
a.privacy.devicestatservice.[盗密诡计]	100874	该病毒被安装激活后，可能会获取您手机的通话记录、短信等个人隐私信息，可能给您的手机造成一定的威胁。
a.privacy.stat	78360	该病毒安装后无图标，会读取手机的短信信息、手机号码IMEI、IMSI等敏感内容，可能会给您的手机隐私造成一定威胁。
a.privacy.fakePowerAlarm	60680	该病毒安装后会拦截用户短信信息，并私自发送短信，可能会给您的手机安全造成一定的威胁。
a.privacy.enginewings	44084	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。
a.privacy.syservice.[系统服务]	23312	该病毒以“系统服务”为名诱导用户下载，安装后无图标显示，运行时病毒会在后台开启多个程序，并记录手机GPS位置信息，通话记录，短信，电话本，通话录音等信息，同时将这些信息保存后上传到服务器，严重泄漏用户隐私。
a.privacy.ju6.[伪谷哥升级]	19620	该病毒安装后没有启动图标，一旦激活便后台自动下载安装其他应用还可能卸载手机应用，不但消耗用户流量，给用户带来一定的经济损失，还可能给用户带来进一步的安全隐患；同时，该病毒还会上传用户数据，跟踪用户位置，造成用户隐私泄露。
数据来源：腾讯移动安全实验室		

第九章　2013 年国内手机安全市场趋势分析

2012 年手机安全市场经历了颠覆性的增长与变化，中国手机安全市场累计用户数累计已

接近 3 亿，在 2013 年，移动安全市场的生态与格局又将发生哪些改变？

1.手机用户安全意识逐步觉醒

随着低价智能机进一步冲击市场与互联网企业大军涌入 Android 系统平台，Android 智能机用户水涨船高，发展迅速。该平台手机用户面临全开放环境和潜在安全风险的现实，Android 终端的手机安全市场份额也随之而提升，Android 智能机市场份额进一步扩展之余，水货手机与山寨应用泛滥使得手机安全风险日益扩大，感染手机病毒与下载到恶意软件的用户也越来越多。另一方面，黑客的病毒投放渠道、攻击技术、利益联盟与黑色产业链的已逐步完善，更多的手机用户开始饱受手机病毒侵袭，与此同时也催生了用户安全意识的觉醒。当手机用户对安全更加注重，市场优势将偏向于更加注重用户需求与具备产业链全覆盖与整合优势的安全软件，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。

2.移动安全产业链合作成为必然

2012 年，伴随着手机安全威胁的凸显，手机安全行业开始与电子市场、终端市场等各类渠道建立了合作。2012 年，腾讯手机管家与 10 多家安全厂商、超过 20 家电子市场、各大运营商、以及多家手机厂商等携手建立了腾讯移动安全产业链。国内以“腾讯移动安全生态系统”建立为代表的手机安全产业链逐步形成并进一步完善，在协助整个移动产业链病毒检测查杀方面，成效显著。终端厂商、安全厂商、运营商、下载渠道之间合作建立的移动安全产业链的积极效应也正在进一步彰显。 据腾讯移动安全实验室后台数据显示，为机锋、安智、豌豆夹、应用汇等电子市场、合作的手机资源站、中国电信、中国联通等运营商、中兴、华为、三星、联想、HTC 等手机厂商以及搜索引擎、刷机厂商、安全厂商等在应用上线前检测出的病毒软件包总数就超过 24 万个。2012 年为电子市场等合作伙伴检测独立软件包 625 万个次。为移动产业链伙伴提供了安全保障之余，也有效切断了移动病毒开发者

的病毒感染传播途径。

在二维码渠道方面，腾讯手机管家自 2012 年 7 月为灵动快拍提供二维码安全检测以来，7 月至 12 月共为灵动快拍检测网址达 956 万条以上，恶意网址检出率为 2.1%，拦截恶意网址超过 20.6 万条。

2012 年，安全问题几乎遍及移动互联网每个环节和链条。因此产业融合的变化正在发生，腾讯手机管家目前正以资源优势建立了完整的产业链安全覆盖体系，从移动安全行业的发展特征来看，这预示着移动安全行业正走向产业链整合的大趋势。

3.手机安全行业深耕细分领域

2012 年，各种电子市场山寨软件开始泛滥，对用户安全又构成另一层威胁。在此背景下，腾讯手机管家联合应用宝、海纳应用搜索等对正版软件进行了官方正版认证，并携手 10 余家电子市场建立“腾讯官方正版安全联盟”，随着手机安全行业各种产业链的深入合作，进一步方便了电子市场、手机下载站等渠道对手机病毒进行检测与查杀，并逐步完善了软件认证机制建设。而手机支付开始流行之后，腾讯手机管家、应用宝、海纳应用搜索等腾讯移动应用平台也针对支付类软件包进行了官方认证，确保用户下载官方正版的手机支付类客户端。

随着国内多家手机安全公司对移动互联网安全行业的投入加大，手机安全环境变得复杂，手机安全也逐步向细分领域发展，移动泛安全概念应运而生。2012 年以来，腾讯移动安全实验室在 MTAA 3.0 明确提出“手机健康专家”的定位，建立了“病毒防护、隐私保护、上网保护、保险防范”四大防御体系。以“终端+云端”为核心，结合产业链联盟，针对骚扰拦截、隐私保护、手机加速、手机防盗、病毒查杀、系统硬件管理等各环节为用户提供全面的安全服务解决方案，成为国内移动泛安全理念首次实践的样板。而整个移动安全产业链共同合作护航安全也必然成为 2013 年手机安全发展的大趋势。

十、腾讯移动安全实验室专家建议

移动互联网不断发展，2013 年的手机安全形势将更加严峻，手机用户应该养成良好的手机使用习惯确保个人财产、隐私等利益不受病毒或恶意软件的损害。

1.从正规渠道购买手机。随着 Rom 内置渠道病毒风险增多，对于山寨手机与水货手机中的内置不明软件，应引起足够的谨慎。安装手机安全软件，及时查杀最新流行病毒。

2.从正规电子市场、官方网站下载应用。用户应去知名的具备相关安全检测能力的应用市场下载软件，比如，腾讯手机管家 PC 版、应用宝等，这些应用均经过腾讯手机管家的安全检测，可确保下载安全。与此同时，应用商店、手机论坛等依然是手机病毒传播的主要渠道，对于论坛网盘分享的诱惑性的情色软件应持谨慎态度；论坛下载软件之前，应通过手机安全软件进行有效的在线检测与查杀扫描，如此则可以在一定程度上规避风险。

3.不要见码就刷。二维码的火爆，使得该渠道逐渐得到黑客的青睐，二维码渠道病毒比例还处在持续增长之中。手机用户应安装具备二维码恶意网址拦截的手机安全软件进行防护，并使用带有安全识别的二维码工具，可有效的将刷二维码染毒的风险降到最低。

4.**刷机的火爆，用户也应谨慎进行刷机操作与刷机软件。**刷机的流行，使得病毒制作者盯上了该渠道，手机用户应谨慎选择正规的刷机渠道刷机，以防 ROM 内置感染。

5.对于收到的不明短信链接，不要轻易点击。黑客往往会通过恶意网址的链接，骗取用户点击，跳转到钓鱼网址，套取用户网银账号与密码等信息，直接造成用户的财产等经济利益损失。为避免遭受钓鱼网址等风险，手机用户可以安装腾讯手机管家开启恶意网址检测，避免钓鱼网址的攻击欺诈。

6.注意隐私权限访问请求。2012 年，恶意软件要求过度权限的问题已经被央视曝光，而隐私窃取类病毒渐渐引起广泛关注。各手机用户应多留意各软件的权限，一般来说，许多隐私权限的要求，腾讯手机管家都会弹窗提醒用户注意，若有莫名的敏感隐私权限要求，用

户应及时拒绝，保护手机隐私。

7.安装手机安全软件，定期升级病毒库与全盘查杀手机病毒。

在 Android 平台恶意扣费类手机病毒泛滥加剧，许多恶意扣费类病毒私自在后台发送扣费短信，定制 SP 业务并自动屏蔽运营商确认短信，让用户无声无息被扣费。用户对于话费会无故减少，流量突然增加，收不到 10086 等运营商短信、不停弹出广告等异常现象的时候，应留心是否手机中毒或遭遇恶意程序吸费。应下载如腾讯手机管家一类的手机安全软件开启防御功能，升级最新病毒库并定期给手机进行体检和病毒查杀，以保证对新型流行病毒的查杀，确保手机安全。

腾讯手机管家

安自心 简随行

腾讯出品 值得信赖