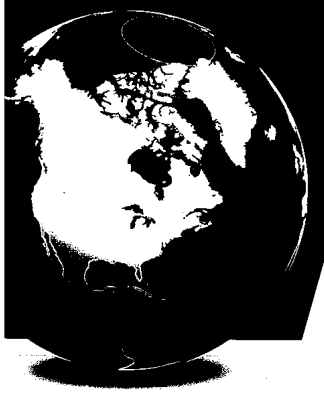
2013 中国移动互联网环境治理报告



国家计算机网络应急技术处理协调中心 著

CNCERT/CC
国家互联网应急中心

关于国家计算机网络应急技术处理协调中心

国家计算机网络应急技术处理协调中心(简称“国家互联网应急中心”,英文简称是CNCERT 或 CNCERT/CC),成立于 2002 年 9 月,为非政府非盈利的网络安全技术中心,是我国网络安全应急体系的核心协调机构。

2003 年,国家互联网应急中心在全国 31 个省(自治区、直辖市)成立分中心。作为国家级应急中心,CNCERT/CC 的主要职责是:按照“积极预防、及时发现、快速响应、力保恢复”的方针,开展互联网网络安全事件的预防、发现、预警和协调处置等工作,维护国家公共互联网安全,保障基础信息网络和重要信息系统的安全运行。

作为中国非政府层面开展网络安全事件跨境处置协助的重要窗口, CNCERT/CC 积极开展网络安全国际合作,致力于构建跨境网络安全事件的快速响应和协调处置机制。CNCERT/CC 为国际著名网络安全合作组织 FIRST 的正式成员以及亚太应急组织 APCERT 的发起者之一。截至 2013 年,CNCERT/CC 已与 59 个国家和地区的 127 个组织建立了“CNCERT/CC 国际合作伙伴”关系。

依据工业和信息化部《移动互联网恶意程序监测与处置机制》(以下简称“《机制》”),CNCERT 在移动互联网安全方面的业务能力主要包括:

- **鉴定**:CNCERT 是国内对移动互联网恶意程序进行鉴定并命名的唯一权威机构,严格参照通信行业标准 YD/T 2439-2012《移动互联网恶意程序描述格式》对移动互联网恶意程序鉴定命名。
- **监测**:CNCERT 依托对移动互联网丰富数据资源的综合分析和多渠道的信息获取实现对移动互联网恶意程序、安全事件、感染用户进行监测和预警。
- **处置**:CNCERT 对于自主发现和接收到的安全事件报告,筛选危害较大的移动互联网恶意程序和安全事件进行及时响应,并协调基础电信运营企业、手机应用商店等进行处置。

版权及免责声明

编者按：

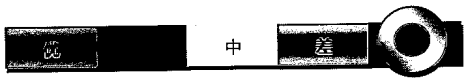
感谢您阅读《移动互联网环境治理报告（2013 年）》，如果您发现本报告存在任何问题，请您及时与我们联系，来信地址为：cncert@cert.org.cn。

目录

第一章 概述篇 2
第二章 监测篇 4
一、2013 年移动互联网恶意程序监测情况 4
二、2013 年移动互联网恶意程序传播服务器监测情况 6
三、2013 年移动互联网恶意程序控制服务器监测情况 9
四、2013 年移动互联网恶意程序感染情况 13
第三章 处置篇 16
第四章 案例篇 19
第五章 白名单篇 32
一、工作背景 32
二、白名单工作机制 32
三、白名单工作体系 34
四、首批白名单企业 37
五、2014 年工作计划 38
第六章 ANVA 篇 39
一、2013 年安全企业报送恶意程序情况 40
二、2013 年应用商店报备应用程序信息情况 43
第七章 总结篇 47
附一、中国反网络病毒联盟介绍 49
附二、中国反网络病毒联盟白名单工作组成员单位 51
附三、中国反网络病毒联盟应用商店自律组成员名单 52
附四、首批移动互联网应用自律白名单企业 53
附五、移动互联网恶意程序行为属性 55

第一章　概述篇

本报告以 CNCERT 监测数据和中国互联网协会反网络病毒联盟（ANVA）成员单位报送数据作为主要依据，对我国移动互联网的网络安全数据进行权威发布，并对重要预警信息和典型安全事件进行探讨。2013 年，中国移动互联网网络安全状况整体评价为危：



主要表现在如下方面：

现状一：移动恶意程序数量 702861 个，新增 3.3 倍，继续呈爆发式增长趋势。

现状二：Android 平台恶意程序占总数 99%以上。

现状三：恶意扣费类和资费消耗类占恶意程序 85%以上，黑客制作恶意程序带有明显趋利性。

现状四：恶意程序向灰色地带发展，增加治理难度。

现状五：移动恶意程序传播次数 12956836 次，传播移动恶意程序的网站域名数 15427 个，分别是 2012 年同期的 23 倍和 11 倍。

现状六：应用商店安全审核机制缺失，导致大量恶意程序的传播。

现状七：移动恶意程序传播服务器 95%以上使用 80 端口传播恶意程序。

现状八：境外位于美国的移动恶意程序传播服务器最多，占总数 70%。

现状九：移动恶意程序控制服务器存在国外注册域名，国内接入服务器的现象，服务器域名几乎均未备案。

现状十：移动恶意程序控制服务器 48%使用 80 端口控制手机肉鸡或者接收用户隐私信息。

现状十一：移动恶意程序境内控制服务器分布较为分散，北京最多，占总数 31%。

现状十二：移动恶意程序境外控制服务器主要集中在美国，占总数 45%。

现状十三：移动恶意程序境内控制服务器所用域名 36%在中国万网注册，域名注册地 53%位于北京。

现状十四：移动恶意程序境外控制服务器所用域名 44%在 GODADDY.COM 注册，域名注册地 73%位于美国。

现状十五：境内感染恶意程序用户数量达 609 万，其中广东用户最多。

现状十六：境内感染恶意程序用户按照运营商统计，中国移动感染用户最多。

现状十七：境内感染恶意程序用户按照操作系统分布，Android 终端感染用户最多。

现状十八：2013 年 CNCERT 协调 95 家应用商店开展 38 次恶意程序清理行动，下架恶意程序 3.7 万个。

现状十九：2013 年 CNCERT 开展 8 次移动恶意程序专项治理行动，切断黑客对 3591520 个感染手机用户的控制权。

现状二十：安丰市场传播 6644 个被植入扣费木马的应用程序（典型案例一）

现状二十一：某电商出售带有“手机预装马”的行货手机（典型案例二）

现状二十二：利用“钓鱼网站”和“仿冒手机银行”进行跨平台网络钓鱼（典型案例三）

现状二十三：利用“二维码”进行“点对点”定向诱骗淘宝信息（典型案例四）

现状二十四：仿冒韩国手机银行的木马通过短信在中国疯狂传播（典型案例五）

现状二十五：2013 年 CNCERT 判定 14 家安全企业报送的恶意程序 105512 个，其中安天公司报送得分排名第一。

现状二十六：2013 年 CNCERT 判定 37 家应用商店报备的应用程序信息 8481374 条，其中“应用汇”报备的应用程序信息数量排名第一。

第二章　监测篇

一、2013 年移动互联网恶意程序监测情况

在工业和信息化部的指导下，依据《机制》要求，CNCERT/CC 组织基础电信企业和中国反网络病毒联盟（ANVA）成员单位开展移动互联网恶意程序监测工作。根据通信行业规范 YD/T 2439-2012《移动互联网恶意程序描述格式》，移动互联网恶意程序是指在用户不知情或未授权的情况下，在移动终端系统中安装、运行以达到不正当目的，或具有违反国家相关法律法规行为的可执行文件、程序模块或程序片段。移动互联网恶意程序一般存在以下一种或多种恶意行为，包括恶意扣费、信息窃取、远程控制、恶意传播、资费消耗、系统破坏、诱骗欺诈和流氓行为。

■ **现状一：移动恶意程序数量 702861 个，新增 3.3 倍，继续呈爆发式增长趋势。**

2013 年 CNCERT 通过移动互联网恶意程序监测体系共监测移动互联网恶意程序 702861 个，比 2012 年同期监测 162981 个恶意程序增长 3.3 倍，涉及移动恶意程序家族 702 个，继续呈现出爆炸式增长趋势。如图 1 所示。

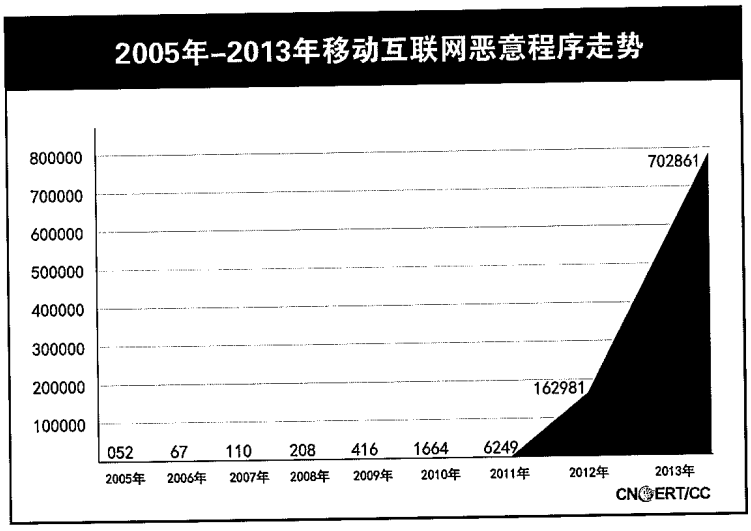


图 1：　2005 年-2013 年移动互联网恶意程序走势图

■ **现状二：Android 平台恶意程序占总数 99%以上。**

2013 年 CNCERT 监测发现的恶意程序按照操作系统分布情况如图 2 所示，其中 Android 平台恶意程序数量为 699514 个，位居第一，占总数 99%以上，其次是 Symbian 平台恶意程序，共有 3341 个，占 0.48%，此外仍有 6 个针对 J2ME 平台的恶意程序。2013 年，随着 Nokia 宣布对 Symbian 操作系统停止开发，Symbian 手机的市场逐渐萎缩，另一方面 Android 手机的市场不断扩大，使得 2013 年 Android 恶意程序数量较 2012 年提高了 17%。

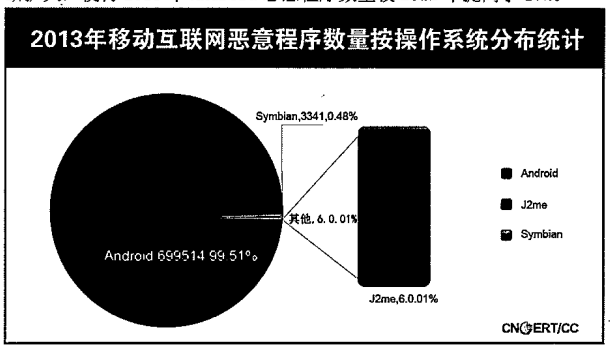


图 2： 2013 年感染移动恶意程序数量按操作系统分布统计图

■ **现状三：恶意扣费类和资费消耗类占恶意程序 85%以上，黑客制作恶意程序带有明显趋利性。**

2013 年 CNCERT 监测发现的恶意程序按照恶意行为属性分类如图 3 所示，其中恶意扣费类的恶意程序数量仍居首位，为 502481 个（占 71.5%），资费消耗类 104069 个（占 15.1%）、系统破坏类 22805 个（占 3.2%）分列第二、三位。结果显示与用户经济利益密切相关的恶意扣费类和资费消耗类恶意程序已占到恶意程序总数的 85%以上，显示了黑客制作恶意程序带有明显的趋利性，也意味着移动互联网黑客地下产业链已经成熟。

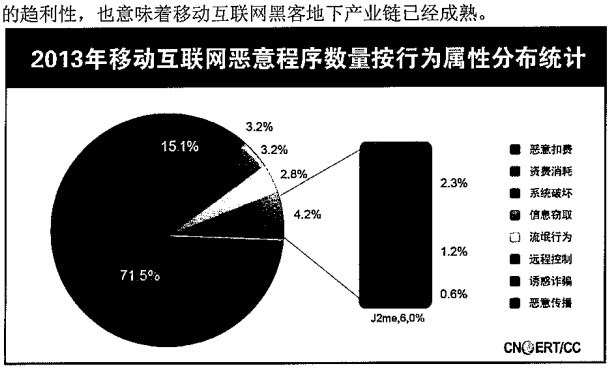


图 3： 2013 年感染移动恶意程序数量按行为属性分布统计图

■ **现状四：恶意程序向灰色地带发展，增加治理难度。**

2013 年 CNCERT 监测发现的恶意程序按照恶意程序危害等级分类如图 4 所示，其中高危的为 7028 个，占 1.0%；中危的为 203830 个，占 29.0%；低危的为 492003 个，占 70.0%。相对于 2012 年，高危移动互联网恶意程序所占比例有所下降，这反映了黑客为逃避监管逐渐向灰色地带发展，不再制作恶意性明显的手机木马等病毒，开始制作恶意广告、恶意第三方插件等灰色应用，达到既逃避监管又获取经济利益的目的。

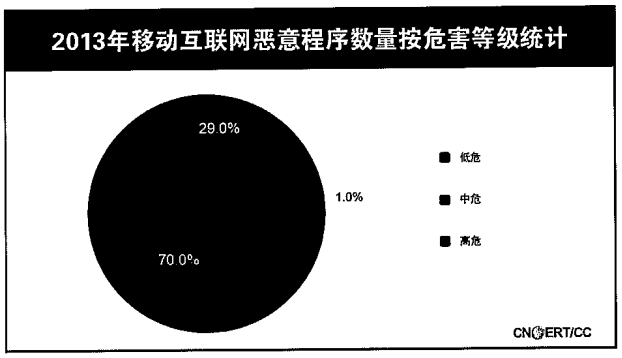


图 4： 2013 年移动互联网恶意程序数量按危害等级统计图

二、2013 年移动互联网恶意程序传播服务器监测情况

■ **现状五：移动恶意程序传播次数 12956836 次，传播移动恶意程序的网站域名数 15427 个，分别是 2012 年同期的 23 倍和 11 倍。**

2013 年手机应用商店、论坛、下载站点等依旧是传播移动互联网恶意程序的主要来源，CNCERT/CC 监测发现移动互联网恶意程序传播事件 12956836 次，是 2012 年同期 562019 次的 23 倍。移动互联网恶意程序 URL 下载链接 1206798 个，是 2012 年同期 36192 个的 33 倍，进行移动互联网恶意程序传播的域名 15427 个、IP 地址 60976 个，分别是 2012 年同期的 11 倍和 23 倍，其中以“.com”域名占 78.8%，“.cn”域名占 15.1%。以上 15427 个恶意域名包含了应用软件商店、论坛、网盘、博客等众多网站类型，其中应用软件商店数量超过 300 家。

2013 年移动互联网恶意程序传播事件的月度统计如图 5 所示，2013 年 1-7 月移动恶意程序传播活动频次相对较低，8 月后传播事件数量有所增长，并维持在较高水平。

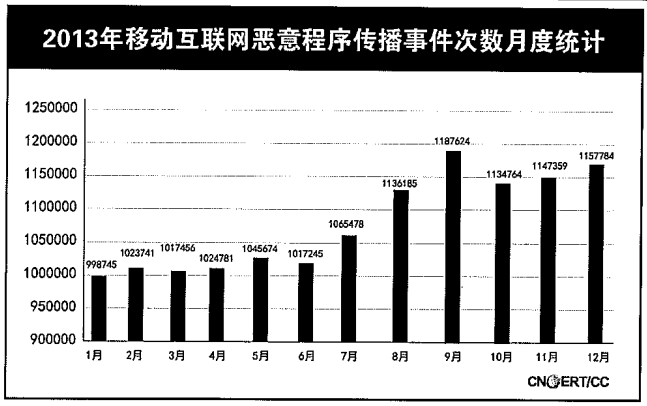


图 5： 2013 年移动互联网恶意程序传播时间次数月度统计图

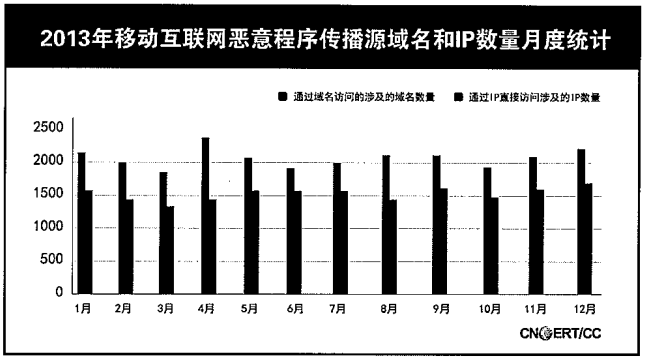


图 6： 2013 年移动互联网恶意程序传播源域名和 IP 数量月度统计图

■ **现状六：应用商店安全审核机制缺失，导致大量恶意程序的传播。**

CNCERT 对传播移动恶意程序的网站域名进行了排序，结果如图 7 所示。结果显示 2013 年国内主流应用商店均存在大量的移动恶意程序，由于这些主流应用商店是国内手机用户下载、安装手机应用的主要来源，导致这些应用商店成为黑客的主要目标。

而应用商店 APP 审查、安全检测等机制不完善，也使得黑客上传的恶意程序得以频繁发布，特别是以 77aoao.com 为例，该网站 2013 年累计传播移动恶意程序 18116 个，严重威胁着移动互联网网民的安全，目前该网站已被关停。

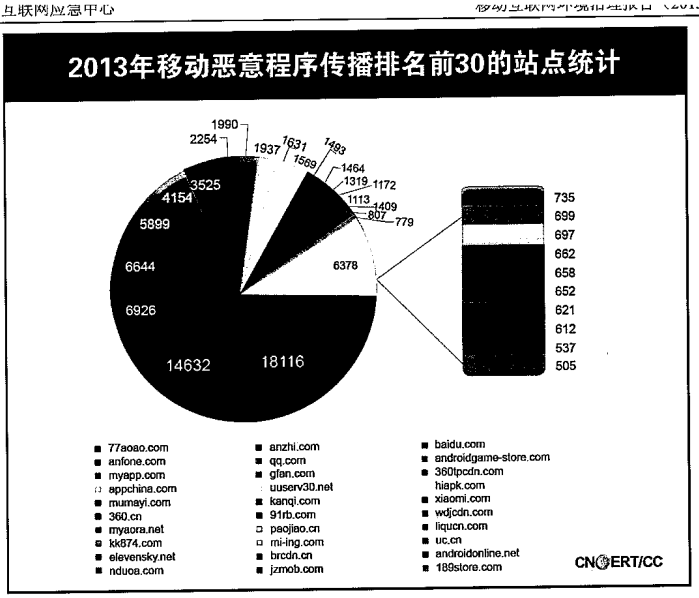


图 7：2013 年传播移动恶意程序排名前 30 的站点统计图

■ **现状七：移动恶意程序传播服务器 95%以上使用 80 端口传播恶意程序。**

CNCERT 对传播移动恶意程序的网站端口进行了排序，结果如图 8 所示。结果显示 95%以上的网站采用 80 端口传播移动恶意程序，其次是 8080 端口，占总数 1.6%，第三是 81 端口，占总数的 1.5%。

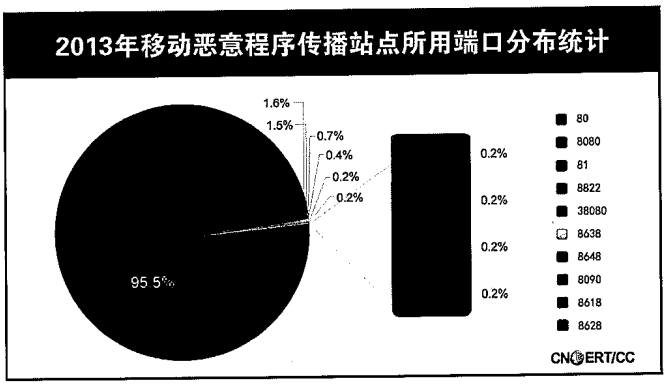


图 8：2013 年移动恶意程序传播站点所用端口分布统计图

■ **现状八：境外位于美国的移动恶意程序传播服务器最多，占总数 70%。**

CNCERT 对传播移动恶意程序的境外网站主机进行地理位置分析，结果如图 9 所示。结果显示 70%的移动恶意程序传播主机位于美国，其次是英国、日本，均占总数的 4%。

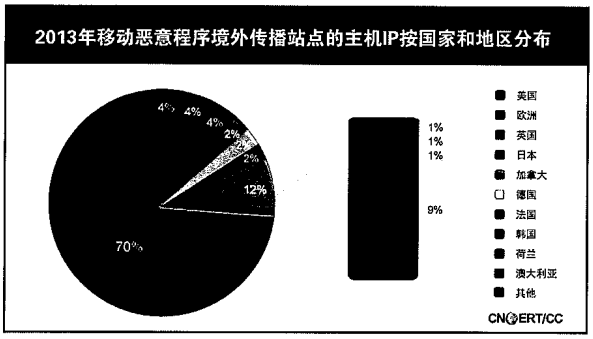


图 9：2013 年移动恶意程序传播站点的主机 IP 按国家和地区分布统计

三、2013 年移动互联网恶意程序控制服务器监测情况

■ **现状九：移动恶意程序控制服务器国外注册域名，国内接入服务器现象普遍，服务器域名几乎均未备案。**

2013 年 CNCERT 对监测发现的 70 万移动恶意程序进行了深度的技术分析，通过静态扫描恶意程序代码、动态模拟恶意程序运行等方式提取恶意程序的网络行为特征，发现了恶意程序控制服务器所使用的网站域名 860 个，几乎均未备案，其中境内注册的域名占 37%，境外注册的域名占 63%。恶意程序控制服务器所使用的主机 IP 地址 571 个，其中境内的主机 IP 地址占 52%，境外的主机 IP 地址占 48。网站域名和主机 IP 地址的境内外分布情况分别如图 10 和图 11 显示。

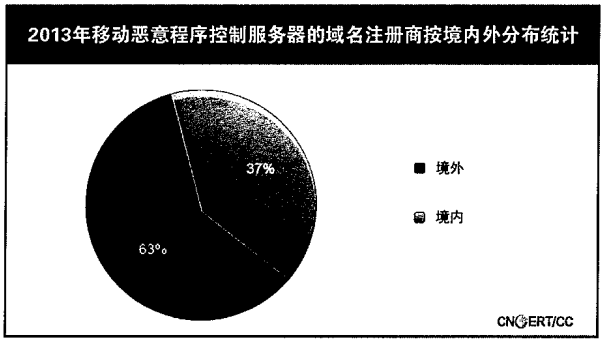


图 10：2013 年移动恶意程序控制服务器的域名注册商按境内外分布统计

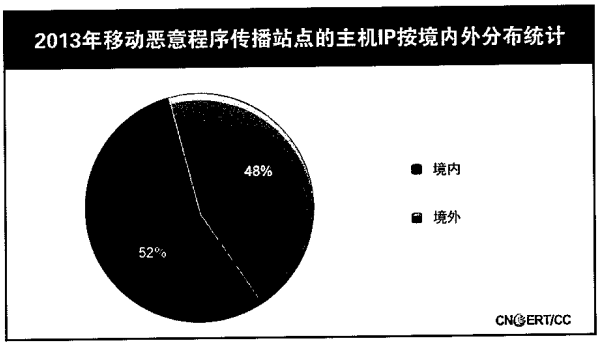


图 11：2013 年移动恶意程序传播站点的主机 IP 按境内外分布统计

- **现状十：移动恶意程序控制服务器 48%使用 80 端口控制手机肉鸡或者接收用户隐私信息。**

CNCERT 对移动恶意程序控制服务器所使用的网站端口进行了排序，结果如图 12 目所示。结果显示 48%的网站采用 80 端口接收手机隐私信息或者控制手机肉鸡，其次是 8080 端口，占总数 18%，第三是 8097 端口、8511 端口、88 端口、8800 端口、8888 端口，均占总数的 2%。

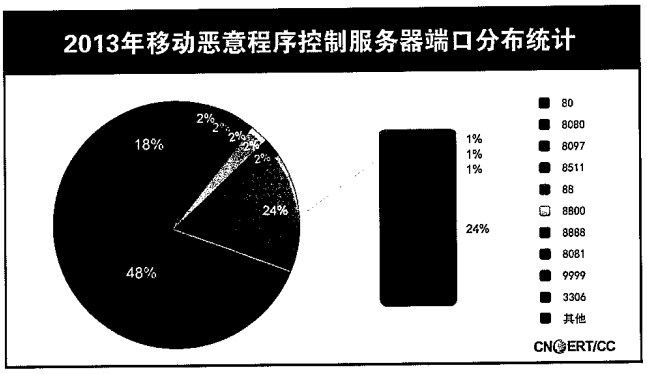


图 12：2013 年移动恶意程序控制服务器端口分布统计

- **现状十一：移动恶意程序境内控制服务器分布较为分散，北京最多，占总数 31%。**

CNCERT 对境内移动恶意程序控制服务器所使用的主机 IP 地址按地区分布进行了统计，结果如图 13 目所示。结果显示 31%的移动恶意程序控制服务器主机位于北京，其次是上海，

占总数的 18%，第三是广东，占总数的 13%。

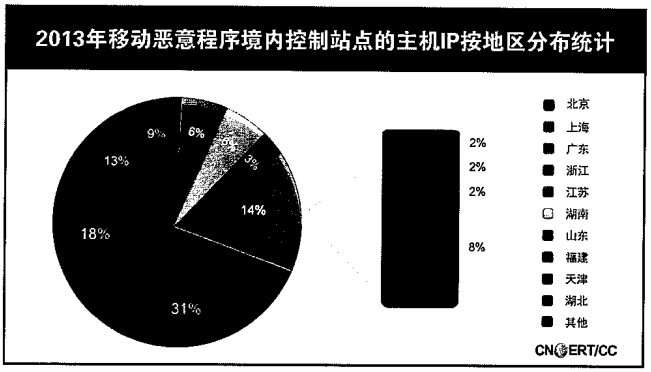


图 13：2013 年移动恶意程序境内控制站点主机 IP 按地区分布统计

- **现状十二：移动恶意程序境外控制服务器主要集中在美国，占总数 45%。**

CNCERT 对境外移动恶意程序控制服务器所使用的主机 IP 地址按地区分布进行了统计，结果如图 14 目所示。结果显示 45%的移动恶意程序控制服务器主机位于美国，其次是中国香港，占总数的 11%，第三是日本，占总数的 8%。

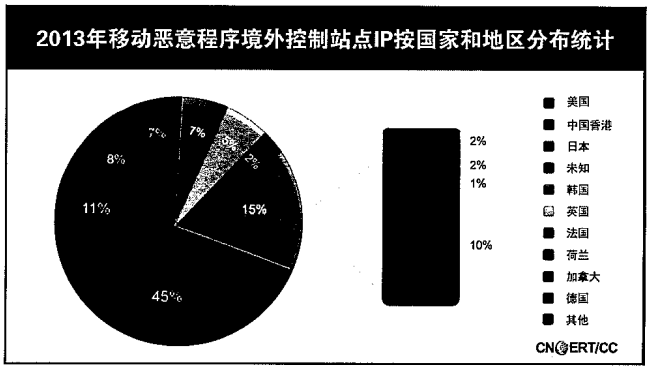


图 14：2013 年移动恶意程序境外控制站点 IP 按国家和地区分布统计

- **现状十三：移动恶意程序境内控制服务器所用域名 36%在中国万网注册，域名注册地 53%位于北京。**

CNCERT 对境内移动恶意程序控制服务器所使用的网站域名按域名注册商进行了统计，结果如图 15 目所示。结果显示 36%的境内移动恶意程序控制服务器所用的域名在北京万网

注册，其次是厦门易名，占总数的 14%，第三是北京新网数码，占总数的 12%。

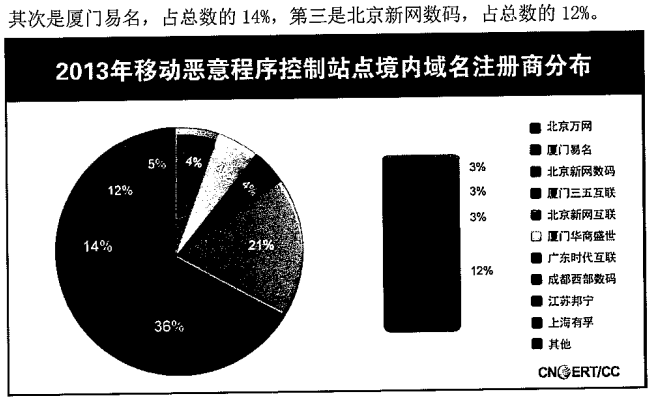


图 15：2013 年移动恶意程序控制站点境内域名注册商分布统计

CNCERT 对境内移动恶意程序控制服务器所使用的网站域名按域名注册地点进行了统计，结果如图 16 所示。结果显示 53%的移动恶意程序控制服务器在北京注册域名，其次是福建，占总数的 22%，第三是广东，占总数的 9%。

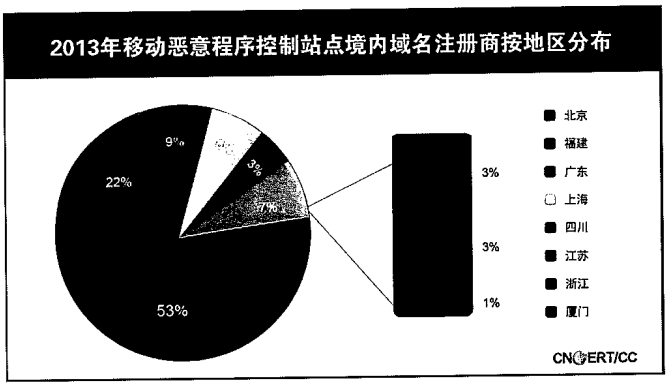


图 16：2013 年移动恶意程序控制站点境内域名注册商按地区分布统计

- **现状十四：移动恶意程序境外控制服务器所用域名 44%在 GODADDY.COM 注册，域名注册地 73%位于美国。**

CNCERT 对境外移动恶意程序控制服务器所使用的网站域名按域名注册商进行了统计，结果如图 17 所示。结果显示 44%的境外移动恶意程序控制服务器所用的域名在 GODADDY.COM 注册，其次是 ENOM，占总数的 6%，第三是 PDR LTD.、MARKMONITOR INC.、WEBNIC.CC，均占总数的 5%。

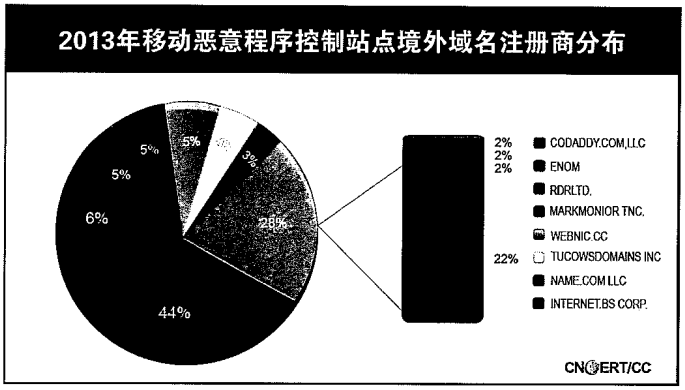


图 17：2013 年移动恶意程序控制站点境外域名注册商分布统计

CNCERT 对境外移动恶意程序控制服务器所使用的网站域名按域名注册地点进行了统计，结果如图 18 所示。结果显示 73%的移动恶意程序控制服务器在美国注册域名，其次是印度，占总数的 6%，第三是马来西亚，占总数的 5%。

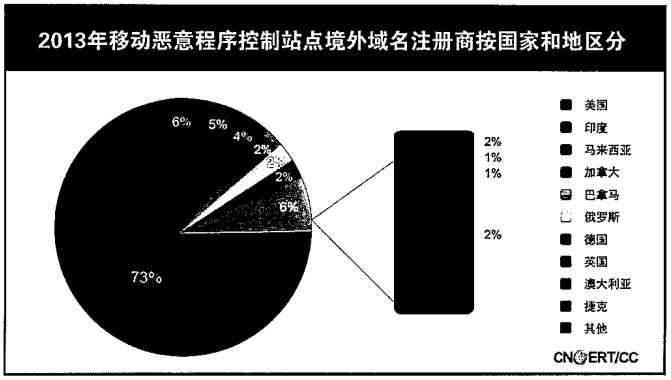


图 18：2013 年移动恶意程序控制站点境外域名注册商按国家和地区分布统计

四、2013 年移动互联网恶意程序感染情况

■ **现状十五：境内感染恶意程序用户数量达 609 万，其中广东用户最多。**

2013 年，我国境内感染移动互联网恶意程序的用户数量达 6094695。其中感染用户数量排名前三的省份为：

排名	省份	感染用户数量
1	广东	1321171
2	四川	689568
3	湖南	485355

按照全国各省感染移动恶意程序的用户数量情况，图 19 显示了各省感染移动恶意程序的严重程度。

图 19：2013 年移动恶意程序感染用户按地区分布统计

■ **现状十六：境内感染恶意程序用户按照运营商统计，中国移动感染用户最多。**

2013 年基础电信运营商中国电信、中国移动、中国联通网内感染移动互联网恶意程序的用户分布情况如图 20 所示。其中，中国移动感染移动恶意程序的用户数量最多，达 4203812 个，占所有感染用户的 69%；中国电信感染移动恶意程序的用户数量最少，达 121798 个，占所有感染用户的 2%。

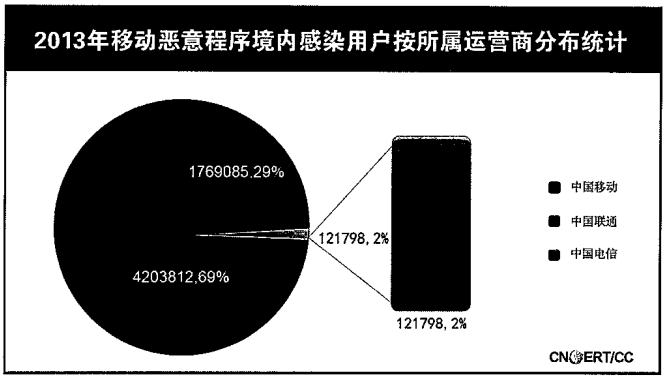


图 20：2013 年移动恶意程序境内感染用户按所属运营商分布统计

■ **现状十七：境内感染恶意程序用户按照操作系统分布，Android 终端感染用户最多。**

2013 年感染移动互联网恶意程序的用户所有操作系统主要集中在 Android 系统、Symbian 系统和 J2ME 系统，相关分布情况如图 21 所示。其中，使用 Android 系统的感染用户数量最多，近 590 万，占所有用户的 83.25%；使用 J2ME 系统的感染用户数量最少，小于 5000，不足所有用户的 1%。

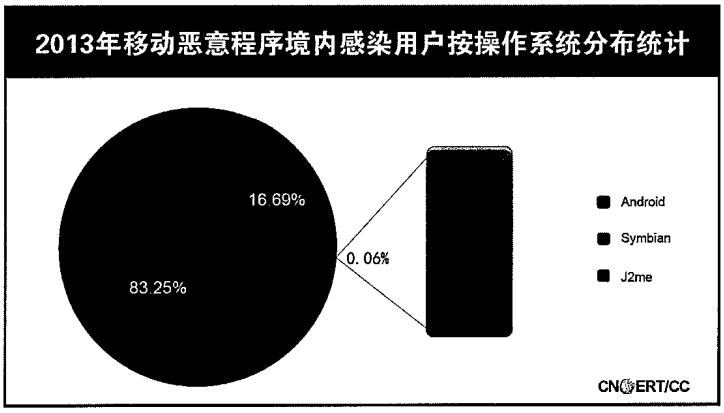


图 21：2013 年移动恶意程序境内感染用户终端按操作系统分布统计

第三章 处置篇

2012年，在工业和信息化部的指导下，依据《机制》要求，CNCERT/CC组织基础电信企业、中国互联网协会12321网络不良与垃圾信息举报中心、中国反网络病毒联盟（ANVA）成员单位以及手机应用商店先后开展6次移动互联网恶意程序专项治理工作，共通知应用商店下架恶意程序621个。

2013年，移动互联网恶意程序继续呈现爆炸式增长速度，且第三方手机应用商店及下载站缺乏严格的应用程序安全审核机制，导致移动互联网恶意程序较2012年更为泛滥，移动互联网生态上游已被恶意程序严重污染。

为有效遏制移动互联网恶意程序的蔓延趋势，净化移动互联网生态上游环境，CNCERT于2013年1月1日起启动了常态化的恶意程序传播源处置工作，以每周一次的频率通知应用商店下架恶意程序，全年累计开展38次处置行动，共开展38次应用商店恶意程序清理行动，下架恶意程序3.7万个。在常态化处置恶意程序传播源的同时，CNCERT针对恶意程序控制服务器开展了8次专项治理行动，切断了黑客对3591520个感染手机用户的控制。

- **现状十八：2013年CNCERT开展38次应用商店恶意程序清理行动，下架恶意程序3.7万个。**

CNCERT自2013年1月1日起，我中心启动了常态化的恶意程序传播源处置工作，全年累计开展38次处置行动，共通知59家应用商店下架恶意应用软件47327个，其中验证下架39216个，总体下架率仅为82.7%。

根据应用商店恶意程序下架率以及处置响应速度等三方面指标，以应用商店下架率是否为100%，处置速度是否及时为评估标准，CNCERT对应用商店进行了排名。

序号	应用商店名称	域名	下架率	处置速度
1	百度网	baidu.com	100.00%	及时
2	应用汇	appchina.com	100.00%	及时
3	91RB	91rb.com	100.00%	及时
4	优亿市场	eoemarket.com	100.00%	及时
5	泡椒网	paojiao.cn	100.00%	及时
6	乐讯	lexun.com	100.00%	及时
7	UC优视	uc.cn	100.00%	及时
8	当乐网	d.cn	100.00%	及时
9	3G门户	3g.cn	100.00%	及时
10	OPPO手机	nearme.com.cn	100.00%	及时

	应用商店			
11	吾爱主题	5izhuti.com	100.00%	及时
12	手机中国	cnmo.com	100.00%	及时
13	小米网	xiaomi.com	100.00%	及时
14	悠悠村	uucum.com	100.00%	及时
15	中国电信 天翼空间	189store.com	100.00%	及时
16	天网手机软件	waptw.com	100.00%	及时
17	飞鹏网	fpwap.com	100.00%	及时
18	91 手机助手	zs.91.com	100.00%	及时
19	安极市场	angeeks.com	100.00%	及时
20	中国移动 MM 商城	mm.10086.cn	100.00%	及时
21	易用汇	anzhuoapk.com	100.00%	及时
22	中国联通 沃商店	wo.com.cn	100.00%	及时
23	安卓中国	androidcn.com	100.00%	及时
24	搜狐	sohu.com	100.00%	及时
25	宝软网	baoruan.com	100.00%	及时
26	风暴数码	fengbao.com	100.00%	及时
27	安丰市场	anfone.com	100.00%	及时
28	中关村在线	zol.com.cn	100.00%	及时
29	飞流社区	feiliu.com	99.44%	及时
30	游戏狗	gamedog.com	99.39%	及时
31	联想乐商店	lenovomm.com	99.03%	及时
32	机锋网	gfan.com	92.82%	及时
33	新浪网	sina.com.cn	90.11%	及时
34	155 安卓	155.cn	84.64%	比较及时
35	安智网	goapk.com	83.63%	比较及时
36	安卓网	hiapk.com	81.59%	比较及时
37	木蚂蚁	mumayi.com	79.90%	比较及时
38	历趣网	liqucn.com	79.32%	比较及时

39	中兴汇天地	ztems.com	77.99%	比较及时
40	N多网	nduoa.com	72.70%	比较及时
41	360手机助手	360.cn	67.56%	比较及时
42	网易应用中心	163.net	65.26%	比较及时
43	十字猫	crossmo.com	63.40%	比较及时
44	酷派应用商店	coolmart.com	59.89%	不及时
45	华为智汇云	hicloud.com	54.30%	不及时
46	宜搜搜索	easou.com	50.86%	不及时
47	豌豆荚	wandoujia.com	50.00%	不及时
48	卓乐网	sjapk.com	48.95%	不及时
49	魅族	meizu.com	46.63%	不及时
50	腾讯应用宝	myapp.com	44.26%	不及时
51	爱卓网	iandroid.cn	43.21%	不及时
52	谷歌	google.com	42.86%	不及时
53	极游网	ggg.cn	33.64%	不及时
54	91市场	sc.91.com	6.34%	不及时
55	91手机娱乐	www.91.com	0.00%	不处理
56	阿里巴巴	alibaba.com	0.00%	不处理
57	HTC应用商店	htc.com	0.00%	不处理
58	诺基亚 应用商店	ovi.com.cn	0.00%	不处理
59	球球搜	qiuqiu.so	0.00%	不处理

- **现状十九：2013年CNCERT开展8次移动恶意程序专项治理行动，切断黑客对3591520个感染手机用户的控制权。**

2013年CNCERT组织8次移动恶意程序专项打击工作，协调处置了17个感染规模较大的移动恶意程序控制域名，关停73个控制服务器主机，切断了黑客对3591520个感染手机用户的控制。

第四章 案例篇

2013 年 CNCERT 监测发现多起移动互联网恶意程序典型安全事件，本章总结了 2013 年度最具特点的 5 个典型案例，表现在通过应用商店、手机预置等“源头”环节传播恶意程序、跨平台网络钓鱼、控制端从网络侧转移到短信侧、利用二维码进行定向诈骗等新现象和新问题，反映了黑客在恶意程序制作、传播等环节所用手段的升级，预示着未来与黑客的斗争将更加激烈，值得安全行业工作人员关注。

■ 典型案例一：安丰市场传播 6644 个被植入扣费木马的应用程序（现状二十）

关键词：“安卓签名漏洞”“应用商店”“扣费木马”

2013 年 7 月 CNCERT 主办的国家信息安全漏洞共享平台（CNVD）收录了 Android 操作系统存在一个签名验证绕过的高危漏洞(编号：CNVD-2013-28152)。利用该签名漏洞，黑客可以在不破坏正常 APP 程序和签名证书的情况下，向正常 APP 中植入恶意程序，一方面利用正常 APP 的签名证书逃避 Android 系统签名验证，另一方面能够在运行时执行被植入的恶意程序。

由于无需对正常 APP 进行修改，利用该签名漏洞向正常 APP 中植入恶意程序的成本非常低。此外，利用该签名漏洞的恶意 APP 具有很强的危害性和隐藏性，终端防护软件无法通过签名来检验程序的安全性。“寄生”在正常 APP 中的恶意程序可以轻松绕过终端防护软件，在用户终端后台执行各种恶意行为，造成用户隐私信息泄露、恶意扣费等严重危害。

7 月下旬，CNCERT 在第三方应用市场“安丰市场”中发现利用该签名漏洞的 Skullkey 扣费木马犹如“寄生虫”般寄生于正常 APP 中并开始疯狂传播，共有 6644 个利用签名漏洞被植入 Skullkey 扣费木马的恶意 APP。在捕获 Skullkey 扣费木马后，CNCERT 对该木马进行了全面分析，并依据通信行业标准 YD/T 2439-2012《移动互联网恶意程序描述格式》判鉴定该手机木马属于“恶意扣费”类恶意程序，将其归入 A.Payment. Skullkey 恶意代码家族中。

Skullkey 扣费木马利用 Android 操作系统签名漏洞，向正常 APP 中植入恶意程序，在用户不知情的情况下，通过后台发送扣费短信，并屏蔽回执短信。此外，该木马还可以在后台读取手机中的通讯录信息，同时具备向联系人发送广告或欺诈短信的权限。

在第三方应用市场“安丰市场”中存在 6644 个由于 Android 操作系统签名漏洞被植入 Skullkey 扣费木马的恶意 APP，按照功能分布如下：

编号	种类	比例
1	游戏类	44%
2	工具类	24%
3	社交类	11%
4	其他	21%

为了提高恶意 APP 的下载量，黑客会优先选择向热门 APP 中植入 Skullkey 扣费木马。在以上 6644 个恶意 APP 中，许多 APP 都为热门 APP：

工具类 APP：新浪微博，腾讯 QQ，搜狐新闻客户端，UC 浏览器，优酷视频，土豆视频，CCTV 客户端等；

经济类 APP：农业银行手机客户端，兴业银行手机客户端，支付宝，淘宝，苏宁易购等；

安全类 APP：腾讯手机管家，360 手机卫士，安全管家，LBE 手机安全大师，赛门铁克，网秦，金山毒霸等。

可以看出，经济类 APP 和安全类 APP 逐渐成为黑客入侵的新目标。根据“安丰市场”网站的下载次数统计显示，这些恶意 APP 的累计下载总次数已超过 200 万次。

第三方“安丰市场”首页具有“热门应用”板块，在该板块中的应用是下载次数是在整个安丰市场中排名最靠前的 APP，其中排名第一的是“手机 QQ2013”。

图 22：安丰市场主页

进入“手机 QQ2013”页面，可以看到该 APP 已累计下载 896844 次。点击“立即下载”后获得“手机 QQ2013”安装文件“1373852745887.apk”。

图 23： 安丰市场下载量排名第一的 APP

利用 7-zip 压缩工具打开该 APK 安装文件，可以看到具备两个“classes.dex”文件，而正常的手机 QQ 安装程序只会有一个“classes.dex”文件，因此可以判定该安装程序已被黑客利用并植入恶意程序。且“classes.dex”文件的创建时间为 2013 年 7 月 21 日，而该 APP 最后的更新时间为 2013 年 7 月 15 日，两个时间不吻合，经判定被植入的文件为扣费木马 Skullkey。

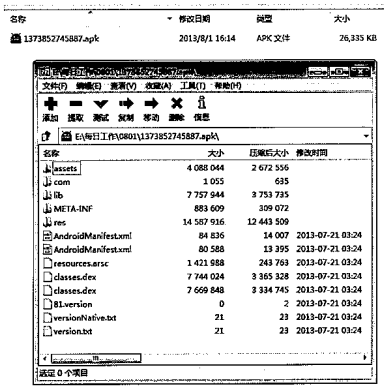


图 24：安丰市场中下载量第一的 APP 文件列表

除手机 QQ2013 外，如 UC 浏览器、腾讯微信、搜狗输入法、360 手机卫士、搜狐客户端等热门 APP 均存在同样问题，被植入扣费木马 Skullkey。通过对整个“安丰市场”进行整体检查，共发现类似被植入扣费木马 Skullkey 的恶意 APP 共计 6644 个。

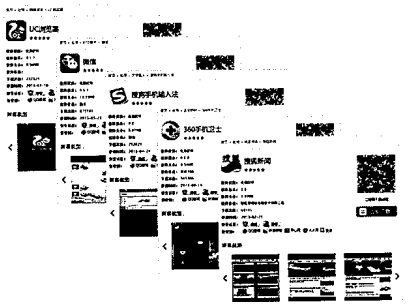


图 25：安丰市场中被植入 Skullkey 扣费木马的热门 APP

CNCERT 在监测发现“安丰市场”中存在 6644 个的被植入 Skullkey 扣费木马的恶意 APP 后，第一时间通知该应用商店下架所有 6644 个恶意 APP，并彻底删除相应的 APP 下载链接。

■ **典型案例二：某电商出售带有“手机预装马”的行货手机（现状二十一）**

关键词：“正规电商”“行货手机”“恶意刷机”

2013 年 CNCERT 监测发现一起利用刷机方式向手机植入“手机预装马”，进而窃取用户信息的典型案例。截至 2014 年 1 月全国范围内感染该“手机预装马”的受害用户达 216 万，不规范的手机刷机行为已经严重威胁到了移动互联网环境的生态健康，移动互联网“白名单”机制将势在必行。

CNCERT 接到网民投诉，称其在某电商购买的行货手机中存在预装的手机病毒。CNCERT 在收到投诉后，及时对网民手机进行了取证调查。通过取证分析，CNCERT 发现该手机中存在一例伪装成安卓系统服务“SystemScan”的应用程序，该应用程序在用户不知情的情况下通过后台窃取用户手机号码、IMEI 号、IMSI 号、用户联网 IP 地址、用户手机当前位置信息、用户手机上所有已安装的应用程序信息以及当前系统运行任务信息等，并将窃取到的用户信息进行压缩后上传到远端服务器。该远端服务器所使用的域名为 cui9.com，相应的服务器 IP 地址为 123.103.63.37，123.103.63.43。

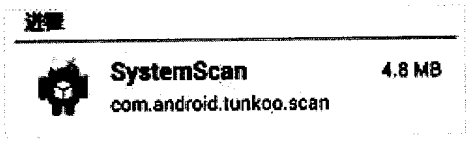


图 26：“手机预装马”所运行的恶意程序信息

依据通信行业标准 YD/T 2439-2012《移动互联网恶意程序描述格式》判定该应用程序属于“信息窃取”类恶意程序，将其归入“A.Privacy.TunkooScan”恶意代码家族中，并将

该恶意代码家族的中文名称命名为“手机预装马”。

CNCERT 通过调查取证，发现投诉者在某电商所购行货手机所预装的应用程序与官方发售的行货手机中预装的应用程序并不一致。由于官方发售的行货手机中并未预装名为“SystemScan”的手机预装马，因此手机预装马系手机出厂后通过二次刷机方式植入手机。

图 27：投诉者提供的感染手机

图 28：投诉者提供的手机交易信息

通过对该手机预装马进行持续监测，截至 2014 年 1 月 CNCERT 发现全国范围内感染该手机预装马的用户数达 2167148 个。感染用户按照区域分布和运营商分布情况分别如图 29 和图 30 所示。

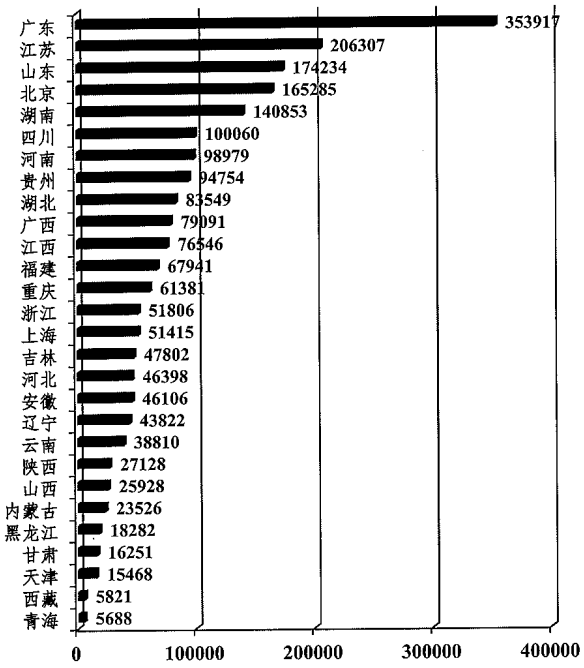


图 29：感染“手机预装马”用户按照区域分布情况

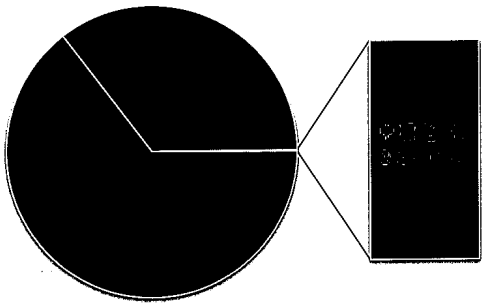


图 30：感染“手机预装马”用户按照运营商分布情况

目前，CNCERT 已协调域名注册商中国万网对“手机预装马”所使用的服务器域名 cui9.com 进行停止解析处理，协调电信增值企业网宿科技对服务器所使用的 IP 地址 123.103.63.37，123.103.63.43 进行停止接入处理。

■ **典型案例三：利用“钓鱼网站”和“仿冒手机银行”进行跨平台网络钓鱼（现状二十二）**

关键词：“钓鱼网站”“仿冒应用”“手机银行”

2013 年 10 月 18 日，我中心监测发现一类新型的跨平台“网络钓鱼”方式，黑客通过仿冒银行网站制作“钓鱼网站”，窃取用户银行账户信息，通过仿冒手机银行安全插件制作“钓鱼 APP”，窃取网银短信验证码信息。

黑客通过线上窃取用户银行账户信息，线下窃取用户手机收到的银行短信验证码，可以在用户不知情的情况下完成转账、网购等交易行为，达到牟取经济利益的目的。该案例不同于普通的手机病毒案例，具有以下两个特点：

1. 该线索是 CNCERT 发现的首例利用手机作为控制端获取网银短信验证码的安全事件；
2. 该恶意程序通过后台发送短信的方式上传短信验证码，并无网络行为。

黑客制作的钓鱼网站截图如下图所示，钓鱼网站通过仿冒某银行网站页面形式，诱骗用户输入手机号和登录密码。黑客利用窃取的用户信息可以登录用户网上银行，获取更多用户的银行账户信息。

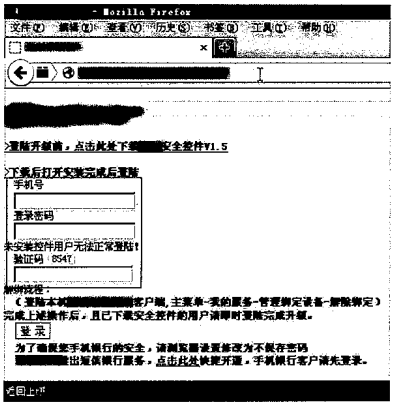


图 31：仿冒银行网站截图

黑客在仿冒银行网页的同时，也仿冒官方手机银行安全插件，在安全插件中植入恶意程序，并在仿冒网站上设立恶意插件的下载链接，诱骗用户下载，达到窃取用户短信验证码的目的，相关截图如下：

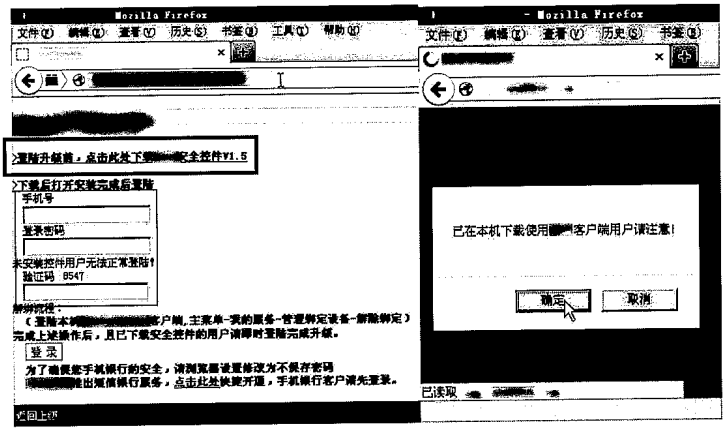


图 32：仿冒手机银行安全插件下载链接截图

仿冒官方手机银行安全插件的运行界面如下，其图标与官方手机银行的图标一致。

图 33：仿冒手机银行的应用截图

经过技术分析，发现被植入恶意程序的手机银行安全插件具有三类恶意行为，具体如下：

1. 在用户不知情的情况下，后台接收特定手机号的短信指令，并在短信收件箱中对来自特定手机号的短信进行屏蔽；

2. 在用户不知情的情况下，后台向特定手机号发送短信，并在短信发件箱中对已发短信进行删除；

3. 通过隐藏安装图标、伪造卸载界面等方式阻止用户卸载，相关截图如下：

图 34：仿冒手机银行的应用防止被卸载的截图

根据以上恶意行为，CNCERT 将此恶意手机银行安全插件命名为 A.Remote.Emial。CNCERT 共监测发现 A.Remote.Emial 的三个变种，分别对应三个控制端手机号，黑客通过制作 A.Remote.Emial 可将用户接收到的网银短信验证码转发到以上手机号中，并结合仿冒网站所得到的用户信息，可完成网银支付、转账等交易行为，达到直接获取经济利益的目的。

针对仿冒网站，我中心已协调相关域名注册商对网站域名进行关停处理，本案例涉及的仿冒网站已无法访问，并协调运营处置了相关手机号。

■ **典型案例四：利用“二维码”进行“点对点”定向诱骗淘宝信息（现状二十三）**

关键词：“二维码”“仿冒应用”“淘宝”

2013 年 11 月，CNCERT 接到奇虎公司举报的一款恶意程序，该恶意程序是一款伪装成淘宝二手的恶意软件，主要目的是窃取用户隐私，病毒运行过程中下载病毒样本 tz.apk(安全中心)，然后诱导用户静默安装，安装后在后台启动 GoogleService 服务。病毒运行过程中获取用户淘宝网账号、淘宝网密码、用户身份证号码、淘宝支付宝密码、手机号码、手机 IMEI 号码，同时收集手机收到的短信号码和短信内容，并联网上传到远程服务器；病毒运行过程中拦截用户手机短信，使用户手机无法收到短信。

1、通过伪造淘宝 APP 界面，获取用户淘宝网账号、淘宝网密码、用户身份证号码、淘宝支付宝密码；

2、在用户不知情的情况下，后台窃取手机号码、手机 IMEI 号码、短信号码和短信内容；

3、将窃取信息上传至 www.g**e****o.com。

图 35：黑客传播恶意程序过程

图 36：恶意程序运行界面

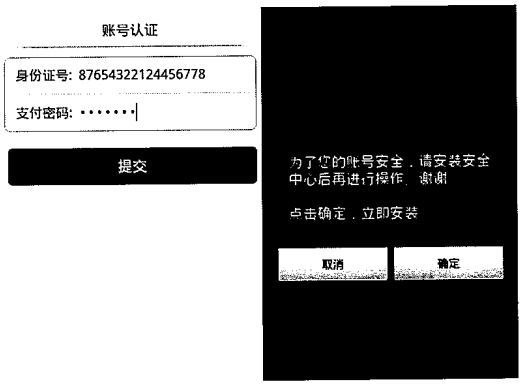


图 37：恶意程序诱骗用户输入淘宝账号和支付密码

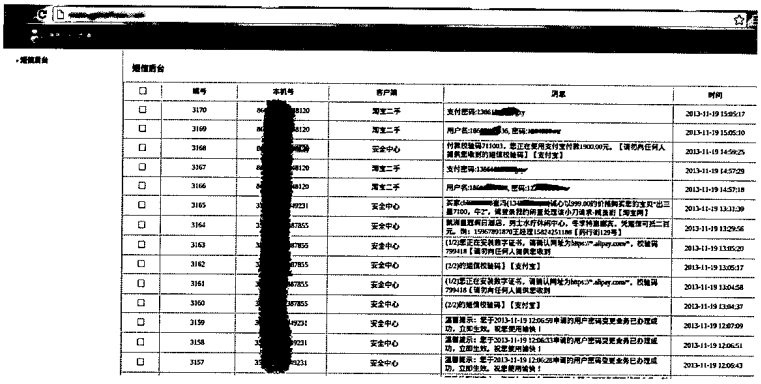


图 38：恶意程序后台服务器信息

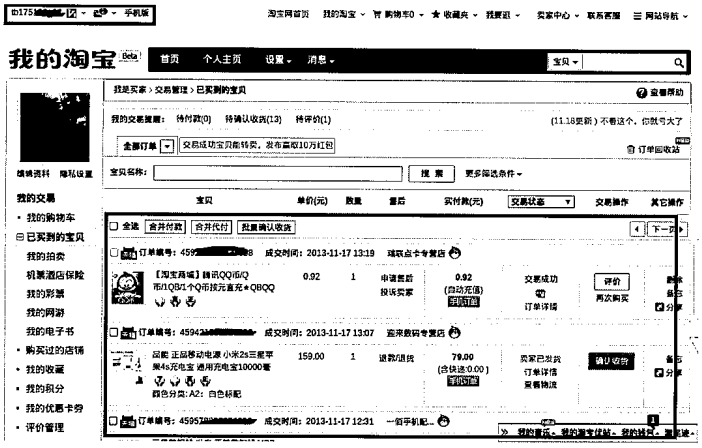


图 39：通过后台信息进入用户淘宝个人页面

■　**典型案例五：仿冒韩国手机银行的木马通过短信在中国疯狂传播（现状二十四）**

关键词：“仿冒韩国手机银行”“短信放马”

2013年9月22日，CNCERT监测发现一个Android平台手机木马病毒A.Privacy.cckun.a，该病毒具有隐私窃取、远程控制、恶意传播、系统破坏等一系列高危恶意行为，通过短信方式向联系人传播该木马病毒，并通过后台下载更为复杂的手机木马病毒A.Privacy.SmsServices.a，窃取用户的银行账户、密码、手机号等隐私信息。

手机木马病毒A.Privacy.cckun.a的运行过程如下：

1、在用户不知情的情况下，通过后台向远程控制端上传手机号码、数字证书等隐私信

息；

2、通过后台从远程控制端下载恶意信息模板，恶意短信内容包含下载该病毒的恶意 URL 链接，涉及域名包括 kakaobe.com 和 sbsbe.com；

3、遍历被感染用户的通讯录，向所有联系人发送恶意短信，诱骗联系人点击恶意 URL 链接下载该病毒；

4、检测用户是否安装韩国友利银行、国民银行、农协银行等 3 个银行的手机银行客户端；

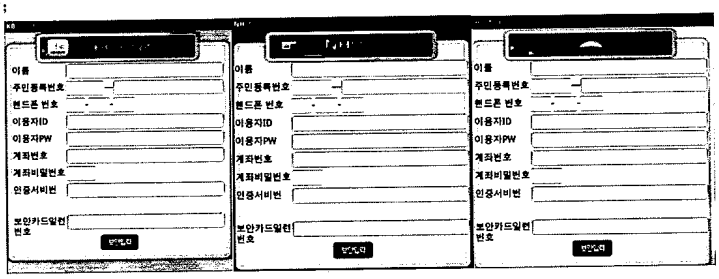


图 40：仿冒韩国手机银行截图

5、如果用户未安装上述手机银行客户端，通过后台从远程控制端下载仿冒以上 3 个手机银行客户端的手机木马病毒 A.Privacy.SmsServices.a；

6、如果用户已安装上述手机银行客户端，会强行卸载已安装的手机银行客户端，并通过后台从远程控制端下载仿冒以上 3 个手机银行客户端的手机木马病毒 A.Privacy.SmsServices.a。

手机木马病毒 A.Privacy.SmsServices.a 的运行过程如下：

1、伪造与原有银行相同的界面，诱骗用户输入银行账户信息进行窃取；

2、在用户不知情的情况下，通过后台上传用户短信、手机号、手机型号等隐私信息；

3、通过后台发送短信，并删除已发送的短信；

4、屏蔽含有数字内容的接收短信；

5、将手机设置为静音，拦截特定手机号的来电，同时将向特定手机号的去电设置为 NULL，导致用户无法向特定手机号拨打电话。

该手机病毒通过向手机联系人发送如下短信“uet http://happy.kakaobe.com”和“Start http://198.148.81.76”来传播。手机用户访问以上 URL 链接后，该手机病毒会被自动下载并安装。同时 CNCERT 还监测发现该病毒会通过 rd.wechat.com 和 m.baidu.com 等

URL 链接进行传播。

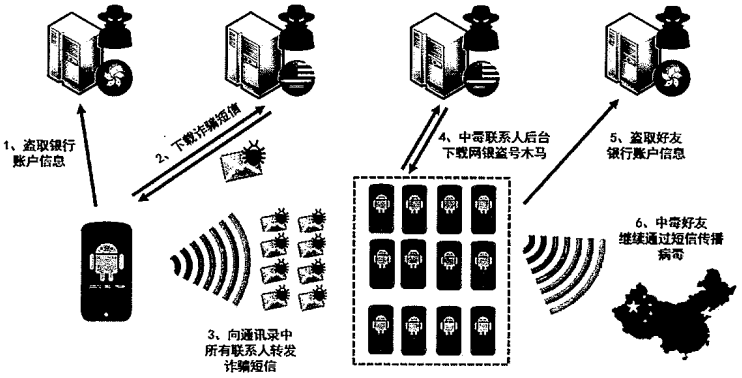


图 41：病毒传播过程图示

9 月 22 日，中国电信、中国移动紧急对该病毒涉及的传播源地址和控制端地址进行网内处置，及时遏制了该病毒的蔓延。为有效遏制该手机木马病毒的大规模蔓延，CNCERT 已在第一时间从网络侧和终端侧两大方面开展处置工作，其中，网络侧处置情况如下：

1、通知该手机病毒涉及域名 kakaobe.com 和 sbsbe.com 所在的域名注册商（成都西部数码）对以上域名进行关停，目前已无法访问；

2、通知各运营商在网内对该恶意程序所涉及的 URL 链接进行处置；

3、要求运营商严查是否存在短信群发机用于传播该恶意短信；

4、该病毒的控制端 IP 地址位于香港和美国，协调 HKCERT 和 USCERT 核查该病毒所涉及的 IP 地址信息。

终端侧处置情况如下：

1、将该病毒信息在 ANVA 移动互联网恶意程序报送平台的黑名单中进行发布；

2、将该病毒程序样本在中国反网络病毒联盟中进行共享，通知 360、腾迅、金山、百度、安全管家、联想等终端安全厂商更新病毒特征，在终端侧查杀该病毒。

第五章 白名单篇

一、工作背景

2013 年移动应用程序在数量上继续呈现爆炸性增长，特别是 Android 平台应用长尾效应逐步凸显，长尾中的移动应用良莠不齐，大部分移动应用处于灰色地带。特别是对正版应用进行二次打包的仿冒应用，用户难以辨别正版应用和仿冒应用，导致正版应用淹没在大量的仿冒应用中，使得用户难以安装正版的移动应用，“劣币驱逐良币”效应明显。基于传统“黑名单”的防护方式，已经不能满足用户进行移动安全信息消费的需要。

另一方面，2013 年移动互联网恶意程序增速 3.3 倍，继续呈现爆发式增长趋势，使移动安全面临严峻的挑战。特别是以“手机预装马”为代表的恶意程序，具有很强的隐蔽性，使得手机安全软件无法及时辨别。目前大多数手机安全软件都是基于“黑名单”机制来查杀移动恶意程序，但是“黑名单”机制是基于已知恶意程序建立的，无法对新出现的恶意程序进行及时识别，因此当 CNCERT 发现“手机预装马”后，测试主流手机安全软件均无法识别“手机预装马”，这也是造成“手机预装马”感染 200 多万用户的一个主要原因。

由于传统“黑名单”方式在保护优质移动应用、打击恶意应用这两方面都存在越来越多的局限性，仅仅依靠“黑名单”的方式已经难以适应当前移动互联网环境治理的需要。

为营造健康的移动互联网生态系统，有效解决目前“黑名单”机制的局限性，中国反网络病毒联盟 ANVA 于 2013 年 8 月推行了“移动互联网应用自律白名单”，帮助应用商店标示白应用，帮助开发者推广白应用，帮助用户选择白应用，通过建立可信的“白名单”保护正版的优质应用，同时防止“未知”移动恶意程序的入侵。

图 42： ANVA 移动互联网应用自律白名单标志

由于移动互联网企业发布应用程序所使用的数字证书具备相对固定和不易伪造的特点，ANVA 采用数字证书作为“白名单”的实体。如果一家移动互联网企业成功申请将本企业数字证书加入“白名单”，则该企业出品的带有该证书的所有移动互联网应用均被 ANVA 认定为安全可信的“白应用”。

二、白名单工作机制

为了严格保证白名单的公正评选和可靠品质，中国反网络病毒联盟 ANVA 制定了《移动

互联网应用自律白名单发布规范》和《移动互联网应用自律白名单数据接口规范》，并逐步推进成为通信行业规范。白名单规范说明了“白名单”的生命周期，包括申请、审核、发布、续签、监督等阶段，并明确了每个环节的工作要求。

申请阶段：白名单规范明确了企业申请资质要求，制定了初审、复审和终审的三级审查机制，对申请加入白名单的移动互联网企业提出了严格的安全要求，并要求企业提供充足的证明材料：

（一）企业独立法人证明；

（二）企业经营许可证；

（三）企业组织机构代码证；

（四）企业税务登记证；

（五）企业注册资本证明，注册资本须大于 500 万；

（六）企业成立时间须大于 3 年；

（七）企业资信证明；

（八）中国反网络病毒联盟成员单位的推荐信。

ANVA 认为申请企业的证明材料合格后，会要求申请企业通过白名单申请平台（http://white.anva.org.cn）提交所申请进入白名单的数字证书文件，并报备利用该数字证书签发的所有历史应用程序文件。

图 43：移动互联网应用自律白名单发布平台

审核阶段：ANVA 设置了初审、复审和终审的三级审查机制，组织 ANVA 中的白名单工作组对申请企业报备的数字证书和所有历史应用程序文件进行安全检查。只有当白名单工作组

中的所有安全企业均认可某企业的白名单申请时，此项申请才能进入终审阶段。在终审阶段，ANVA 将根据初审和复审结果，评估企业的安全信誉，最终决定是否同意某企业的数字证书加入白名单。

发布阶段：在通过三级安全审查后，ANVA 将对进入白名单的企业和数字证书信息进行公示。若公示期内无异议，申请企业的数字证书将正式作为白名单。

监督阶段：当企业的数字证书进入白名单后，ANVA 要求企业继续报备利用该数字证书签发的所有应用程序文件进行安全抽查，同时开通网站投诉举报通道，接收对于白名单企业的投诉举报。当发现白名单企业有违规行为时，ANVA 将严肃处理违规企业，撤销白名单并向社会公示。

续签阶段：白名单有效期为两年，白名单企业在白名单到期时须向 ANVA 提出续签请求，否则视为自动放弃白名单。

三、白名单工作体系

白名单工作体系包括 ANVA、白名单工作组、应用商店自律组和开发者四个部分，其中 ANVA 负责对白名单工作的指导和监督，对白名单的审核、发布具有最终决定权。

为保证白名单审查工作的公正公平，ANVA 成立了由 11 家专业安全企业组成的白名单工作组，并设置了初审、复审和终审的三级审查机制，要求白名单工作组对白名单申请进行严格审查。白名单工作组成员既享有三大权利又须履行三大义务，其中，

三大权利：1、推荐权，具备推荐移动互联网企业加入白名单的权利；2、投票权，具备对申请企业是否加入白名单的投票表决权；3、监督权，具备对白名单企业的监督投诉权利。

三大义务：1、白名单审查义务，须完成 ANVA 组织的白名单审查工作任务；2、信任白名单义务，须在自有手机安全软件中信任白名单，并对白名单应用进行明显标识；3、阻截仿冒白名单应用义务，须在自有手机安全软件中对仿冒白名单应用的软件进行风险提示，并建议用户安装正版的白名单应用。

为保护安全的白名单应用，使更多的用户放心使用安全的白名单应用，ANVA 成立了由 23 家应用商店组成的应用商店自律组。加入应用商店自律组的成员单位须满足三项要求：1、自身安全要求，须报备本应用商店内的所有应用程序信息进行安全检查；2、黑白名单标识要求，须对本应用商店中的恶意应用和白名单应用进行醒目标识；3、积极响应要求，须及时响应政府部门对于恶意应用程序的下架要求。

2013 年 9 月 27 日，ANVA 举行了白名单工作组和应用商店自律组的成立仪式，首批移动互联网应用自律白名单工作组成员包括：北京奇虎科技有限公司、深圳市腾讯计算机系统有限公司、北京网秦天下科技有限公司、北京百度网讯科技有限公司、北京金山软件有限公司、北京安管佳科技有限公司、北京联想软件有限公司、趋势科技（中国）有限公司、恒安嘉新

（北京）科技有限公司、北京瑞星信息技术有限公司、哈尔滨安天科技股份有限公司。

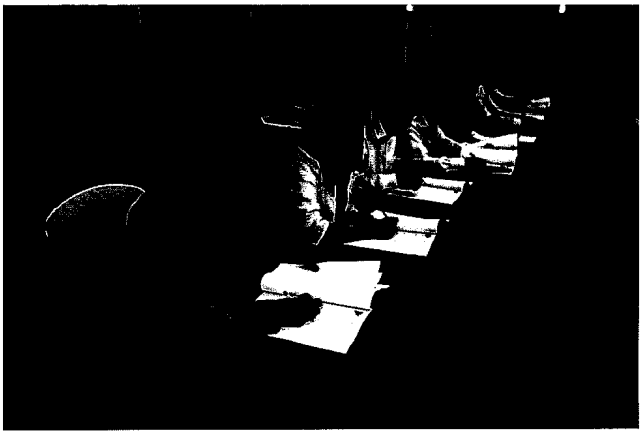


图 44：白名单工作组成员单位签约仪式

图 45：白名单工作组成员单位代表合影

首批 ANVA 应用商店自律组包括：中国移动 MM 商城、中国电信天翼空间、中国联通沃商店、中国移动手机游戏基地、360 手机助手、百度应用、腾迅应用宝、新浪应用中心、搜狐应用中心、网易应用中心、华为智汇云、联想乐商店、小米应用商店、OPPO 手机应用商店(NearMe)、UC 应用商店、N 多市场、安智市场、应用汇、91 无线、游戏狗、木蚂蚁、优亿市场、悠悠村。

图 46：应用商店自律组成员单位签约仪式（一）

图 47：应用商店自律组成员单位签约仪式（二）

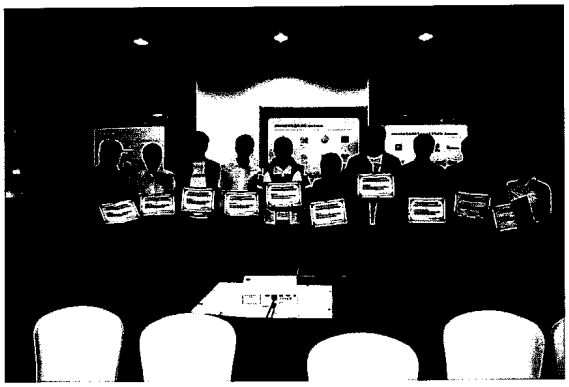


图 48：应用商店自律组成员单位代表合影（一）

图 49：应用商店自律组成员代表合影（二）

四、首批白名单企业

2013 年 9 月至 11 月期间，ANVA 在众多申请加入白名单的企业中，筛选出 14 家符合资质要求的申请企业，随之启动了首批“白名单”的审查工作。审查要求白名单工作组对申请者以往发布的应用程序进行多轮审查，若发现申请者曾经开发过恶意程序且未及时整改，应于第一时间取消该申请者的“白名单”资格。

经审查，中国移动和游戏、深圳市腾讯计算机系统有限公司、北京奇虎科技有限公司、北京金山网络科技有限公司、北京瑞星信息技术有限公司、北京安管佳科技有限公司、高德软件有限公司、哈尔滨安天科技股份有限公司、优视科技有限公司等 9 家移动互联网企业的 16 款数字证书和 25 款 APP 通过了反网络病毒联盟的认证，成为首批“移动互联网应用自律白名单”成员。

2013 年 12 月 27 日， ANVA 公布了首批“移动互联网应用自律白名单”，以上 9 家移动互联网企业的 16 款数字证书和 25 款应用程序进入白名单（具体信息请见附录）。白名单工作组将在其终端安全软件中信任由这 16 款数字证书所签发的 APP 程序，并对篡改自这 25 款 APP 的仿冒应用软件进行提示。

图 50：首批移动互联网应用自律白名单企业代表签约仪式

图 51：首批移动互联网应用自律白名单企业代表合影

五、2014 年工作计划

2014 年，ANVA 将继续推动“移动互联网应用自律白名单”工作，落实白名单工作组和应用商店自律组对“白名单”应用的标示工作，并开展打击仿冒白名单的恶意盗版应用工作，同时积极吸纳更多的优质移动互联网企业加入白名单。

ANVA 希望通过“白名单”工作传播移动互联网“正能量”，引导开发者、应用商店和终端安全企业共同构建健康的移动互联网生态系统，真正把“网民”的正当权益放在首位，有力地推动了移动互联网行业的安全有序发展。

第六章 ANVA 篇

2009 年 7 月，中国互联网协会网络与信息安全工作委员会发起成立了中国反网络病毒联盟（ANVA），由 CNCERT/CC 负责具体运营管理。联盟旨在广泛联合基础电信企业、互联网内容和服务提供商、网络安全企业等行业机构，积极动员社会力量，通过行业自律机制共同开展互联网网络病毒信息收集、样本分析、技术交流、防范治理、宣传教育等工作，以净化公共互联网网络环境，提升互联网网络安全水平。

中国反网络病毒联盟
Anti Network-Virus Alliance of china

图 52：中国互联网协会反网络病毒联盟（ANVA）标志

2013 年，为应对日益严峻的移动互联网网络安全威胁，ANVA 扩充了移动互联网领域的工作体系，积极吸纳安全管家、赛门铁克等移动互联网安全企业加入联盟，组织 23 家国内主流的应用商店成立 ANVA 应用商店自律组，并大力开展“移动互联网应用自律白名单”工作，成立了由 11 家安全企业组成的白名单工作组。截至 2013 年 12 月，ANVA 联盟成员单位数量增至 37 家，2013 年新增 6 家企业，包括北京联想软件有限公司、北京安管佳科技有限公司、赛门铁克软件（北京）有限公司、深圳市深信服电子科技有限公司、招商银行、卓望公司。

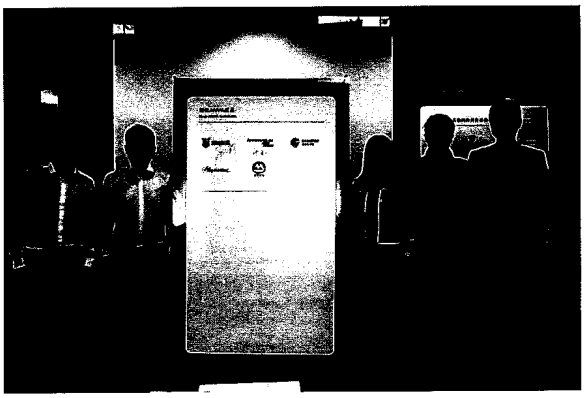


图 53：2013 年 9 月加入 ANVA 的企业代表合影
（左起：联想、深信服、安全管家、招商银行、赛门铁克）

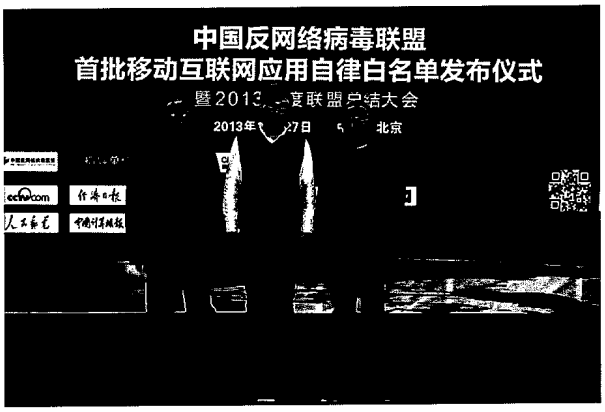


图 54：2013 年 12 月加入 ANVA 的企业代表合影

在联盟成员单位的大力协助下，ANVA 于 2013 年组织开展联盟内移动互联网恶意程序样本、恶意程序传播链接的共享和判定工作，全年发布传播恶意程序的 URL 链接黑名单 22025 条，判定移动互联网恶意样本 105512 个，发布移动互联网恶意程序黑名单 97621 条，有效促进了成员单位在恶意程序样本共享、分析研判等方面的协作，成为支撑政府主管部门，协助 CNCERT/CC 加强恶意程序治理工作的重要平台。

一、2013 年安全企业报送恶意程序情况

- **现状二十五：2013 年 CNCERT 判定 14 家安全企业和 19 个 CNCERT 分中心报送的疑似恶意程序 105512 个，其中安天报送得分排名第一。**

依据《机制》要求，CNCERT 受工业和信息化部委托，负责对移动互联网恶意程序样本进行认定命名，是国内认定移动互联网恶意程序的权威机构。

2013 年 CNCERT 建立了移动互联网恶意程序报送平台(https://msample.anva.org.cn)并投入使用，要求基础电信运营企业、中国互联网协会 12321 网络不良与垃圾信息举报中心、CNCERT 分中心以及部分 ANVA 成员单位进行常态化的恶意程序报送工作，报送样本数量较 2012 年提高超过 20 倍。

ANVA 全年共接收 14 家安全企业和 19 个 CNCERT 分中心报送的移动恶意程序疑似样本数量总计 105512 个（已按 MD5 值去重），其中 Android 平台样本 104539 个，Symbian 平台样本 964 个，J2ME 平台样本 1 个，linux 平台 1 个，WindowsPhone 平台样本 2 个。此外，接收到相关样本详细分析报告 272 份。

CNCERT 对接收到的样本进行了分析和鉴定，依照通信行业标准 YD/T 2439-2012《移动

互联网恶意程序描述格式》，判定其中 97621 个样本为恶意程序，其中 Android 平台样本 97011 个，Symbian 平台样本 609 个，WindowsPhone 平台样本 1 个。各报送单位的报送得分排名情况如下表所示1：

单位名称	样本数量	恶意程序数量	恶意程序家族数	恶意程序变种数	分析报告数量	纳入处置的样本数量	报送得分
安天	4708	4618	85	198	0	1919	201048
网秦	3827	3383	168	297	1	760	87413
金山	74662	74399	79	157	1	1	78459
奇虎	28620	25190	252	427	0	0	37020
恒安嘉新	1374	1006	201	248	99	130	24496
腾讯	5139	4053	169	253	0	0	11653
CNCERT 江苏分中心	134	91	33	37	28	20	4011
CNCERT 辽宁分中心	32	31	23	26	5	29	3981
CNCERT 福建分中心	23	23	16	17	16	23	3293
安全管家	594	453	56	92	0	0	3053
CNCERT 新疆分中心	21	20	14	17	0	20	2610
CNCERT 湖北分中心	69	65	19	24	0	17	2575
CNCERT 宁夏分中心	17	17	10	12	16	17	2457
CNCERT 内蒙古分中心	13	12	11	12	13	12	1922
CNCERT 江西分中心	15	15	12	13	10	12	1905
百度	600	572	26	47	0	0	1822

1 报送得分=+“恶意程序数量”*1+“恶意程序家族数量”*30+“恶意程序变种数量”*10+“分析报告数量”*20+“纳入处置的样本数量”*100

洋浦科技	801	782	23	31	0	0	1782
中国移动	24	21	17	18	28	4	1671
CNCERT 广东分中心	19	16	11	12	8	9	1526
CNCERT 上海分中心	11	10	8	8	7	10	1470
CNCERT 甘肃分中心	9	9	6	7	5	9	1259
CNCERT 青海分中心	9	7	6	7	8	6	1017
CNCERT 湖南分中心	11	7	7	7	1	7	1007
赛门铁克	1962	66	11	12	0	4	916
CNCERT 黑龙江分中心	32	28	4	7	28	1	878
CNCERT 河北分中心	8	8	7	8	6	3	718
华为	155	34	11	14	0	0	504
CNCERT 山东分中心	3	3	2	2	3	3	443
中国电信	2	2	1	2	1	2	272
CNCERT 河南分中心	1	1	1	1	1	1	161
CNCERT 安徽分中心	1	1	1	1	1	1	161
CNCERT 吉林分中心	1	1	1	1	0	1	141

对于样本报送得分超过 10000 的企业，ANVA 在 2013 年度总结大会中向其颁发了“2013 年安全企业杰出贡献奖”。对于其他报送样本得分较高的企业以及参与白名单审查工作的企业，ANVA 向其颁发了“2013 年安全企业优秀贡献奖”。

图 55：2013 年 ANVA 安全企业杰出贡献奖

图 56：2013 年 ANVA 安全企业优秀贡献奖

二、2013 年应用商店报备应用程序信息情况

- **现状二十六： 2013 年 CNCERT 判定 37 家应用商店报备的应用程序信息 8481374 个，其中“应用汇”报备的应用数量排名第一。**

依据《移动互联网恶意程序监测与处置机制》，CNCERT 受工业和信息化部委托，负责对传播移动互联网恶意程序的传播服务器进行处置。CNCERT 通过监测发现国内存在传播移动恶意程序现象的应用商店超过 300 家（域名去重），并已与其中传播量较大的 95 家应用商店建立处置工作机制，并要求应用商店报备本商店的应用程序信息，包括应用程序名称、类别、

版本、描述、开发者信息、文件 MD5 和下载链接等信息。

2013 年 37 家国内主流应用商店向 CNCERT 送检其应用商店内全量的移动应用程序，全年共收到以上 37 家应用商店送检应用程序达 8481374 条。通过对上述样本进行分析和检测，CNCERT 依照通信行业标准 YD/T 2439-2012《移动互联网恶意程序描述格式》，判定 38677 个应用程序为恶意程序，且均为 Android 平台恶意程序，共涉及到 38632 个恶意程序发布或下载链接。CNCERT 建议国内其他应用商店向上述 37 家应用商店学习，主动送检移动应用程序以提高应用商店的安全性。对于在应用商店中检测发现的恶意程序，CNCERT 已在第一时间通知相关应用商店进行下架处置，相关情况请参考本报告第二篇“处置篇”。

排名	应用商店名称	应用商店域名	恶意信息数量
1	应用汇	appchina.com	1068226
2	91RB	91rb.com	1049827
3	安卓市场	hiapk.com	863395
4	安智市场	anzhi.com	786035
5	新浪应用中心	sina.com.cn	757469
6	机锋市场	gfan.com	428653
7	360 手机助手	360tpcdn.com	394705
8	联想乐商店	lenovomm.com	363421
9	魅族应用中心	meizu.com	329264
10	历趣手机应用商店	liqucn.com	312068
11	百度应用中心	baidu.com	293478
12	N 多网	nduoa.com	266866
13	木蚂蚁应用市场	mumayi.com	263015
14	91 市场	91.com	169486
15	宜搜搜索	easou.com	141043
16	十字猫手机资源站	crossmo.com	132193
17	网易应用中心	163.com	106145
18	腾讯应用宝	myapp.com	101420
19	华为智汇云	hicloud.com	73565
20	UC 应用商店	uc.cn	70509
21	优亿市场	eoemarket.com	66823

22	OPPO 手机应用商店	nearme.com.cn	59075
23	3G 门户	3g.cn	51073
24	球球搜	qiuqiu.so	50000
25	155 安卓	155.cn	46345
26	爱卓网	iandroid.cn	36847
27	卓乐网	sjapk.com	36287
28	飞流网	feiliu.com	30689
29	极游网	ggg.cn	29462
30	泡椒网	paojiao.cn	27452
31	中兴汇天地	ztems.com	25651
32	悠悠村	uuserv30.net	15489
33	飞鹏网	fpwap.com	15041
34	酷派应用商店	coolmart.net.cn	9505
35	游戏狗	gamedog.cn	8533
36	吾爱主题	5izhuti.com	1986
37	乐讯	lexun.com	333

通过综合考虑应用程序信息数量，响应 CNCERT 处置工作情况等因素，ANVA 在 2013 年度总结大会中向报送信息数量大、下架恶意程序快的 9 家应用商店颁发了“2013 年应用商店杰出贡献奖”，对报送信息数量较大、下架恶意程序快的 16 家应用商店颁发了“2013 年应用商店优秀贡献奖”。

图 57：2013 年 ANVA 应用商店杰出贡献奖

图 58：2013 年 ANVA 应用商店优秀贡献奖

附一、中国反网络病毒联盟介绍

中国反网络病毒联盟（以下简称联盟，英文 China Anti-Network Virus Alliance,缩写 ANVA，官方网站：www.anva.org.cn）。由中国互联网协会发起成立、国家互联网应急中心具体组织运作，在中国互联网协会网络与信息安全工作委员会中成立专门的工作组——中国反网络病毒联盟，致力于通过行业自律机制开展互联网网络病毒防范、治理工作。作为公益性社团组织，联盟依托国家互联网应急中心的技术和资源基础，动员社会积极力量广泛参与，通过社会化机制组织开展互联网网络病毒防范、治理相关的信息收集发布、技术研发交流、宣传教育、联合打击等工作，并面向社会提供信息咨询、技术支持等服务，以净化公共互联网网络环境，提升互联网网络安全水平。

联盟成员单位主要包括互联网运营机构（基础电信运营商、域名注册管理和服务机构、IDC 等）、互联网服务机构（门户网站、搜索引擎服务商、网络游戏服务商、网络应用软件提供商、电子商务服务商等内容和应用服务提供商）、网络安全机构（网络安全产品提供商和服务提供商、网络安全研究机构等）、依托互联网开展业务的重要信息系统单位（银行、证券、保险等金融行业，水电能源等基础设施行业）等相关行业机构以及广大互联网用户，具体名单如下（排名不分先后）：

- 国家互联网应急中心
- 中国电信集团公司
- 中国移动通信集团公司
- 中国联合网络通信集团有限公司
- 中国互联网络信息中心
- 中国软件测评中心
- 北京百度网讯科技有限公司
- 深圳市腾讯计算机系统有限公司
- 北京启明星辰信息安全技术有限公司
- 北京神州绿盟科技有限公司
- 奇虎 360 软件(北京)有限公司
- 阿里巴巴（中国）有限公司
- 金山网络科技有限公司
- 北京江民新科技术有限公司
- 北京搜狐互联网信息服务有限公司
- 新浪网技术（中国）有限公司

- 网之易信息技术（北京）有限公司
- 北京万网志成科技有限公司
- 北京世纪互联宽带数据中心有限公司
- 北京天融信科技有限公司
- 北京瑞星信息技术有限公司
- 哈尔滨安天科技股份有限公司
- 北京网秦天下科技有限公司
- 华为技术有限公司
- 西门子（中国）有限公司
- 优视科技有限公司
- 北京西塔网络科技股份有限公司
- 北京知道创宇信息技术有限公司
- 北京洋浦伟业科技发展有限公司
- 趋势科技（中国）有限公司
- 恒安嘉新（北京）科技有限公司
- 北京联想软件有限公司
- 北京安管佳科技有限公司
- 赛门铁克软件（北京）有限公司
- 深圳市深信服电子科技有限公司
- 招商银行
- 卓望公司

附二、中国反网络病毒联盟白名单工作组成员单位

北京奇虎科技有限公司

深圳市腾讯计算机系统有限公司

北京网秦天下科技有限公司

北京百度网讯科技有限公司

北京金山软件有限公司

北京安管佳科技有限公司

北京联想软件有限公司

趋势科技（中国）有限公司

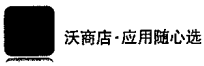
恒安嘉新（北京）科技有限公司

北京瑞星信息技术有限公司

哈尔滨安天科技股份有限公司

附三、中国反网络病毒联盟应用商店自律组成员名单

中国电信天翼空间



中国联通沃商店


中国移动 MM

网易应用中心

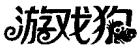
小米应用商店

OPPO 手机应用商店

N 多市场

安智市场

91 无线



游戏狗

木蚂蚁

悠悠村

搜狐应用中心


百度应用


腾迅应用宝

中国移动和游戏

华为智汇云

360 手机助手


联想乐商店


UC 应用商店

优亿市场

应用汇


新浪应用中心

附四、首批移动互联网应用自律白名单企业

公司 Logo	单位名称	证书信息	应用信息	
和游戏	中国移动和游戏	040709F8DFDDC66DAB6C13EB41AA91A8	移动游戏大厅 移动飞牙	
腾讯网 QQ.com	深圳市腾讯计算机系统有限公司	00B1208638DE0FCD3E920886D658DAF6	腾讯手机管家	
360 www.360.cn	北京奇虎科技有限公司	DC27396CF677DD234244DEE1E5FF01ED DC6DBD6E49682A57A8B82889043B93A8 CA45263BC938DA16EF1B069C95E61BA2	360 手机助手 优化大师 手机卫士 手机卫士双卡版 省电王 隐私保险箱	
金山网络 www.ijinshan.com	北京金山网络科技有限公司	EE3200D6E4D372FB12ABC923EA5633C1 010D2888DD080F062E00BFAAF9C3982F 6DD3A71E2B769691670C30CABAB5B34E D7FC8D1E5125BD280B944A61A48F5399 FE2E35D0D11D0C2CB4E56F61A352F030 1B387924D85B6FC3E8B975572A521C24	微看电视 手机毒霸 猎豹浏览器 猎豹清理大师 金山手机助手 金山电池医生	
RISING 瑞星 www.rising.com.cn	北京瑞星信息技术有限公司	4E2C644BEA1559E70D65BCADF8518100	瑞星手机安全软件 瑞星手机应用中心	

安全管家	北京安管佳科技有限公司	D96A400B3079C1838E0818FA5F1E4E7A	安全管家 安全优化 安全省电	
高德 AutoNavi	高德软件有限公司	3F9EAEA4F2D4285C2DDBBDA739136479	高德地图	
ANTIY 安天实验室	哈尔滨安天科技股份有限公司	3E3975551502F736092E5CAE4409955F	AVL 手机引擎	ANTIY
UC优视	优视科技有限公司	51A5EB6E85033F42271535AAD119A2F4 F7C81DF3BA970E4B4B661DB3169B09F2	UC 浏览器 UC 浏览器（PAD） UC 浏览器（U3）	

附五、移动互联网恶意程序行为属性[2]

1） 恶意扣费

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，具有恶意扣费属性。包括但不限于具有以下任意一种行为的移动互联网恶意程序具有恶意扣费属性：

——在用户不知情或未授权的情况下，自动订购移动增值业务的；

——在用户不知情或未授权的情况下，自动利用移动终端支付功能进行消费的；

——在用户不知情或未授权的情况下，自动拨打收费声讯电话的；

——在用户不知情或未授权的情况下，自动订购其它收费业务的；

——在用户不知情或未授权的情况下，自动通过其它方式扣除用户资费的。

2） 信息窃取

在用户不知情或未授权的情况下，获取涉及用户个人信息、工作信息或其它非公开信息的，具有信息窃取属性。包括但不限于具有以下任意一种行为的移动互联网恶意程序具有信息窃取属性：

——在用户不知情或未授权的情况下，获取短信内容的；

——在用户不知情或未授权的情况下，获取彩信内容的；

——在用户不知情或未授权的情况下，获取邮件内容的；

——在用户不知情或未授权的情况下，获取通讯录内容的；

——在用户不知情或未授权的情况下，获取通话记录的；

——在用户不知情或未授权的情况下，获取通话内容的；

——在用户不知情或未授权的情况下，获取地理位置信息的；

——在用户不知情或未授权的情况下，获取本机手机号码的；

——在用户不知情或未授权的情况下，获取本机已安装软件信息的；

——在用户不知情或未授权的情况下，获取本机运行进程信息的；

——在用户不知情或未授权的情况下，获取用户各类帐号信息的；

——在用户不知情或未授权的情况下，获取用户各类密码信息的；

——在用户不知情或未授权的情况下，获取用户文件内容的；

——在用户不知情或未授权的情况下，记录分析用户行为的；

——在用户不知情或未授权的情况下，获取用户网络交易信息的；

[2] 依照通信行业规范 YD/T 2439-2012《移动互联网恶意程序描述格式》。

——在用户不知情或未授权的情况下，获取用户收藏夹信息的；

——在用户不知情或未授权的情况下，获取用户联网信息的；

——在用户不知情或未授权的情况下，获取用户下载信息的；

——在用户不知情或未授权的情况下，利用移动终端麦克风、摄像头等设备获取音频、视频、图片信息的；

——在用户不知情或未授权的情况下，获取用户其它个人信息的；

——在用户不知情或未授权的情况下，获取用户其它工作信息的；

——在用户不知情或未授权的情况下，获取其它非公开信息的。

3） 远程控制

在用户不知情或未授权的情况下，能够接受远程控制端指令并进行相关操作的，具有远程控制属性。包括但不限于具有以下任意一种行为的移动互联网恶意程序具有远程控制属性：

——由控制端主动发出指令进行远程控制的；

——由受控端主动向控制端请求指令的。

4） 恶意传播

自动通过复制、感染、投递、下载等方式将自身、自身的衍生物或其它恶意程序进行扩散的行为，具有恶意传播属性。包括但不限于具有以下任意一种行为的移动互联网恶意程序具有恶意传播属性：

——自动发送包含恶意程序链接的短信、彩信、邮件、WAP 信息等；

——自动发送包含恶意程序的彩信、邮件等；

——自动利用蓝牙通讯技术向其它设备发送恶意程序的；

——自动利用红外通讯技术向其它设备发送恶意程序的；

——自动利用无线网络技术向其它设备发送恶意程序的；

——自动向存储卡等移动存储设备上复制恶意程序的；

——自动下载恶意程序的；

——自动感染其它文件的。

5） 资费消耗

在用户不知情或未授权的情况下，通过自动拨打电话、发送短信、彩信、邮件、频繁连接网络等方式，导致用户资费损失的，具有资费消耗属性。包括但不限于具有以下任意一种行为的移动互联网恶意程序具有资费消耗属性：

——在用户不知情或未授权的情况下，自动拨打电话的；

——在用户不知情或未授权的情况下，自动发送短信的；

——在用户不知情或未授权的情况下，自动发送彩信的；

——在用户不知情或未授权的情况下，自动发送邮件的；

——在用户不知情或未授权的情况下，频繁连接网络，产生异常数据流量的。

6） 系统破坏

通过感染、劫持、篡改、删除、终止进程等手段导致移动终端或其它非恶意软件部分或全部功能、用户文件等无法正常使用的，干扰、破坏、阻断移动通信网络、网络服务或其它合法业务正常运行的，具有系统破坏属性。包括但不限于具有以下任意一种行为的移动互联网恶意程序具有系统破坏属性：

——导致移动终端硬件无法正常工作的；

——导致移动终端操作系统无法正常运行的；

——导致移动终端其它非恶意软件无法正常运行的；

——导致移动终端网络通讯功能无法正常使用的；

——导致移动终端电池电量非正常消耗的；

——导致移动终端发射功率异常的；

——导致运营商通信网络无法正常工作的；

——导致其它合法业务无法正常运行的；

——对用户文件、系统文件或其它非恶意软件进行感染、劫持、篡改的；

——在用户不知情或未授权的情况下，对系统文件或其它非恶意软件进行删除、卸载、终止进程或限制运行的；

——在用户不知情或未授权的情况下，对用户文件进行删除的。

7） 诱骗欺诈

通过伪造、篡改、劫持短信、彩信、邮件、通讯录、通话记录、收藏夹、桌面等方式，诱骗用户，而达到不正当目的的，具有诱骗欺诈属性。包括但不限于具有以下任意一种行为的移动互联网恶意程序具有诱骗欺诈属性：

——伪造、篡改、劫持短信，以诱骗用户，而达到不正当目的的；

——伪造、篡改、劫持彩信，以诱骗用户，而达到不正当目的的；

——伪造、篡改、劫持邮件，以诱骗用户，而达到不正当目的的；

——伪造、篡改通讯录，以诱骗用户，而达到不正当目的的；

——伪造、篡改收藏夹，以诱骗用户，而达到不正当目的的；

——伪造、篡改通讯记录，以诱骗用户，而达到不正当目的的；

——伪造、篡改、劫持用户文件；以诱骗用户，而达到不正当目的的。

——伪造、篡改、劫持用户网络交易数据，以诱骗用户，而达到不正当目的的；

——冒充国家机关、金融机构、移动终端厂商、运营商或其它机构和个人，以诱骗用户，

而达到不正当目的的；

——伪造事实，诱骗用户退出、关闭、卸载、禁用或限制使用其它合法产品或退订服务的。

8） 流氓行为

执行对系统没有直接损害，也不对用户个人信息、资费造成侵害的其它恶意行为具有流氓行为属性。包括但不限于具有以下任意一种行为的移动互联网恶意程序具有流氓行为属性：

——在用户不知情或未授权的情况下，长期驻留系统内存的；

——在用户不知情或未授权的情况下，长期占用移动终端中央处理器计算资源的；

——在用户不知情或未授权的情况下，自动捆绑安装的；

——在用户不知情或未授权的情况下，自动添加、修改、删除收藏夹、快捷方式的；

——在用户未授权的情况下，弹出广告窗口的；

——导致用户无法正常退出程序的；

——导致用户无法正常卸载、删除程序的；

——在用户未授权的情况下，执行其它操作的。