网秦 手机安全专家
NetQin
www.netqin.com

WORLD ECONOMIC FORUM
Technology Pioneer 2011

NetQin 网秦

2010年中国大陆地区手机安全报告

www.netqin.com

北京网秦天下科技有限公司
2010年12月

目录

免责声明：

该报告综合网秦“云安全”数据分析中心、网秦全球手机安全中心等部门的统计、研究数据和分析资料，针对中国大陆地区 2010 年手机安全形势发展进行统计、研究和分析。本报告提供给媒体、公众和相关政府及行业机构、厂商作为移动互联网信息安全状况的介绍和研究资料，请相关单位酌情使用，如若本报告阐述之状况、数据与其它机构研究结果有差异，请使用方自行辨别，北京网秦天下科技有限公司不承担于此相关的一切法律责任。

关于本报告数据：

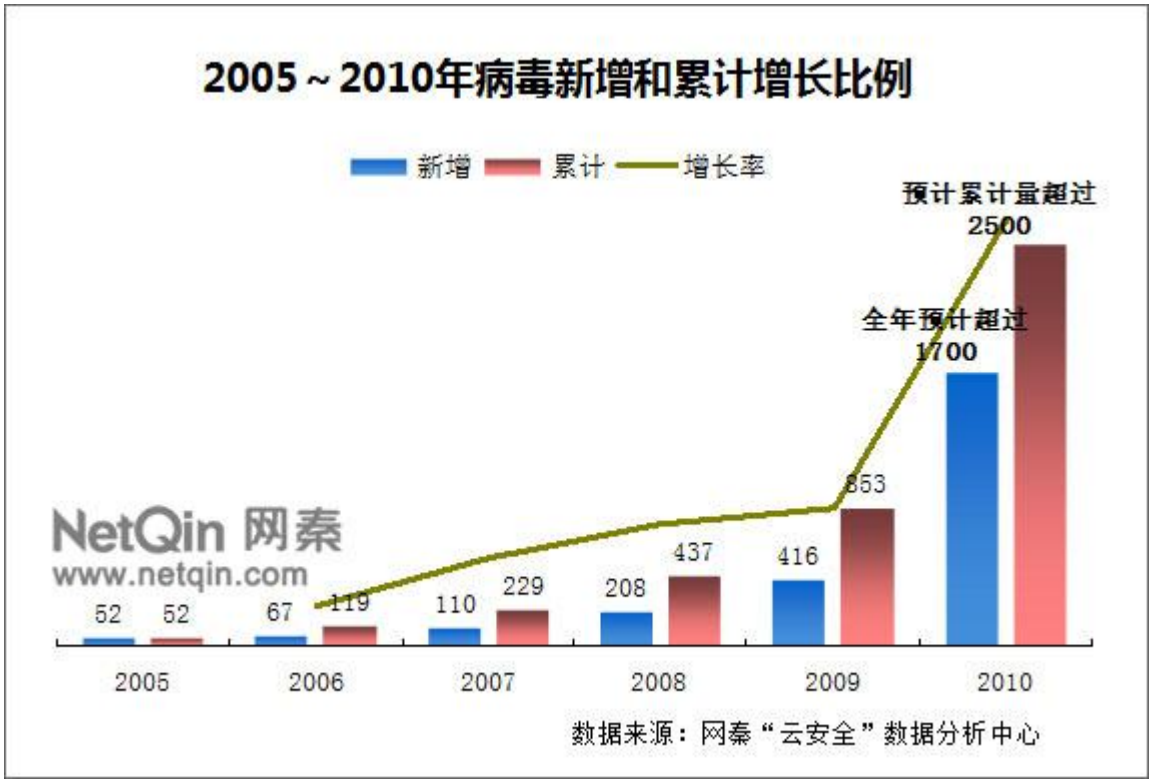
本报告讨论的范畴为手机恶意软件（mobile malware），手机恶意软件指的是在用户不知情情况下给用户带来损害的各种手机软件。由于病毒一词比较形象，也一直被用做恶意软件的俗称，本报告为方便读者阅读，余下全文除非特指，“手机病毒”一词，都指的是“手机恶意软件”。

【报告全文】

第一节 2010 年手机病毒疫情统计和分析

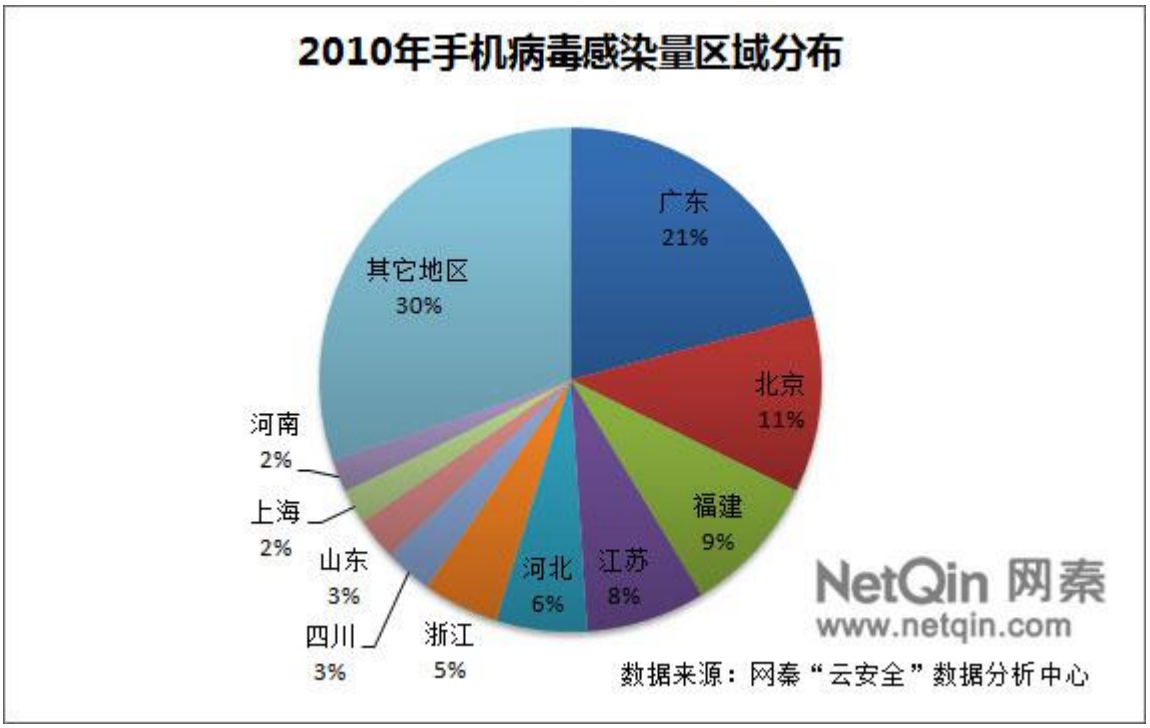
一、2010 年手机病毒增长情况和地域分布情况

数据显示：截至 2010 年 11 月，网秦“云安全”数据分析中心新截获手机病毒 1513 个（预计全年将超过 1700 种），累计截获病毒 2357 个（2009 年共截获手机病毒 416 个）。**预计 2010 年，手机病毒总数将超过 2500 种以上，同比增长超过 193%，累计感染手机 800 万部以上，**病毒变种数量在 231 次以上。



2005~2010 年手机病毒新增和累计增长比例

地域分布方面，据网秦“云安全”数据分析中心对网秦注册用户主动反馈的数据进行分析：**在国内，广东地区以 21%的感染比例，成为手机病毒的感染重灾区，北京、福建、江苏、河北、浙江、四川、山东、上海等地区位居其后。**



2010 年手机病毒感染量区域分布图

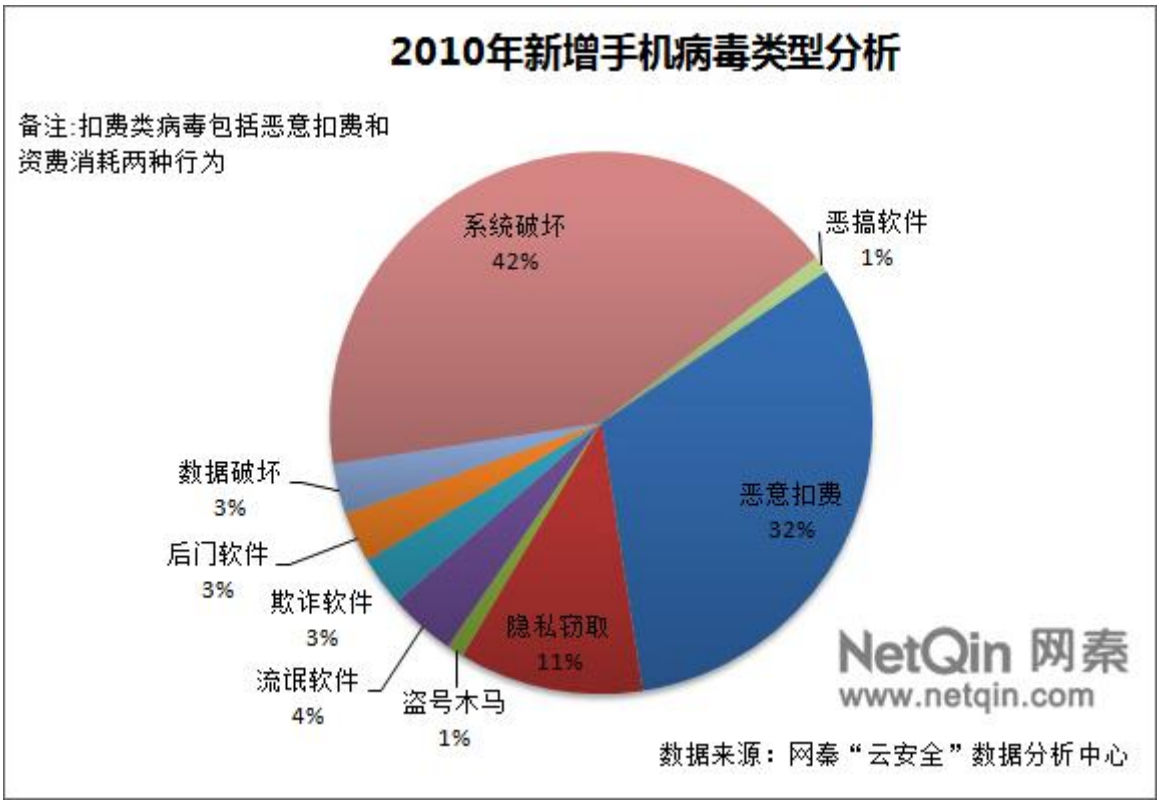
其中，由于我国东南沿海地区移动互联网发展迅速，智能手机用户量也保持领先，使得用户在享受更丰富的手机应用的同时，也时刻面临着手机病毒的威胁。例如，2010 年 11 月爆发的“手机僵尸”病毒，和 2010 年上半年肆虐手机的“手机骷髅”病毒等，上述省份的智能机用户感染量都位居前列。

二、2010 年手机病毒感染类型分析

进入 2010 年，手机病毒的感染类型已覆盖到多个层面，从破坏手机系统到破坏用户手机中的重要数据，再演变至窃取手机中的隐私内容、盗取手机软件的账户密码和开启后门、上传用户信息等。同时，手机病毒也出现了一个病毒同时存在多个特征的现象，对用户的手机安全造成了极大威胁。

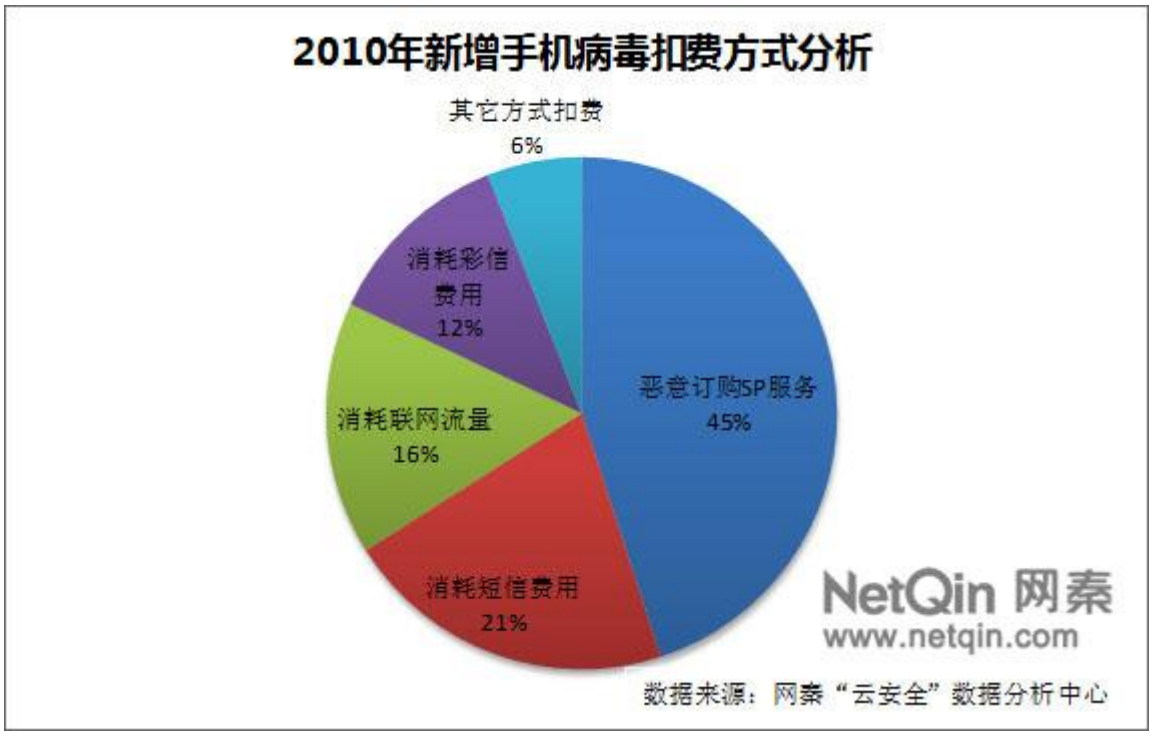
据网秦“云安全”数据分析中心统计：2010 年截获的手机病毒（截至 2010 年 11 月）中，存在扣费行为的手机病毒达到 968 个（其中 454 个存在恶意扣费行为，514 个病毒存在资费消耗行为），存在窃取用户隐私行为的病毒 334 个，盗号木马病毒 12 个，手机流氓软件 130 个，80 个欺诈软件和后门软件 94 个、并有 96 个手机病毒存在破坏手机数据的现象，另外有 1280 个手机病毒存在破坏手机系统的现象，以及 36 个以恶搞为目的的恶作剧软件（注：一个手机病毒会存在多个破坏行为，故以实际的破坏行为作为统计基准）。

其中**存在恶意扣费行为的手机病毒从去年的 171 个，快速增长到 968 个，并已占据 2010 年新增手机病毒 32%的比例，累计感染手机 250 万部以上，使得其成为影响用户手机安全的主要威胁。同时后门程序在 2010 年末出现了增长趋势。**



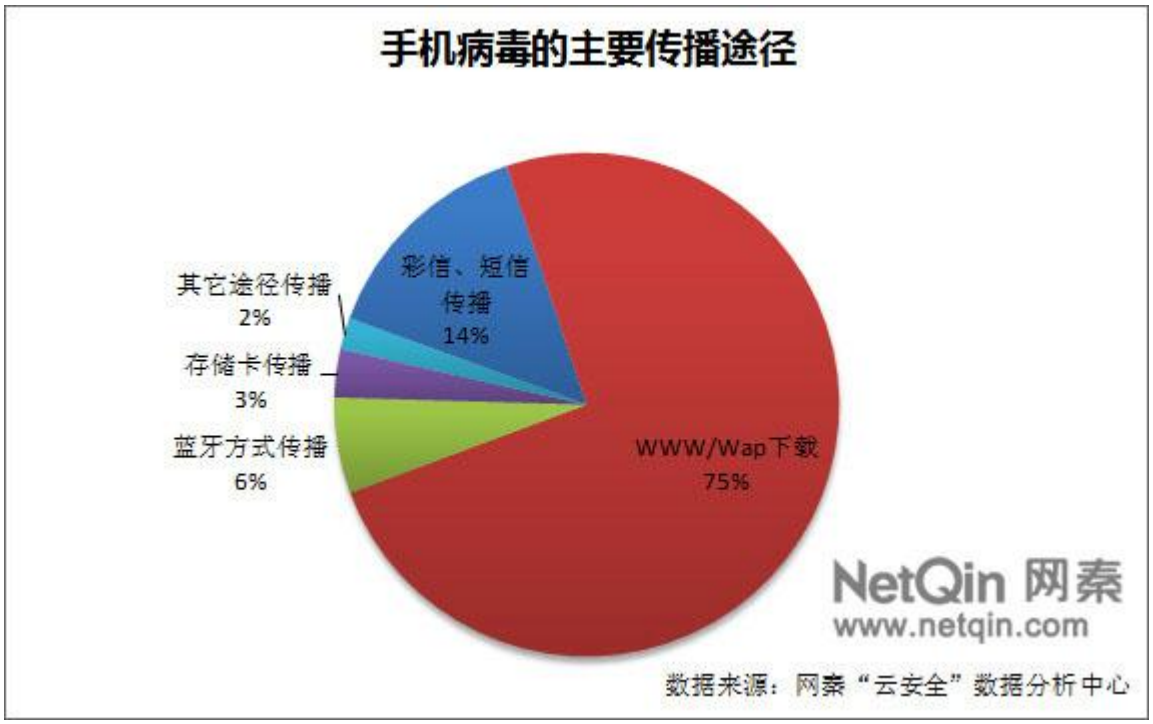
2010 年新增手机病毒类型（网秦“云安全分析中心数据）

扣费类病毒感染用户后，45%的病毒以恶意订购 SP 服务的方式扣去用户费用；21%的病毒以消耗用户短信费用的方式来进行扣费；16%的病毒是以联网消耗用户流量的方式为目的；12%的病毒通过骗发彩信消耗用户费用；6% 的病毒以其它方式，如“自动拨号”等方式扣费。



三、2010 年手机病毒感染方式分析

感染途径：当前**通过手机访问 wap 和 www 网站感染病毒的比率达 75%；**通过短信、彩信感染病毒的比率占 14%；通过蓝牙传输方式感染病毒的比率占 6%；通过存储卡等途径感染病毒的比率占 3%；另外 2%的用户则是被其它传播途径的病毒感染。其中联网感染病毒的机率最大，成为用户面临的最主要威胁。



网秦“云安全”数据统计的 2010 年手机病毒主要感染途径

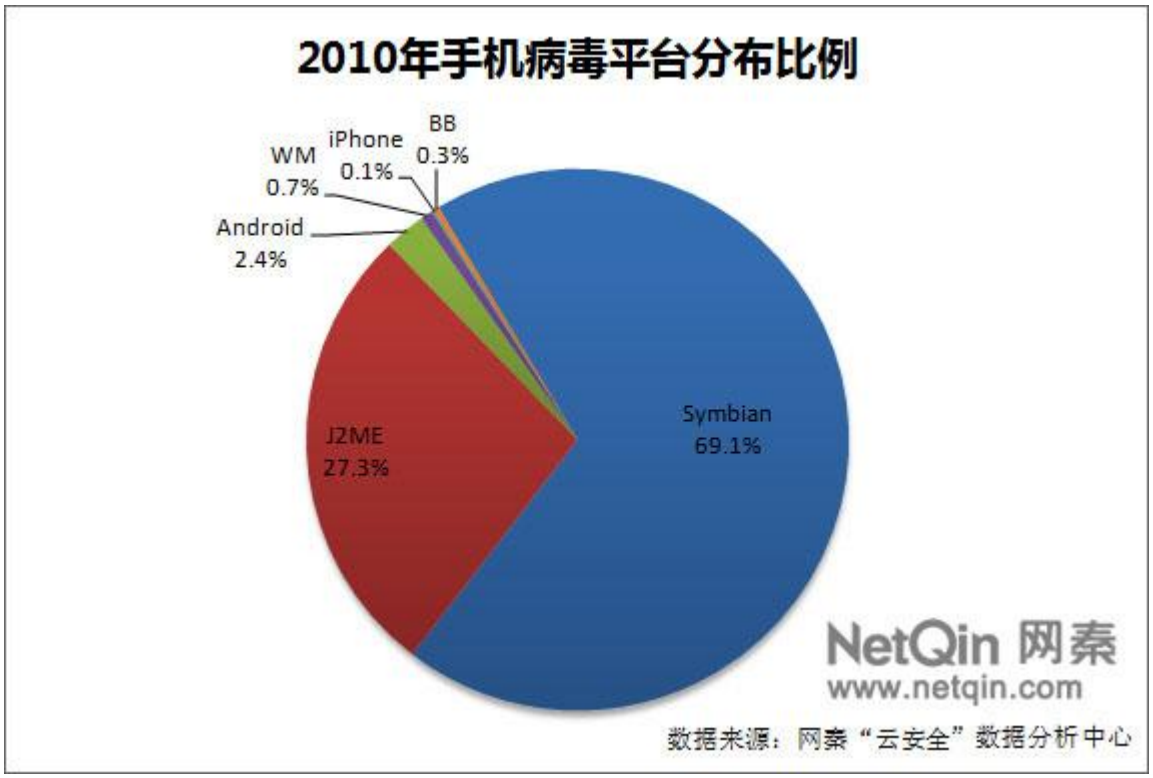
通过联网传播的威胁中，伪装为各类手机软件的病毒占总比例的 75%，成为用户手机的主要感染源。2010 年，网秦累计截获伪装为常用程序的手机病毒 56 个，以包括“系统升级包”、“手机 QQ”、“手机输入法”、“开心农场手机版”等名义下载，并存在自动联网扣费、上传用户隐私、盗号等行为。

同时，据网秦“云安全”数据分析中心的统计，手机软件下载网站当前也多存在严重的安全风险。其中，分析中心选取了 5 家当前用户关注度、下载率较高的软件网站，通过对其安全性进行检测后发现，部分网站的软件资源染毒率高达 57%以上。可见即使通过下载网站下载手机软件，也极易感染手机病毒。某省运营商的分析数据中，更指出当前 6%的上网流量中存在安全隐患。

四、手机病毒感染平台分析

伴随手机病毒的快速增长和传播及感染范围的增加，不同手机平台均已成为病毒作者关注的对象，尽管从攻击成本考虑，Symbian 平台是黑客的攻击重点，但包括“给你米”（Geinimi）等“后门”程序的相继出现，也反映出 Android 平台的安全威胁正高速增长，感染比例也在持续上升。

其中，据网秦“云安全”数据分析中心的数据显示，截至 2010 年 11 月，Symbian 平台依然是手机病毒感染的重点对象，69%以上的手机病毒对 Symbian 手机构成威胁，J2ME 以 27%的感染比例位居第二大感染平台。Android 平台的整体感染量也在持续上升，目前已占据 3%的感染比例。2010 年底，国际知名的 GIK 调研结构公布的手机平台调查中，Android 平台的手机销量在亚洲地区已超过 Symbian，伴随新平台的高速发展，安全形势同样不容乐观。



2010 年手机病毒平台分布比例

例如 Android 手机病毒会将自身伪装成 Android 系统的常用软件、游戏、壁纸等，在包括软件商店、Android 软件商店和 Android 论坛上骗取用户下载安装，从而达到大范围传播的目的。一旦不慎运行此程序，病毒会自动联网、在系统后台启动恶意进程，窃取手机中的隐私内容，直接威胁用户的财产安全。

第二节 2010 年十大手机病毒和案例分析

一、2010 年十大手机病毒

2010 年的十大病毒为：手机僵尸、手机骷髅、终极密盗、变装恶铃、彩秀画皮、短信海盗、QQ 盗号手、Android 短信卧底、盗密空间、“给你米”后门程序。

当智能手机的“梦想照进现实”，却不料成了手机病毒“暗恋”的对象。2010 年是手机病毒大肆泛滥的一年。1 月，“钓鱼王”手机病毒在用户安装一些手机游戏后生成诈骗短信窃取银行卡账号和密码；2 月，“手机骷髅”病毒，主要针对 S603 版操作系统的智能手机，超过十万部手机被其感染，直接经济损失超过 2000 万元；3 月，“手机骷髅”的变种“短信海盗”病毒迅速蔓延，让用户话费耗尽，隐私外泄；5 月，“老千大富翁”大量消耗用户流量并盗取用户隐私……

早期的手机病毒主要是破坏手机的运行使用，现在手机病毒有了新的动向——恶性欺诈病毒成了“主力军”，通过感染手机窃取话费、盗得数据，让用户遭受重大损失。走过 2010，我们对威胁手机安全的十大病毒进行重点盘点：

1.手机僵尸病毒【资费消耗】

2010 年 10 月中下旬，“手机僵尸病毒”大面积爆发。央视《每周质量报告》报道称：在 9 月的第一周，全国就发现将近一百万部手机感染“手机僵尸病毒”，感染病毒后的“僵尸手机”以不易被人察觉的方式自动向他人发送短信传播病毒，并暗中扣取用户的手机话费。这些手机数量相加，算起来每天约有 200 万元话费被“僵尸”吸干。

而早在 2010 年 6 月，网秦就对此病毒进行解读。其以手机常用软件的名义来诱骗用户安装，安装会后不仅会窃取用户手机隐私信息，还会自动向手机上的通讯录发送含有病毒链接的短信，以此做到进一步传播，给用户带来隐私、名誉和资费等多重损失。

2.手机骷髅【资费消耗】

2010 年 2 月份，网秦率先截获“彩信骷髅炸弹”并将其命名为 “手机骷髅”。该病毒累计感染超过 10 万智能手机。遭受彩信骷髅后，手机会不断自动联网且向外发送带有病毒链接的彩信和短信。平均每位中毒用户向外发送彩信数为 200 条左右，用户需为这个恶意行为付出大量话费，每位每天最高可达 300 多元。

3.终极密盗【盗号病毒】

“终极密盗”是高危盗号类手机病毒，其会通过伪装成塞班手机系统的“系统升级包”骗取用户下载安装。感染手机后，在用户登录手机 QQ、网银、手机炒股软件时，窃取用户密码，并通过短信形式发送到其指定号码。用户若未安装专业的手机安全软件，密码安全将面临严重威胁。

4.变装恶灵【资费消耗】

“变装恶灵”是一款以消耗用户资费为目的的恶性手机病毒。该病毒侵入用户手机后，会在本地生成一条由 10086 发送的彩信，内容大致为：“……拨此号码立刻免费赠送 50 元大闸蟹代金券……”。这类病毒以 10086 之名制造虚假彩信，具有很强的欺骗性，很可能给用户造成经济损失。

5.彩秀画皮【隐私窃取】

“彩秀画皮”手机病毒会伪装成来电设置软件“彩秀”诱骗用户安装，安装后不仅会使手机自动联网，还会窃取用户手机的 IMEI 号与 IMSI 号，更严重的是会使用户订购高额 SP 业务，造成话费隐私的双重损失。

6.短信海盗【隐私窃取】

“短信海盗”病毒是吸光无数手机用户话费的“手机骷髅”病毒的新变种。“短信海盗”和“手机骷髅”一样，会自动发送彩信，但其比“手机骷髅”更为恶劣的是它会将用户收件箱的内容发送给其他好友，在很大程度上造成用户隐私泄露。

7.QQ 盗号手【恶意盗号】

“QQ 盗号手”病毒以“QQ 花园助理”、“刷 Q 币工具”之名诱骗机友下载，中毒后的手机会出现 QQ 登陆框，诱使手机用户输入 QQ 账号和密码，此时 QQ 盗号手会将账号和密码发到某特定手机号上，导致账号和密码丢失。

8.Android 短信卧底【隐私窃取】

“短信卧底”手机病毒是首款出现在 Android 手机中的病毒，它能偷偷窃取手机中的短信内容，造成用户隐私严重泄露。而可怕的是，短期内，网秦又截获了它的变种，这个变种不但能窃取短信，还能监控用户的通话记录！此类病毒的出现，可见 Android 作为逐渐主流的智能手机平台，已经被黑客盯上，且病毒变种如此迅速，不得不引起大家关注。

9.盗密空间【隐私窃取】

“盗密空间”手机病毒以“收件箱”之名诱骗用户下载安装。中毒后，病毒会在后台偷偷联网向外发送用户的 IMEI 号和和手机型号等个人信息，泄露用户的个人隐私，并且该病毒具有开机自启功能且又无法正常删除，给用户的手机安全造成损害。因此该病毒被命名为“盗密空间”。

10.“给你米”（Geinimi）的后门程序【后门程序】

“给你米”（Geinimi）的后门程序，基于 Android 平台，通过植入到“入侵脑细胞”、“植物人大战僵尸”等多款流行手机游戏软件中，生成新的软件安装包后在手机论坛、手机软件下载站进行线上分发。

感染用户手机后，“给你米”（Geinimi）后门程序会自动在手机后台启动，并定期连接到“给你米”（Geinimi）网站，推广各类恶意广告短信，在用户不知情的情况下，自动下载各类恶意推广软件。

二、2010 年手机病毒案例分析

【案例 1】 手机僵尸病毒肆虐

11 月 7 日，央视曝光了手机僵尸病毒泛滥的最新消息，手机僵尸病毒成为当前危害用户移动安全的主要威胁。据网秦全球手机安全中心介绍，截至 2010 年 10 月，手机僵尸病毒变种已达 10 种以上，6 月，网秦全球手机安全中心率先曝光手机僵尸病毒后，累计感染量已突破 150 万以上。百万用户面临手机僵尸病毒威胁，使其成为了威胁用户手机安全的严重隐患。

手机僵尸病毒是一类捆绑在应用软件上的病毒，被感染后的手机成为“僵尸手机”，自动向其他用户发送带有病毒链接的短信，一旦其他人收到短信并点击链接，其手机也会成为“僵尸手机”。

1）僵尸病毒的诞生

在今年 6 月底超过 500 个手机用户救助，用户手机因下载小游戏类应用软件而中毒，中毒后，手机会自动向外发送含有有毒链接的短信息。中了这些病毒后，其手机就成为“僵尸”，任由病毒摆布。众多的机友在不知不觉中如同中国古老传说中的僵尸群一样被人驱赶和指挥着，成为被人利用的一种工具。因此网秦将此类病毒统一命名为“手机僵尸”病毒群。

2）僵尸病毒的进化

手机僵尸病毒被发现后，随机出现了多次进化。例如，手机僵尸病毒与之前的僵尸病毒群相比有了一个很大的变化——它开始有 IQ（智商）了。它会根据手机内安装的程序，来判断是否安装插件；还会在用户手机锁机的状态下暗地联网和发送短信；同时会删除相关的安装程序和手机通讯记录；更有自我保护机制以防止被用户卸载。一切都是在暗中，僵尸也开始玩起来了计谋。

3）僵尸病毒的变种

同时，在僵尸病毒的变种方面，以“毒媒(AVK.DuMusic)”变种病毒为例，据国家互联网应急中心(CNCERT)统计，自 2010 年 8 月，该病毒的感染峰值一度达到 100 万以上，严重威胁用户的移动安全。后经 CNCERT 和网秦等专业安全厂商的协力打击，已初步得到遏制。但在当前，由于病毒再现多个新变种，据相关数据显示，依然有 40 万手机用户正面临此病毒威胁。

【案例 2】 “手机骷髅”病毒爆发

2010 年 2 月，一个名叫“彩信骷髅”（又名“手机骷髅”/“章子怡私房门”）的病毒对手机用户造成了严重威胁，影响超过 10 万智能手机。遭受“彩信骷髅”病毒后，手机会不断自动联网且向外发送带有病毒链接的彩信和短信。平均每位中毒用户向外发送彩信数为 200 条左右，用户需为这个恶意行为付出大量话费，每位每天最高可达 300 多元。

彩信骷髅危害行为：

1）私自发彩信和短信

中毒的手机会不停自动联网，并私自向手机里存储的联系人发送大量彩信，内容同样是一张黑白的骷髅头和具有诱惑性的文字及链接，同时会向号码 15810***754、137536***70 等随机号码发送短信，直至手机费耗尽或电池耗尽才停止，给手机用户带来无尽骚扰和金钱损失。

2）自动联网和安装程序

彩信骷髅还会在后台悄悄下载和安装另一程序“设置向导”，该程序也会联网，消耗流量。

3）第三方文件管理工具失效，且开机自启动

会使 Activefile、TaskSpy 等常用的文件浏览软件失效，并且病毒会开机自启动，使用户无法手动停止病毒进程。

4）锁定程序管理，无法正常卸载

会终止程序管理进程，x_plore 无法删除相关程序和目录，使用户无法卸载病毒程序。

5）频繁关机或重新重启

手机处于被控制的状态，不停的被关机和开机。

【案例 3】 “终极密盗”伪装手机软件狂盗 QQ 密码

2010 年 11 月，网秦全球手机安全中心截获了一个名为“终极密盗”的手机病毒，其会伪装成“系统升级包”诱骗用户下载安装。安装后并无图标和界面，在用户登录手机网银、QQ、MSN 之类的客户端时，该病毒会记录账号和密码，并以短信的形式发送给特定手机号码，严重威胁密码隐私安全，可能给用户造成严重的经济损失！

“终极密盗”危害行为：

1、窃取账号密码：向指定号码发送含有账号和密码的短信，泄露用户重要信息，可能给用户造成严重的经济损失！

2、自动发短信：手机会自动向外发送 2 条短信，包含银行帐号和登录时输入的密码。

3、难以卸载：病毒采用自保护机制，安装后没有图标没有界面，无法手动卸载。

4、病毒开机自启动：病毒在安装和开机后会自启，如果此时你习惯性的开机后登陆 QQ、炒股软件，极易让账号立刻被盗。

【案例 4】 “给你米”（Geinimi）后门窃取用户隐私

2010 年 12 月初，网秦全球手机安全中心发布手机安全预警：一组名为“给你米”（Geinimi）的手机后门程序，正在大量手机软件下载站、论坛中疯狂传播。经检测，该程序存在恶意广告推广行为，并且会

窃取用户隐私和产生恶意扣费等行为。用户若未及时安装专业手机安全软件，将面临严重安全威胁。

据悉，这组名为“给你米”（Geinimi）的后门程序，基于 Android 平台，通过植入到“入侵脑细胞”、“植物人大战僵尸”等多款流行手机游戏软件中，生成新的软件安装包后在手机论坛、手机软件下载站进行线上分发。

感染用户手机后，“给你米”（Geinimi）后门程序会自动在手机后台启动，并定期连接到“给你米”（Geinimi）网站，上传用户的位置信息，并根据所在地域，推广各类恶意广告短信，在用户不知情的情况下，自动下载各类恶意推广软件。

同时，“给你米”（Geinimi）后门程序出现之后，网秦“云安全”数据分析中心还相继截获了包括伪装成唐诗、手机 QQ 软件，骗取用户下载安装后开启系统后门的恶性病毒。使得 2010 年底，Android 平台出现的一系列案例获得了用户的关注。

第三节、手机用户面临的安全隐患

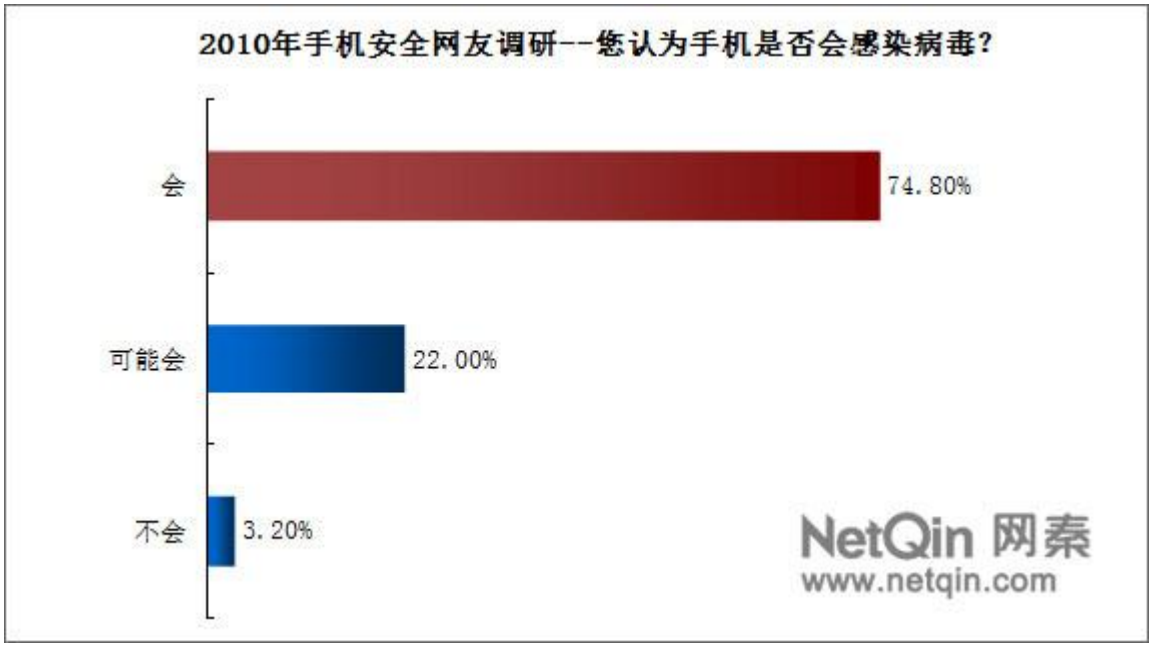
1）用户面临的主要安全隐患

随着智能手机的功能越来越强大，手机上使用的无线网络应用软件逐渐成为黑客攻击的目标，给手机用户的个人信息带来安全隐患。而除了“僵尸网络”、“网络钓鱼”等直接利用互联网的传统网络犯罪外，利用智能手机和无线局域网进行的网络犯罪正快速增多。如果用户使用的智能手机没有足够的安全防护，黑客就可以通过无线局域网或“蓝牙”传输等手段侵入手机下载的应用程序，诱使手机用户登录“网络钓鱼”网站等非法网站。

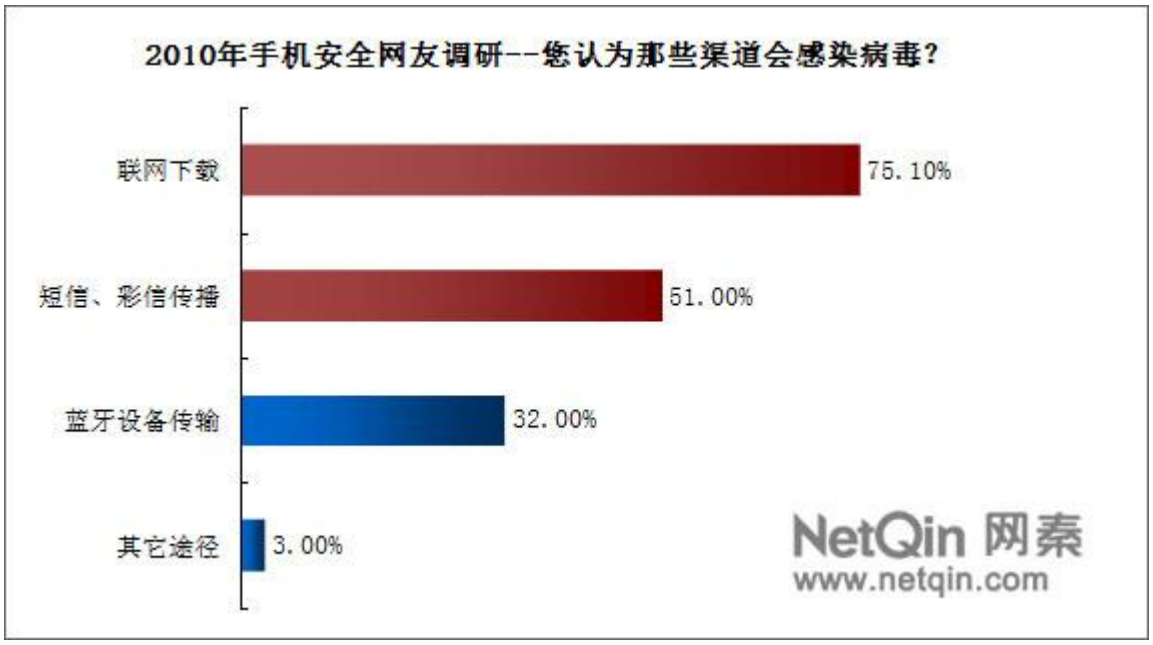
然而，追踪病毒源头的技术还不够成熟，病毒制造者都可以仿冒 IP 发布带有病毒的恶意软件供人下载。但智能手机的致命弱点即无法像电脑一样重装系统，只能任期报废。智能手机用户应像对电脑进行安全防护一样保护自己的手机。有效方法包括定期进行安全防护软件升级，安装防病毒软件，以及在不使用无线局域网、蓝牙传输等手段获取信息时关闭手机上与此有关的功能。

2）用户对手机安全隐患的感知

通过网秦对新浪网、太平洋电脑网等垂直媒体的调查分析：74.8%的受访者表示手机会感染病毒，而在手机病毒感染渠道上，75.1%的用户因联网下载而感染病毒，其次是盲目点击短信中的链接，通过短信、彩信传播。



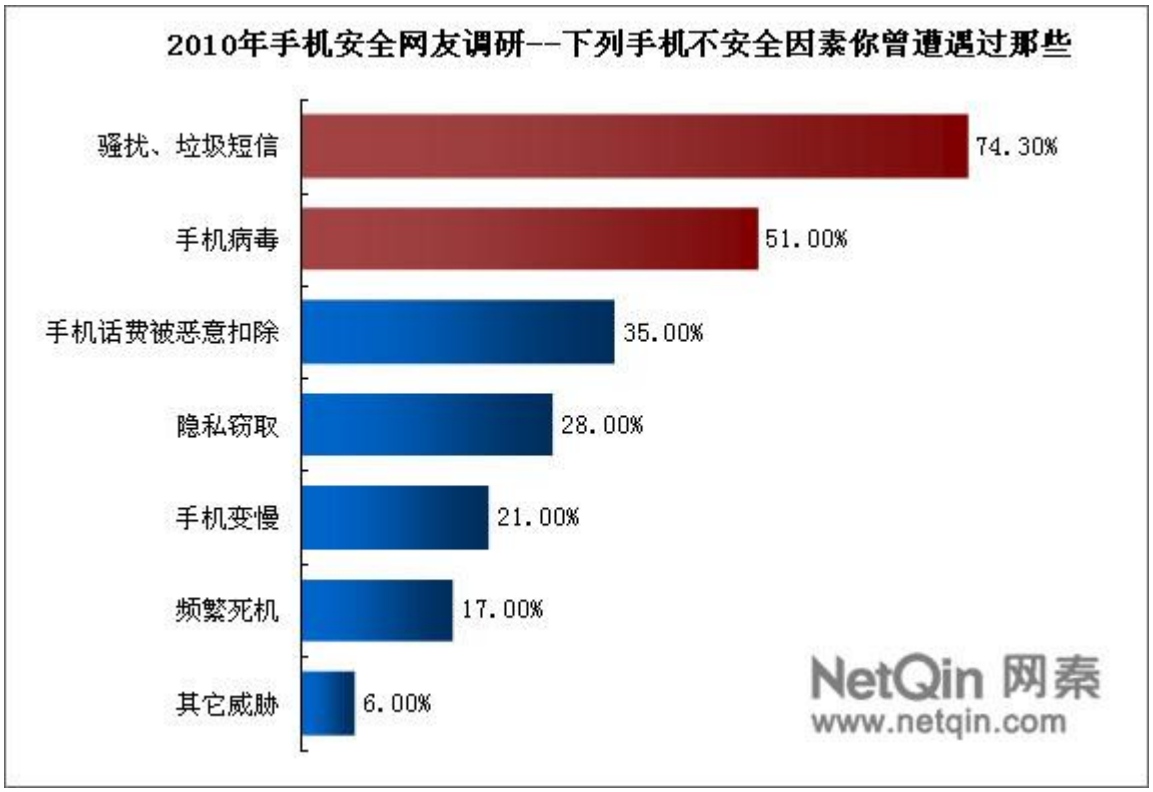
调研平台：新浪网、太平洋电脑网（N=8200）



调研平台：新浪网、太平洋电脑网（N=8200）

3）用户面临的十大手机安全隐患

在手机不安全因素调查中，垃圾短信、骚扰电话和手机病毒等，成为用户面临的十大安全难题之重，其中，有 74.3%的用户表示都曾遭受到骚扰、垃圾短信的威胁，恶意扣费对用户的影响正在加深，有 35%的用户都受到此类不安全因素的威胁。

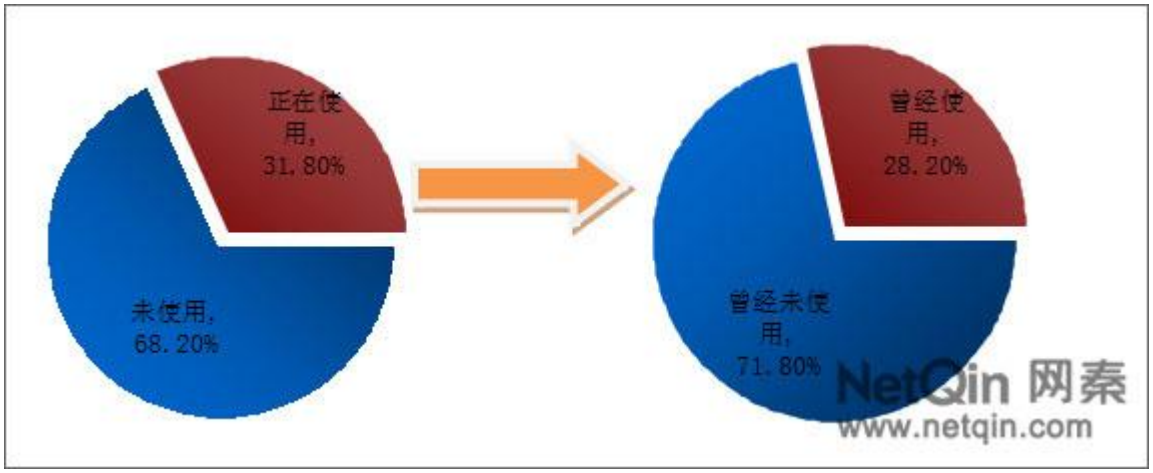


调研平台：新浪网、太平洋电脑网（N=8200）

3）手机安全软件的普及情况

而在针对手机安全软件使用情况的调研过程中发现，31.8%的用户正在使用安全手机软件；而在使用过手机安全软件的用户中，28.2%的用户曾经使用过手机安全软件。

2010 年手机安全网友调研--你是否正在使用安全软件？　　您曾经是否有使用过手机安全软件



调研平台：新浪网、太平洋电脑网（N=8200）

调查结果显示，当前用户虽已深刻了解到手机安全的严峻性，却有近 7 成用户并未使用过手机安全软件，无法得到专业、系统的安全保护。

第四节、2010 年手机安全形势/2011 发展趋势解析

一、手机病毒的传播和威胁趋势

1．传播趋势：病毒植入方式更灵活、多变，增加了安全防护的难度。

传播方面，新兴手机病毒植入方式更为灵活、多变，并紧随移动互联网的应用而广泛发展。传播方式更为巧妙，从简单的以“中奖”等诱骗用户回复短信、拨打电话，进入到假借“中国移动”官方名义传播“官方”通知、将病毒主体伪装为常用的手机软件，和通过短信、彩信链接诱导用户点击等，同时会利用蓝牙、手机存储卡等方式进行植入传播。更加多元化的传播方式，增加了感染手机病毒的机率，对安全防护更增加了难度。

更多的病毒传播方式为安全防护增加了极大难度

2．威胁趋势：手机病毒将继续向多元化、层次化方向倾斜。

2011 年，手机病毒将继续向多元化、层次化方向倾斜，扣费类病毒有望在 2011 年超越传统的以破坏手机运行为目的手机病毒，成为对用户威胁最大的移动安全威胁。盗号类病毒也在 2010 年底开始呈现迅猛发展势头。同时，手机病毒在此前主要针对塞班平台的基础上，今后将对更多手机系统平台构成威胁。

例如，伴随 Android 平台目前在智能机市场的占有率狂飙似的增长，以及该系统平台自身开源性较强，签名验证机制较为薄弱，和系统自身存在漏洞等原因。2011 年，Android 手机将有望成为黑客重点攻击目标。尽管 iPhone 和黑莓的操作系统由于对外接口有限开放性不够，在牺牲了手机功能的情况下，安全性得到了一定保障。但是，国内一些用户的 iPhone“越狱”版则没有任何安全性可言。也极易遭遇手机病毒威胁。

1）“盗号”类病毒将集体迸发

伴随手机应用体系的日益完善，更多的用户将通过手机运行 QQ、网银、炒股软件、Tiwitter 等。因此，账户密码的安全，将成为未来用户关注的重点。2010 年底，伴随“终极密盗”等盗号类病毒的快速增长。可以预见，基于手机端的盗号病毒将会在 2011 年集体迸发。

盗号类病毒感染用户手机后，会自动启动后台进程，通过拦截键盘记录和拆解数据包等方式盗取用户手机应用程序密码。同时，通过自动联网上传或直接通过外发短信方式进行传播，对用户造成了极大威胁。

2）“后门”程序增长迅速

利用软件存在的漏洞开启“后门”发起攻击的现象，在 2010 年末也出现了抬头趋势。塞班、Android 操作系统中存在的漏洞若未能及时修补，或未能通过安装专业手机安全软件的方式给予遏制，以及通过网络端进行封堵，将对用户的手机造成严重威胁。

“后门”程序在后台强行添加恶意代码后，利用软件漏洞上传隐私数据，并远程控制实行扣费操作，通过开通 GPS 的手机窃取用户地域位置，有针对性推广恶意广告内容等。同时存在弹出伪装提示，诱骗用户消费的行为。

同时，如网秦全球手机安全中心 2010 年底拦截的“Geinimi”后门程序，基于 Android 平台，通过植入到“入侵脑细胞”、“植物人大战僵尸”等多款流行手机游戏软件中，生成新的软件安装包后在手机论坛、手机软件下载站进行线上分发。

感染用户手机后，“给你米”（Geinimi）后门程序会自动在手机后台启动，并定期连接到“给你米”（Geinimi）网站，上传用户的位置信息，在用户不知情的情况下，自动下载各类恶意推广软件。并可能会根据所在地域，有针对性的推广各类恶意广告短信。

3）手机病毒将愈发难以发现和清除

2010 年，手机病毒更为隐蔽，如：伪装为手机常用软件，诱骗用户下载安装；以插件形式植入常用软件，在后台进行恶意行为而不影响软件正常功能；长期“潜伏”，由外来指令控制发作；清除自身痕迹等。

同时，手机病毒制作者通过代码混淆、数据加密等手段，增加病毒分析判定的难度。

另外，2010 年手机病毒已出现程序“自我保护”机制，多个威胁进程互相守护，用户安装后，无法利用系统自带卸载功能进行手工清除。

预计 2011 年，手机病毒制造者会更多的采用类似技术，使手机病毒更加难以发现和清除，将对安全厂商的技术实力和专业性做出考验，而用户若未使用专业手机安全软件，很难及时发现并有效应对手机内存在的安全隐患。

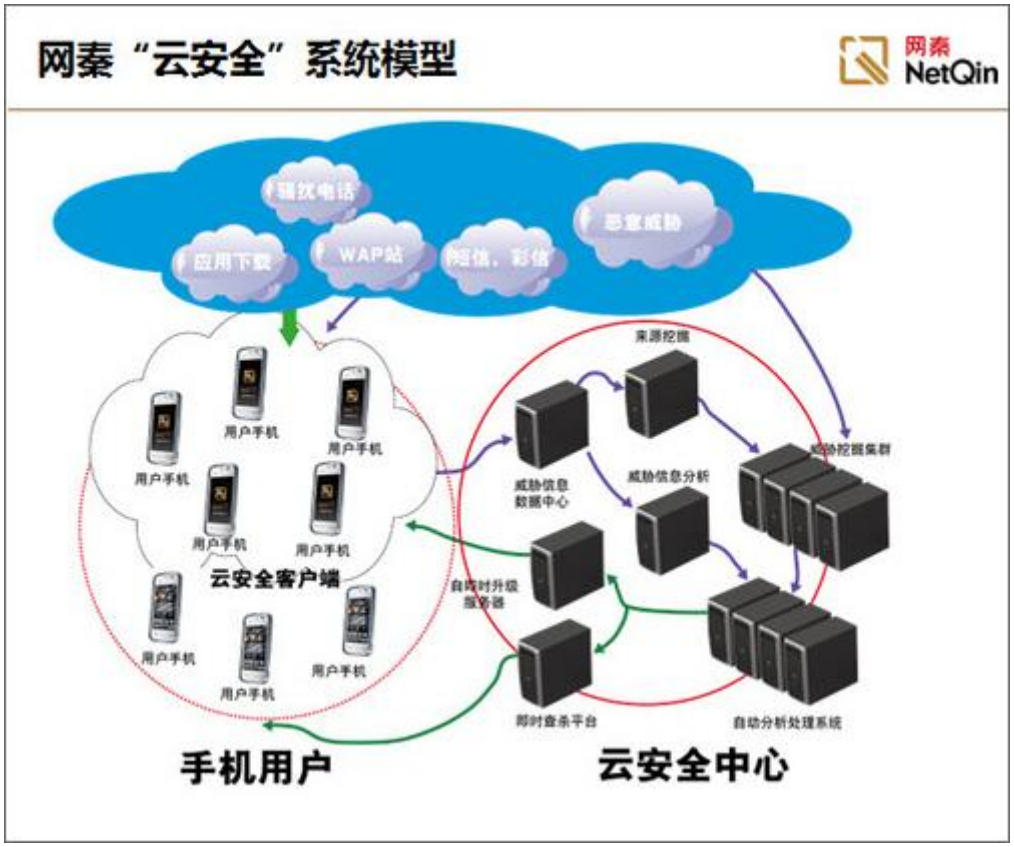
二、“云安全”分析系统的发展趋势

伴随手机病毒数量的高速增长，传统手机杀毒软件的病毒库升级方式已难以满足用户实际的反病毒需求。通过用户分享和样本集成，构筑“云安全”系统来快速识别、分析和对手机病毒进行响应，成为手机安全技术新的发展趋势。

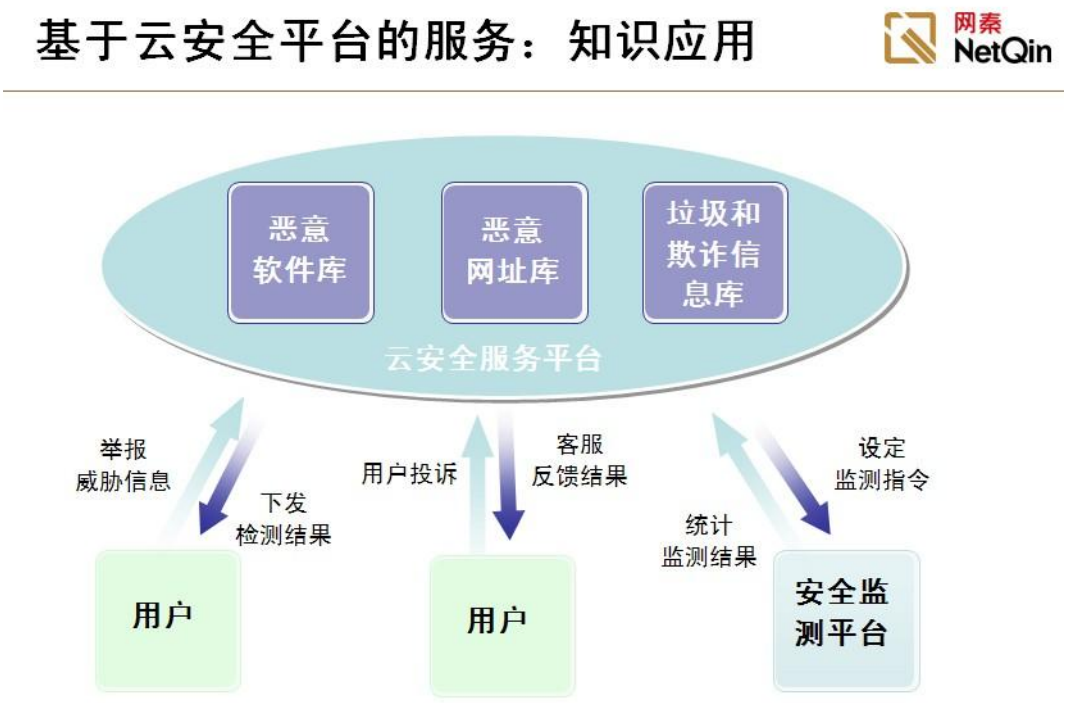
当前，网秦“云安全”数据分析中心已实现在得到用户授权同意的前提下，及时收集用户上传的安全威胁，并对病毒行为智能分析方式作出反应，快速同步返回到手机安全端和手机用户实现共享。

同时，2011 年，网秦“云安全”数据分析中心在已为网秦手机杀毒、网秦手机卫士提供云端数据支持的基础上，还将对网秦通讯管家产品提供支持。将增加更多的“云安全”分析介入端，增加垃圾短信、骚扰电话库等内容，并对通讯类软件安全提供保障。

随着网秦和中国移动、中国电信、相关手机厂商等合作伙伴业务的开展，也将进一步提供网秦“云安全”系统接口，和亿万手机用户同享网秦“云安全”数据分析中心的数据资源。



网秦“云安全”安全威胁分析系统模型



基于“云安全”技术的网秦手机安全服务平台

三、手机反病毒技术的发展趋势

手机病毒当前已实现通过代码混淆等方式，对专业安全厂商的病毒分析增加了难度、并极大拖慢了响应速度。传统简单的分析方式，已无法实现对手机病毒有效查杀。针对手机病毒的发展趋势，专业安全厂商也在不断促进技术革新。

1.病毒行为亟待智能判定

未来的病毒分析技术，也将向更为自动化和智能化的方向发展，如面临手机病毒感染率持续上升的情况，面对大量待分析数据，如何通过智能分析系统快速分类判定，成为安全厂商的研究课题。

2.行为分析技术攻克代码混淆难题

由于手机病毒通过代码混淆等手段提升分析难度、隐蔽其威胁行为，传统的分析手段较难准确定位恶意行为，需要模拟程序在实际运行中的状态，通过捕捉和分析程序的行为来对程序安全性进行判定。

3.全生态系协同防护

随着移动互联网的发展，手机病毒除了会给手机终端带来威胁，也会给运营商网络带来较大的压力。同时，手机软件来源的渠道日益丰富，开放的下载网站以及各种应用商场等会成为重要的病毒传播源。因此，需要打造一个针对病毒传播源（包括应用程序开发者，网站等）、病毒传播渠道（网络）、以及病毒最终目标对象（智能终端）的全生态系的全方位防护，从而更有效的应对手机病毒威胁。

附录 2010 网秦大事记

2010 年 11 月 国际知名的调研公司赛诺（SINO Marker Research Ltd）发布了 2010 年第三季度《中国手机安全市场调研》。根据实际激活用户数的市场份额，网秦以 4041 万的激活用户，65.1%的市场份额排名第一，全面领先手机安全市场。

2010 年 11 月 网秦全新推出基于 Andorid 平台的网秦手机卫士产品，其不仅拥有全新一键优化功能，可以有效降低耗电，并且贴心的流量监控能让用户随时查看计费周期内 GPRS 和 WIFI 所花费的流量，防止流量超额。

2010 年 11 月 中国科学院心理研究所公布了 2010 年《智能手机用户对手机安全威胁的感知与应对行为》调研结果，网秦系列产品以 55.7%的用户满意度和低于 41%的流失率排名第一，全面领先市场。

2010 年 10 月 网秦以总排名第 9 入选德勤“2010 高科技、高成长中国 50 强”。

2010 年 10 月 网秦手机杀毒 v4.0 S60 3rd S60 5th 英语版全球上市。

2010 年 10 月 网秦迎来 5 周年生日，旗下手机杀毒、通讯管家、手机卫士三款产品都推出五周年纪念版，与用户共同见证 5 年辉煌。

2010 年 9 月 网秦被《美国时代周刊》评价为“可以改变人们未来生活的十大创新企业之一”。

2010 年 9 月 网秦被世界经济论坛评选为夏季达沃斯 2011“科技先锋” (Technology Pioneer 2011)。

2010 年 8 月 网秦通讯管家 iPhone 1.0 全新上市，这是国内首款基于 iPhone 平台的手机安全软件。也是网秦继覆盖 Android、Symbian、Windows Mobile 主流手机操作系统之后的又一领军之作。

2010 年 8 月 国际知名的调研公司 Frost & Sullivan 发布了 2010 年上半年的《中国手机安全市场白皮书》。白皮书显示，网秦占据国内 64.8%排名第一，已成为手机安全最大服务商。

2010 年 8 月 网秦推出了新一代手机安全产品——“网秦手机杀毒 v4.0”。该产品独创的“云+端”双引擎查杀，使其成为全球查杀速度最快的手机杀毒软件之一。

2010 年 6 月 网秦手机卫士 v2.6 世界杯纪念版推出，它加入了“云查杀”功能，为用户提供更高级别的在线安全检测，带来更全面的软件安全防护！

2010 年 4 月 网秦手机杀毒 v3.2 正式推出了包括英、俄、意、西、葡、法、德、阿在内的八种语言版本，以适应全球范围内的用户需求。

2010 年 1 月 网秦荣获第二届易观 EnfoNet Award 移动互联网奖-最佳服务提供商奖，最具发展潜力奖。

2010 年 1 月 网秦手机杀毒 3.0 英文版全球公开发布。