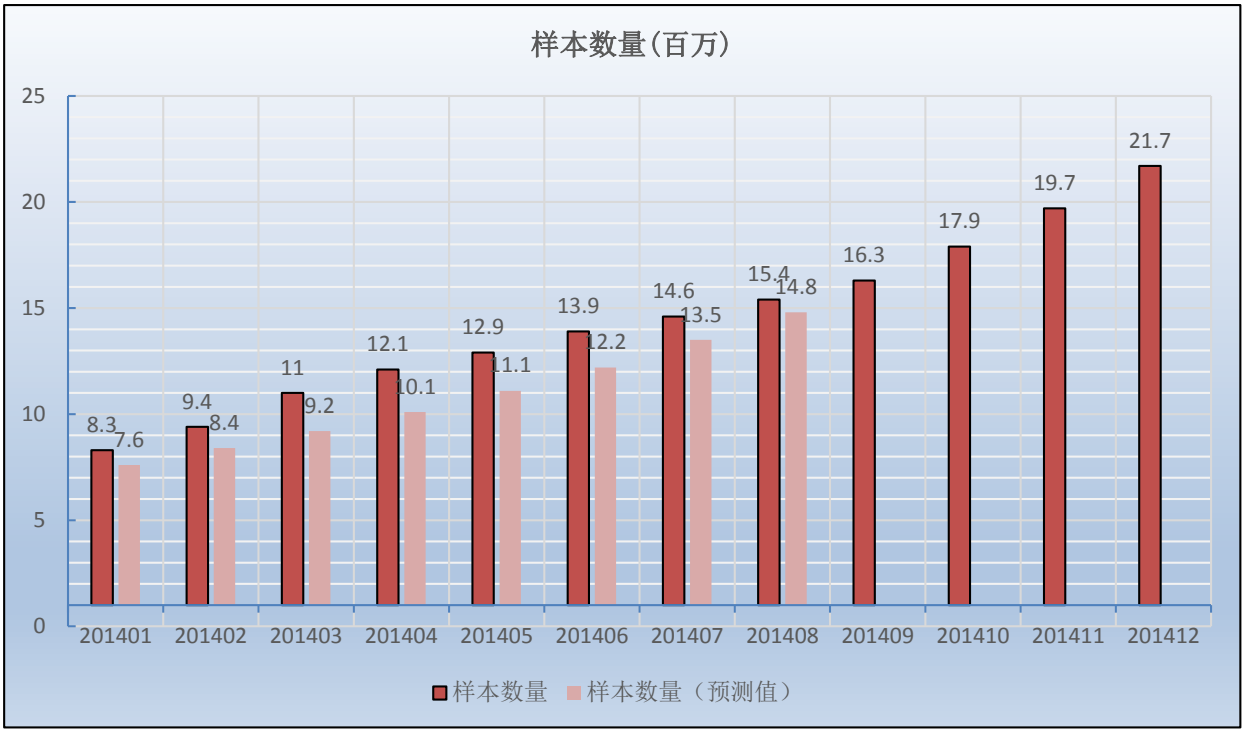
趋势科技移动客户端病毒报告

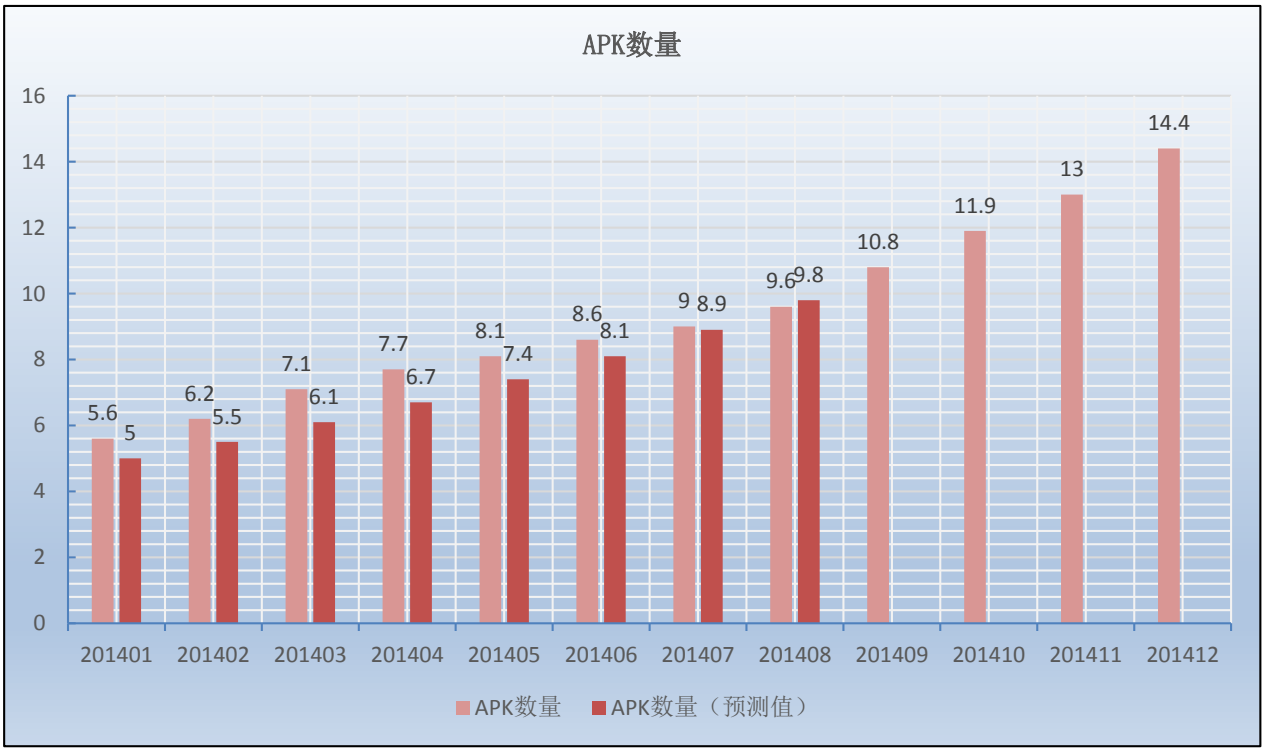
2014年8月移动客户端安全威胁概况

本月，截至 2014.8.31 日，发布中国区移动客户端病毒码 1.739.00，大小 22,727,239 字节。

样本处理数量



APK数量


APK数量
16
14
12
10
8
6
4
2
0
5.6
5
6.2
5.5
7.1
6.1
7.7
6.7
8.1
7.4
8.6
8.1
9
8.9
9.6
9.8
10.8
11.9
13
14.4
201401
201402
201403
201404
201405
201406
201407
201408
201409
201410
201411
201412
APK数量
APK数量（预测值）

危险的 Android FakeID 漏洞

来自 Bluebox 实验室的安全研究员最近发现了一个可能导致恶意程序冒充合法程序的漏洞。该漏洞被命名为“FakeID”，漏洞源于使用证书和签名证明程序合法性这一做法。值得关注的是从 2.1 到 4.4 版本的 Android 系统都受到了该漏洞的影响。

证书和签名

Android 应用程序在发布之前必须经过签名才能被安装到设备上。签名过程涉及到证书的使用。比如 HTTP/SSL 证书，是由可信机构来颁发的。证书保证了发布后程序的完整性，避免任何的篡改攻击。这些证书作为程序的“包签名”来使用，是 Android 系统识别程序的依据。

Android 是如何分配这些签名的呢？对于每一个安装到设备上的应用程序，都有一个对应的 PackageInfo 类被创建，用于描述程序的基本信息。PackageInfo 包含了一个名为“signatures”的属性，这个属性起着关键的作用。当两个程序具有相同的签名时，一个应用程序可以作为另一个应用程序的更新包，或着这两个应用程序可以共享它们的数据（以某种形式的共享机制）。有时，系统可以通过比较程序的签名和属性中签名是否一致来决定是否授予相关权限。

为了说明这个过程，Bluebox 举例两个实际的例子。一个例子是支付相关的应用程序被允许访问移动设备的 NFC SE 硬件，因为程序的签名和设备的 NFC 相关文件中指定的签名相同。另外一个是，一个应用程序被允许作为其他程序的一个 webview 插件（例如，Adobe Flash 插件），因为该应用程序有 Adobe 的签名。

证书链中的缺陷

程序被安装到设备上后，系统用程序的证书文件为其创建证书链。然而，由于这个漏洞，系统不会验证证书链的真实性，只会检查签名的“主体”和“发行人”。很不幸，这两项都是简单的字符串，恶意程序可以轻易地伪造。

漏洞的利用

因为该漏洞涉及到程序的“真实性”，黑客可以做出在毫不被人怀疑的情况下访问敏感数据的恶意程序。例如，NFC 相关的支付经常使用到谷歌钱包。如果一个恶意程序被授予使用 NFC 的特权，它将能够窃取用户的谷歌钱包账户信息，替换指定的付款帐户，并窃取用户的钱。

恶意应用程序还可以利用 WebKit 插件的权限，只要它有所需的签名。每当被攻击者用浏览器浏览网站或使用其他需要 WebView 组件的应用时，恶意程序将自动作为一个 WebKit 插件运行。因为该恶意软件已经成为正常程序的组件，几乎拥有了对程序数据的全部控制能力。所有相关的数据，如用户凭证，银行帐户和电子邮件的细节，都可以被访问，泄露或篡改。

受影响的 Android 用户

正如我们前面所说的，所有没从 OEM 厂商处打过补丁的设备都会受到此漏洞的影响。谷歌目前的数据显示，约 82%的 Android 设备受该漏洞影响。 这一巨大数字让人们联想起去年发现的 master key 漏洞。

谷歌已经发布了修补这个 bug 的补丁。然而，Android 生态系统的碎片化决定了并不是所有的用户都可以让自己的设备免受此漏洞影响。只要有相关更新，我们建议用户立即打上这个补丁。

谷歌已经发表声明说他们已经“扫描了所有提交给 Google Play 的应用，并检查了 Google Play 外的一些应用，尚没有看到企图利用这个漏洞的程序。”

为了保护我们的用户，我们密切关注利用此漏洞的威胁和攻击的动向。利用此漏洞的恶意程序已经可以被检测为 ANDROIDOS_FAKEID.A。

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。