



CNCERT移动互联网安全监测与处置专报

2013 年 7 月 总第 1 期



热线电话: +8610 82990999 (中文), 82991000 (英文) 传真: +8610 82990399

摘要:

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 7 月, 移动互联网网络安全状况整体评价为差。主要数据如下:

- 境内感染移动互联网恶意程序的用户数为976904个, 感染用户最多的省份为广东, 感染用户最多的运营商为中国联通;
- 中国互联网协会反网络病毒联盟 (ANVA) 接收各成员单位报送移动互联网恶意程序9699个, 具有网络控制端的恶意程序有1507个, 可被用于远程控制、隐私窃取的恶意攻击。
- 境内33家主流手机应用商店送检在架移动应用程序6593532个, 其中恶意程序38632个 (占应用总数的0.58%), 经CNCERT通知后, 下架30364个, 下架率达78.6%。

电子邮件: cncert@cert.org.cn

PGP Key: <http://www.cert.org.cn/cncert.asc>

网址: <http://www.cert.org.cn/>

关于国家互联网应急中心（CNCERT）

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 1999 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。

2003 年，CNCERT 在全国 31 个省、直辖市、自治区成立分中心，形成了全国性的互联网网络安全信息共享、技术协同能力。目前，CNCERT 作为国家公共互联网网络安全应急体系的核心技术协调机构，在社会网络安全防范机构、公司、大学、科研院所的支撑和支援下，在协调骨干网络运营单位应急组织、域名服务机构应急组织等国内网络安全应急组织共同处理网络安全事件方面发挥着重要作用。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，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。截止 2012 年，CNCERT 与 51 个国家和地区的 91 个组织建立了“CNCERT 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

《CNCERT 移动互联网安全监测与处置专报》以下简称“CNCERT 移动互联网专报”) 为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, CNCERT 或 CNCERT/CC)的电子刊物,由 CNCERT 编制并拥有版权。报告中凡摘录或引用内容均已指明出处,其版权归相应单位所有。本报告所有权利及许可由 CNCERT 进行管理,未经 CNCERT 同意,任何单位或个人不得将本报告以及其中内容转发或用于其他用途。

CNCERT 力争保证本报告的准确性和可靠性,其中的信息、数据、图片等仅供参考,不作为您个人或您企业实施安全决策的依据,CNCERT 不承担与此相关的一切法律责任。

编者按:

感谢您阅读《CNCERT 移动互联网安全监测与处置专报》,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: cnccert@cert.org.cn。

一、移动互联网恶意程序监测情况

➤ CNCERT 掌握境内移动互联网恶意程序的情况

截至 2013 年 7 月,CNCERT 通过自主监测和样本交换共掌握移动互联网恶意程序 233347 个,涉及家族 833 个。其中恶意程序按照操作系统分类如图 1 所示,恶意程序按照恶意行为属性分类如图 2 所示。

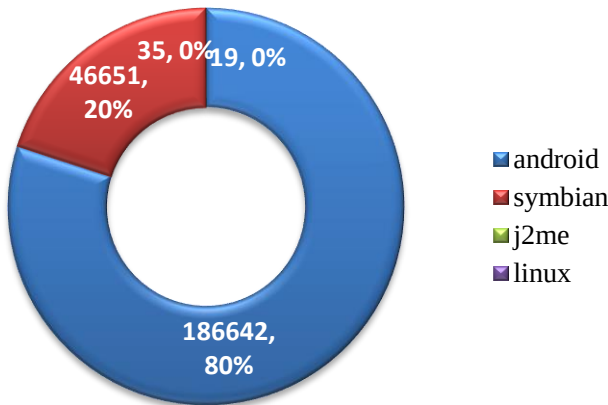


图 1: 2013 年 7 月感染移动恶意程序用户所用终端的操作系统分布图

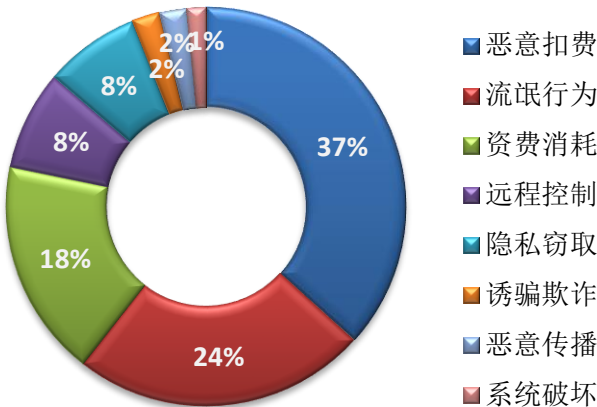


图 2: 2013 年 7 月感染移动恶意程序用户所用终端的操作系统分布图

➤ 各省感染移动互联网恶意程序的情况

2013 年 7 月,我国境内感染移动互联网恶意程序的用户数量达

976904，其中感染用户数量排名前三的省份为：

表 1：2013 年 7 月感染移动互联网恶意程序用户数量排名前三的省份

排名	省份	感染用户数量
1	广东	233345
2	浙江	133555
3	四川	109494

按照全国各省感染移动恶意程序的用户数量情况，图 3 显示了各省感染移动恶意程序的严重程度。



图 3： 2013 年 7 月全国各省感染移动恶意程序的热度图

➤ 感染移动互联网恶意程序的运营商分布情况

2013 年 7 月，基础电信运营商中国电信、中国移动、中国联通感染移动互联网恶意程序的用户分布情况如图 4 所示。其中，中国联通感染移动恶意程序的用户数量最多¹，达 571121 个，占有所有感染用

注 1：根据运营商 2013 年 1 月份公布的运营数据：中国移动用户总数达 7.15 亿，在网 3G 用户总数达 9498 万；中国联通的用户总数则为 2.43 亿，3G 用户数为 8013 万；而中国电信用户总数为 1.63 亿户，其中 3G 用户增至 7206 万户。

户的 62%；中国电信感染移动恶意程序的用户数量最少，达 64790 个，占有所有感染用户的 7%。

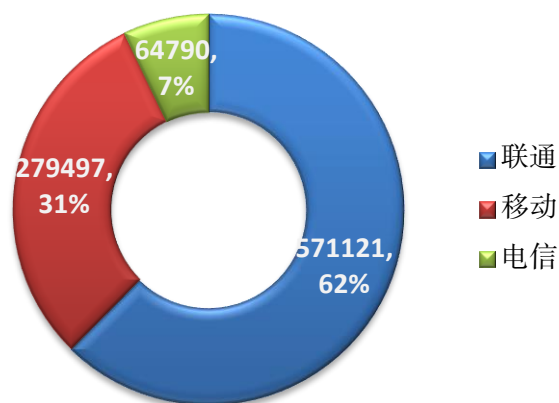


图 4： 2013 年 7 月感染移动恶意程序用户所属运营商的分布图

➤ 感染移动互联网恶意程序的终端操作系统分布情况

2013 年 7 月，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 5 所示。其中，使用 Android 系统的感染用户数量最多，近 70 万，占有所有用户的 76%；使用 J2ME 系统的感染用户数量最少，小于 500，不足所有用户的 1%。

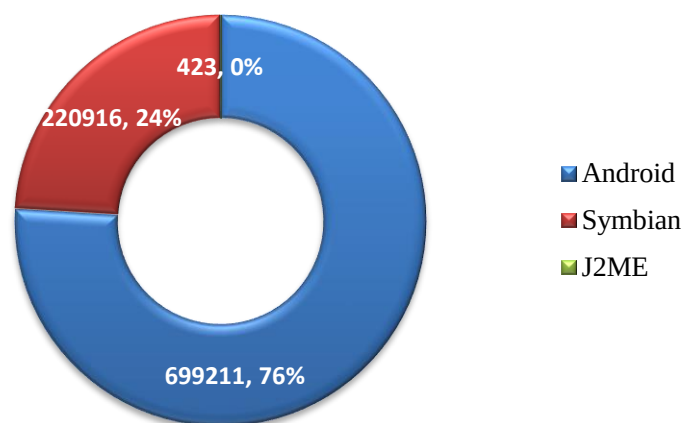


图 5： 2013 年 7 月感染移动恶意程序用户所用终端的操作系统分布图

➤ 感染用户数量排名前十的恶意程序家族情况

2013 年 7 月，感染用户量排名前十的移动互联网恶意程序家族如表 2 所示，其中有 9 个 Android 平台下的恶意程序家族、1 个 Symbian 平台下的恶意程序家族。感染用户量最多的家族是 ooqqxx 家族，在全国范围内感染用户 220269 个。

表 2： 2013 年 7 月感染用户量排名前十的移动互联网恶意程序家族

排名	恶意程序家族名称	感染用户数量	所属平台	恶意行为类型 ²
1	A.expense.ooqqxx	220269	Android	资费消耗
2	A.rogue.airpush	113100	Android	流氓行为
3	A.privacy.counterclank	79450	Android	信息窃取
4	A.expense.adaisrs	32209	Android	资费消耗
5	A.expense.apxxpush	31388	Android	资费消耗
6	A.privacy.skirtup	29790	Android	信息窃取
7	A.privacy.appperhand	27740	Android	信息窃取
8	A.payment.nl	18704	Android	恶意扣费
9	S.payment.CoolCaller	16151	Symbian	恶意扣费
10	A.fraud.smishing	7257	Android	诱骗欺诈

以上感染用户量排名前十移动恶意程序家族的具体说明如下：

1) A.expense.ooqqxx

该病毒插件的主要目的是后台运行，未经用户允许联网下载应用程序，消耗大量流量资源，造成资费消耗。

2) A.rogue.airpush

该家族为恶意广告插件，会在通知栏推送广告，同时会在用户不知情的状态下后台私自上传用户地理位置等隐私信息到远程服务器，此外还可能修改书签，在桌面创建快捷方式。

3) A.privacy.counterclank

注 2：恶意行为属性分类参照通信行业标准 YD/T 2439-2012《移动互联网恶意程序描述格式》中定义的八大类恶意行为，具体内容参见附录。

该家族在用户不知情的状态下后台私自获取用户浏览器书签,手机固件信息,进行隐私窃取;在桌面创建快捷方式,并修改书签等,具有流氓行为。

4) A.expense.adaisrs

该家族被捆绑了恶意广告插件 adaisrs,运行后会在用户不知情的状态下后台私自下载推广软件;下载完推广软件后,该应用还会弹出通知栏诱导用户点击安装,造成用户资费消耗。

5) A.expense.apxxpush

该家族被捆绑了恶意推广广告包 com.aseiei.appxxx,运行后会在用户不知情的状态下后台私自下载推广软件,大量消耗用户流量,造成资费消耗。

6) A.privacy.skirtup

该家族运行后会在用户不知情的状态下后台私自收集应用程序进程名,程序安装名称,网络类型名称等用户隐私上传到远程服务器。

7) A.privacy.appperhand

该家族在用户不知情或者未授权的情况下,接收远端服务器端控制指令,执行下载安装程序、打开网页删除数据等操作;窃取用户手机 IMEI 号、手机 wifi mac 地址等信息,上传至远程服务器;在桌面创建快捷方式,并且收集用户浏览器书签、手机设备等信息,同时修改手机的默认浏览器主页为 searchmobileonline.com,并为其添加的书签。包含广告包的程序可能被利用来恶意推送广告,给用户造成一定的安全威胁。

8) A.payment.nl

该家族在用户不知情或者未授权的情况下,在运行过程中通过后台联网获取特定 SP 服务号码,并发送短信订制 SP 服务,同时拦截特定号码发送的扣费确认短信,以及拦截带有“客服”、“资费”、“1.00 元”、“2.00 元”、“元/条”、“元/次”等关键词信息的短信,达到恶意扣费的目的;窃取手机号码等隐私信息,上传到服务器;私自下载安装程序,造成资费消耗。

9) S.payment.CoolCaller

该家族在用户不知情或者未授权的情况下,在运行过程中会获取用户手机的 IMEI、IMSI 号码以及手机型号和 SIM 卡服务中心号码,并将获得信息发送到远端服务器。同时病毒在后台接受远程服务器命令控制,可能下载新的恶意插件到用户手机执行。病毒在执行过程中会向 SP 端口 10657301、10657525 发送订购业务短信,并屏蔽 10086 的业务订购回执短信,达到其隐藏恶意订购的目的。

10) A.fraud.smishing

该家族主要目的是利用 Android 系统未对该广播来源进行核实的漏洞制造虚假短信,直接构造发往 com.android.mms (系统短信) 的通知,从而让用户以为是接收到的短信,可以进行诱骗欺诈。

二、移动互联网恶意程序报送情况

依据《机制》，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 年初，CNCERT 建立了移动互联网恶意程序报送平台（<https://msample.anva.org.cn>）并投入试用，向基础电信运营企业、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 成员单位提供报送通道，同时通知各单位进行常态化的恶意程序报送工作。

报送平台于在 2013 年 7 月 1 日正式运行，7 月 1 日至 7 月 31 日期间，本报送平台运行正常，报送情况汇总说明如下：

共接收样本数量总计 9699 个（已按 MD5 值去重），其中 Android 平台样本 9372 个，Symbian 平台样本 327 个。此外，接收到相关样本详细分析报告 92 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 8099 个样本为恶意程序，根据恶意行为属性分类如图 6 所示，另有 1455 个 Android 平台样本未认定为恶意或暂未能认定。

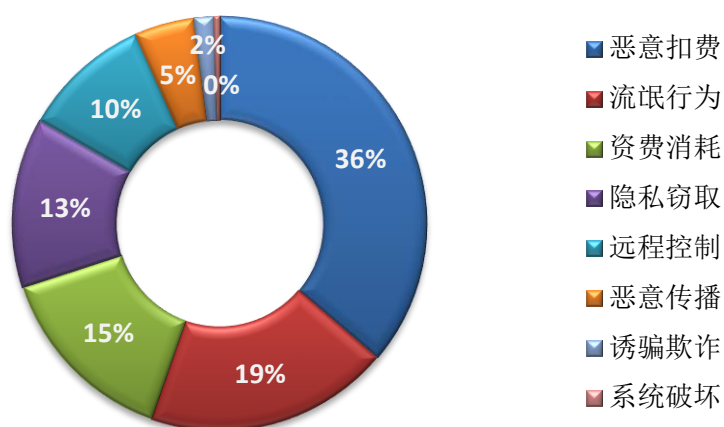


图 6： 2013 年 7 月各单位报送移动互联网恶意程序按照恶意行为属性的分布图

CNCERT 整理了 1507 个识别为恶意且获得网络控制端（域名或 IP）的样本以及对应的 324 条 URL 记录，将协调基础电信运营企业进行处置。

表 3： 2013 年 7 月各单位报送移动互联网恶意程序的情况统计

排名	报送单位名称	恶意程序 报送数量	恶意程序 家族数	恶意程序 变种数	纳入处置的 恶意程序数量
1	奇虎	6209	198	312	14
2	安天	2430	71	133	1456
3	恒安嘉新	410	94	102	35
4	金山毒霸	247	7	10	8
5	安全管家	198	28	47	2
6	百度	100	12	20	0
7	梆梆	68	10	10	1
8	华为	28	7	6	0
9	网秦	10	7	8	5
	总计(MD5 去重)	9699	302	491	1507

2013 年 7 月，各单位报送移动互联网恶意程序的具体信息如表 3 所示。通过综合评价各单位的恶意程序报送数量、家族数、变种数、纳入处置数四个指标，CNCERT 每月会通报表扬排名位于前三的单位。7 月通报表扬的报送单位为：

表 4： 2013 年 7 月通报表扬的移动互联网恶意程序报送单位

排名	恶意程序报送表扬单位 ³
1	奇虎
2	安天
3	恒安嘉新

通过 7 月各单位报送的恶意程序，CNCERT 认定新出现的移动互

注 3：恶意程序报送表扬单位的全称：奇虎 360 软件(北京)有限公司、哈尔滨安天科技股份有限公司、恒安嘉新（北京）科技有限公司。

联网恶意程序家族 2 个，具体信息如下：

表 5： 2013 年 7 月 CNCERT 认定新出现移动互联网恶意程序家族情况

编号	新出现恶意家族名称	所属平台	恶意行为类型
1	A.expense.gtadpush	Android	资费消耗
2	A.expense.ad2push	Android	资费消耗

以上两个新出现恶意程序家族信息如下：

1) A.expense.gtadpush

该家族捆绑恶意广告插件 gtadpush，运行一段时间后会在用户不知情的状态下后台私自下载推广软件；下载完推广软件后，该应用还会弹出通知栏诱导用户点击安装，造成用户资费消耗。

2) A.expense.ad2push

该家族捆绑恶意广告插件 ad2push，运行一段时间后会在用户不知情的状态下后台私自下载推广软件，造成用户资费消耗。

三、应用商店恶意程序鉴定和处置情况

依据《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⁴。

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。

截至 2013 年 7 月，33 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，相关应用商店名单参见附录表 10，CNCERT 建议国内其他应用商店向上述 33 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。

CNCERT 共收到以上 33 家应用商店送检应用程序达 6593532 个，按 MD5 去重后样本共 1658745 个，包括 Android 平台应用程序 1587454 个、Symbian 平台应用程序 6377 个和 J2ME 平台应用程序 64914 个。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 19166 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。

针对检测发现的移动恶意应用，CNCERT 于 2013 年 1 月启动常态化的恶意应用处置工作，以每周 1 次频率通知应用商店对恶意应用进行下架处理，同时清除相应的下载链接。

截至 2013 年 7 月⁵，CNCERT 累计开展 24 次处置行动，共通知 53 家应用商店下架恶意应用数 38632 个，验证下架数为 30364 个，

注 4：对于存在移动互联网恶意程序的应用商店，CNCERT 会通过邮件和电话方式通知应用商店下架恶意程序。对于不下架恶意程序的应用商店，CNCERT 发送三次下架通知。当发送三次下架通知后，如应用商店仍不下架恶意程序，CNCERT 将依据《刑法》第二百八十六条和工信部《机制》要求协调基础电信运营企业、域名注册机构等单位对不下架恶意程序的应用商店进行处置。

注 5：由于本次月报为第一期，应用商店的处置数据范围为 2013 年 1 月至 2013 年 7 月。从第二期月报起，应用商店的处置数据范围为当月。

总体下架率为 78.6%。

表 6： 2013 年 7 月应用商店下架恶意程序的情况（按照验证下架数排序）

编号	应用商店名称	域名	通知下架数	验证下架数	下架率	下架速度
1	安丰市场	anfone.com	6644	6644	100%	及时
2	百度网	baidu.com	4008	4001	99.83%	及时
3	安智网	goapk.com	2741	2282	83.25%	及时
4	应用汇	appchina.com	1695	1610	94.99%	及时
5	十字猫	crossmo.com	2153	1365	63.40%	及时
6	联想乐商店	lenovomm.com	1332	1309	98.27%	及时
7	91RB	91rb.com	1107	1107	100.00%	及时
8	魅族	meizu.com	2576	1091	42.35%	及时
9	优亿市场	eoemarket.com	1070	1061	99.16%	及时
10	腾讯应用宝	myapp.com	2467	1009	40.90%	比较及时
11	安卓网	hiapk.com	1178	927	78.69%	及时
12	新浪网	sina.com.cn	916	890	97.16%	不及时
13	泡椒	paojiao.cn	729	729	100.00%	及时
14	机锋网	gfan.com	678	674	99.41%	及时
15	历趣网	liqucn.com	815	645	79.14%	及时
16	乐讯	lexun.com	538	538	100.00%	不及时
17	N 度网	nduoa.com	1041	527	50.62%	及时
18	360 手机助手	360.cn	722	481	66.62%	及时
19	游戏狗	gamedog.com	471	471	100.00%	及时
20	爱卓网	iandroid.cn	1039	449	43.21%	不及时
21	宜搜搜索	easou.com	577	292	50.61%	及时
22	UC	uc.cn	270	270	100.00%	及时
23	吾爱主题	5izhuti.com	244	244	100.00%	及时
24	中关村在线	zol.com.cn	176	176	100.00%	不及时
25	飞流社区	feiliu.com	177	176	99.44%	及时
26	3G 门户	3g.cn	328	155	47.26%	比较及时
27	155 安卓	155.cn	219	152	69.41%	及时

28	木蚂蚁	mumayi.com	191	139	72.77%	及时
29	中兴汇天地	zte.com.cn	139	120	86.33%	及时
30	卓乐网	sjapk.com	239	113	47.28%	比较及时
31	酷派应用商店	coolmart.com	182	108	59.34%	及时
32	网易应用中心	163.net	169	107	63.31%	不及时
33	手机中国	cnmo.com	94	94	100.00%	比较及时
34	小米	xiaomi.com	77	77	100.00%	比较及时
35	OPPO 应用商店	nearme.com.cn	229	71	31.00%	比较及时
36	91 手机助手	91.com	680	58	8.53%	比较及时
37	中国电信 天翼空间	189store.com	45	45	100.00%	及时
38	天网手机软件	waptw.com	38	38	100.00%	及时
39	悠悠村	uucum.com	36	36	100.00%	及时
40	飞鹏网	fpwap.com	36	36	100.00%	及时
41	中国移动 MM 商城	mmarket.com	14	14	100.00%	及时
42	华为智汇云	hicloud.com	81	9	11.11%	不及时
43	谷歌	google.com	21	9	42.86%	不及时
44	易用汇	anzhuoapk.com	5	5	100.00%	比较及时
45	中国联通 沃商店	wo.com.cn	5	5	100.00%	及时
46	当乐网	d.cn	14	3	21.43%	及时
47	搜狐	sohu.com	2	2	100.00%	比较及时
48	诺基亚	ovi.com.cn	178	0	0.00%	不及时
49	球球搜	qiuqiu.so	121	0	0.00%	不及时
50	极游网	ggg.cn	94	0	0.00%	不及时
51	阿里巴巴	alibaba.com	22	0	0.00%	不及时
52	HTC	htc.com	7	0	0.00%	不及时
53	豌豆荚	wandoujia.com	2	0	0.00%	不及时

通过综合考虑应用商店恶意程序的下架数量、下架率、下架速度，

CNCERT 对 2013 年 7 月处置移动恶意程序排名前十的应用商店进行表扬如下：

表 7： 2013 年 7 月处置移动恶意程序的应用商店表扬名单

编号	应用商店名称	域名	通知下架数	验证下架数	下架率	下架速度
1	百度	baidu.com	4008	4001	99.83%	及时
2	应用汇	appchina.com	1695	1610	94.99%	及时
3	联想乐商店	lenovomm.com	1332	1309	98.27%	及时
4	91RB	91rb.com	1107	1107	100.00%	及时
5	优亿市场	eoemarket.com	1070	1061	99.16%	及时
6	泡椒	paojiao.cn	729	729	100.00%	及时
7	机锋网	gfan.com	678	674	99.41%	及时
8	游戏狗	gamedog.com	471	471	100.00%	及时
9	UC	uc.cn	270	270	100.00%	及时
10	吾爱主题	5izhuti.com	244	244	100.00%	及时

对 2013 年 7 月不处置移动恶意程序、处置移动恶意程序不及时、处置移动恶意程序下架率低的应用商店进行批评如下：

表 8： 2013 年 7 月处置移动恶意程序的应用商店批评名单

编号	应用商店名称	域名	通知下架数	验证下架数	下架率	下架速度
1	诺基亚	ovi.com.cn	178	0	0.00%	不及时
2	球球搜	qiuqiu.so	121	0	0.00%	不及时
3	极游网	ggg.cn	94	0	0.00%	不及时
4	阿里巴巴	alibaba.com	22	0	0.00%	不及时
5	HTC	htc.com	7	0	0.00%	不及时
6	豌豆荚	wandoujia.com	2	0	0.00%	不及时
7	当乐网	d.cn	14	3	21.43%	及时
8	华为智汇云	hicloud.com	81	9	11.11%	不及时
9	91 手机助手	91.com	680	58	8.53%	比较及时
10	谷歌	google.com	21	9	42.86%	不及时

表 8 所示，例如诺基亚、HTC、华为、谷歌等知名手机厂商自身的应用商店均存在移动恶意程序，并在 CNCERT 发送恶意程序下架通知后仍不架或不全下架恶意程序，特此通报批评。

四、本月移动互联网重大网络安全事件

➤ 安卓签名漏洞疯狂爆发正版应用遭遇“寄生虫”

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),并将该漏洞信息在通信行业内进行通报。

7月下旬,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。CNCERT 监测发现在第三方应用市场“安丰市场”中存在 6644 个利用签名漏洞被植入 Skullkey 扣费木马的恶意 APP。

- 签名漏洞利用成本低,危害性大

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。

- 利用签名漏洞,正版 APP 被植入扣费木马 Skullkey

CNCERT 在捕获 Skullkey 扣费木马后,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。

● 第三方“安丰市场”成为“恶意传播源”

CNCERT 监测发现在第三方应用市场“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：

表 9： 安丰市场恶意 APP 分布比例

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。

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。同时，CNCERT 将 6644 个恶意 APP 信息和相应 URL 下载链接通过中国反网络病毒联盟向全社会进行黑名单发布。

● 图解安丰市场中被植入扣费木马的腾讯 QQ

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 7： 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 8： 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。经我中心深入分析，判定植入的恶意程序为扣费木马 Skullkey。

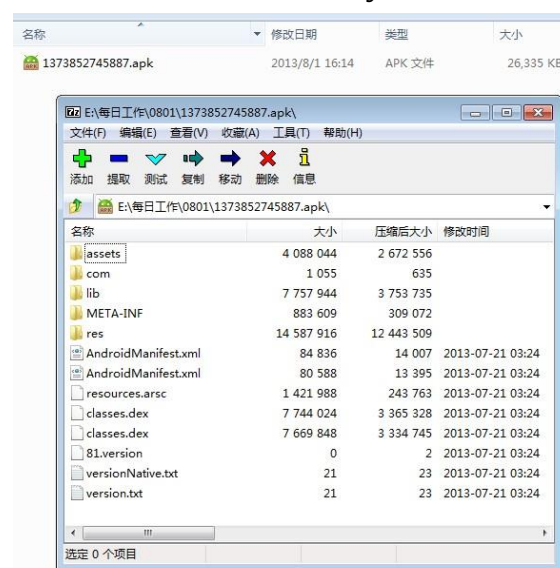


图 9：安丰市场中下载量第一的 APP 文件列表

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，我中心共发现类似被植入扣费木马 Skullkey 的恶意 APP 共计 6644 个。



图 10：安丰市场中被植入 Skullkey 扣费木马的热门 APP

附：

● 移动互联网恶意程序行为属性⁶

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；

注 6：摘自通信行业标准 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，获取用户网络交易信息的；
- 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。

● 主动提交 APP 进行送检的应用商店表扬名单

表 10：截至 2013 年 7 月向 CNCERT 送检全量 APP 的应用商店情况

编号	应用商店名称	应用商店域名	送检 APP 总数
1	91RB	91rb.com	901222
2	安卓网	hiapk.com	778495
3	新浪网	sina.com.cn	757469
4	安智网	anzhi.com	620550
5	应用汇	appchina.com	478737
6	360 手机助手	360.cn	365809
7	联想乐商店	lenovomm.com	363421
8	百度网	baidu.com	283493
9	乐趣网	liqcn.com	280368
10	魅族	meizu.com	255486
11	木蚂蚁	mumayi.com	246389
12	N 多网	nduo.com	237798
13	91 手机助手	91.com	169486
14	宜搜搜索	easou.com	141043
15	十字猫	crossmo.com	132193
16	机锋网	gfan.com	110888
17	优亿市场	eoemarket.com	66823
18	3G 门户	3g.cn	51073
19	球球搜	qiuqiu.so	50000
20	UC	uc.cn	39931
21	爱卓网	iandroid.cn	36847
22	卓乐网	sjapk.com	32409
23	飞流社区	feiliu.com	30689
24	OPPO 应用商店	nearme.com.cn	27433
25	泡椒	paojiao.cn	26195
26	155 安卓	155.cn	25577
27	极游网	ggg.cn	24684
28	中兴汇天地	zte.com.cn	20768

29	飞鹏网	fpwap.com	15041
30	华为智汇云	hicloud.com	10000
31	酷派应用商店	coolmart.com	9505
32	吾爱主题	5izhuti.com	1986
33	悠悠村	uucum.com	1724