腾讯移动安全实验室第 2 期报告：伪装病毒爆发式增长

第一章　摘要

中国移动互联网继续高速发展，最明显的特征是手机软件应用也在海量增长，这不但丰富了用户的手机生活，同时也为手机病毒提供了有效的传播工具。

由于热门应用有很强的号召力，传播起来也非常容易，同时用户会放松对这些热门应用的安全性考虑，因此大量手机病毒伪装成热门手机应用进行大规模的传播。与此同时，移动互联网上的流氓软件或病毒，也在面临转型期，由以前的疯狂吸费，开始转型为更隐蔽、更委婉的方式来榨取用户的价值。

目前，手机病毒按照病毒危害行为分类，主要包括诱骗欺诈、资费消耗、系统破坏、恶意扣费、隐私获取、远程监控、恶意传播、流氓行为等 8 个类别，伪装类病毒通常具有“诱骗欺诈”这一类别的危害，但同时又会具有“恶意扣费”、“资费消耗”等的其他危害。

截至到 2011 年 10 月 9 日为止，腾讯移动安全实验室最新的病毒数据分析显示：在 Symbian 平台发高达 13000 多个手机病毒，其中诱骗欺诈类病毒所占比例为 46%，在所有类别中占据第一的位置；在 Android 平台发现高达 6000 多个手机病毒，其中诱骗欺诈类病毒所占比例为 18%，在所有类别中也占据到前三的位置。

Symbian 平台病毒主危害行为类别比例：

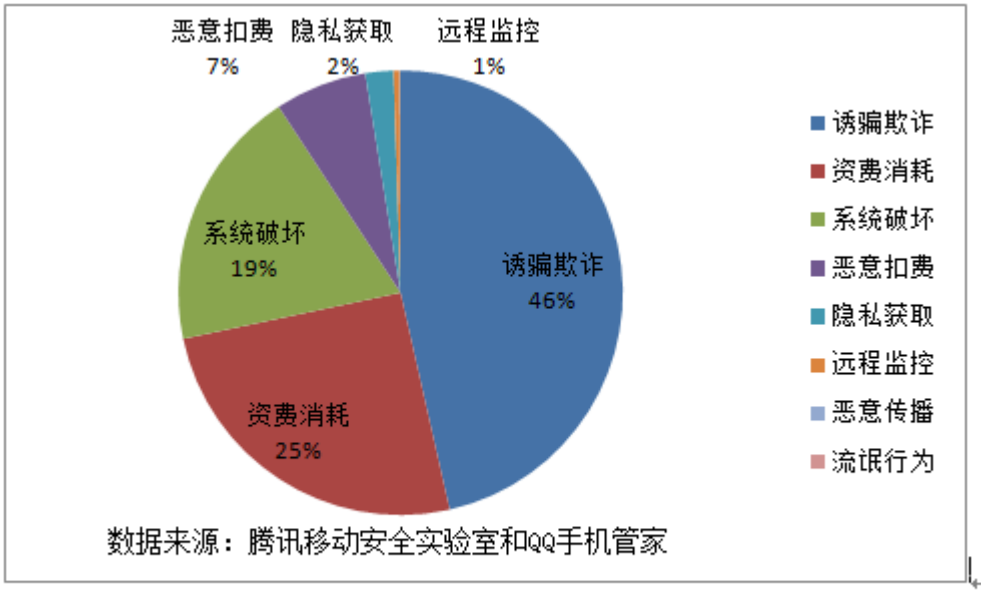


图 1：Symbian 平台诱骗欺诈类病毒所占比例为 46%

Android 平台病毒主危害行为类别比例：

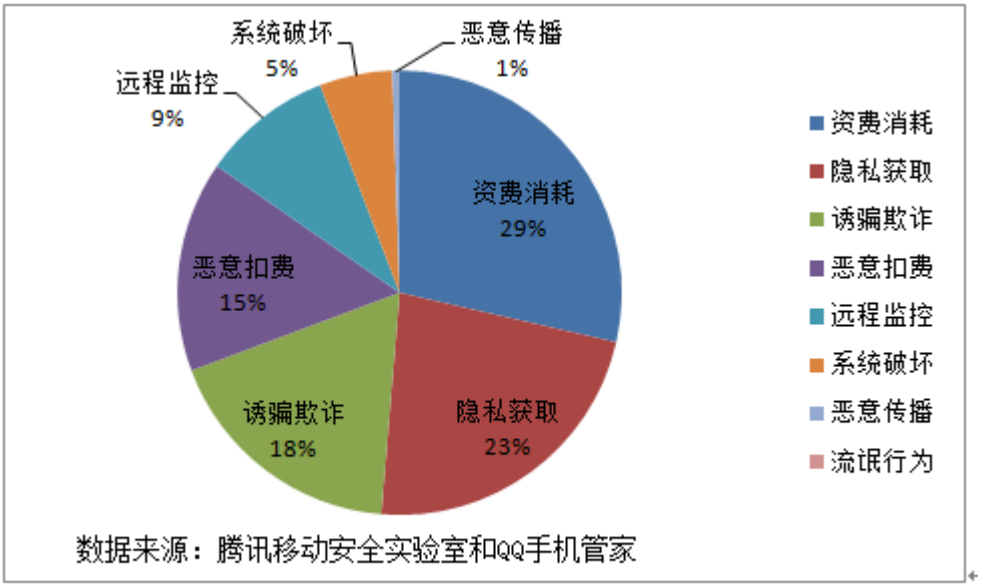


图 2：Android 平台诱骗欺诈类病毒所占比例为 46%

本报告将深入探讨“伪装类病毒”的主要原理、传播方式、危害性、病毒案例，并且还将提供预防和查杀伪装类手机病毒的有效方法。

备注：本报告所有内容均为腾讯移动安全实验室及旗下 QQ 手机管家、在线查毒平台、恶意线索举报平台通过对各类吸费病毒样本和病毒产业链进行细致研究后所得成果，如有引用，请注明出处。

第二章 伪装类病毒主要原理

腾讯移动安全实验室针对大部分的伪装类病毒进行研究发现，其伪装类别可以分为三大类：捆绑应用式伪装类、独立封装式伪装类和篡改应用式伪装类。接下来，我们将依次分析这三大类伪装病毒的工作原理。

1. 捆绑应用式伪装类

该类病毒主要通过在正常软件内嵌病毒程序，变成携毒软件包，包名称、应用名称、图标都体现为正常软件。正常软件在安装过程中静默安装了内嵌病毒程序，从而导致手机中毒，而用户安装主程序时并不知情或无法判断有内嵌病毒。

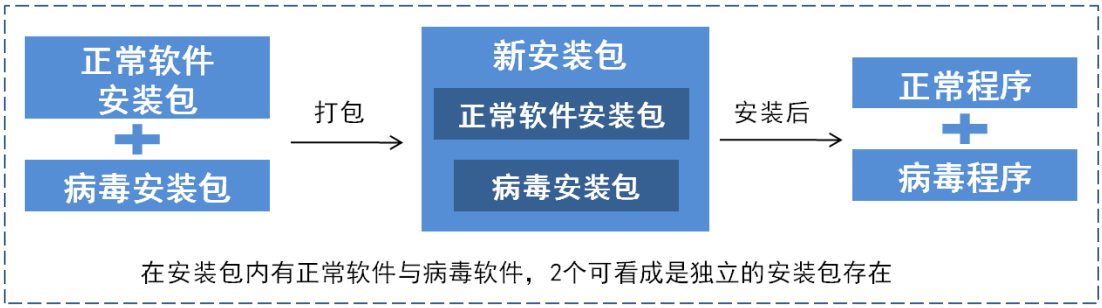


图 3：捆绑应用式伪装类病毒原理示意

2．独立封装式伪装类

该类病毒以独立应用程序出现，通过某种渠道进入手机，导致手机中毒，此类程序模仿系统应用、知名应用、热门软件的包名，软件名称，图标 icon 等达到伪装的目的，但是此应用的签名与其模仿的应用功能和形式往往不一样。

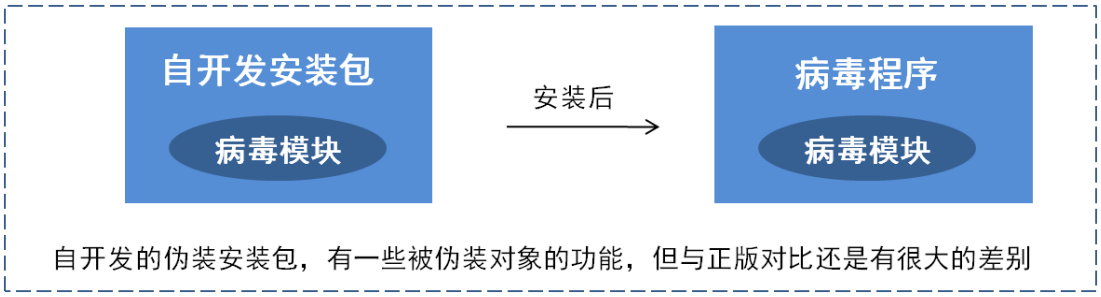


图 4：独立封装式伪装类病毒原理示意

3．篡改应用式伪装类

通过把知名程序拿来反编译，篡改知名程序并进一步植入病毒代码，再签名重新打包，伪装成知名应用进行传播。重新打包的包名称、应用名称、图标都一致，但签名与知名应用不同。

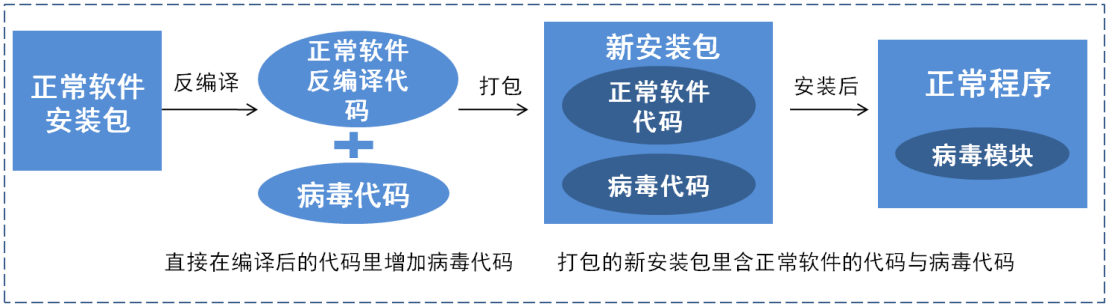


图 5：篡改应用式伪装类病毒原理示意

以上主要是以病毒存在的形式进行分类，腾讯移动安全实验室研究发现从病毒的恶意行为上也会存在伪装欺骗，主要包括以下两种：

A. 病毒程序读取联系人后给所有联系人发信息，信息内容包含汇款账号等等。

B. 病毒程序制造未读短信存到短信收件箱，用户误以为是未读信息，此短信可伪装来信号码，信息可包括中奖，求助等等，进行诈骗。

第三章 伪装类病毒主要传播方式

腾讯移动安全实验室研究发现，目前伪装类病毒一般通过手机群发、手机论坛、电子市场、手机资源下载站、微博、博客文章和其他方式进行传播。除了手机群发之外，基本都采取了较为草根的传播方式，通常也是用户最常用的搜索下载软件的方式，由于这些伪装类病毒普通用户无法直观辨别，因此是用户安全最薄弱环节，务必需要提高警惕。而手机群发相对比较封闭，只有一个连接和简短的介绍语，而且病毒包会设计的非常小，以便用户快速下载。所以有不少群发渠道不会进行病毒与正常软件的捆绑，因为这样无形增加了病毒的体积，而是直接让用户下载病毒本身，所以这种方式的传播对用户的直接威胁也

很大。

1. 手机群发：通过短信附带下载链接，引诱下载的方式；

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；

3. 电子市场：通过一些没有接入安全检测的电子市场进行传播；

4. 手机资源站：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；

5. 微博、博客：通过发博微博附带下载地址链接；

6. ROM 系统自带：ROM 制作者因为利益的驱动在 ROM 里预装病毒软件；

7. 软件捆绑：热门软件尤其是游戏软件经常包含病毒或者远程下载；

8. 其他：互联网任何形式的自助发布渠道和平台。

根据腾讯移动安全实验室后台的统计数据分析，病毒的主要传播途径，手机论坛传播占据了 31%的比例，其次是电子市场 24%，说明通过手机论坛感染病毒的比重非常大，提醒手机用户务必小心。

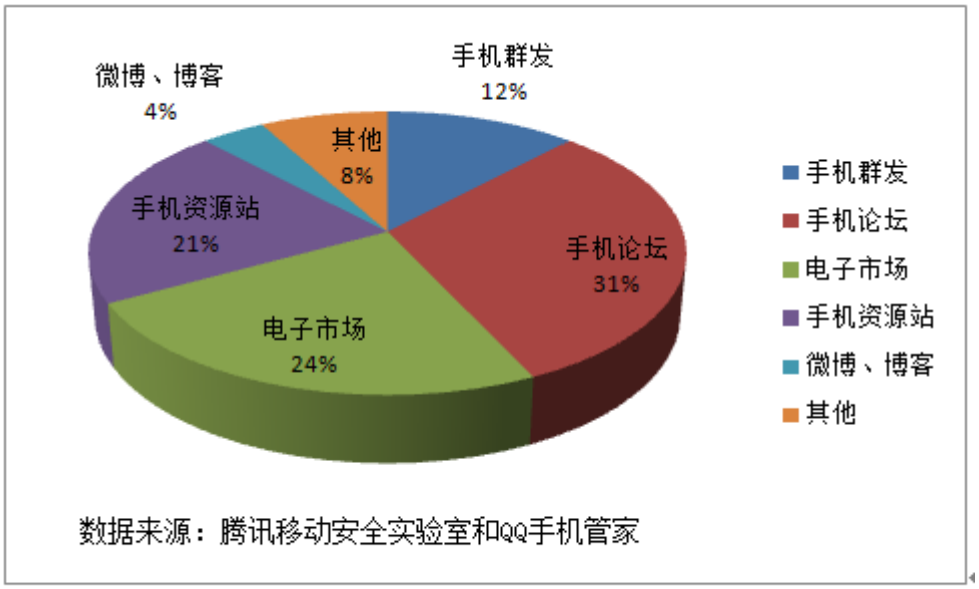


图 6：病毒主要传播方式所占比例

第四章 典型伪装类病毒案例

本章会通过腾讯移动安全实验室截获的多款 Symbian 和 Android 平台伪装类手机病毒案例，让读者能够认识到伪装类手机病毒的伪装方式以及严重危害。

4.1 Symbian 平台伪装类病毒案例

1. “伪杀毒软件”系列病毒

腾讯移动安全实验室率先截获的伪杀毒软件病毒主要包括：伪系统杀毒、伪杀毒中心、伪手机杀毒、伪加速助手、伪安全杀毒中心、伪卡巴杀毒等等，这些病毒的伪装方式大同

小异。接下来，我们举两个例子来说明。

“伪杀毒”系列吸费病毒相比其他手机病毒非常用心的设计 UI，并尽可能模仿知名手机安全软件的 UI 和名称，而且界面做的很美观、逼真，从而起到诱惑用户使用的目的。比如，有一款吸费病毒直接就叫“卡巴杀毒”，并模仿卡巴斯基的 UI，让用户倍感迷惑。

“伪杀毒”吸费病毒不仅模仿知名杀毒软件的 UI、名字，同时还惟妙惟肖的模仿查杀流程，有模有样的对手机各盘符进行扫描，事实上这只是读取手机里的一些文件信息，在形式上对文件进行的“虚假扫描”，给用户制造一种病毒查杀扫描的错觉。

2. “伪完美闹钟”病毒

该病毒的最大特点是伪装成“完美闹钟”工具软件，引诱用户下载安装。该病毒一旦发作，手机便会自动联网静默下载多款病毒软件，大量占用手机内存，肆意破坏手机的安全软件和操作系统，导致手机频繁重启、无法使用，让许多的用户苦不堪言。

3. “伪懒人看书”病毒

该病毒最主要的特点是依附在流行的看书阅读软件“懒人看书”上，并且软件名称也做了进一步的标题优化，比如重新命名为“华丽的万能懒人看书”，制造一种软件应用功能更强大的噱头，诱骗用户下载安装。

4. “伪 OVI 商店”病毒

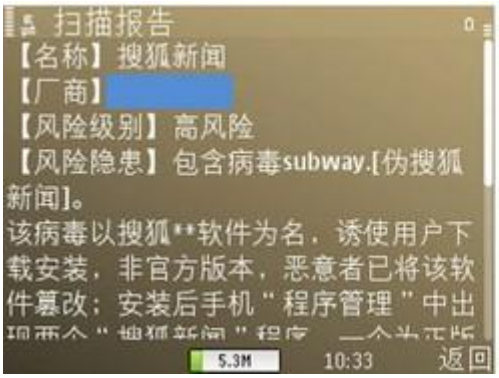
该病毒以知名的诺基亚手机网店客户端“Ovi 商店”为名，诱使用户下载安装，并非官方版本，而是被其他恶意者篡改过的盗版软件。而且病毒前台不生成图标，后台以“Ovi 商店”的程序进程的形式出现，普通用户完全无法判断真假。

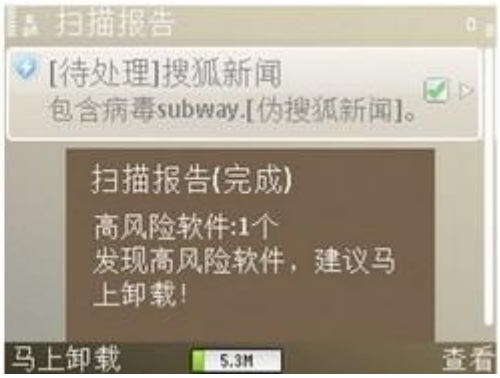
5. “伪谷歌地图”病毒

该病毒以“Google Maps”为名诱使用户下载安装，病毒激活后会无提示自动联网，并下载一款名叫“程序管理”的恶意插件，无提示自动安装。该插件一旦被激活，便会在后台私自定制收费 SP 业务，用户将会收到运营商发送的扣费提醒短信“尊敬的客户，您好!您于**时间点播了北京***公司的冰***传奇 T 业务，资费每次**元 •••”给用户带来严重的经济损失;同时，该恶意插件无法卸载，造成手机或软件无法使用！

6. “伪搜狐新闻”病毒

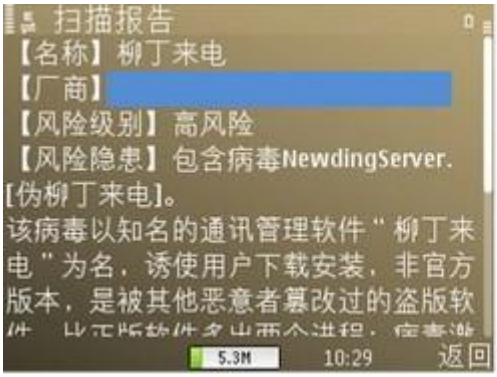
该病毒以搜狐**软件为名，诱使用户下载安装，非官方版本，恶意者已将该软件篡改;安装后手机“程序管理”中出现两个“搜狐新闻”程序，一个为正版搜狐新闻，另一个则为没有正常显示图标的恶意强制联网软件，病毒一旦激活便无提示偷偷联网，在后台进行下载与上传，给用户手机带来更严重的潜在危害;并且本程序无法完全关闭，占用手机系统资源，使手机的运行速度越来越慢!原本是新闻资讯类的软件，却变成了手机流量的持续杀手。

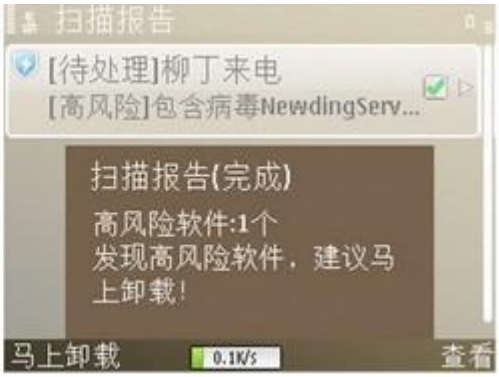




7. “伪柳丁来电”病毒

该病毒以知名的通讯管理软件“柳丁*电”为名，诱使用户下载安装，非官方版本，是被其他恶意者篡改过的盗版软件，比正版软件多出两个进程，进程无法完全退出，占用大量系统资源，影响手机或其他软件的正常运行，同时无提示偷偷联网，在后台进行反复的下载与上传，持续消耗用户数据流量，给用户带来高额的流量费，系统增强软件一下子变成了话费吸血鬼。





4.2 Android 平台伪装类病毒案例

1. “伪 Flash 卧底”病毒

该病毒是一款间谍软件，它以常用软件“Flash”为名，诱导用户下载安装，安装后无软件图标生成。如果病毒一旦被激活，将可能会出现以下高度恶意行为：（1）手机通话录音，并将录音文件上传到指定服务器；（2）私自调用摄像头拍照，上传到指定服务器；（3）窃取行踪，上传地理位置信息；（4）窃取用户隐私信息，如联系人信息等；（5）停止指定进程，卸载指定程序；（6）发送扣费短信并删除确认订购短信。给用户手机使用带极大的破坏和安全隐患！

2. “伪酷 6 视频”病毒

该病毒以“酷 6 视*”名义诱导用户下载安装，每次启动该病毒程序，便自动后台发送“8”到“10661566**”扣费端口，同时删除“10”开头的号码发送的短信，让用户在不知情的情况下造成严重的经济损失。

3. “伪 Google 服务框架”病毒

该病毒主要通过其他恶意软件进行传播。当恶意软件安装后，会弹出所谓“用户许可协议”引导用户点击，用户点击“确定”按钮后病毒会被静默安装到手机上，并进一步深度伪装成系统关键程序，即“Google 服务框架”，高度模拟系统程序的图标，名称描述有细微差别，表面上跟一般的系统关键程序无异，单看表面甚至还有可能骗过专业工程师的眼睛，对于一般的手机用户更可能是完全“隐形”。它属于独立封装式伪装类病毒。

从以上伪装类病毒举例来看，热门安全软件、工具软件、系统进程都是该类病毒常用的伪装形式，通过与热门应用相近甚至相同的图标和名称欺骗用户下载安装，一旦成功安装便会恶意吸费、偷窥隐私、偷偷联网、下载恶意程序等，给用户造成严重的经济损失。

第五章　手机伪装类病毒发展预测

在国内，纵观各大主流智能手机系统，Symbian 平台目前仍是病毒重灾区；iPhone 平台较为封闭，因此病毒相对较少；而 Android 平台占有率不断增长，软件增长迅速，同时 Android 平台的开放性导致漏洞也较多，手机应用市场也比较混乱，给手机病毒产业链带来了更多的机会。

5.1　伪装类病毒将会迎来爆发式的增长阶段

伪装类病毒一直将会是制毒者、制毒机构永恒的“创作”主题，随着手机终端系统的越来越开放，这类病毒将迎来爆发式增长，特别是在 Android 系统平台上，发现的伪装类病毒越来越多，根据后台病毒数据趋势分析，Android 系统将成为伪装类病毒的重大疫区。

5.2 伪装类病毒制毒技术含量参差不齐

伪装类病毒在技术含量上形成高低并存局面，在绝对数量上，各式各样的伪装类病毒还是会占据更大比例。因为传播效果较好，制毒速度非常快，制作的成本比较低廉，制毒可以起到立竿见影的效果，特别受到很多制毒者、制毒结构的青睐。而追求达到更大影响力、更大传播效果的高技术含量的病毒也将持续盛行，形成伪装类病毒技术含量参差不齐的局面。

5.3 SP 业务定制仍然是手机病毒利益驱动者

SP 业务的推广受到的限制越来越多，手机病毒成为了一种非常有效的推广方式，目前许许多多的手机病毒都难以跟 SP 业务定制分开，加上政策在手机病毒方面的监管还不太够，手机病毒变成了最行之有效的传播途径。

5.4 手机应用快速增长让病毒传播更有价值

国内移动互联网行业已经开始迅速发展，大小企业竞争激烈，发布的移动软件应用也越来越多，伪装类病毒有了越来越多的伪装依附载体，同时在整个移动互联网应用软件方面的推广传播需求也越来越大，各类电子市场的活跃、移动应用网盟推广、软件下载广告的利益交错，通过手机病毒带动移动应用传播的价值也越来越大。

5.5 手机病毒产业链日趋完善

虽然手机应用开发者越来越多，但是基本上都以免费的形式提供给用户下载。加之目前移动互联网广告体系不成熟，很多开发者无法通过手机应用获取报酬，因此很可能与制毒者或制度机构之间合作在应用中植入病毒；而大量 SP 在遭遇工信部、运营商的严格二次确认政策下诱骗赚钱的模式无法继续，于是也开始同制毒者合作，提供扣费端口，从而形成了手机病毒产业链。

5.6 云端控制技术加大手机病毒整治难度

之前的手机病毒更多的是病毒本身内嵌指令，而现在更多的是由云端指令控制，如果没有接收到指令，病毒表现得跟正常软件无异,因此隐蔽性极强。可一旦接收到了云端发来的指令就会控制用户手机，实施吸费、偷窥隐私等恶意行为，而这些都是在用户不知不觉地基础上进行的。此外，通过云端控制可以随时更换恶意扣费 SP 端口，从而躲避监管部门审查和封堵。

第六章 专家支招：如何规避伪装类病毒风险

当前，不少用户是通过手机论坛、搜索引擎来获取软件，提醒用户在论坛、博客附带下载的相关软件的时候要格外小心谨慎，不要随意去下载陌生软件，警惕话费异常扣费现象，不要轻易给软件授予更高的权限等等。同时，建议用户一定要在安装软件之前给手机装上专业的手机杀毒软件，比如 QQ 手机管家等，以便进行最有效的进程监控和病毒防御。

目前，QQ 手机管家最新版已经可以实现对各类伪装病毒进行独家精准查杀。用户可以立即在线更新 QQ 手机管家病毒库实现精准查杀，也可以登录 QQ 手机管家官方网站(http://msm.qq.com)下载最新 QQ 手机管家，并立即升级病毒库至最新版。

腾讯移动安全实验室研究发现，伪装类病毒已经潜伏在各大手机论坛、草根电子市场的热门应用中供用户下载。为了能够保证下载安全，建议用户到腾讯应用中心、QQ 手机管家的"软件管理"中下载，这些应用都经过 QQ 手机管家和安全管家双重安全认证，可以

有效保证应用的安全。也可以使用 QQ 电脑管家的手机管理功能，直接在电脑上安装 QQ 手机管家，同时还提供万款手机软件免费安全下载。用户还可关注@腾讯移动安全实验室的腾讯微博，掌握最新的手机安全资讯。