3 “您的手机安全吗？”—移动互联网安全监测情况

2010 年是 3G 网络迅速发展的一年，移动互联网智能终端迅速普及，应用程序日益丰富，生产成本不断降低，手机上网已经成为人们生活中随处可见的一景。当您在享受移动上网带来的便利与高效时，您是否意识到智能手机也面临着严重的安全威胁？

伴随着互联网与移动网络的界限日渐模糊，互联网的安全问题也在移动网络中逐步突显。移动智能终端漏洞日益增多，恶意代码已开始出现并在移动互联网内快速蔓延，并被用于窃取用户的个人隐私信息、恶意订购各类增值业务或发送大量垃圾短信。

3.1 移动互联网恶意代码监测情况

2010 年 CNCERT 抽样监测结果显示，境内感染“毒媒”手机木马的用户达 2003515 个，感染“手机骷髅”病毒的用户达 831843 个，感染“FC.MapUp.A”手机病毒的用户达 216147 个，感染“Boothelper.A”手机病毒的用户达 1431 个。

■ “毒媒”

2010 年 9 月初，一种名为“毒媒”的手机木马悄然出现并大肆传播。“毒媒”是一种针对 Symbian S60 系统的手机木马，会影响 Symbian S60 系列第 3 版和第 5 版操作系统的手机，诺基亚大部分智能手机都使用该操作系统。

CNCERT 通过对该木马进行监测和深入分析发现，黑客通过互联网上的一台控制服务器秘密控制着大量感染了该木马的手机，不仅可以收集用户手机的信息，还会卸载手机上的其它程序，包括手机杀毒软件等，并指挥手机向外发送短信和在收藏夹加入广告网址诱惑用户点击等。不仅如此，由于该木马可以接受黑客的控制指令，感染手机只要开机就会被黑客控制，所以形成了一个类似于传统互联网僵尸网络的移动互联网僵尸网络。2010 年 CNCERT 监测感染“毒媒”的手机用户按地区分布情况如图 3-1 所示，从“毒媒”的感染地区分布情况可以看出，广东省、福建省等沿海发达省区及河北省、江苏省等人口大省是移动互联网恶意代码感染密集的地区。

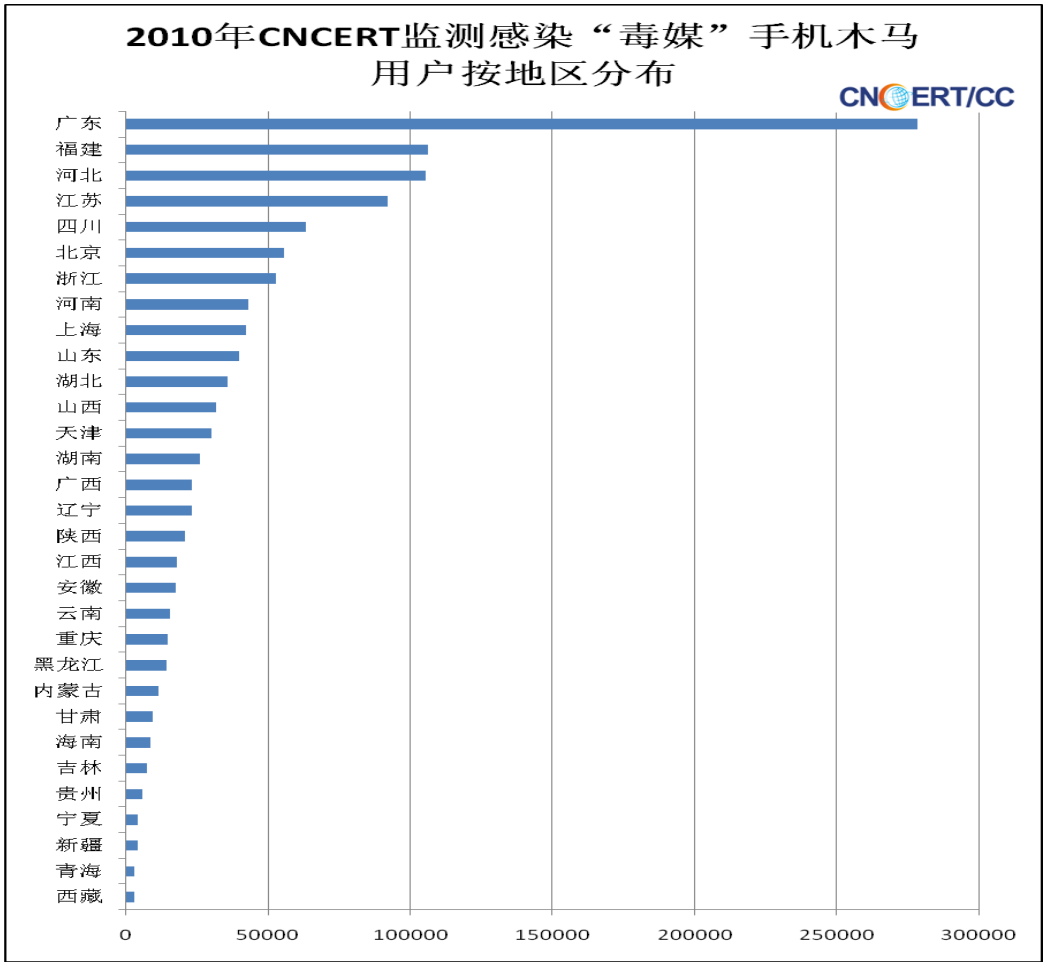

图 3-1 2010 年 CNCERT 监测感染“毒媒”手机木马的用户按地区分布

CNCERT 在对“毒媒”手机木马开始监测的第一周，发现境内有近 100 万部智能手机被其控制。随后，CNCERT 联合运营商、域名注册机构等相关单位对其进行了专项处置，11 月，“毒媒”手机木马的感染数量下降至 40 万部左右，并呈逐步下降趋势。截至 2010 年底最后一周，仅存 17 万部智能手机被感染，如图 3-2 所示。

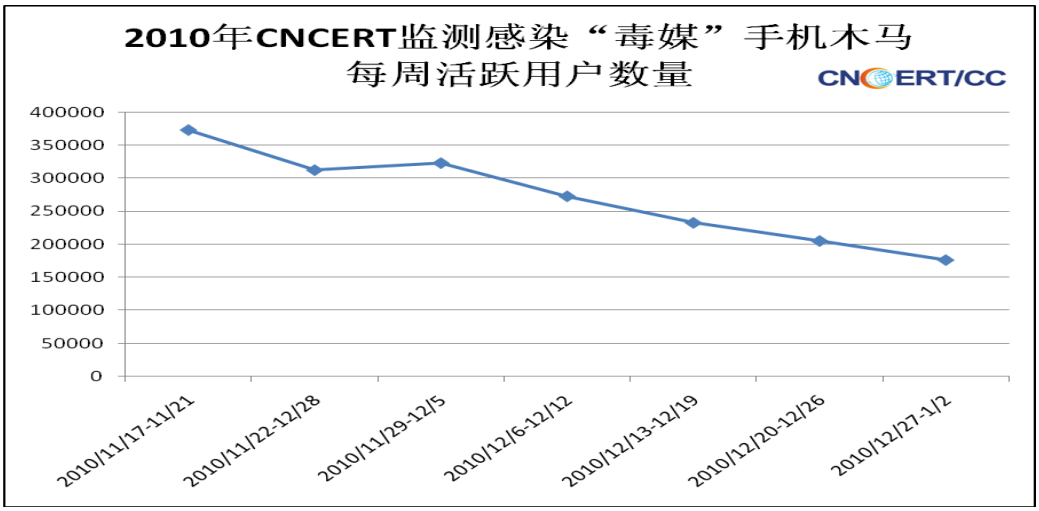

图 3-2 2010 年 CNCERT 监测感染“毒媒”手机木马的每周活跃用户数量

尽管如此，“毒媒”手机木马仍然可以给用户造成了巨大的安全威胁和经济损失。在巨大利益驱使下，黑客将可能继续对智能手机采取更多、更复杂的渗透和控制，境内移动互联网安全状况不容乐观。

■ “X 卧底”

2010 年 8 月，一款名为“X 卧底”的手机木马再次引起了 CNCERT 的注意。“X 卧底”由国外 Vervata 公司开发，2006 年 7 月被南京特洛伊科技有限公司引进中国。南京市国家安全局于 2007 年 7 月 17 日认定“X 卧底”为间谍器材，并查封了南京特洛伊科技有限公司。2008 年 3 月 18 日，特洛伊科技有限公司搬迁至泰国，服务总部设立到香港，继续传播该间谍软件。

“X 卧底”可以被安装到大部分智能手机上，运行后可记录被感染手机收发的所有短信、通话记录、联系人、联系时间等内容，甚至还可通过手机内置的 GPS 功能记录手机所在的地理位置，并将这些数据自动上传到控制者指定的服务器。同时，“X 卧底”还可以实现远程窃听的功能，只要控制者通过预先设置的“控制号码”拨打感染了“X 卧底”间谍软件的手机，该手机就可以在屏幕没有任何提示的情况下自动接通并监听麦克风进行窃听。此外，“X 卧底”软件在手机内安装激活之后完全隐形，手机菜单及已安装的程序列表中均不可见，具有很强的隐蔽性。

尽管早已经被国家有关部门查封，但根据 CNCERT 监测发现，2010 年“X 卧底”的通信记录累计达 79 万余条，可见其在国内的活动仍然十分频繁。

由于手机恶意代码可以带来比计算机恶意代码更大的经济利益，而且手机中往往包含有更多的用户隐私信息，与用户关系更为紧密，因此编写和散播手机恶意代码将更受黑客所青睐，加之用户在使用手机时的安全意识非常薄弱，移动互联网面临的安全问题将比传统互联网更为严峻。

3.2通报成员单位报送情况

■ 手机病毒样本捕获情况

根据网秦公司[1]监测结果，2009 至 2010 年手机病毒进入高速增长时期。截止到 2010 年底，网秦公司在国内累计截获手机病毒样本 2517 个，较去年增长

[1] 网秦公司即北京网秦天下科技有限公司，是通信行业互联网网络安全信息通报工作单位。

195%，具体如图 3-3 所示。

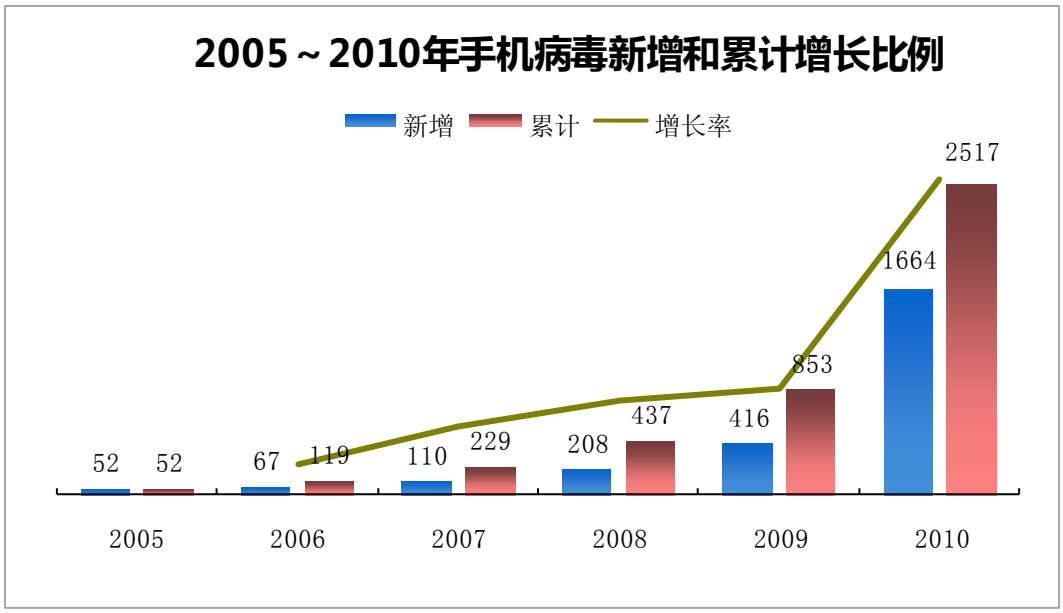

图 3-3 2005-2010 年手机病毒新增和累计增长比例

■ 手机病毒感染量区域排行

根据网秦公司监测数据，2010 年手机病毒感染区域分布如图 3-4 所示，广东省以 21%的感染比例，成为手机病毒的感染重灾区，北京市、福建省分列二、三位。

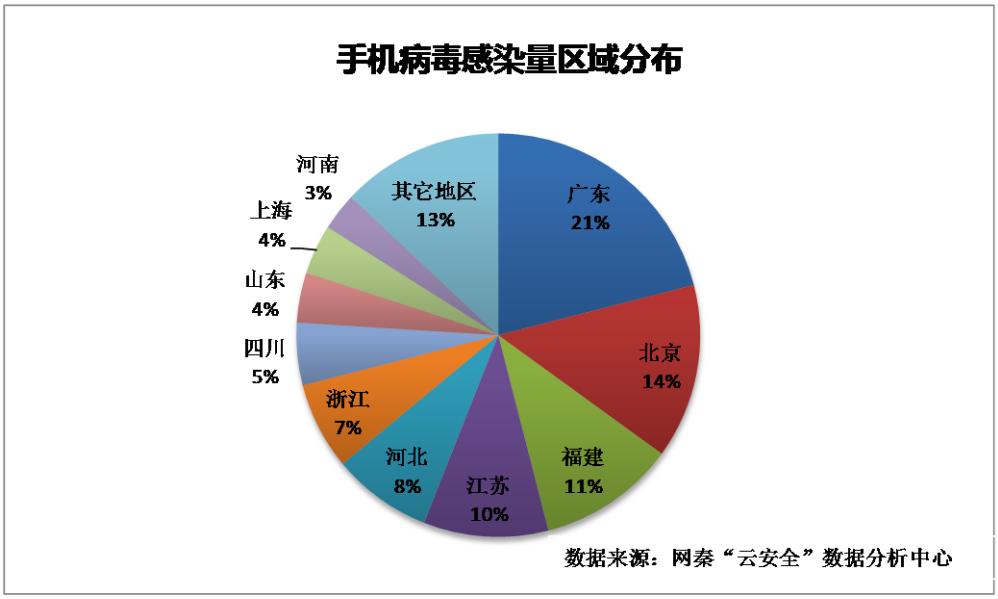

图 3-4 2010 年感染手机病毒用户分布图

我国东南沿海地区移动互联网发展迅速，智能手机保有量也保持领先，因此

在享受更丰富的手机应用的同时，用户也面临着更大的手机病毒威胁。例如，在2010 年上半年“手机骷髅”病毒肆虐和 2010 年下半年“毒媒”手机木马大规模爆发期间，上述省份的被感染手机用户量都位居前列。

■ 手机病毒行为类型分析

2010 年，手机病毒的行为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，再演变至盗取手机软件的账户密码、开启后门、窃取用户信息等。同时，手机病毒也出现了一个病毒同时存在多个行为的现象，对用户的手机安全造成了极大威胁。

根据网秦公司监测数据，2010 年截获的手机病毒中，扣费行为类的手机病毒达到 1062 个（其中恶意扣费行为类的手机病毒 498 个，资费消耗行为类的手机病毒 564 个），窃取用户隐私行为类的手机病毒 366 个，盗号木马病毒 12 个，手机流氓软件 142 个，欺诈软件 87 个和后门软件 102 个。此外，有 104 个手机病毒存在破坏手机数据的现象，有 1407 个手机病毒存在破坏手机系统的现象，以及有 38 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）。2010 年新增手机病毒的行为类型如图 3-5 所示，其中存在恶意扣费行为的手机病毒从去年的 265 个快速增长到 1062 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。后门软件在 2010 年末出现了增长趋势。

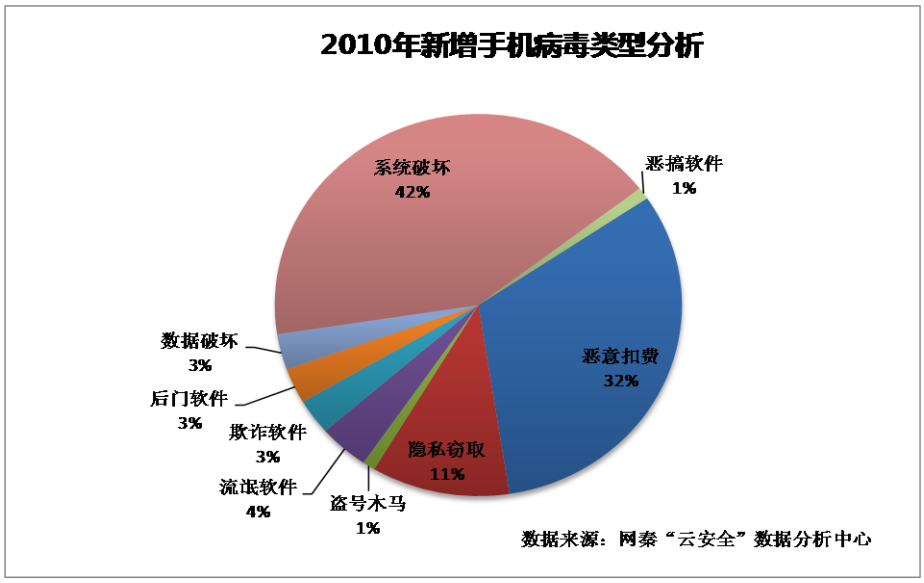

图 3-52010 年新增手机病毒行为类型分析

2010 年新增手机病毒的扣费方式如图 3-6 所示。扣费类病毒感染用户后，45%的病毒以恶意订购 SP 服务的方式扣取用户费用,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来进行扣费,12%的病毒通过发送彩信消耗用户费用,6%的病毒以其它方式，如“自动拨号”等方式扣费。

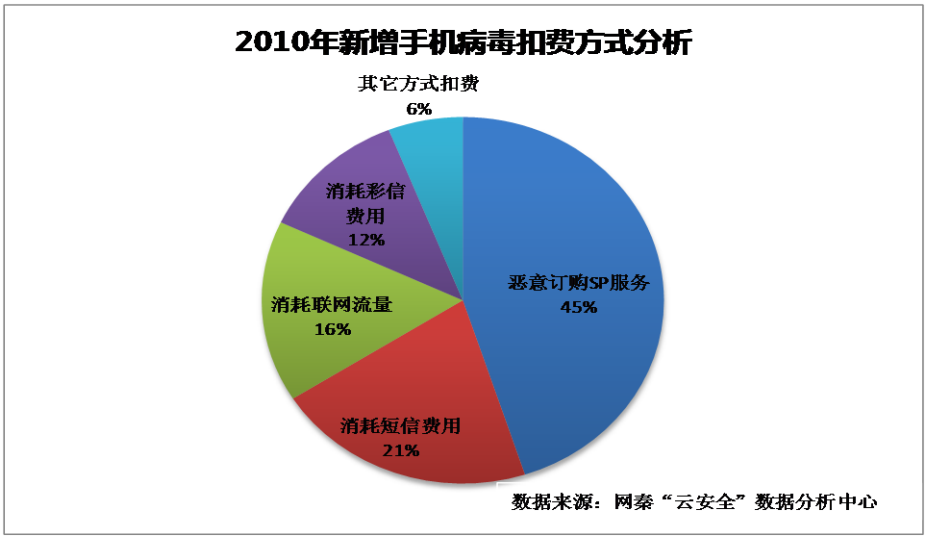

图 3-6 2010 年新增手机病毒扣费方式分析

■ 手机病毒传播途径分析

根据网秦公司监测数据，2010 年手机病毒主要传播途径如图 3-7 所示。从图中可以看出，通过手机访问 wap 和 www 网站感染病毒的比率高达 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。

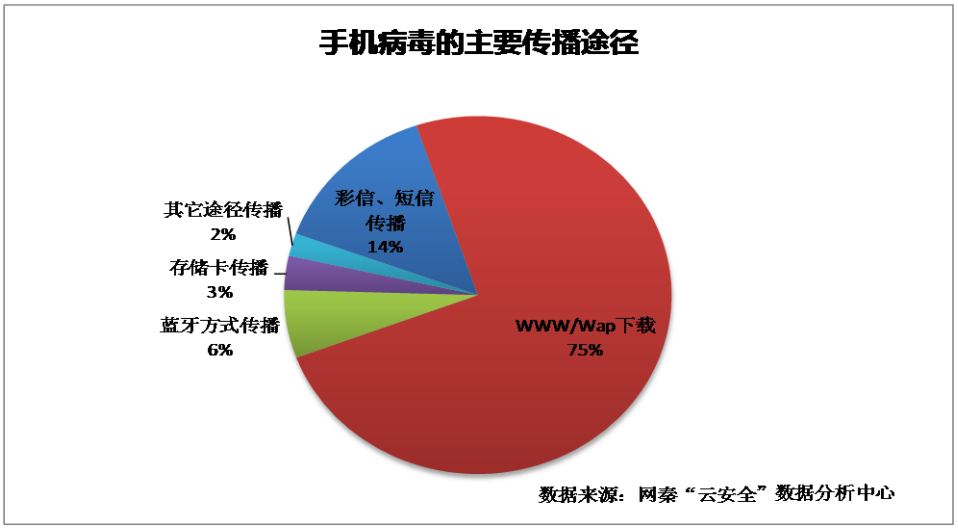

图 3-7 2010 年手机病毒主要传播途径分析

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，网秦公司累计截获伪装为常用程序的手机病毒 56 个，以 “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，据网秦公司数据统计，手机软件下载网站当前也大多存在严重的安全风险。网秦公司选取了 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，部分网站的手机软件资源染毒率高达 57%以上。可见用户即使通过下载网站下载手机软件，也极易感染手机病毒。

■ 手机病毒感染平台分析

伴随手机病毒的快速增长和传播范围的增加，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 平台仍是黑客的攻击重点，但随着“给你米”（Geinimi）等后门程序的相继出现，Android 平台的安全威胁正高速增长，感染比例也在持续上升。

根据网秦公司监测数据，2010 年手机病毒平台分布情况如图 3-8 所示。截至 2010 年 12 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。

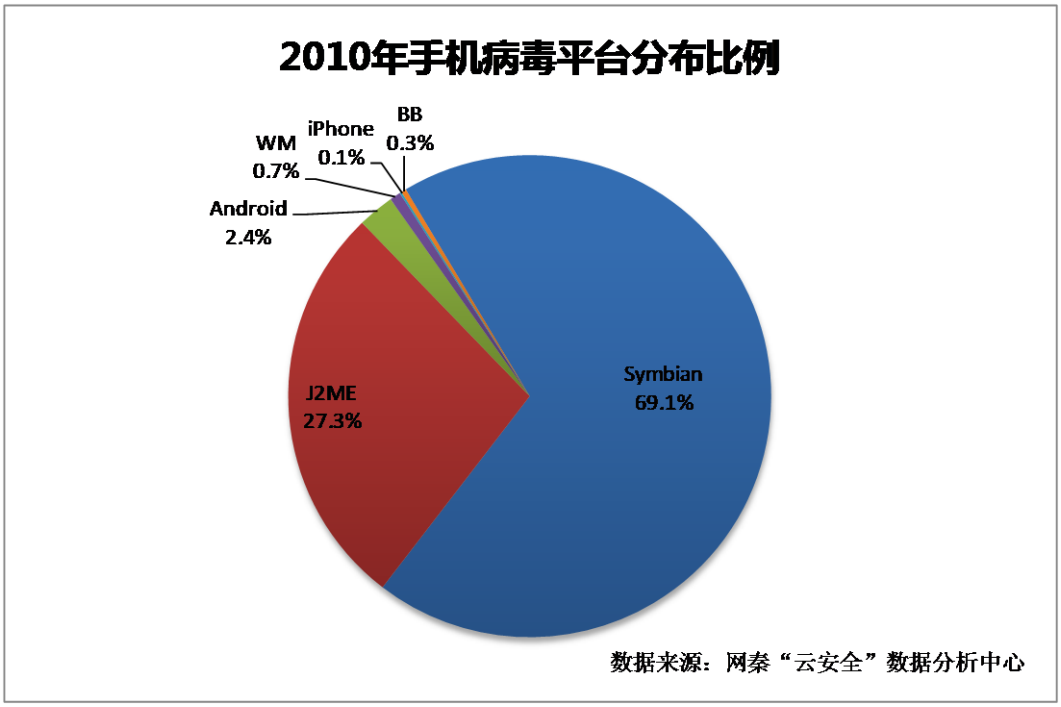

图 3-8 2010 年手机病毒平台分布比例