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年第三季度

手机安全报告

Mobile Security Report of Third Quarter of 2012

目录

腾讯移动安全实验室 2012 年第三季度手机安全报告

第一章 2012 年第三季度手机安全报告概要

2012 年以来，手机病毒的爆发式持续增长了三个季度，并在第三季度达到一个增长高峰，手机病毒的攻击方式与传播渠道覆盖逐渐趋于稳定与成熟。Android 系统的开放性和免费性，不仅让开发者趋之若鹜，更让第三方手机安全行业获得了更广大的市场基础与用户认同与支持。与此同时，制毒者和制毒机构打包植入病毒渠道来源也变得更加广泛。

在 2012 年第三季度，基于腾讯手机管家产品服务的腾讯移动安全实验室截获的病毒包软件总数为 78176 个，其中，Android 系统截获的病毒包占据了总数的 94%。2012 年第三季度，7、8、9 三个月截获的 Android 病毒软件包分别为 18267、26260、29194 个，Android 病毒包总数达到 73721 个，呈连续递增趋势。Symbian 系统第三季度截获的病毒包总数为：4455 个，递减趋势明显。而 2012 年第三季度截获的 Android 的病毒软件包已经超过了 2012 年上半年截获的 Android 病毒包总数之和。

2012 年第三季度以来，手机病毒可针对网银、支付、汇款等敏感财产信息进行收集窃取等新的特征显露，并有成规模化发展的趋势。另一方面，手机病毒二次打包伪装成热门软件的继续呈现泛滥之势，也因此推动山寨软件蓬勃发展。

随着手机支付逐渐流行，手机病毒伪装成支付类网银客户端等现象开始抬头，不少伪支付类客户端潜藏在各大应用商店盗取用户的网银密码与资费，已造成部分手机用户的经济损失。与此同时，腾讯手机管家等第三方安全软件也采取了相关官方包安全认证等手段进行应对。

由于巨大利益的诱惑，手机病毒黑色产业链进一步强化，这使得 Android 平台安全风险进一步增强。目前，手机安全行业的产品功能进一步持续优化，病毒查杀技术进一步加强，以及产业链布局开始向纵深发展，另一方面，制毒者和制毒机构也相对应的提升了病毒攻击技术与攻击方式，智能手机各种软硬件技术的开发与各种应用的野蛮生长一定程度上催生了手机病毒的滋生和传播渠道扩大，更加大了监控与截杀的难度。如此一来，手机安全行业与制毒机构双方的攻守形式博弈已经进入到战略相持阶段。

第二章 2012 年第三季度各平台病毒类型发展分布

2.1 Android 平台病毒类型分布

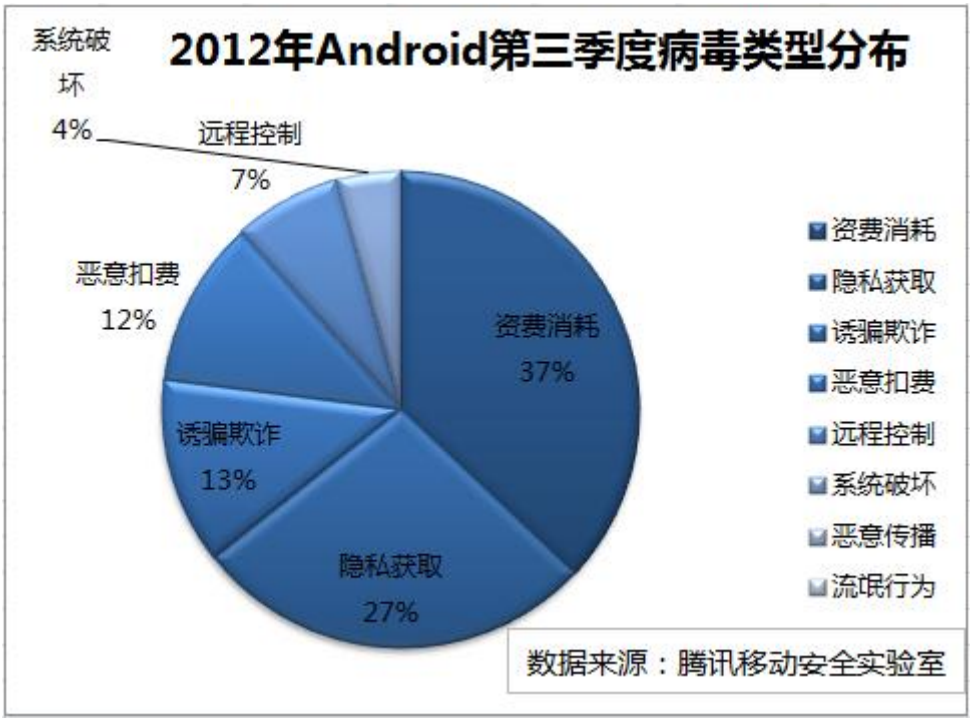
2012 年第三季度以来，Android 系统平台共截获病毒软件包数 73721 个，其中资费消耗类病毒占据 37%的比例，隐私获取占据 27%；诱骗欺诈占 12%；恶意扣费占 12%，远程控制占据 7%，系统破坏占据 4%。

在第三季度中，病毒发展呈现出来的多元化、趋利性特征依旧明显。资费消耗病毒虽然占比第一，但却在三月之中呈现出较大的比重落差。三个月来，隐私获取类病毒发展出更多的新特征，从 GPS 定位信息、手机固件信息到监听、窃听短信甚至伪装成系统软件偷偷录

音收集手机用户图片、音乐、视频等重要私密信息，隐私窃取的过程中消耗大量用户资费，使得资费消耗类病毒与隐私获取类病毒成为“连体婴儿”，一涨俱涨，并呈稳定发展的态势，隐私获取病毒逐步形成了完善的隐私窃取手段、方式与渠道，隐私打包贩卖渠道也进一步形成。手机病毒攻击行为从消耗流量资费转向更直接的窃取网银帐号盗取用户资金。而与此同时，这类病毒也体现出了隐私窃取与诱骗欺诈的的特征。

诱骗欺诈类病毒会通过欺骗的方式诱使用户安装恶意程序或利用手机漏洞远程下载并安装恶意程序，而恶意软件不会合法的告知受影响的手机用户，一切都是在系统后台偷偷完成。

恶意扣费病毒主要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。比如“伪画皮”病毒在 7 月与 9 月两次卷土重来，模拟运营商的扣费端口，大肆扣取用户资费。



2.2 Symbian 平台病毒类型分布

2012 年第三季度，在 Symbian 系统平台上，资费消耗类病毒占据 31%，居于第一位；系统破坏类病毒占据 30%，居于第二位；诱骗欺诈类病毒占比 22%，隐私获取与恶意扣费类病毒分别占据 12%与 5%；Symbian 系统平台总体上表现出一种稳定的格局。这种稳定性在 8 月份表现得尤为明显。

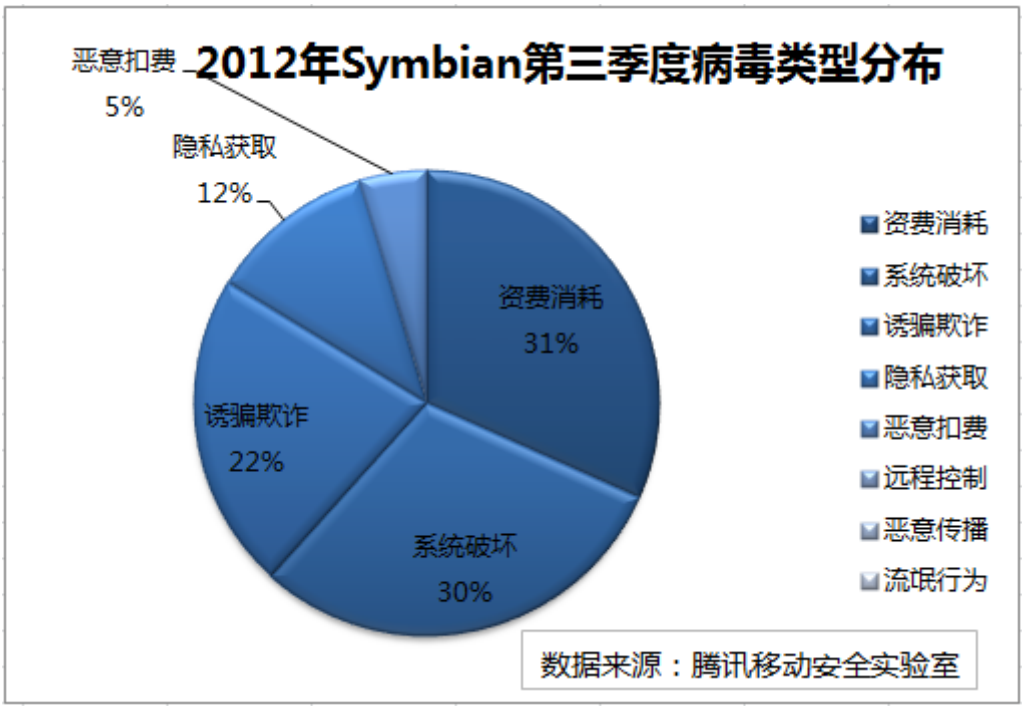
在第三季度中，资费消耗、系统破坏、诱骗欺诈这三种常态传统的病毒类型在 Symbian 系统一直是主要病毒类型。

手机病毒试图破坏手机中的安全杀毒软件成为非常明显的特征；Symbian 制毒者或制毒机构也开始提升其攻击技术，寄望于通过攻击并卸载用户的手机安全软件来深入推广手机病毒之目的。

Symbian 系统平台在第三季度呈现持续衰落趋势，7、8、9 三个月腾讯移动安全实验室拦截的 Symbian 病毒软件包数分别为：1589、1496、1370 个，呈现缓慢递减之势。也因此可以看出，Symbian 制毒者或制毒机构也在不断向 Android 平台转移，并逐步缓慢降低对

Symbian 系统的病毒投放权重，而这一切的推动因素则来源于制毒者或制毒机构的趋利性。

第三季度 Symbian 平台病毒的另一个趋势则与 Android 平台趋向雷同：即隐私保护与恶意扣费类病毒开始呈缓慢上升趋势，隐私窃取类病毒进一步发展，从窃取手机用户地理位置到开始收集用户短信、照片等重要隐私，也因此导致在 Symbian 平台病毒种类从三分天下的稳定特征走向均衡性与多元化的趋势与发展格局。



第三章　2012 年第三季度手机病毒发展特点

1、流行病毒不断发布变种升级

2012 年第三季度以来，手机病毒攻击性与伪装性明显增强，流行的病毒往往呈现多个变种，深度伪装进行传播。8 月份可针对网银、支付、汇款等高度机密信息进行欺诈的“短信巫毒”病毒曾引起广大手机用户的恐慌，感染用户数百万计。同时，该病毒在后期又呈现多个变种，表现为混淆代码、不断变换伪装形式进行传播。7 月份的“伪 MM 画皮”模拟扣费接口疯狂吸金，导致了 10 万手机用户感染。在 9 月份又卷土重来，通过多个变种依靠捆绑在热门正常应用中传播，手机病毒变种增多的背后则是手机病毒的各种吸费、模拟、伪装手段越来越先进。

2、恶意推广类病毒快速捆绑繁殖

比较具有代表性的是腾讯移动安全实验室 2012 年 8 月初截获的牛皮癣系列手机病毒（a.rogue.gamex），该病毒可以让用户手机沦为恶意推广的无底洞。该病毒一旦被安装，便会诱导用户获取 ROOT 权限，私自静默安装多款恶意安装包，让用户手机彻底变成病毒的“天堂”。针对越来越频繁的恶意植入广告与通知栏弹窗广告，手机安全行业针对恶意广告进行全面拦截的呼声也变得越来越强烈。

3、手机病毒捆绑海量应用程序，快速发布快速感染

无论是瞬间感染 70 万用户的“黑暗骑士”、还是短时间感染上百万的“短信巫毒”、以及已经迅速感染 20 万用户的“隐私蛔虫”等热点病毒案例，一个典型特征在于快速发布快

速感染。这一季度以来，制毒者或制毒机构开始通过一个病毒多次打包捆绑海量应用程序，批量复制，快速发布感染海量用户群，并通过时间差或者技术手段绕过电子市场的安全检测，这方面也体现出制毒者或制毒机构的投毒技术进一步提升，逐利性进一步加强。

4、隐私窃取类病毒增长迅猛

第三季度以来，隐私窃取类病毒开始通过收集用户照片、视频、录音、网银密码等各种涉及用户核心利益的强隐私。9 月份腾讯移动安全实验室截获的“隐私蛔虫”病毒是 Android 平台上极其少见的隐私窃取类手机病毒，集多种窃取隐私的手段和信息于一体，强大的隐私信息获取能力让手机用户甚为恐慌。“短信巫毒”更是开始向手机用户的网银、支付等关系用户核心经济利益的隐私动刀，这也是更先进的病毒攻击技术与手段促使隐私窃取类病毒迅猛增长的表现。

第四章　2012年第三季度手机病毒传播分布

手机病毒增长迅猛的背后，另一个变化就是手机病毒传播渠道变得更加多元化和均衡化。制毒者或制毒机构针对资费消耗与隐私获取、恶意扣费类病毒的投放比重逐步加大，这在于制毒机构急于短平快的盈利心理所致，但另一方面，手机病毒投放渠道多元化的趋势表征背后，又透露出制毒机构意图建立更加稳健的盈利模式的倾向。

第三季度以来，手机论坛与电子市场传播比重持平，均占 24%。电子市场与手机论坛虽然依然占据主要的病毒传播渠道，但病毒感染比重开始逐渐削弱。国内知名的应用市场基本与手机安全厂商建立了安全检测合作，但制毒者或制毒机构又迅速找到了突破口，即针对中小型手机厂商内置电子市场进行投毒。由于中小型厂商内置应用市场安全检测率低，感染手机病毒的情况正在加剧。

Android 智能机刷机、应用下载的需求强劲，促使各大手机论坛的软件资源共享变得更加活跃，比如 7 月份泷泽萝拉的走红，相关壁纸类手机病毒在论坛的泛滥程度加剧；奥运期间，手机病毒也捆绑奥运等热门软件大肆在手机论坛攻城略地，8 月网银窃取类病毒短信巫毒（又称“短信僵尸”）、9 月份的隐私蛔虫等病毒也曾通过手机论坛大肆传播。这一季度以来，手机病毒家族也在成群增长，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一大特点。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。第三季度，软件捆绑渠道的手机用户中毒现象占据了 16%的高比例，上升为主流传播方式的趋势非常明显。随着刷机需求的增长，ROM 制作者可以通过内置大量应用并对 UI 进行定制来满足用户的差异化需求，但在利益驱使下，往往也在集成过程中存在预装病毒软件的情况。如此一来，使得 ROM 刷机包的隐患进一步增大。

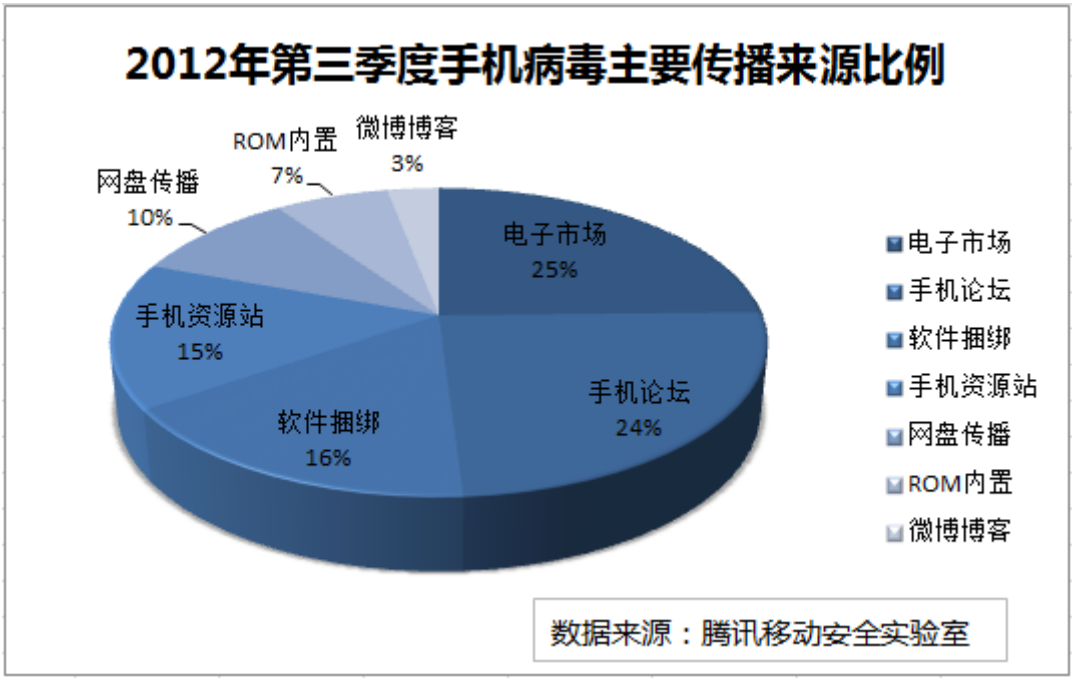
这个黑色产业链由于利益关系的捆绑，使病毒植入更显得肆无忌惮，也加大了手机安全市场对其监控的难度。

尽管如此，手机安全市场针对各个渠道的监控与布局也正在加强，加大了针对电子市场、刷机市场等渠道的检测与查杀力度，也有效地阻止了手机病毒进一步肆意泛滥的势头。

2012 年第三季度各渠道来源占比：

1. 电子市场：病毒企图绕开电子市场的安全检测系统在审核上线之前被截获、又或者是通过一些没有接入安全检测的电子市场进行传播，占 25%；
2. 手机论坛：通过上传论坛附件或提供下载网络硬盘下载地址方式，占 24%；
3. 软件捆绑：通过录入或开设手机下载 WEB/WAP 资源站点，提供直接的软件下载地址，占 16%；

4. 手机资源站：热门软件尤其是游戏软件经常包含病毒或者远程下载，占 15%；
5. 网盘传播：通过网盘捆绑手机论坛提供下载链接，占 10%的比例。
6. ROM 系统内置：rom 制作者因为利益的驱动在 ROM 里预装病毒软件，占 7%；
7. 微博、博客与其他互联网任何形式的自助发布渠道和平台，占 3%。



第五章　2012年第三季度手机病毒区域分布

在 Android 与 Symbian 系统，广东省中毒手机用户再度双双排名第一。其中，在 Android 平台，中毒手机用户排名前十的省份或直辖市是：广东、江苏、浙江、北京、辽宁、福建、四川、山东、湖北、河南。从前十名手机中毒省份来看，病毒泛滥的区域也是经济水平发展较快较高的地区，广东省作为经济大省，手机中毒用户占比达到 15%，第二季度排名也是第一，广东省已经连续两个季度中毒手机占比位居全国第一。

2012年第三季度手机病毒主要分布区域			
Android手机中毒区域分布		Symbian手机中毒区域分布	
区域	中毒手机占比	区域	中毒手机占比
广东省	15.0%	广东省	11.7%
江苏省	8.1%	北京市	6.6%
浙江省	7.0%	辽宁省	6.2%
北京市	6.3%	江苏省	5.9%
辽宁省	5.6%	浙江省	5.8%
福建省	4.8%	四川省	5.8%
四川省	4.6%	福建省	5.2%
山东省	3.8%	重庆市	4.6%
湖北省	3.7%	山东省	4.5%
河南省	3.7%	河南省	4.2%
湖南省	3.1%	湖北省	3.4%
上海市	3.1%	广西	3.1%
河北省	3.0%	山西省	3.0%
广西	2.9%	湖南省	2.9%
陕西省	2.7%	云南省	2.6%
数据来源：腾讯移动安全实验室			

沿海发达省份与直辖市成为制毒者或制毒机构的主攻方向，随着辽宁、四川、山东、湖北等经济发达地区辐射城市与中西部快速崛起省份智能机用户的迅猛增长，制毒者或制毒机构迅速布局各种应用下载渠道与手机病毒植入入口。在广东、北京、江苏、浙江等经济发达地区，随着这些地区应用开发者、应用商店、手机水货厂商等发展迅速，Android 刷机用户也日益庞大，制毒者与制毒机构可以有更多的渠道来传播病毒，随着制毒者团队的日益庞大与快速攫取利益的需求，集开发、分成、推广、扣费等病毒传播黑色产业链与利益分配机制也在这些地区集中。

第三季度，各类型手机病毒也针对区域特征集中爆发或感染，北京、江苏、浙江与广东等省份或直辖市，经济发达，资费消耗、恶意扣费类病毒占据主流；而在辽宁、四川、湖北、福建等经济发展地区，隐私窃取、诱骗欺诈类病毒迅速增长。

在新兴智能机用户增长区：辽宁、福建、四川、山东等地，处于换机大潮的核心区域，这些地区从 Symbian 转化到 Android 系统的新兴智能机用户增长较快，新兴用户缺乏手机病毒防御措施，手机中毒的几率较高。加之手机病毒监管机制的薄弱，制毒者或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，这些地区的病毒投放渠道与机制也开始逐步稳定与完善。

在 Symbian 平台，手机中毒用户排名前六的省份分别是：广东、北京、辽宁、江苏、浙江、四川。广东占比 11.7%，排名第一，也依然占据最大的手机中毒比例。另一方面，广东省是华南地区最大的电子产品集散中心区域，也是 Android、iOS 智能机用户大省，Symbian 用户换机潮在这里尤为突出，广东省的 Symbian 用户向 Android 系统用户转化正在进一步加

速。因此，相对 Android 平台，Symbian 系统广东省手机中毒比例偏少，并呈现缓慢下降的趋势。

在 Symbian 系统，北京与辽宁的手机中毒比例之和超过了广东。在这些地区，Symbian、Android 手机用户均大规模存在，同时，这些地区 Symbian 忠实用户却更加稳定，比重也较大，加之忠实用户群体手机安全意识相对淡薄，这促使这些区域的 Symbian 用户手机中毒比例占据着较大的用户比重。

第六章　手机病毒及安全行业发展预测

毋庸置疑，智能手机发展迎来了全新的发展局面，Android 系统以压倒性的优势超越 iOS 系统占领主要市场份额之后，其发展未见颓势。另一方面，手机病毒依赖其越来越先进的攻击手段与技术大肆从 Android 用户手机中攫取经济利益。Symbian 的颓势与稳定性依旧，但尽管如此，制毒者与制毒机构依然投入一定的资源将此平台作为稳定的攫取利润的渠道。

1、病毒安全产业链不断发展壮大

在目前的手机安全行业，包括电子市场、论坛、下载网站等，为用户提供安全认证、云查杀等合作的越来越多。具有代表性是腾讯在今年来建立的“腾讯移动安全生态系统”、“腾讯官方正版安全联盟”等各种产业链的深入合作，进一步推动了应用市场、移动网站、下载网站渠道对手机病毒进行甄别与查杀的便利，并逐步完善了软件认证机制建设。

2、隐私窃取类病毒将会大规模爆发

2012 年 9 月，腾讯移动安全实验室截获的隐私蛔虫（a.privacy.laucass）手机病毒，预示着隐私窃取类病毒发展到达一个新的高峰，此类病毒可以收集手机上的所有图片、音乐、视频等强隐私内容，在短短 5 天内感染了 20 万用户。另一面，手机用户的安全意识并没有跟上手机安全的严峻局势，致使围绕隐私利益点的转卖获利产业链的发展步伐并没有受到太多来自用户方的阻力，与此同时，制毒者与制毒机构通过收集手机用户照片、视频、短信等更私密的信息来倒卖牟取暴利变得更加容易，而病毒者或者制毒机构的趋利性是重要推手。

3、手机病毒层出不穷变化多端

随着制毒者和制毒机构的病毒攻击手段与方式不断进步，病毒的伪装性与攻击性越来越强。而热门病毒呈现多个变种是第三季度的一个重要特征，隐私信息窃取类病毒发展至能够集多种窃取隐私的手段和信息于一体、恶意扣费类病毒能够模拟点击扣费接口能自主完成一系列的验证以及扣费操作、资费消耗类病毒则可以捆绑热门软件二次打包快速感染海量手机用户。当病毒伪装性加强，传播速度更快，传播覆盖渠道更广，手机病毒的变化性与多元性特征已越来越明显。

4、用户开始逐步重视手机终端安全

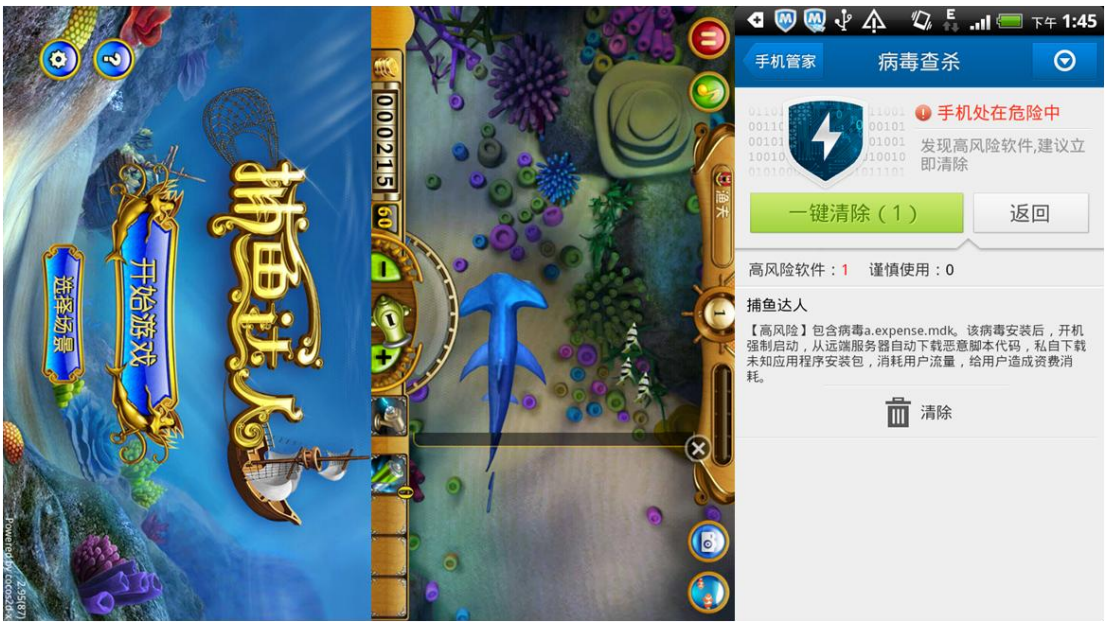
2012 年第三季度以来，盗取用户网银密码以及账单支付信息“短信巫毒“感染上百万用户，引起广泛的关注。随着手机病毒黑色产业链进一步建立，手机病毒攻击方式与技术更加多样化，智能机用户遭遇病毒感染也逐渐增多，促使手机用户的安全意识也进一步提升。而随着更多的智能机新手进入到 Android 系统，各种软件下载渠道覆盖变得更加广阔，手机用户则需要进一步培育良好的软件下载习惯。

第七章　2012 年第三季度主要病毒列表

7.1 Android 主要病毒列表

a.expense.mdk

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，给用户造成资费消耗。



a.privacy.laucass.[隐私蛔虫]

该病毒伪装成系统软件骗取用户安装，启动后可能会发送短信、彩信,获取 GPS 地理位置、偷偷录音、并收集手机上的所有图片、音乐、视频等内容信息，可能会给您的手机安全造成一定的威胁。

a.rogue.smszombie.[短信巫毒]

该病毒诱导用户安装恶意子包，不断重复弹出安装页面，具有监控用户收件箱、插入恶意短信、私自发送和拦截短信的行为，同时诱导用户激活设备管理器，使用户无法正常卸载。

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.expense.forge.d

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.privacy.mailx.a.[古哥]

该病毒安装后无启动图标，并在后台自动启动程序，读取用户短信信息、通话记录和 QQ 聊天记录等信息，通过邮件的形式发送到指定邮箱，严重泄露用户的隐私信息。

a.expense.cc

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一定的威胁。

a.rogue.updater

该病毒安装后无图标，强制开机启动，后台私自联网下载，恶意推广软件子安装包，协助其它病毒静默安装未知软件，存在流氓行为。

a.expense.jxkj

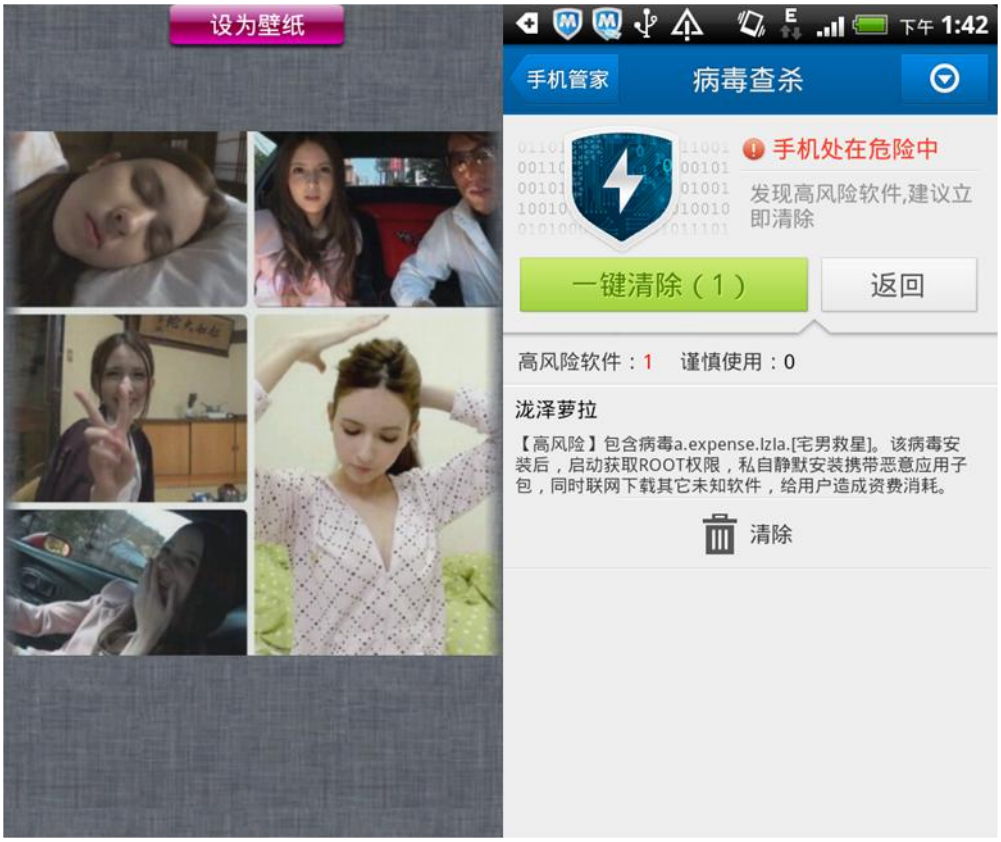
该病毒安装后无图标，开机自启动，在后台自动下载程序并静默安装，给用户的手机安全造成了一定的威胁。

a.expense.emuint

该病毒安装后，开机强制启动，获取 ROOT 权限，未经用户允许私自联网下载未知软件并安装，消耗用户流量，给用户造成资费消耗。

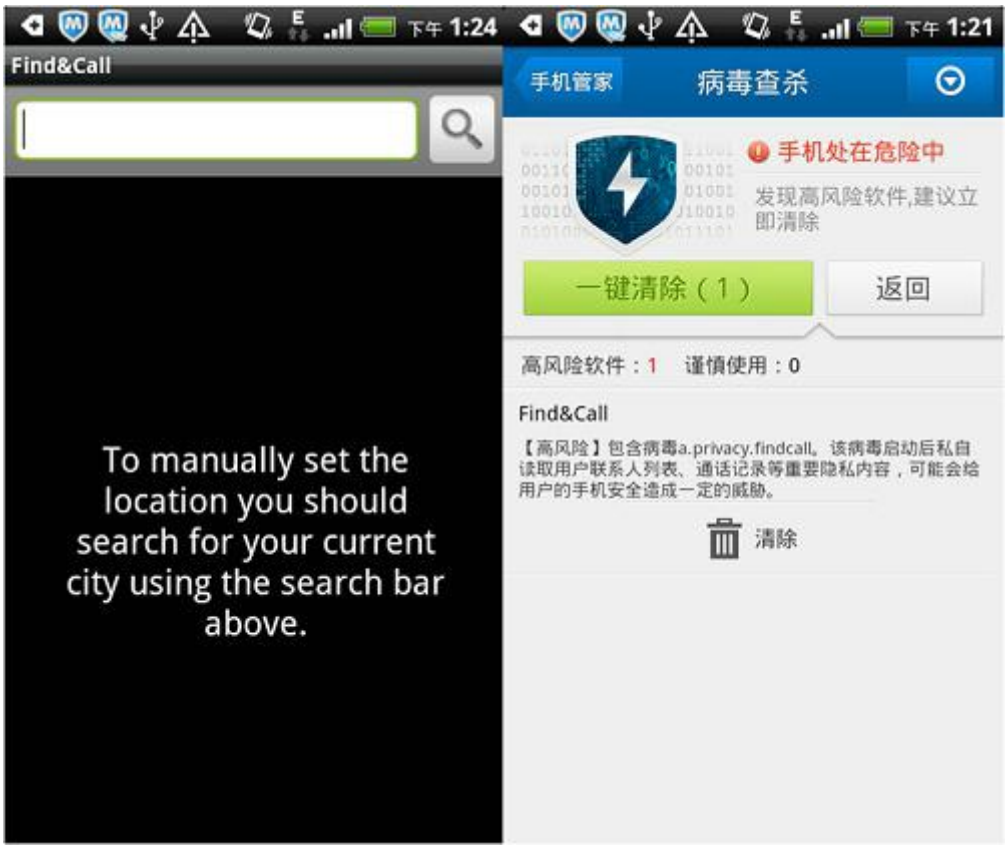
a.expense.lzla.[宅男救星]

该病毒安装后，启动获取 ROOT 权限，私自静默安装携带恶意应用子包，同时联网下载其它未知软件，给用户造成资费消耗。



a.privacy.findcall

该病毒启动后私自读取用户联系人列表、通话记录等重要隐私内容，可能会给用户的手机安全造成一定的威胁。



a.expense.za

该病毒安装后无图标，在后台私自下载软件消耗用户流量，并骗取用户安装，还可能给你的手机安全造成其他威胁。

a.payment.fakekoogame.a

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.fakeinstall.d

该病毒激活后向多个号码发送短信，并会诱导用户下载安装其他恶意软件，给用户带来一定的经济损失和手机安全隐患。

a.expense.megall

该病毒安装后，后台启动服务无提示静默下载推广软件，消耗用户流量，给用户造成资费消耗。

7.2 Symbian 主要病毒列表

s.expense.mwcqsvr

该病毒自激活后常驻后台私自联网，并静默安装一款无法手动卸载的恶意插件，无法完全关闭，占用系统资源，可能影响手机和其他软件的正常使用。

s.expense.kecerysig

该病毒伪装成系统程序驻留于手机中，自激活后私自联网下载恶意插件；无法手动删除，试图破坏手机中的安全杀毒软件，可能威胁到用户手机安全。

s.expense.ssru.a

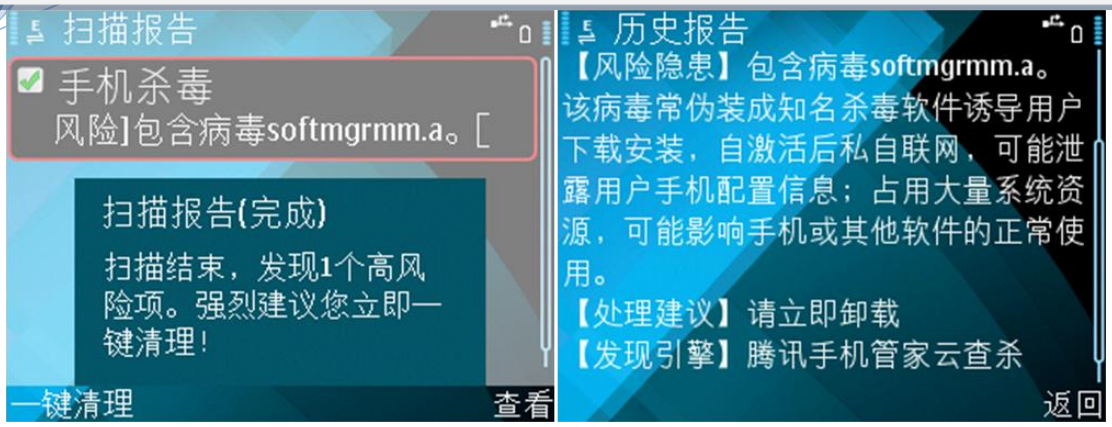
该病毒伪装成影音播放类软件诱导用户下载安装,无提示私自联网；私自修改主页，占用系统资源；破坏手机中的安全杀毒类软件，可能威胁到用户手机安全。

s.expense.advancegate

该病毒无图标生成，自激活后常驻后台私自联网下载其他恶意插件；占用大量系统资源，可能影响手机和其他软件的正常使用。

s.privacy.softmgrmm.a

该病毒常伪装成知名杀毒软件诱导用户下载安装，自激活后私自联网，可能泄露用户手机配置信息；占用大量系统资源，可能影响手机或其他软件的正常使用。



s.payment.apibridges

该病毒安装后无图标生成，私自联网，无法手动删除，占用系统资源；无提示私自发送短信，可能订购 SP 收费业务，给用户带来经济损失。

s.privacy.winsserver

该病毒安装后无任何图标生成，自激活后常驻后台私自联网,获取手机配置相关信息；占用大量系统资源，可能影响手机和其他软件的正常使用。

第八章 2012 年十大高危病毒

目前，腾讯移动安全实验室通过后台监测，筛选出了“2012 年十大高危病毒”，希望手机用户引起高度警惕。如下所示，其中，a.expense.apkquq 病毒排名第一，排名第二与第三的手机病毒名称分别为：a.expense.mdk 与 a.remote.i22hk。

从 2012 年十大高危病毒的病毒描述特征可以知道，感染人数最多、排名前三的高危病毒是以资费消耗与隐私窃取类病毒为主。可以看出，制毒者发布的高危病毒都是倾向于攫取用户资费或者紧盯手机用户的强隐私，病毒的逐利性进一步彰显。总体上看，2012 年 10 大高危病毒类型构成则是以资费消耗、隐私窃取、恶意扣费、恶意广告推广类病毒为主。恶意扣费类病毒已成为制毒者或制毒机构常规的逐利手段。而恶意广告推广、隐私获取类病毒发展势头强劲，成为手机用户经济利益的重要潜在威胁。

目前，腾讯手机管家对下图所列的“2012 年十大高危病毒”已经全面支持查杀，与此同时，对其病毒变种正在进一步监测之中。

2012年Android手机十大高危病毒	
病毒列表	病毒描述
a.expense.apkquq	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，可能给用户带来一定的影响。
a.expense.mdk	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，给用户造成资费消耗。
a.remote.i22hk	该病毒安装后，自动上传IMEI、IMSI等信息,并获取云端指令控制用户手机，同时会修改浏览器书签以及联网下载未知程序。
a.expense.cc	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一定的威胁。
a.expense.forge.c	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.payment.lemei	该病毒启动后会私自发送扣费短信，定制PS业务，可能会给用户的手机安全带来一定的威胁。
a.system.deviceadmin	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。
a.propagation.rootsmart	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.forge.b	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.system.droiddream	该病毒安装后会获取手机root权限，并在后台静默安装内嵌子包，同时搜集手机上的IMEI、IMSI、SDK等信息，发送到指定服务器并在后台下载一些其他恶意安装包，给用户的隐私带来严重安全威胁。

第九章　规避手机病毒的方法

随着手机应用的激增，手机病毒捆绑正常应用进行传播已经常态化，用户最好不从来历不明的渠道购买手机，尤其是山寨机和水货手机。这些手机是目前滋养吸费陷阱的大温床，具备先期植入各类病毒、木马、流氓软件的可能与条件。

目前在 Android 平台，广告推广类手机病毒泛滥加剧，许多开发者也通过“病毒式”传播的方式推广手机应用，将恶意代码内置到热门软件中，提供用户下载，病毒制作者与制作机构也依靠这种手段赚取利润，用户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。

目前二维码中毒情况也开始逐步增长，手机用户对于一些网站上来路不明的二维码应该引起警惕，应该选择那些具备恶意网址拦截的手机安全软件进行查杀与拦截。

山寨软件变得普遍之后，用户应该选择知名的电子市场下载软件，杜绝山寨软件进入手机，以免对手机安全构成威胁。目前腾讯手机管家游戏软件中心、PC 版等应用市场均对正版软件进行了官方正版认证，而手机支付开始流行之后，腾讯手机管家 PC 版、应用宝、海纳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，确保下载官方正版的手机银行客户端。

对于安全性较低同时软件下载量较大的手机论坛，用户应选择安装口碑相对较好、评价较高的手机应用软件，及时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。

2012 年 9 月份以来，伪装类病毒与隐私窃取类病毒进一步多元化，基于此，手机用户应留意安装软件的权限，比如用户通过腾讯手机管家等相关安全软件的功能操作禁止某些软件的联网与访问隐私的权限。

用户应该定期升级手机安全软件的最新病毒库并开启全盘扫描，定期给手机进行体检和病毒查杀、及时更新病毒库，抵御手机病毒侵害自身利益。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。

腾讯手机管家官方网站：http://msm.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/qqmanager
腾讯移动安全实验室官方微博：http://t.qq.com/QQSecurityLab

腾讯移动安全实验室
2012 年 10 月 24 日

腾讯手机管家

安全心 简随行

腾讯出品 值得信赖