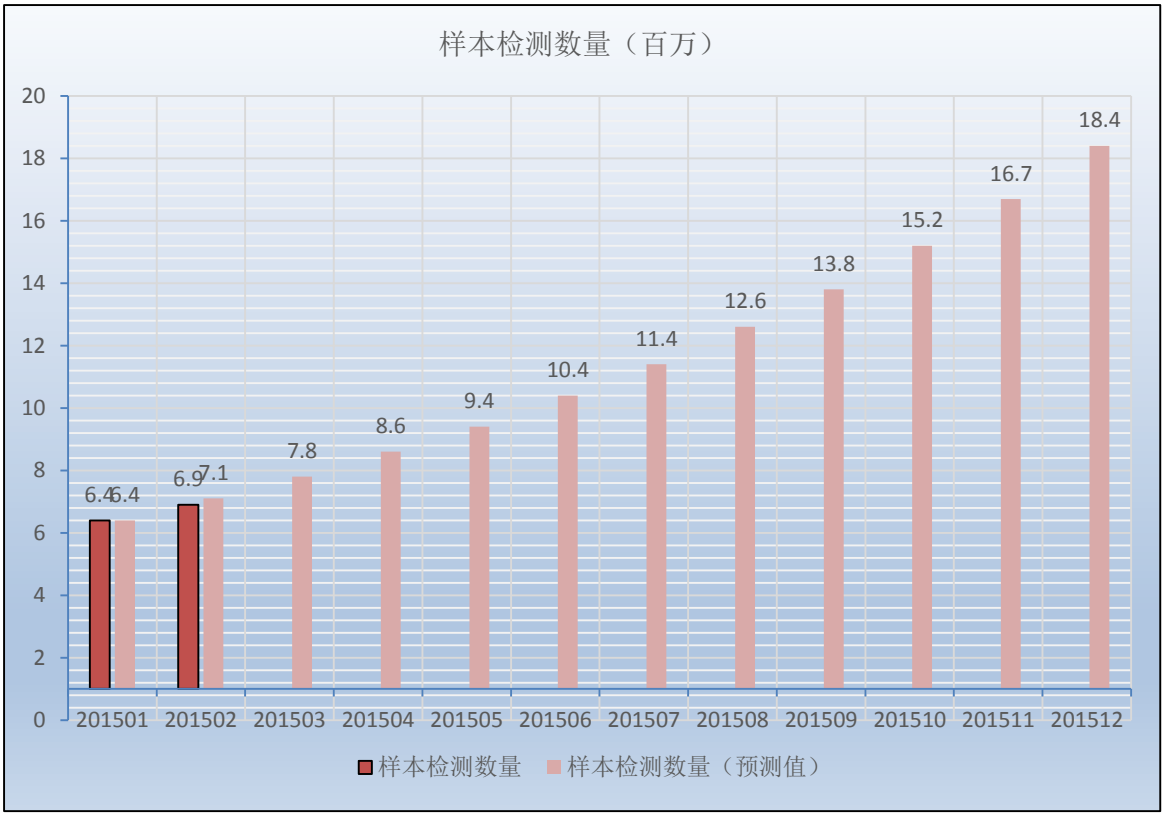
趋势科技移动客户端病毒报告

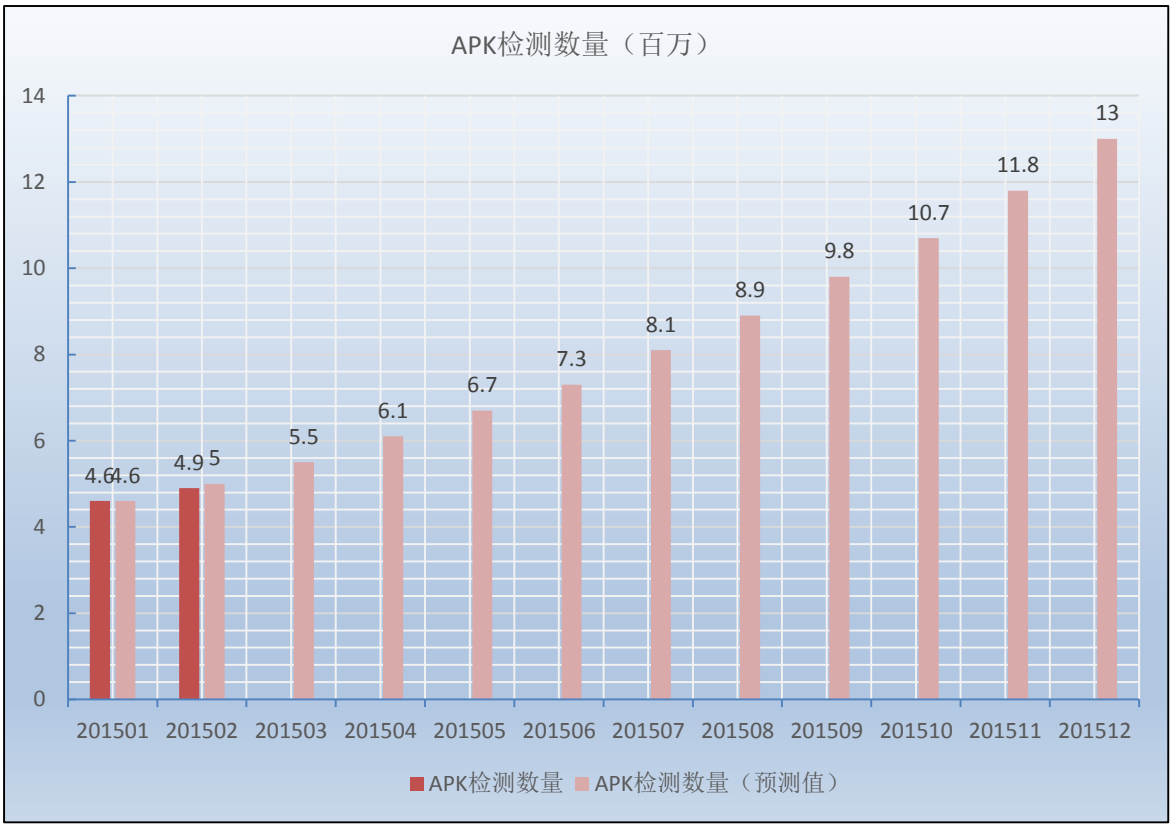
2015年2月移动客户端安全威胁概况

本月，截至 2015.2.28 日，发布中国区移动客户端病毒 1.839.00，大小 12,239,982 字节。

样本检测数量



APK检测数量


APK检测数量（百万）
14
12
10
8
6
4
2
0
4.6
4.6
4.9
5
5.5
6.1
6.7
7.3
8.1
8.9
9.8
10.7
11.8
13
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）

移动恶意软件制作者已窃取韩国银行用户百万元

我们在早前发布过一篇研究员撰写的文章，文章是关于一个中国的黑客组织利用移动平台恶意软件窃取韩国银行用户账户财产的案例。2013 年以来，他们已经从受害者账户中转移了约合每天 1600 美元的资金。

这一调查结果是我们对移动安全威胁形势持续观测的成果。我们对新出现的威胁保持高度关注，尤其是活跃的中国地下黑色产业链。而许多移动平台的安全威胁背后基本都隐藏着较大的地下黑市。

资金盗窃背后的恶意工具

这个来自吉林延边的黑客组织，从 2013 年开始就从银行客户的账户中窃取资金。他们利用各种安卓病毒来达到他们牟利的目的。

- **假冒银行软件：**
  我们研究发现，黑客利用了 5 家韩国银行的假冒网银程序，他们包括国民银行，NH 农协银行，韩亚银行，新韩银行，友利银行。这些假冒程序会窃取用户的隐私信息。同时还可以卸载并替代已经安装的官方网银程序。这样可以最大程度的避免被用户发现。
- **对银行交易进行会话劫持**
  他们利用伪造正常程序的图标迷惑网银用户，让用户误以为是官方的程序。假冒程序会记录用户输入的信息，包括账号，姓名，密码，以及其他一些个人信息。
- **假冒知名程序**
  黑客还伪造了一些安卓平台上比较流行的程序。例如 Google Play，搜索，Adobe Flash Player 以及一些色情程序。这些假冒程序会下载并安装恶意程序，删除用户文件，拦截短信，后台拍照，窃取文件等等。

该团伙利用假冒程序迷惑银行用户，受害者会收到钓鱼短信，恐吓他们如果不点击短信正文中的链接就将被有关部门调查。当用户点击后，该链接会在受害者手机上安装恶意软件。

团伙内部利用 QQ 进行通信

该黑客团伙利用 QQ 进行招聘，和内部交流、沟通。QQ 已经迅速成为网络犯罪者喜欢的沟通方式。地下产业越来越猖狂，在报告 The Chinese Underground in 2013 中我们讲到，仅 2013 年一年，地下产业活动数量与 2012 同期相比，已经翻了一倍。

更多关于此案的信息，请您参考我们的研究报告 *The Yanbian Gang: Using Mobile Threats to Go after South Korean Targets*.

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。