腾讯移动安全实验室 2012 年第一季度手机安全报告

第一章　第一季手机安全报告概要

进入 2012 年以来，我国移动终端出货量呈现井喷式发展，手机安全进一步被重视，移动互联网产业链相对更加成熟，另一方面，手机病毒蔓延之势更加猖獗，仅仅第一季度，从 Android 到 Symbian,1、2、3 月份的病毒均呈现连月大幅递增趋势。目前总的发展趋势是，手机病毒正大规模向 Android 平台迁移，但 symbian 平台用户基数大，利润价值依旧存在，手机病毒将占据 Symbian 平台长期存在并稳定发展，但 Symbian 平台的衰落趋势还是难以阻挡，Symbian 病毒也终将会迎来衰退的一天。

第一季度以来，各类应用程序成爆发式增长，让智能手机的互联网色彩愈加浓厚，与此同时，Android 平台开源性特征让各类应用程序缺乏监管，外加上越来越多的智能手机用户由 Symbian 转向 Android 系统平台，手机病毒对 Android 平台的青睐程度进一步加深，这些因素都在一定程度上促进了 Android 手机病毒的大爆发。据进一步观察，手机病毒却呈现出比 PC 病毒传播方式更加复杂的传播规律与特点，而且病毒的繁殖衍生手段更为先进与隐蔽，比如手机吸费病毒的数量和种类呈现多样化的特征，各类病毒的伪装能力也越来越强，而隐私窃取类病毒等更显示出无孔不入的顽强生命力，并且将成为手机病毒的重要发展趋势。

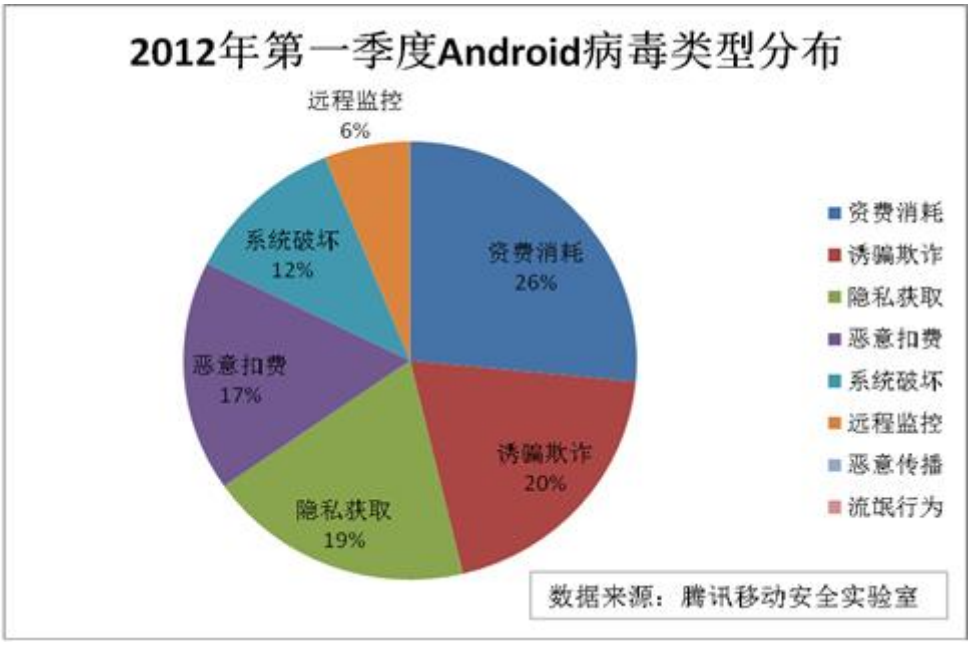
今年第一季度以来，各类恶意吸费、窃取隐私、资费消耗、诱骗欺诈类手机病毒层出不穷且形式多变，受危害的用户数也在激增。根据腾讯移动安全实验室病毒后台数据显示：2012 年第一季度，腾讯移动安全实验室一共截获被植入手机病毒软件包数 11883 个，其中 Symbian 平台截获被植入病毒软件包数 4981 个，Android 平台截获被植入病毒软件包数 6902 个。从数据看出，第一季度的手机病毒软件包数几乎接近 2011 年全年的一半，而 Android 病毒软件包更是超过了 2011 年全年病毒包的 3/4。

第二章 各平台病毒类型发展分布

2.1　2012 年第一季度 Android 平台病毒类型分布

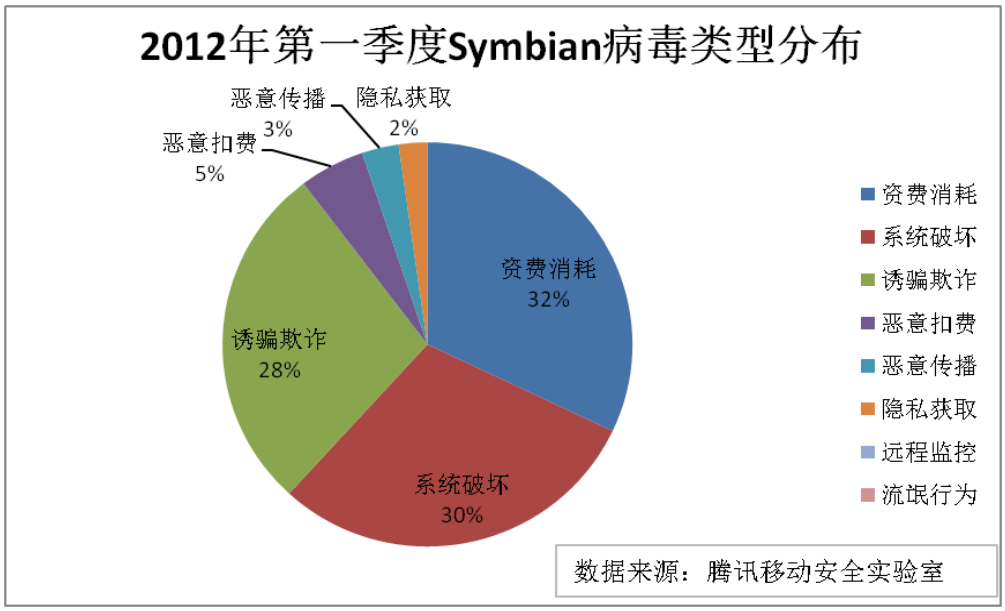
2012 年第一季度，Android 平台截获被植入病毒软件包数 6902 个，其中资费消耗占 26%、诱骗欺诈类占了 20%，隐私获取占 19%、恶意扣费占 17%。系统破坏占 12%，远程监控占 6%。

从 2012 年第一季度 Android 病毒类型分布图看出，病毒类型占据比例更加均衡与多样化，一方面在于 Android 平台的病毒潜入方式更加高明，另一方面在于 Android 平台的价值也开始显露，手机病毒开始与时俱进，伪装手段与吸费模式更加先进。其中资费消耗占据 26%的比例，相对比例最大。因为 Android 开源开放的特征，各类权限也会轻易被手机获取。目前，通过获取 Root 权限私自联网静默安装内嵌的病毒子包或恶意插件消耗用户自费流量开始成为 Android 平台的手机病毒的明显特点。根据手机用户的 GPS 地理位置发送扣费短信的手机病毒有潜在上升趋势。其次，隐私窃取类病毒通过后台窃取手机通讯录、短信等隐私信息也在一定程度上广泛存在。而 Android 平台伪装类病毒发展趋势依旧明显，通过伪装成系统正常软件骗取用户下载安装，消耗资费流量的这些病毒行为已发展成为常态的病毒行为特征。



2.2 2012 年第一季度 Symbian 平台病毒类型分布

2012 年第一季度，Symbian 平台截获被植入病毒软件包数 4981 个，其中资费消耗占 32%、系统破坏占 30%、诱骗欺诈类占了 28%，这三类病毒占据了 Symbian 平台病毒的 90%。其中，资费消耗类病毒呈现总体上升的趋势，而系统破坏与诱骗欺诈类病毒平稳增长。根据分析可知，Symbian 平台病毒稳定增长的发展趋势进一步明显。Symbian 系统平台本身安全性薄弱，加之用户安全意识欠缺，制毒者或制毒机构可以轻易的进行恶意扣费类病毒的投放，这类病毒常表现为通过包中包形式反复潜伏、对热门应用进行捆绑、伪装成热门应用或系统组件，诱导用户下载安装，激活后通过私自联网下载恶意插件或发送短信定制 SP 服务等行为，消耗用户资费。同时，这些病毒无法删除，大量占用手机内存，破坏手机系统和信息安全。Symbian 平台的手机病毒往往表现出诱骗欺诈、系统破坏、资费消耗三位一体的特征，也就是说，一个手机病毒软件包在下载安装后会同时表现出这三种恶意行为。



第三章　2012 年第一季手机病毒发展特点

进入 2012 年第一季度，各类手机病毒凶猛发展的态势超越行业预期。Android 平台病毒多样化趋势明显，一路高歌猛进，增势明显。Symbian 系统的手机病毒数量也在平稳增长，移动互联网发展速度惊人，第一季度的手机病毒也呈现出多样化的特征。根据病毒的细分特点，2012 年第一季度手机病毒可以分为四个发展特点。

1、广告推广类病毒增长迅速，影响扩大

2012 年刚刚进入一月份，伪壁纸手机病毒类病毒以广告推广其他软件的特征开始浮出水面。 影响 500 万人的“Android.Counterclank”病毒的大规模爆发预示着诱骗欺诈类病毒传播的加速，“图标密雷”病毒越演越烈将软件推广类病毒推向传播高潮，通过捆绑正常软件，消耗资费、推广应用与广告，以推广软件为目的手机病毒已形成产业链，显示了伪装类病毒顽强的生命力。显而易见的是，以广告推广为主要形式的诱骗欺诈类病毒将会在 2012 年全年继续裹挟用户，持续榨取用户隐形价值，呈现大幅增长的趋势，并影响到越来越庞大的手机用户

2、隐私获取类病毒规模见长，呈现多样化趋势

2012 年 2 月中旬，“Root 狙击手”病毒的大规模席卷，隐私窃取类病再次步入大众视野；各类监听类手机病毒也开始通过伪装正常软件小规模出现；通过定位用户位置、访问用户敏感信息内容的隐私窃取类病毒进一步频繁亮相，并呈现出形式多样化发展的特征。隐私获取类病毒将会是制毒机构未来利润来源的重要方向，并且已经非常直接地危害到用户的隐私安全，此外各种常规应用软件与用户手机的隐私信息零距离接触，加剧了隐私泄露的风险，隐私保护问题迫在眉睫。

3、定位扣费类病毒猖獗肆虐

今年 2~3 月份，伪装成知名游戏软件诱骗用户下载安装，进而恶意扣费的病毒行为影响了海量用户；根据用户地理位置发送扣费短信也是这类病毒明显的特征。这类病毒也同时通过跟踪手机用户行踪，通过发送位置信息到远程服务器而泄漏用户隐私信息。

4、资费消耗类病毒进一步活跃

资费消耗类病毒在 2012 年整个第一季度贯穿始终。无论是隐私窃取、恶意扣费、远程控制等危害行为，往往都伴随着资费消耗。病毒作者越来越懂得用户的心理与习惯，在第一季度后期，许多手机病毒通过伪装成诱惑性图标的应用或热门应用，获取用户的 root 权限，病毒也借此入侵。群发短信推广网站链接的资费消耗类病毒在第一季度大涨，不少手机用户的手机资费也因此被无形消耗。资费消耗类病毒将依然是今年的重要病毒类型。

第四章　2012 年第一季度手机病毒传播分布

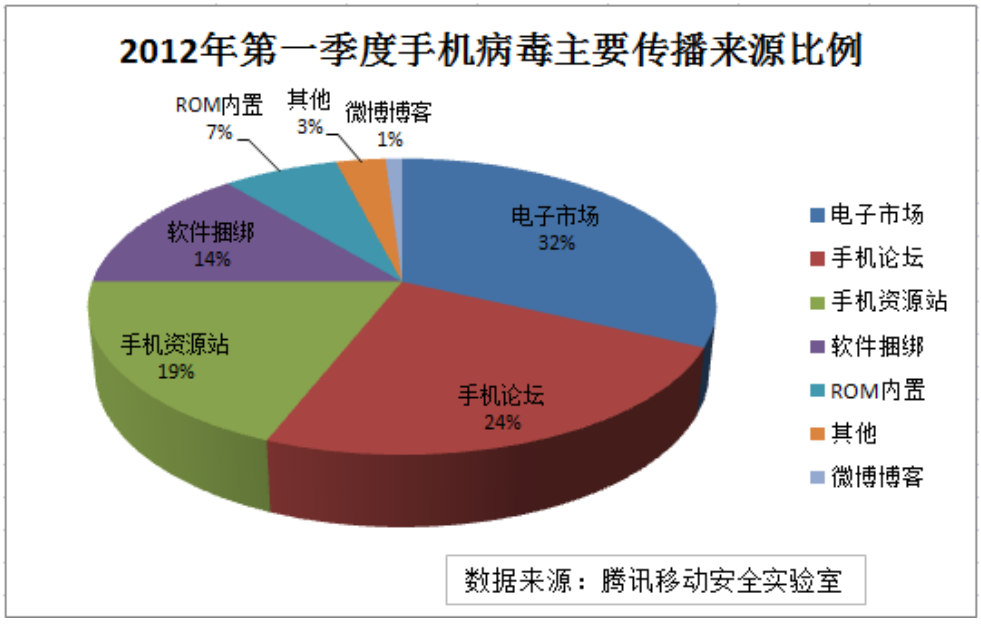
根据 2012 年腾讯移动安全实验室后台病毒渠道的第一季度数据分析显示：

电子市场、手机论坛、和手机资源站点占据了 75%的高比例，成为病毒传播的最主要的渠道来源；电子市场依旧毫无悬念的坐上病毒传播来源的头把交椅，但另一个变化是，电子市场的监管趋向严格，加之腾讯移动生态产业链的建立，电子市场的病毒检测也将变得专业，因此，总体来看，电子市场的病毒传播正呈现逐步下降的趋势。从第一季度占据比例 14%

的高比例的软件捆绑传播来看，软件捆绑正成为流行的病毒传播方式，并总体呈上升趋势，从发展趋势来看，比重也会越来越大；手机论坛病毒来源一直处于高比例，源于不少手机病毒潜伏在手机论坛借助论坛附件、网盘存储等提供用户直接下载，而手机论坛用户缺乏专业的检测工具与以及对手机病毒缺乏理性的认知，加之论坛编辑对用户下载附件应用欠缺机制性的规范与技术引导，手机论坛作为病毒高发区将会一直存在。

各渠道发现占比：

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 32%；
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. 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，占 19%；
4. 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，占 14%；
5. 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：通过发博客、微博附带下载地址链接，占 1%；
8. 其他：互联网任何形式的自助发布渠道和平台，占 3%。



第五章　手机病毒及安全行业发展预测

2012 年第一季度的手机安全行业一定程度上延续了 2011 年的发展特点：移动互联网的商业模式与盈利模式欠缺，加之技术产品标准欠缺规范、系统漏洞风险很大、手机软件市场良莠不齐，用户个人隐私和信息安全进一步受到威胁。第一季度以来，面对恶意程序、病毒木马、吸费、吸流量、大量软件广告等手机病毒变得更加专业与智能化，并且毫无忌惮的大规模肆意入侵，移动安全产业链开始进行某种程度的合作，共建安全防护网，这无疑也是一种行业利好，但移动安全行业对于病毒的监管手段需要进一步强化。手机病毒及安全行业发展趋势主要如下：

1、移动安全生态产业链进一步构建与完善

2012 年第一季度以来，手机病毒大肆席卷 Android 平台，面对手机病毒的肆虐而造成的资费消耗、隐私窃取、系统破坏等各种手机安全问题，手机安全行业对病毒的防护从被动转向主动。目前腾讯手机管家不仅为国内数十家应用检测商店提供病毒检测服务，而且与应用汇共推“双倍赔付”计划，同时更联合 20 多家企业共建移动安全生态系统，涵盖运营商、终端厂商、应用商店、安全厂商等上下游产业链，从产业链各个环节入手，打造安全的病毒防护生态网。第一季度以来，手机安全行业迎来一个显著的变化是，各类手机商家纷纷与杀毒软件厂商、安全软件商携手展开各种形式的合作，因此手机病毒特别是在 Android 平台的传播将在一定程度上会遭遇阻力。但从整体来看，整个手机安全产业如果想要构建好，那么产业链各方都要做出自己的努力并进行合理的协作。

2、病毒入侵手段智能化、目的驱利化

由于目前手机病毒肆虐，很多反病毒软件厂商、手机安全软件商纷纷进入了这个市场。为应对杀毒软件与手机安全应用的防御与查杀，手机病毒的攻击和传播、伪装手段会更加复杂，技术也将更加专业。入侵技术的专业化、攻击目的的驱利化将是未来病毒发展的重要特征。与此同时，随着国内智能手机更广泛的普及和 3G 网络业务的推广，手机病毒不再是技术爱好者发现手机软件缺陷、炫耀自己技术能力的手段，而是更多的用于制毒者与制度机构用来谋取个人或组织利益，加深损害了手机用户的切身经济利益。随着人们安全意识的增强，手机病毒的攻击技术也从初期的短信类或者是诱骗类病毒转向更加智能化、多样化的特征，这也是 3G 网络普及下，手机安全发展的一个趋势。

3、手机病毒因逐利向热门系统平台迁移、病毒应用技术增强

随着 Symbian 平台的没落，越来越多制毒者和制毒机构进一步迁移到 Android 平台，Android 平台成为病毒的最热门的系统平台这一大趋势不可逆转。同时随着运营商监管收紧甚至直接进入手机安全领域，手机安全软件的病毒查杀能力越来越强，而手机病毒的隐蔽手段与伪装方式等技术手段也将变得更加高明。手机病毒的形式也将会呈现出更多新型的特征与变种，并通过不断变换各种形式与提升技术来入侵用户手机，获取利润价值。

4、手机病毒窃取隐私成潜在重大趋势

第一季度以来，许多手机病毒开始针对用户的通讯录、短信、照片等隐私信息调用系统权限，这些应用软件未必都是手机病毒，甚至不少是正常的手机应用，但目前许多应用程序超出本身的功能范围私自对权限进行修改，调用用户隐私信息，手机面临的隐私安全问题已经不容小觑。另外，目前不少隐私窃取的手机病毒开始进一步泛滥，用户无疑将面临着自己的私隐信息被保留在恶意程序产品服务器上或者被窃取的风险。随着 3G 网络的发展，智能手机的的数据业务、网络应用、手机支付会进一步发展，因而，涉及到手机用户隐私相关的信息将会潜藏着更大的价值，对用户而言，这些隐私泄露无疑将造成重要的财产损失甚至人身安全受威胁，因此手机隐私无疑将是制毒者与制毒机构紧盯与觊觎的目标。

第六章　2012 年第一季度各平台类典型病毒

6.1　Android 典型病毒

（1）a.remote.lbs52loc.[隐秘追踪]

该病毒安装后会强制开机启动，隐藏桌面图标，同时拦截特定短信，以获取用户 GPS 位置信息，并上传远程服务器，严重泄漏用户隐私。

（2）a.remote.mzx.[卧底大盗]

该软件安装后无图标开机自启动，启动后会监听手机的通话内容、发送短信并使用 GPS 跟踪您的行踪，同时会拦截短信内容、通话记录、邮件、手机号码等隐私内容上传到服务器，给用户的隐私安全带来严重威胁。

（3）a.payment.gpssms.[定位扣费]

该病毒伪装成正常软件骗取用户安装，一旦激活后会根据地理位置来发送扣费短信，并屏蔽运营商的确认短信，用户根本无法察觉这一扣费行为，给用户的财产安全造成了威胁。

（4）a.payment.smsspy.[短信间谍]

该病毒安装后无图标，开机自动启动，启动后会发送扣费短信，并同时会删除短信信息和获取用户 GPS 位置，给用户的财产安全和个人隐私造成严重威胁。

（5）a.system.androidbot.[Root 狙击手]

该病毒包含两个可疑的 bin 程序，并且利用 png 图片把自身进行伪装；该病毒激活后对部分机型获取 root 权限，一旦获取成功便静默安装内嵌的病毒子包；给用户手机带来一定的安全威胁。

（6）a.remote.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。

（7）a.payment.fish.a

该病毒经常伪装成正常软件诱骗用户下载，启动后私自发送扣费短信，给用户的财产安全造成一定损失。

（8）a.consumption.androidme

该病毒安装后无启动图标，一旦激活将会对部分号码的短信进行拦截，并且后台私自联网，消耗用户资费，给用户造成一定的经济损失。

（9）a.payment.fakegooglemap.[伪谷歌地图]

该病毒伪装成 Google Map 骗取用户安装，安装后无图标，会在后台发送短信、拦截短信，读取通信录，给用户的手机安全和隐私造成一定的威胁。

（10）a.consumption.servicr

该病毒伪装成 Google Service 类软件骗取用户下载，开机自动启动，安装后无图标，病毒启动后分别从远程服务器“http://s2.m***o.com:9899/”和“http://s2.a***y.org:9899/”站点可能会下载其它恶意应用，并强制安装到用户手机，浪费用户手机流量，给用户带来一定的经济损失，并可能给用户造成严重的安全威胁。

（11）a.remote.klservice

该病毒安装后无图标，开机自动启动，在后台获取通话记录、短信信息、图片、录音等文件信息保存到 SDcard 卡下，并定时通过网络发送到远程服务器。给用户的隐私安全造成一定威胁。

（12）a.privacy.smart.[系统快捷设置]

该病毒经常伪装成系统组件骗取用户下载，启动后私自下载未知软件，并伴有静默安装行为，同时收集用户手机 IMEI，IMSI，用户软件等信息。

（13）a.privacy. counterclank

该病毒启动后在用户不知情或者未授权的情况下，在桌面创建快捷方式，并且收集用户浏览器书签、手机制造商等信息，黑客可以通过这一 恶意软件向用户发送广告，并同时修改手机的默认浏览器主页，给用户造成一定的安全威胁。

（14）a.consumption.fakePatch.[伪系统补丁]

该病毒伪装成系统补丁骗取用户安装，无图标自启动,在后台下载多款推荐软件，同时申请 ROOT 权限成功后静默安装下载下来的软件，给用户的手机造成一定的威胁。

（15）a.consumption.fakealSalah.[恶推流氓]

该病毒伪装成“AlSalah”软件，开机自启动,一旦激活会从配置文件里读取推广列表并且随机选取列表里的链接，向手机里全部的联系人发送包含该链接的推广短信，可能造成用户的手机资费消耗。

（16）a.privacy.safesys.b.[root 破坏王]

该病毒通常伪装成某些热门小型应用，在使用过程中会弹出 root 权限授予请求。如果被授予了 root 权限，则在后台下载其它恶意程序并静默安装，给用户手机安全造成威胁。

（17）a.payment.mobi.c.[魔比扣费]

该病毒一旦被激活，则会在后台私自从 raw 目录中读取 sms.cfg 文件获取发送地址，并偷偷发送扣费短信，使用户不觉察的情况下遭受经济损失。

（18）a.privacy. eula

该病毒安装后，启动无图标，私自收集用户手机内的照片并发送到远端指定网址 http://fy**kit.dk/photoCopy, 同时收集用户 IMEI 等硬件设备信息，导致用户隐私泄漏。

6.2 Symbian 典型病毒

（1）s.privacy.poec

该病毒伪装成正常软件诱骗用户安装使用，自激活后常驻后台，消耗手机内存资源；无提示获取手机联系人列表并删改手机联系人信息，严重影响手机的正常使用

（2）s.consumption.minimapguide.[伪 E 都市地图]

该病毒伪装知名的地图导航软件，诱导用户下载安装，自激活后常驻后台私自联网；无法完全关闭，占用大量系统资源，可能影响手机或其他软件的正常运行。

（3）s.consumption.imidaemon.[伪艾米视频聊天]

该病毒伪装成知名的视频聊天软件诱导用户下载安装，自激活后私自联网静默安装其他恶意插件，并常驻后台占用系统资源，可能影响手机的正常使用。

（4）s.privacy.e3dgdisplay.[伪手机酷秀]

该病毒以“手机酷秀”为名，诱导用户下载安装，非官方版本，而是被其他恶意者篡改过的盗版软件自激活后常驻后台私自联网，静默安装其他恶意插件，可能给用户带来一定流量损失，还有可能联网时泄露用户手机

（5）s.payment.anvisak.a.[伪杀毒吸费中心]

该病毒以“杀毒中心”为名诱导用户下载安装，实际无任何杀毒功效，安装后提示手机存在 3 个病毒 BIT.***Plug【盗号木马】,FC.Dow***【恶意扣费】,Sha***Srv【隐私窃取】，需用户支付**元的费用来进行病毒清理，用户一旦确认，病毒便会在后台自动点播 SP 收费业务，同时屏蔽运营商发送的收费提示短信，给用户带来严重经济损失。

（6）s.payment. superupdate.[系统辅助包]

该病毒常伪装成手机系统组件，诱使用户下载安装，无任何图标，自激活后私自联网下载其他恶意软件，

消耗用户手机一定数据流量；私自发送短信并屏蔽运营商的反馈信息，有可能在用户毫不知情的情况下订购高额的 SP 收费业务，给用户带来一定经济损失；无法完全关闭，占用大量系统资源，无法手动删除，可能影响手机或其他软件的正常运行。

（7）s.payment.sysinbestsafe

该病毒安装后开机自启，无法完全退出，占用手机内存，可能使手机或者软件无法使用；且在没有提示联网的情况下自动联接网络，消耗流量，给用户带来一定的经济损失；同时该病毒静默安装几款恶意插件，可能给用户手机带来一定的安全威胁。

（8）s. consumption.datastart

该病毒以市面实用工具（如：**闹钟，**来电）名义诱导用户下载安装，激活后会向指定号码：106*****3 发送短信定制 SP 服务并伴有后台联网行为，消耗用户资费，不但给用户造成一定的经济损失，同时可能造成成用户手机信息的泄露。

（9）s.payment.notesend

该病毒以市面实用工具（如：**闹钟，**来电）名义诱导用户下载安装，激活后会向指定号码：106*****3 发送短信定制 SP 服务并伴有后台联网行为，消耗用户资费，不但给用户造成一定的经济损失，同时可能造成成用户手机信息的泄露。

（10）s. consumption.swhelp

该病毒捆绑主题类软件诱导安装，安装完成后以“nokia_helper”名义冒充手机系统程序驻留用户手机，一旦激活便后台无提示链接网络，消耗用户资费，给用户带来一定的经济损失。

（11）s. consumption.Privatevideo

该病毒以“**视频”名义诱导用户下载安装，安装后无启动图标，激活后边后台无提示链接网络，消耗用户资费，给用户带来一定的经济损失；联网成功后边下载其它恶意程序后台静默安装，一旦安装失败，便不停弹出安装提示，不但给用户的手机造成进一步的安全威胁，而且用户手机内存，给用户正常使用手机带来一定影响。

（12）s. consumption.phogd

该病毒激活后边便后台无提示自动联网，消耗用户资费，给用户带来一定的经济损失；同时该病毒开机自启，无法完全关闭，占用手机内存，可能造成手机假死，给用户正常使用手机带来一定的影响。

（13）s. consumption.acceleration.c.[伪手机加速]

该病毒激活后无提示自动连接网络，消耗资费，给用户带来一定的经济损失；同时该病毒无法完全关闭，占用手机内存，给正常使用带来一定的影响；使用该病毒软件扫描提示手机内存在病毒程序，清除后再次扫描，所谓的病毒程序依然存在，欺骗误导用户使用。

第七章　专家支招规避手机病毒的方法

手机病毒的伪装能力千变万化，手机病毒数量进一步水涨船高，多种新技术的结合运用更让病毒难以察觉。手机用户学会规避病毒风险变得十分必要。

电子市场是用户下载软件的第一渠道。用户在此可以有针对性的去选择口碑不错、评价较好或者是打分高的软件，这样无疑可以一定程度上规避风险，但是目前应用市场刷票频繁，

加之更多的手机病毒捆绑热门软件进行打包潜伏，因此下载热门软件依旧风险暗藏，需保持一定的警惕性。所以对于电子市场的软件下载，用户应该从信任的来源下载软件，最好去腾讯应用中心下载，而应尽量避免从非正规论坛、电子市场或者资源站下载手机软件，另外，用户还可以选择去腾讯手机管家自带“软件游戏”功能中下载，或通过 QQ 电脑管家的手机管理功能直接在电脑免费下载上万款手机软件，这些应用都经过腾讯手机管家的安全认证，可以有效保证应用的安全。

一款好用的手机安全软件对于用户而言十分必要，如果用户一定需要去论坛下载手机应用，请安装如腾讯手机管家一类专业的手机安全软件开启保护，及时升级病毒库，定期扫描查杀，定期监控手机流量与包月套餐费用，删除乱码短信、彩信，谨慎选择刷机 ROM，可以避免手机中毒等问题而造成的严重损失。另外，用户还可以关注@腾讯移动安全实验室的腾讯微博，对最新的手机安全资讯做到全面把握与掌控，从而放心畅享移动互联网生活。

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 4 月 18 日