3 移动智能终端恶意程序传播和活动情况

2011 年移动互联网迅速发展，手机网民数量不断增长，移动互联网恶意程序数量和感染规模也在不断提高。恶意程序已经严重威胁到用户的切身利益和移动互联网的健康发展。工业和信息化部于 2011 年 11 月出台《移动互联网恶意程序监测与处置机制》，进一步加强移动互联网安全监管工作。CNCERT 持续对移动互联网进行安全监测，根据监测结果，2011 年国内移动互联网安全事件数量呈现增长趋势。

3.1移动互联网恶意程序监测情况

移动互联网恶意程序是指运行在包括智能手机在内的具有移动通信功能的移动终端上，存在窃听用户电话、窃取用户信息、破坏用户数据、擅自使用付费业务、发送垃圾信息、推送广告或欺诈信息、影响移动终端运行、危害互联网网络安全等恶意行为的计算机程序。移动互联网恶意程序的内涵比手机病毒广的多，如手机吸费软件不属于手机病毒，但属于移动互联网恶意程序。

2011 年 CNCERT 捕获移动互联网恶意程序 6249 个，其中有控制域名的 3060 个，占 49.0%。

ANVA 成员单位报送移动互联网恶意程序样本及分析报告 1674 个, 其中有控制域名的 878 个，占 52.5%。

■ 总体情况

2011 年 CNCERT 捕获移动互联网恶意程序按行为属性统计如图 3-1 所示。

具有恶意扣费行为的恶意程序最多，达到 1317 个，占 21.1%。恶意扣费指在用户不知情或未授权的情况下，通过隐蔽执行、欺骗用户点击等手段，订购各类收费业务或使用移动终端支付，导致用户经济损失的恶意行为。有两种典型的恶意扣费程序，一种是恶意程序在后台向某些移动增值业务服务商（以下简称 SP）发送业务订购短信，并拦截 SP 返回的扣费提示短信，达到替用户订购增值业务的目的，黑客通常可以从不法 SP 处分成获利；另一种是恶意程序定期在后台联网，访问黑客指定的广告页面，达到为广告商带去大量点击流量的目的，黑客也可以与这些不法的广告商进行分成。由于有经济利益的诱惑，大量黑客参与此类恶意程序的开发，严重危害广大移动互联网用户的经济利益。

具有恶意传播行为的恶意程序为 1235 个，占 19.8%，排名第二；排名第三的是具有信息窃取行为的恶意程序，达 1180 个，占 18.9%。这类恶意程序会将被感染用户的手机号码、手机型号、短信内容、通讯录内容、用户所在位置的 GPS 坐标等信息发送到黑客手里，不仅严重侵犯了用户隐私，而且这些信息可能会被恶意利用，造成进一步的损失。

此外，远程控制、资费消耗、系统破坏、诱骗欺诈等恶意行为也会不同程度地侵害用户利益。

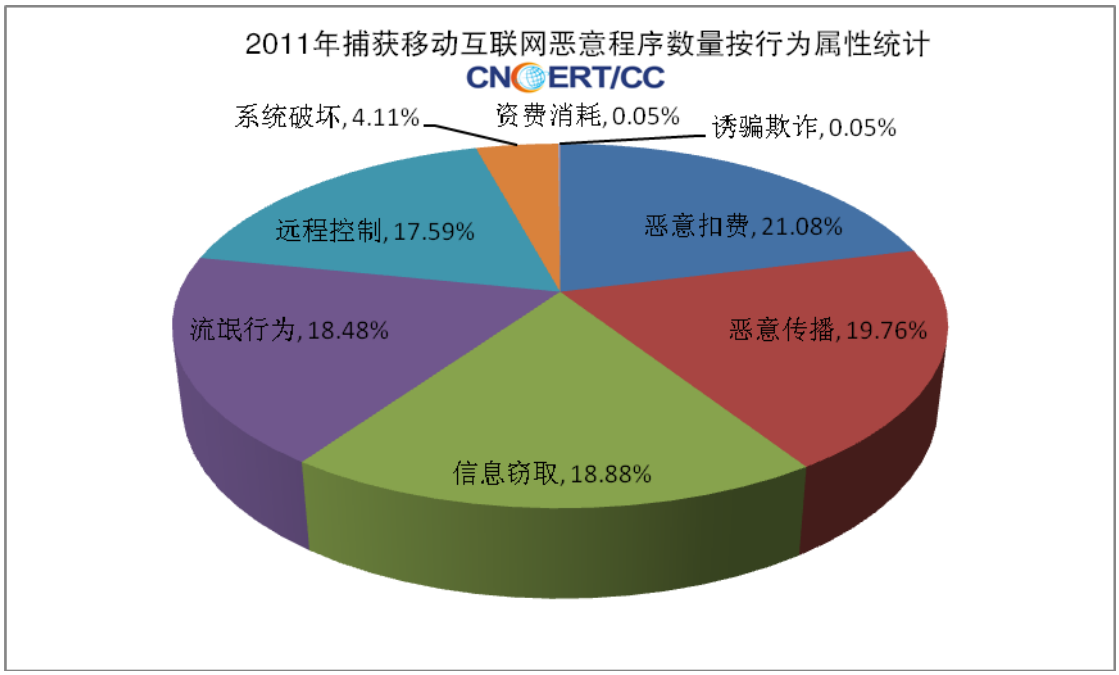

图 3-1　2011 年 CNCERT 捕获移动互联网恶意程序数量按行为属性统计

按操作系统统计，目前 CNCERT 捕获的主要是 Symbian 和 Android 平台恶意程序。其中，Symbian 平台恶意程序 3792 个，Android 平台恶意程序 2456 个。Symbian 平台由于当前有大量用户使用，感染该平台的恶意程序最多，占 60.7%。Android 平台上的恶意程序增长迅速，目前已经占到 39.3%。增长较快的原因一方面是由于 Android 平台的开放性在为程序开发人员提供便利的同时也使黑客易于掌握并编写恶意程序；另一方面，Android 用户的迅速增长使其成为黑客重点关注的攻击目标。2011 年 CNCERT 捕获的移动互联网恶意程序数量按操作系统统计如图 3-2 所示。

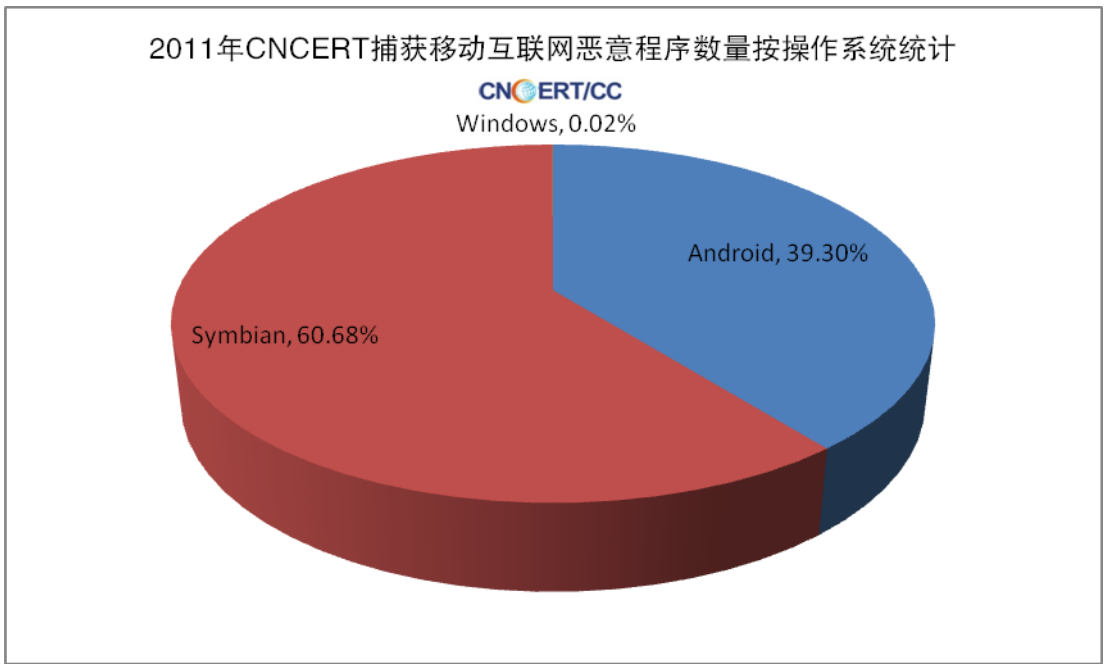

图 3-2　2011 年 CNCERT 捕获移动互联网恶意程序数量按操作系统统计

如图 3-3 所示，按危害等级统计，2011 年 CNCERT 捕获高危移动互联网恶意程序 2544 个，占 40.7%；中危移动互联网恶意程序 2445 个，占 39.1%；低危移动互联网恶意程序 1260 个，占 20.2%。可以看出，大部分移动互联网恶意程序都具有严重的危害性。

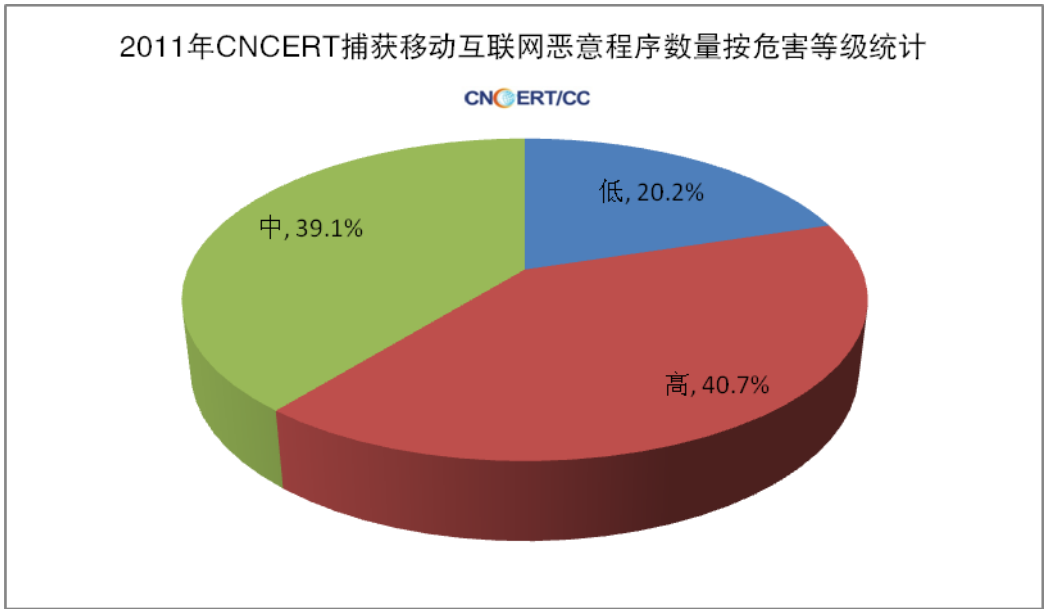

图 3-3　2011 年 CNCERT 捕获移动互联网恶意程序数量按危害等级统计

2011 年 11 月 18 日，工业和信息化部印发《移动互联网恶意程序监测与处置机制》（工信部保[2011]545 号）文件。这是工业和信息化部首次出台移动互联网网络安全管理方面的规范性文件，引起了业界的广泛关注。

《移动互联网恶意程序监测与处置机制》规定，依据《移动互联网恶意程序

描述规范》行业标准开展移动互联网恶意程序的认定和命名工作，由各单位对恶意程序样本进行初步分析，并将信息汇总到 CNCERT，由 CNCERT 统一认定和命名。移动通信运营企业负责本企业网内恶意程序的样本捕获、监测处置和事件通报，CNCERT 负责恶意程序跨网监测、汇总通报和验证企业处置结果。

工业和信息化部作为互联网行业主管部门，肩负维护公共互联网安全、保护用户利益的职责。今年将进一步加强移动互联网恶意程序治理工作，指导移动通信运营企业、安全企业、域名服务机构、科研机构等相关方合力净化移动互联网环境。

下面介绍几个 CNCERT 在 2011 年重点关注和监测的移动互联网恶意程序：

■ “毒媒”手机病毒监测情况

2010 年 9 月，“毒媒”手机病毒开始大肆传播，CNCERT 对其进行了持续的监测和处置。经过多次打击，“毒媒”手机病毒感染用户数量从最初的每月 100 多万个，到 2010 年底约 40 万个，2011 年 3 月以后被感染用户数均维持在每月 5 万个左右，治理工作取得了一定的效果。2011 年 5 月初，大量被“毒媒”手机病毒控制的移动终端向某运营商分公司业务网站发起拒绝服务攻击，造成该网站一度瘫痪。由于黑客仍在不断变换控制域名和升级病毒以逃避打击，2011 年全年仍有 666396 个用户感染“毒媒”手机病毒,感染用户数按月度统计如图 3-4 所示。

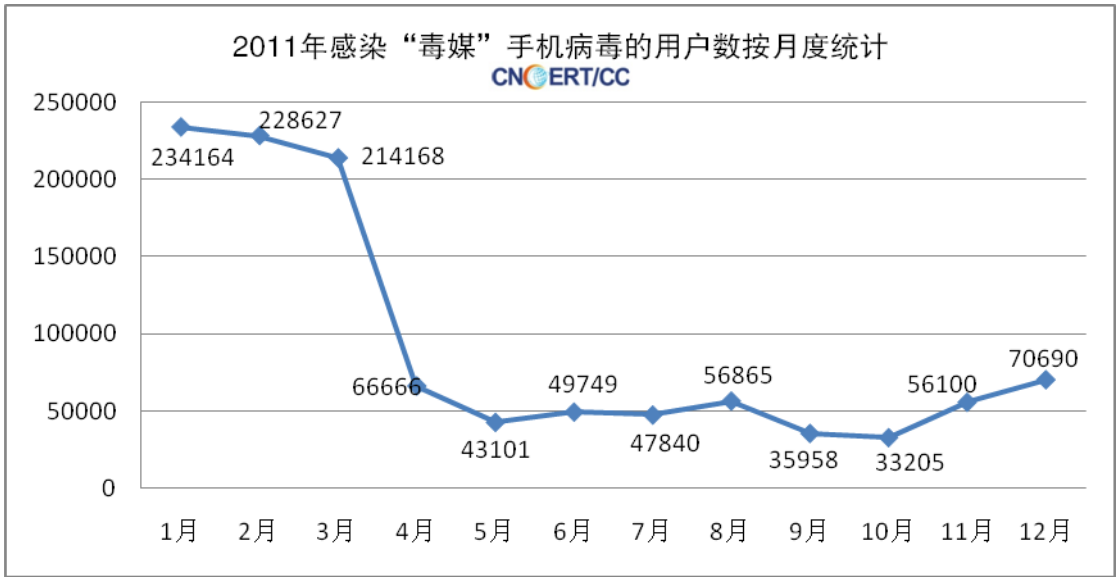

图 3-4　2011 年感染“毒媒”手机病毒的用户数按月度统计

■ “X 卧底”手机病毒监测情况

“X 卧底”手机病毒由于具有窃听功能而备受关注，CNCERT 也对其进行了持续监测。从监测结果来看，“X 卧底”手机病毒在境内的活动仍然非常频繁，平均每月均有 10 万至 20 万次通信活动，最少的时候也有近 5 万次，可见其仍然具有较大的危害性，如图 3-5 所示。感染“X 卧底”手机病毒的用户信息有被泄漏的风险。

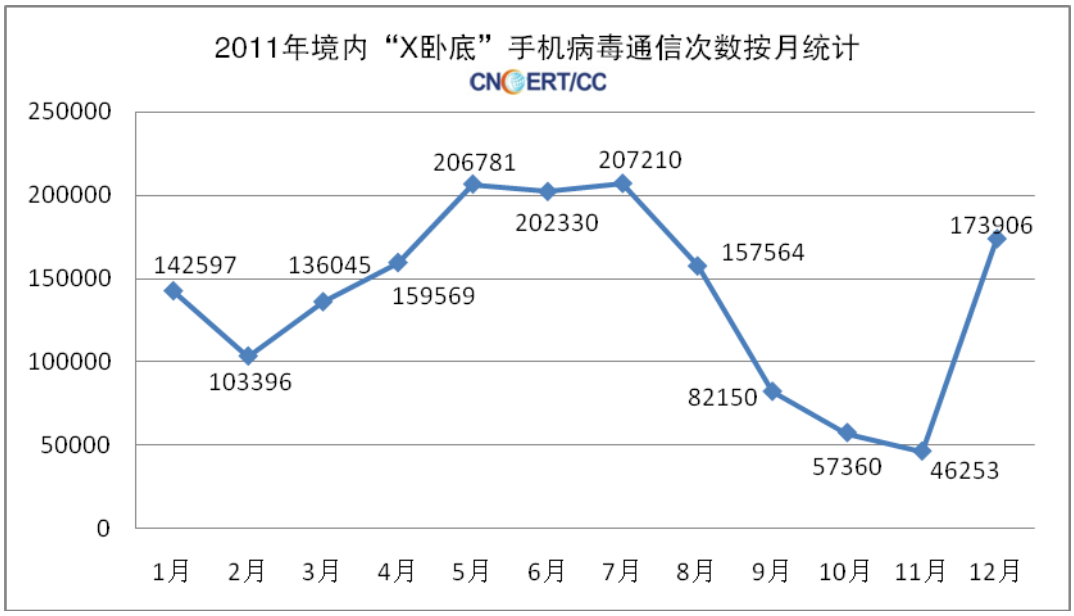

图 3-5　2011 年境内“X 卧底”手机病毒通信次数按月统计

■ “手机骷髅”病毒监测情况

“手机骷髅”病毒自 2010 年爆发以来，经过 CNCERT 联合运营商进行多次打击，感染数量已经不大，但根据监测结果，在 2011 年 9 月起，感染数量又有急剧的上升，据分析认为是病毒出现新的变种，开始大肆传播，感染用户数量最高达 6 万余个，如图 3-6 所示。

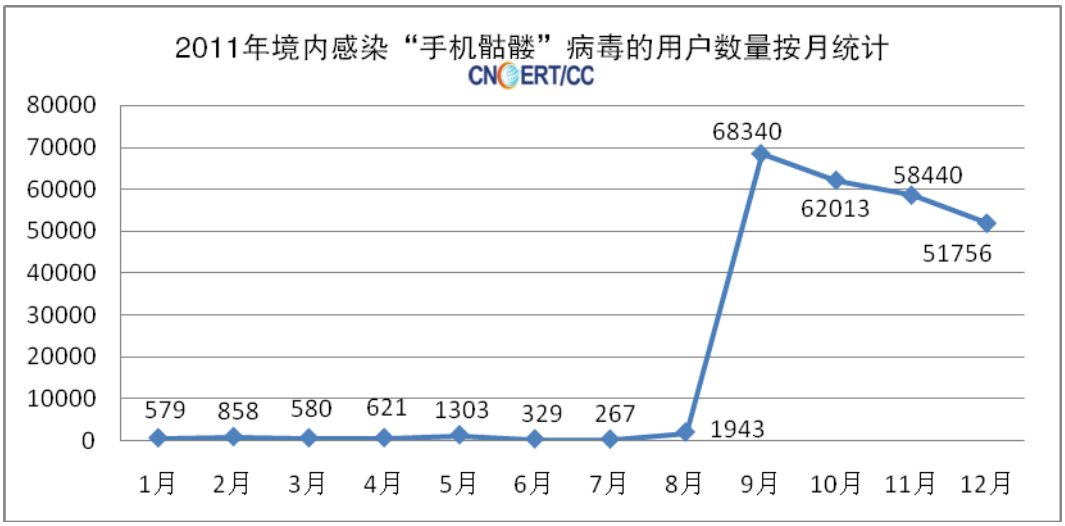

图 3-6　2011 年境内感染“手机骷髅”病毒的用户数量按月统计

■ a.privacy.sndapps.a 手机病毒监测情况

a.privacy.sndapps.a 手机病毒于 2011 年 7 月中旬首次捕获，感染后会在后台秘密获取用户手机号码、IMEI 号码、谷歌帐号等隐私信息，并联网发送到 http://www.typ3studios.com/android_notifier/notifier.php，从而窃取用户信息。从图 3-7 监测数据可以看出，该病毒每月均有数千次通信活动，最高时达到近万次。

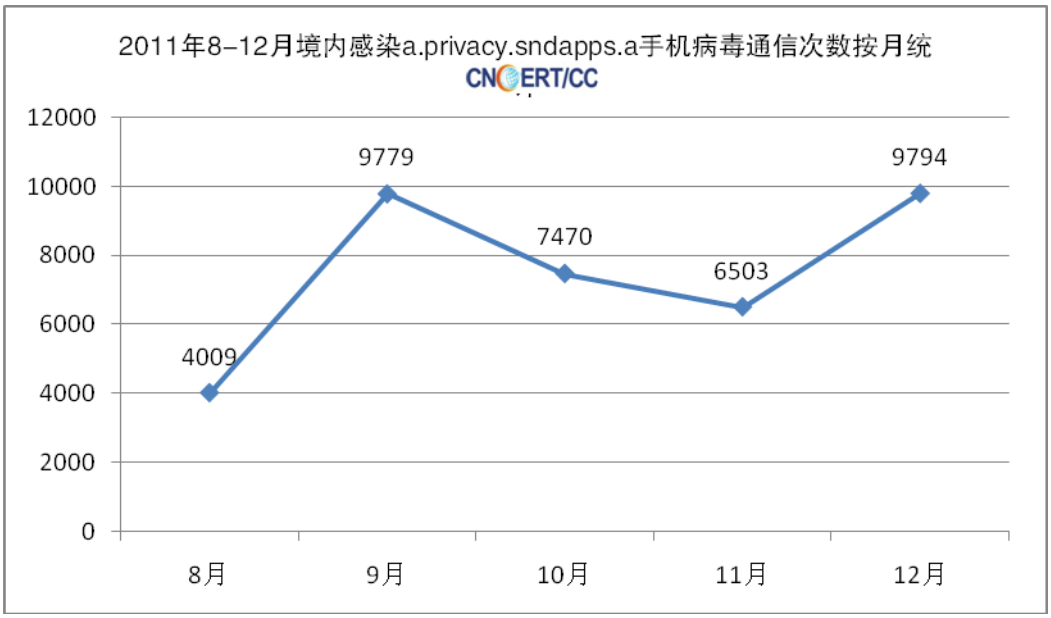

图 3-7　2011 年 8-12 月境内感染 a.privacy.sndapps.a 手机病毒通信次数按月统计

■ a.remote.adrd.a 手机病毒监测情况

a.remote.adrd.a 手机病毒最早被发现嵌入一款 Android 系统的动态壁纸软件

中，后来又发现了其嵌入其它多个应用软件中的变种。感染该恶意程序的手机，会每 6 小时向控制服务器 http://adrd.taxuan.net/index.aspx 提交一次被感染手机的 IMEI 号码、IMSI 号码、手机型号等信息，并接收服务器返回的指令；然后访问一台数据服务器 http://adrd.xiaxiab.com/pic.aspx 获取一个 URL 列表，并依次访问这些 URL 链接；最后该恶意程序还会根据控制服务器返回的指令获取一个病毒更新程序保存到/sdcard/uc/myupdate.apk。根据对该恶意程序行为的深入分析，发现其目的是为了通过点击 URL 链接为其带去广告流量，提高广告点击数或网站访问次数进而获利。

a.remote.adrd.a 手机病毒自 2011 年 8 月发现以来传播广泛，最高时有 1600 万余次通信活动，如图 3-8 所示。由于该病毒可以通过接收控制服务器指令进行一系列操作，除了目前控制用户手机联网消耗一定流量外，还可能进一步造成用户信息泄漏等损害，危害较大。

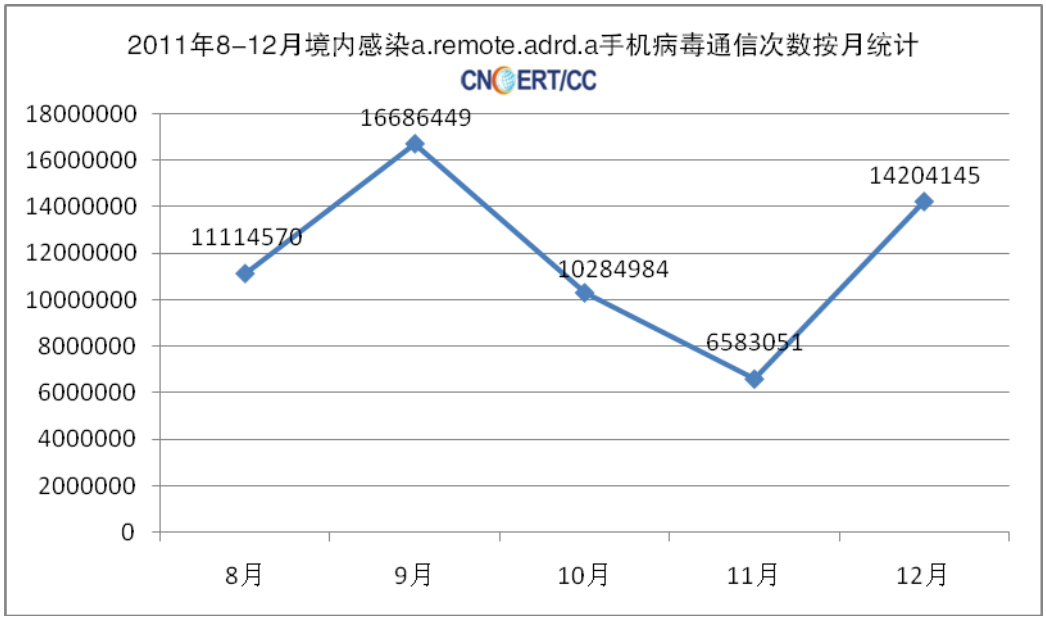

图 3-8　2011 年 8-12 月境内感染 a.remote.adrd.a 手机病毒通信次数按月统计

■ s.remote.botsms.a 手机病毒监测情况

s.remote.botsms.a 是一个典型的手机僵尸网络恶意程序，被用来大量发送垃圾短信和彩信。感染该病毒的手机将接收控制服务器指令，从控制服务器获取最新的垃圾短信和彩信内容，然后向外大量发送。该行为在制造大量垃圾信息的同时，也会给用户带来一定的经济损失。据 CNCERT 的监测数据，2011 年该手机病毒通信次数统计情况如图 3-9 所示，各月数据波动较大，最高时有 56 万余次通信活动。

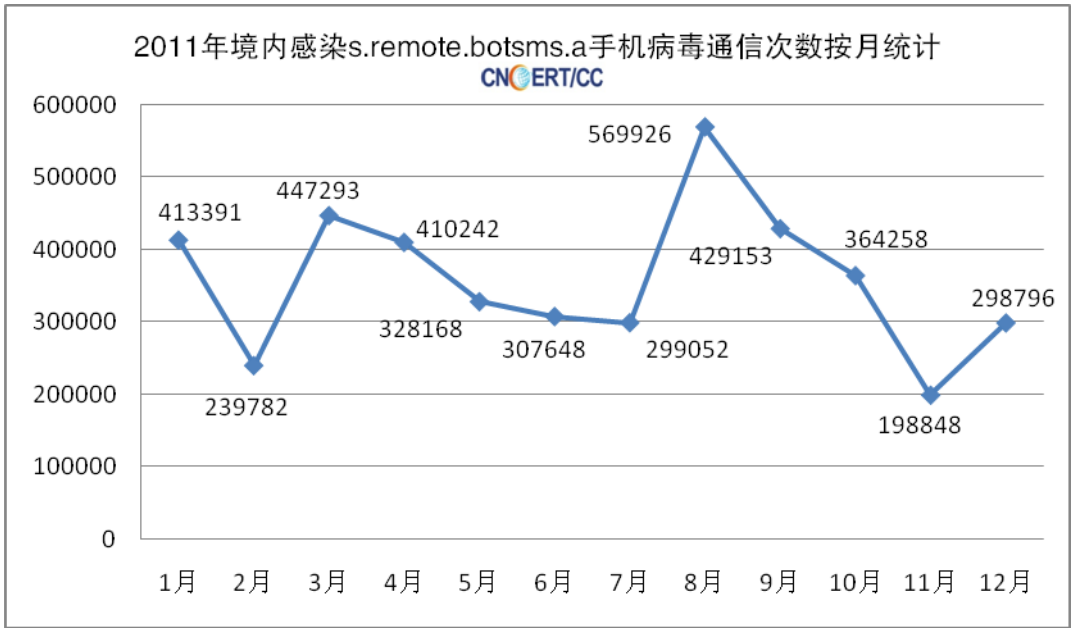

图 3-9　2011 年境内感染 s.remote.botsms.a 手机病毒通信次数按月统计

■ s.privacy.infostealer.a 手机病毒监测情况

专门窃取用户信息的手机病毒 s.privacy.infostealer.a 感染用户数量平均每月在 20 万左右，对用户隐私信息构成了极大的危害，如图 3-10 所示。

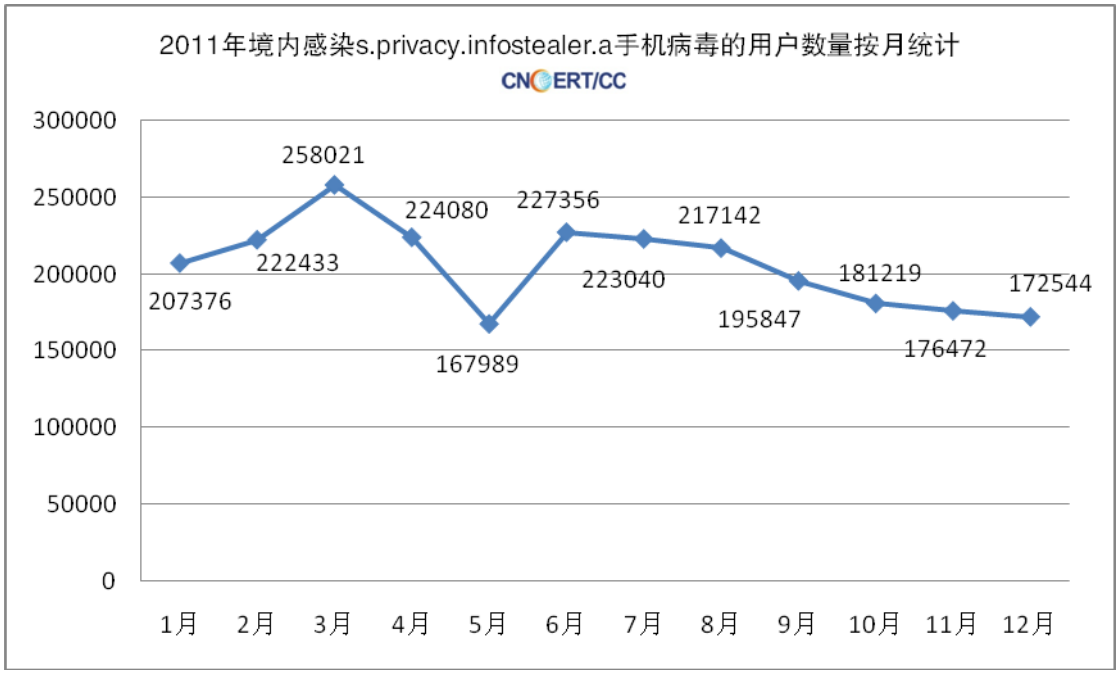

图 3-10　2011 年境内感染 s.privacy.infostealer.a 手机病毒的用户数量按月统计

3.2通报成员单位报送情况

■ 网秦公司[10]移动互联网恶意程序捕获情况

网秦公司监测结果，截至 2011 年底，累计发现移动互联网恶意程序 5460 个，其中 2011 年新发现 2943 个。截至 2011 年底，累计捕获移动互联网恶意程序样本 42869 个，其中 2011 年新捕获样本 24794 个。按照《移动互联网恶意程序描述格式》的八类分类标准，2011 年发现的移动互联网恶意程序分类统计数据为：恶意扣费 973 个；信息窃取 396 个；远程控制 798 个；恶意传播 49 个；资费消耗 272 个；系统破坏 232 个；诱骗欺诈 99 个；流氓行为 124 个。

2011 年各月捕获移动互联网恶意程序数量如图 3-11 所示，其中 1 月新增数量达到全年最低值 77 个，12 月新增数量达到全年最高值 597 个。

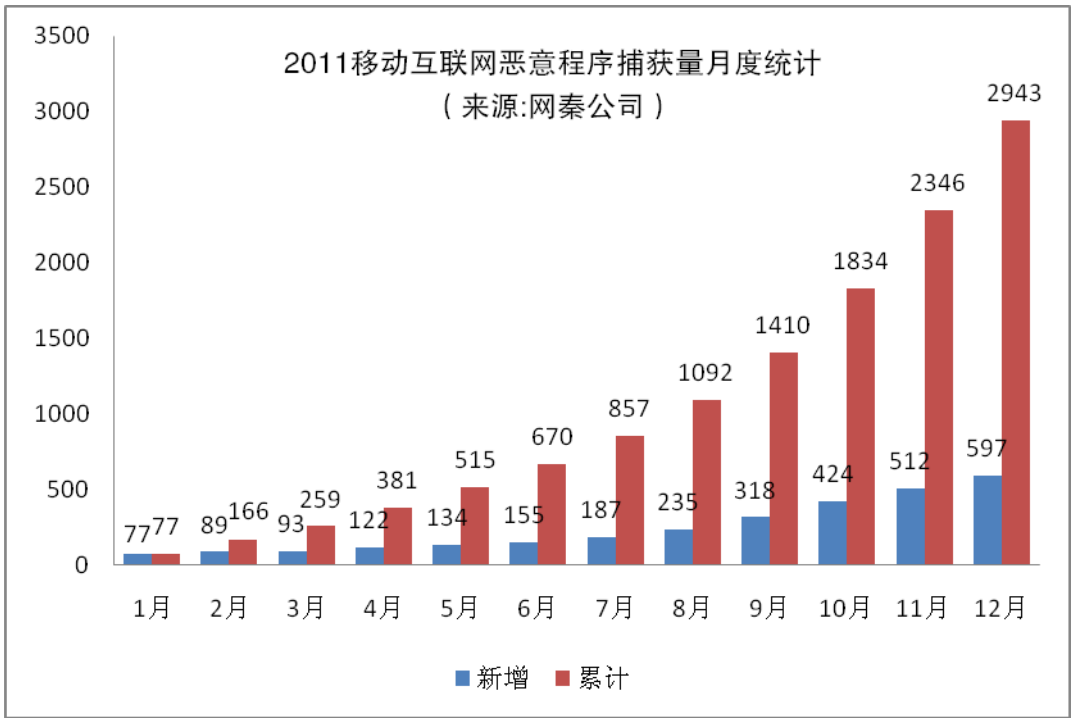

图 3-11　2011 年移动互联网恶意程序捕获月度统计（来源：网秦公司）

2011 年各月捕获移动互联网恶意程序样本数量如图 3-12 所示，其中 5 月新增数量达到全年最低值 1900 个，11 月新增数量达到全年最高值 2228 个。

[10]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。

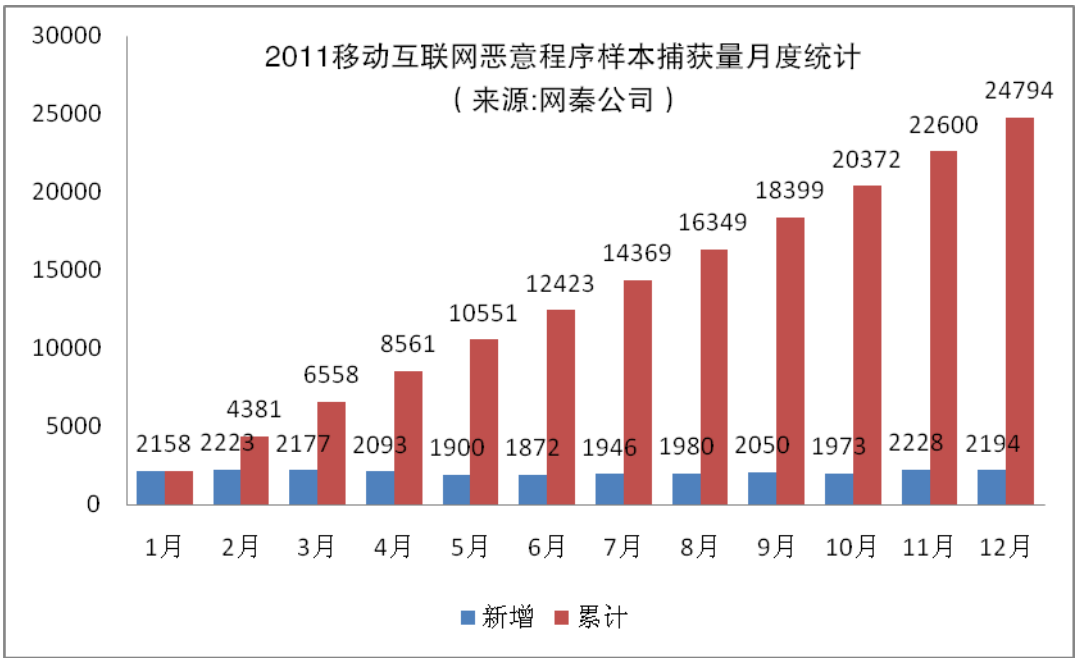

图 3-12　2011 年移动互联网恶意程序样本捕获月度统计（来源：网秦公司）

2005 年至 2011 年发现移动互联网恶意程序数量走势如图 3-13 所示。

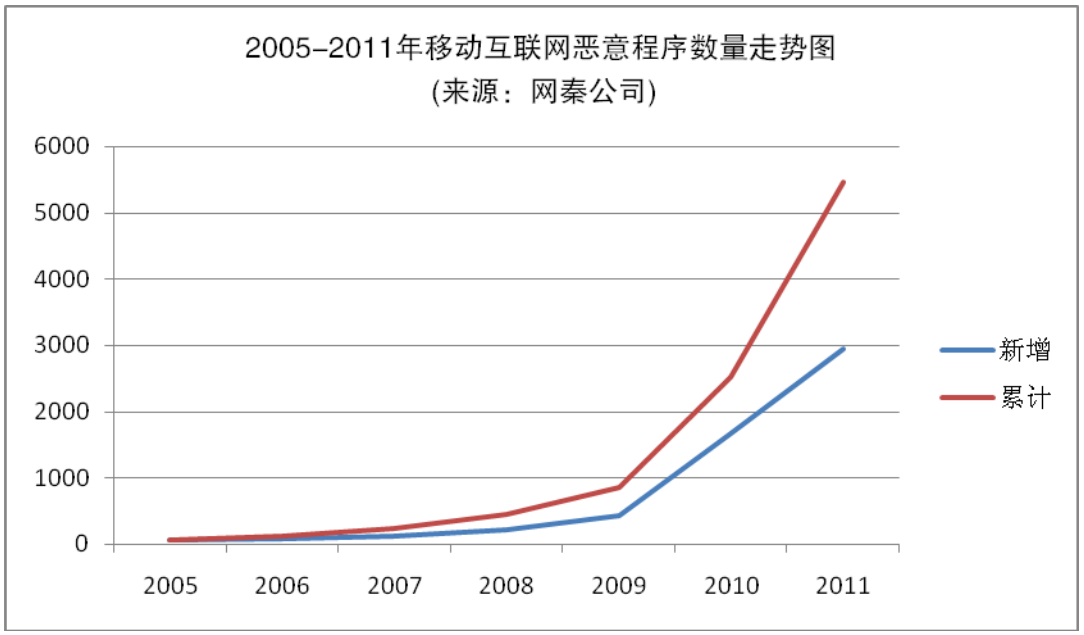

图 3-13　2005-2011 年移动互联网恶意程序数量走势图（来源：网秦公司）

2005 年至 2011 年发现移动互联网恶意程序样本数量走势如图 3-14 所示。

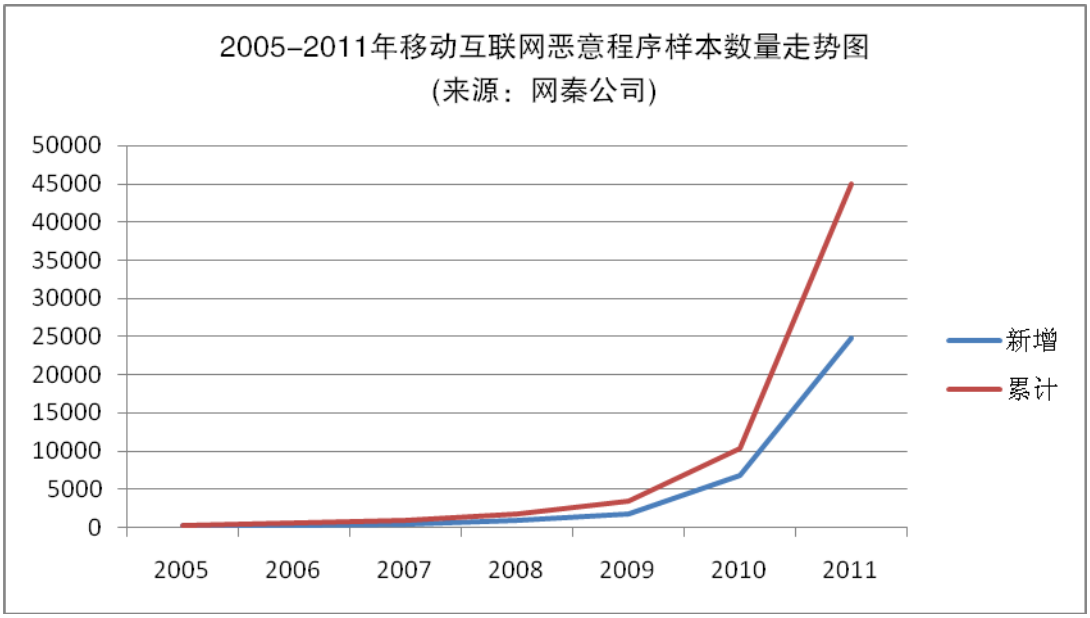

图 3-14　2005-2011 年移动互联网恶意程序样本数量走势图 (来源：网秦公司)

■ 安天公司移动互联网恶意程序捕获情况

根据安天公司监测结果，截至 2011 年底，发现移动互联网恶意程序 190 个，其中 2011 年新发现 190 个。截至 2011 年底，捕获移动互联网恶意程序样本 8188 个。按照《移动互联网恶意程序描述格式》的八类分类标准，2011 年发现的移动互联网恶意程序分类统计数据为：恶意扣费 65 个；信息窃取 51 个；远程控制 30 个；恶意传播 3 个；资费消耗 7 个；系统破坏 14 个；诱骗欺诈 5 个；流氓行为 15 个。

■ 瑞星公司移动互联网恶意程序捕获情况

瑞星公司 2011 年全年截获移动互联网病毒 4590 种，截获移动互联网恶意程序 9042 种，按月度统计如图 3-15 所示。

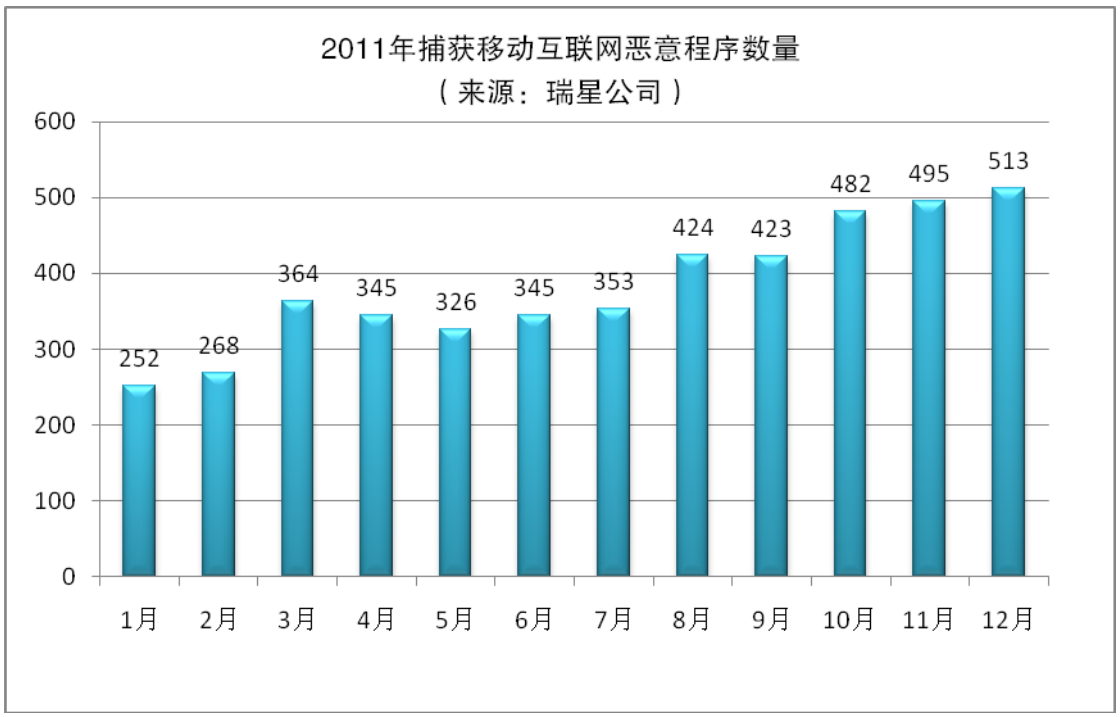

图 3-15　2011 年捕获移动互联网恶意程序数量(来源：瑞星公司)