2013 上半年手机病毒发展趋势报告

作者：王磊

目录

引言

2013 年上半年，以手机恶意软件为主的移动安全威胁越发严重，手机病毒爆发式增长。整体上看，移动安全威胁呈现“哑铃式”发展趋势。病毒制造猖獗，病毒危害严重，但是病毒传播仍然需要依靠社会工程学的手段。

报告摘要

2013 年上半年，恶意软件的发展趋势:

1. 恶意软件的增长速度已经大大超出高危软件的增长速度。

2. 恶意软件的增速在 6 月份骤增。

3. 恶意软件新增感染用户量过千万。

4. 吸费是最主要的手机恶意软件行为。

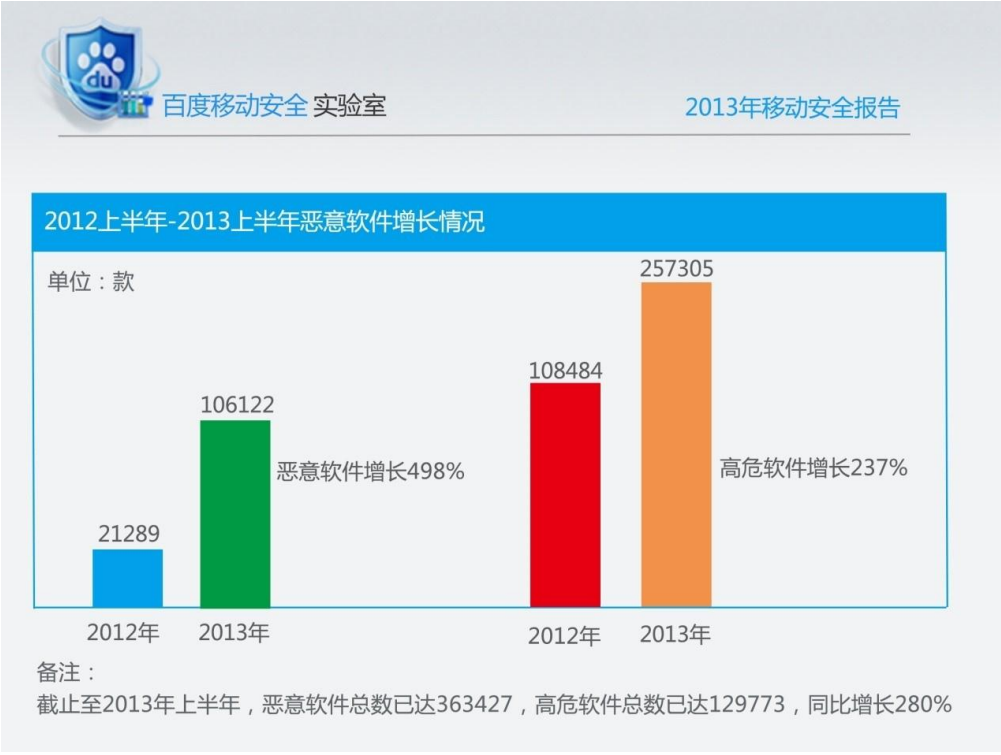
报告正文

一、2013 年恶意软件增长情况

1. 病毒制造数量激增，同比增长 280%

2013 年上半年，百度移动安全实验室共截获 Android 平台手机病毒 363427 款，同比去年增加 280%。

其中，恶意软件同比增长 498%，高危软件同比增长 237%。恶意软件的增长速度已经超过高危软件。越来越多的病毒制造者已经不满足于高危软件带来的经济利益，转而开发获利更高的恶意软件。



2012 年上半年和 2013 年上半年恶意软件增长情况（来源：百度移动安全实验室）

根据百度移动安全实验室 2013 年上半年的调研数据，手机恶意软件的增速在 6 月份出现陡增趋势。预计到 2013 年下半年，恶意软件的增速，还将持续这样的涨势。手机安全问题已经迫在眉睫，需要解决。

2013 年上半年恶意软件增长趋势数据分析图（来源：百度移动安全实验室）

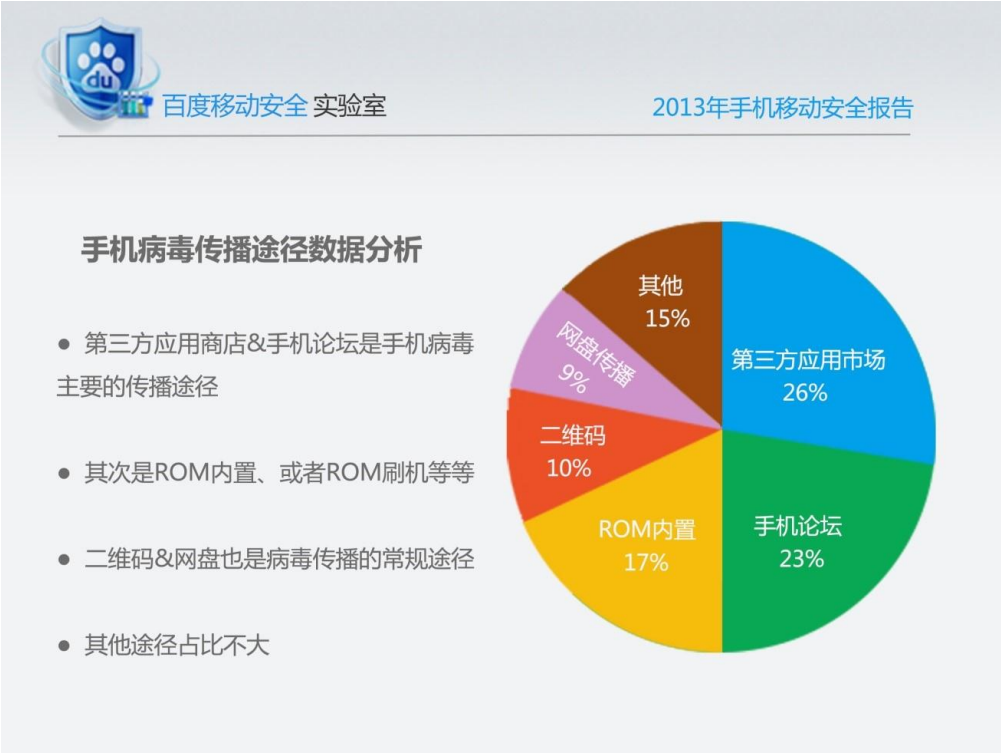
2. 病毒传播途径，第三方应用商店、论坛占比近半数

在病毒传播渠道方面，第三方应用商店和手机论坛仍然是最主要的手机病毒传播渠道，占到接近一半的比例。这主要是由于国内有很多的第三方应用商店，安全检测水平参差不齐。同时，手机论坛缺乏安全监管，造成大量手机病毒伪装成流行应用，诱惑用户下载安装，感染用户。

ROM 内置紧随其后，成为第三大病毒传播渠道。由于 Android 刷机用户越来越多，恶意 ROM 开发者为了谋取暴利，在 ROM 中内置病毒，甚至和水货厂商勾结。ROM 内置的病毒不易被用户发觉，而且不容易清除。

二维码和网盘分别占到 10%和 9%的比例。恶意开发者将病毒存放到网盘里，然后通过微博微信等渠道将二维码或者网盘链接传播出去，诱导用户安装病毒。

在这些主要的病毒传播渠道中，病毒都是需要通过社会工程学的手段，诱导用户下载安装，感染用户的手机。这在一定程度上限制了手机病毒的泛滥。



病毒传播途径数据分析图（来源：百度移动安全实验室）

3. 病毒危害的趋势及行为体现

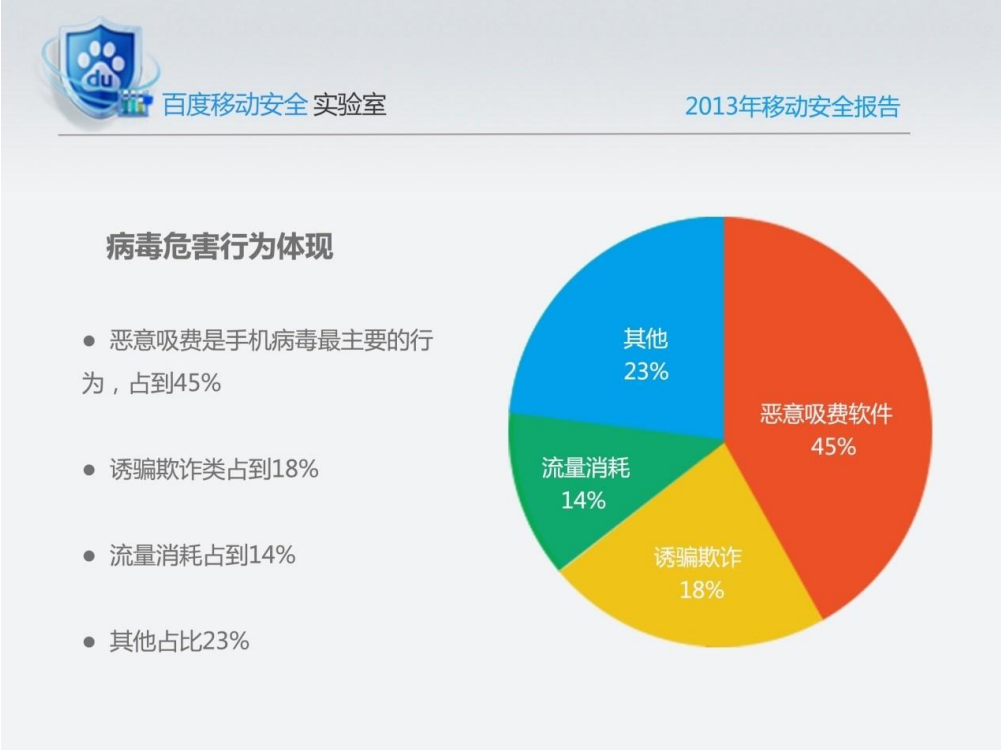
2013 年上半年，被手机恶意软件感染的用户超过 12299746。每月感染用户呈现稳步增长趋势。预计 2013 年下半年，这种增长趋势还将延续。

恶意软件危害趋势数据分析图（来源：百度移动安全实验室）

从恶意软件的行为上看，恶意吸费是手机病毒最主要的行为，占到 45%。

诱骗欺诈类占到 18%。用户一旦感染诱骗欺诈类病毒，手机就会私自给联系人发送欺诈短信，造成用户的亲朋好友资费损失。

流量消耗类软件占 14%，有大量的病毒会在后台私自下载应用，访问网站，造成流量消耗，资费损失。



病毒危害行为体现数据分析图（来源：百度移动安全实验室）

由于恶意开发者可以通过吸费病毒获取巨大的经济利益 ,这极大的刺激了吸费病毒制造技术的发展。从最早期的通过非法 SP 吸费通道吸费，到现在私自修改 APN，利用应用商店付费流程漏洞，利用游戏充值漏洞等技术制造吸费病毒。吸费病毒五花八门，概括起来，大概有如下几类吸费形式：

1. 偷偷发送短信，拨打电 话到付费号码。
2. 偷偷下载付费应用，点播付费视频，访问付费网站。
3. 电信诈骗。
4. 网银大盗。
5. 流量消耗，造成资费损失。

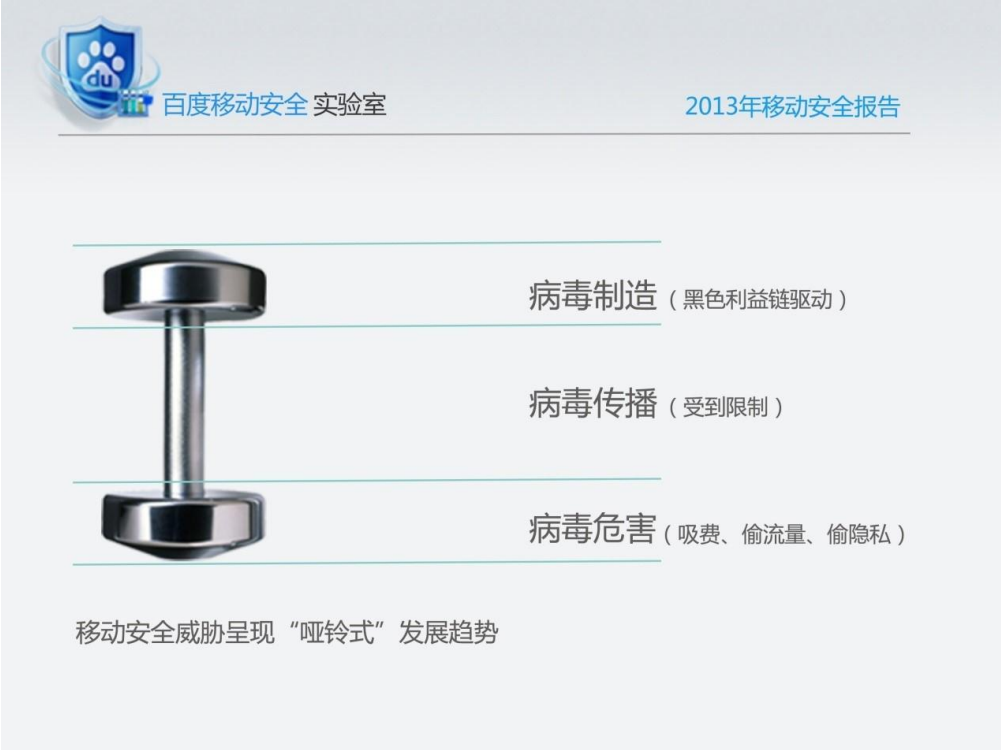
百度移动安全实验室监测到的 2013 年上半年感染用户最多的吸费病毒如下表所列。仅以 SMSFraud.A 这一款病毒为例。粗略估算，如果该病毒每天发作一次，每次感染 10 个手机联系人，每人被骗 10 元，那么，该病毒每天可以造成用户资费损失就达到 4.47 亿元。

病毒名称	恶意行为	感染量
Trojan!SMSFraud.A@Android	发送诈骗短信给手机联系人。	4478556
Trojan!UaPush.B@Android	私自下载，耗费流量，发送垃圾短信，窃取隐私。	2231584
Trojan!SimpleTemai.A@Android	私自下载，恶意推广，造成流量损失，资费消耗。	859657
Trojan!MMarketPay.A@Android	私自下载付费应用，造成扣费。	345080
Trojan!BadNews.A@Android	私自下载，窃取隐私。	204751

病毒危害行为体现数据分析图（来源：百度移动安全实验室）

二、 移动安全威胁呈现“哑铃式”发展趋势

从上面图片中的数据可以看出，病毒制造和病毒危害都很严重，是“哑铃”的两个大头，而病毒传播由于受到社会工程学的束缚，很大程度上受到了限制。



移动安全呈现哑铃式发展示意图（来源：百度移动安全实验室）

病毒制造者在经济利益的驱动下，疯狂制造手机病毒。而且，Android 手机病毒制造的技术门槛低，这就进一步加剧了病毒制造的泛滥。

从病毒危害看，由于手机上有用户的资费、流量和隐私，手机病毒可以直接造成扣费、流量消耗和隐私泄露，给用户造成巨大的危害。

然而，在病毒传播上，由于目前主要的病毒传播手段都需要社会工程学的参与，伪装成流行应用，诱骗诱导用户下载安装病毒，不能像 PC 病毒一样自动的感染其他软件和自动传播，所以手机病毒在传播上受到了限制，这也是目前手机上还没有大规模爆发像“梅丽莎”那样

病毒的重要原因。

但是，百度移动安全实验室也注意到，即使在这样的传播限制下，手机病毒仍然造成了大量用户的感染和用户损失。更重要的是，照这样的趋势发展下去，手机病毒传播的瓶颈很快会被技术手段突破。百度移动安全实验室已经截获到了一种跨界手机病毒。这样的手机病毒可以从远程服务器下载病毒代码，当手机连接到 PC 的时候感染 PC。如果成功感染 PC，那么病毒完全可以利用 PC 端病毒技术，自动传播并感染其他 PC，最终可以实现自动感染其他手机！

如果手机病毒的传播限制被突破，那么必然会造成手机病毒更大规模的爆发，其后果将不堪设想。

三、 百度移动云安全平台：从安全到优质，全产业链合作

移动安全，绝不仅仅是安全。手机病毒只是移动安全威胁的一部分。用户感知程度更大的移动安全问题还有很多，比如垃圾短信、骚扰电话、省电等泛安全的问题。同时，由于移动用户的即时性，如何帮助用户找到优质的应用，省去移动用户的流量损失和时间消耗，都是移动安全的问题。

移动安全的问题也不仅仅是手机端的问题。移动安全需要全产业链合作，打造安全的移动生态系统。从源头的应用开发者开始，到分发渠道、应用商店、论坛，再到手机厂商，安全厂商，政府监管，这样组成了整个移动生态系统。只有生态系统安全了，移动用户才真正安全。

百度移动安全实验室，致力于打造完全开放的百度移动云安全平台，全产业链合作，从安全到优质，实现安全的移动生态系统。

百度移动安全实验室网站： http://seclab.safe.baidu.com

百度安全管家网站： http://safe.baidu.com