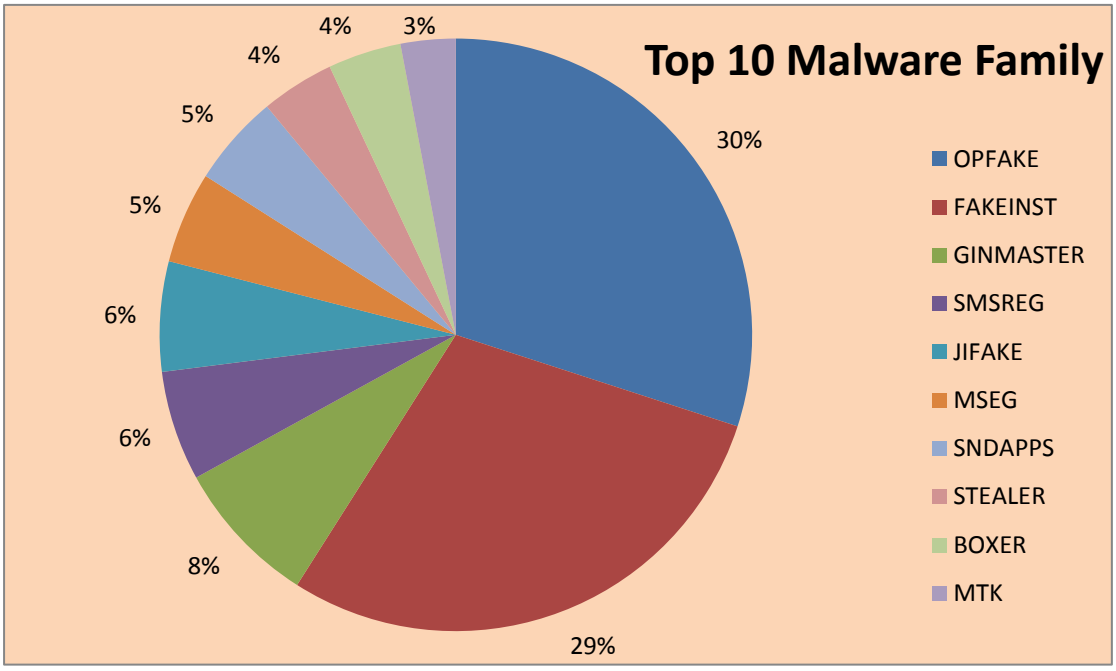
趋势科技移动客户端病毒报告

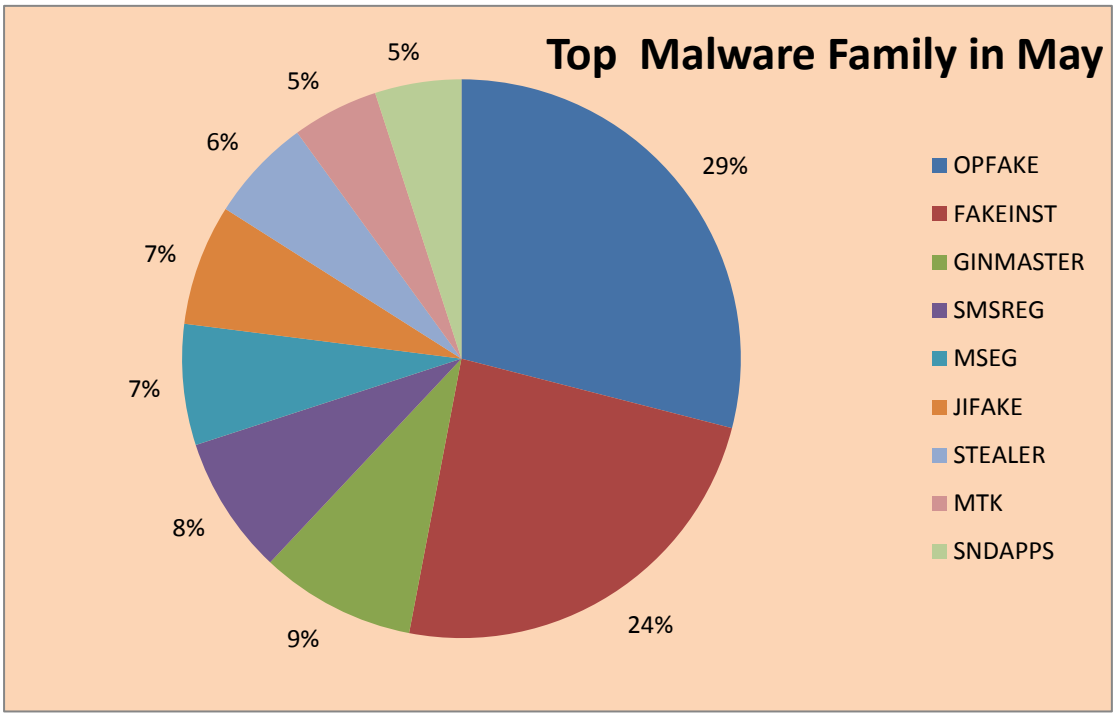
2014年5月移动客户端安全威胁概况

本月，截至 2014.5.31 日，中国区移动客户端病毒码 1.687.00 ，大小 16,054,052 字节，可以检测病毒约 250 万个。本月趋势科技新发现移动客户端病毒约 21 万个。

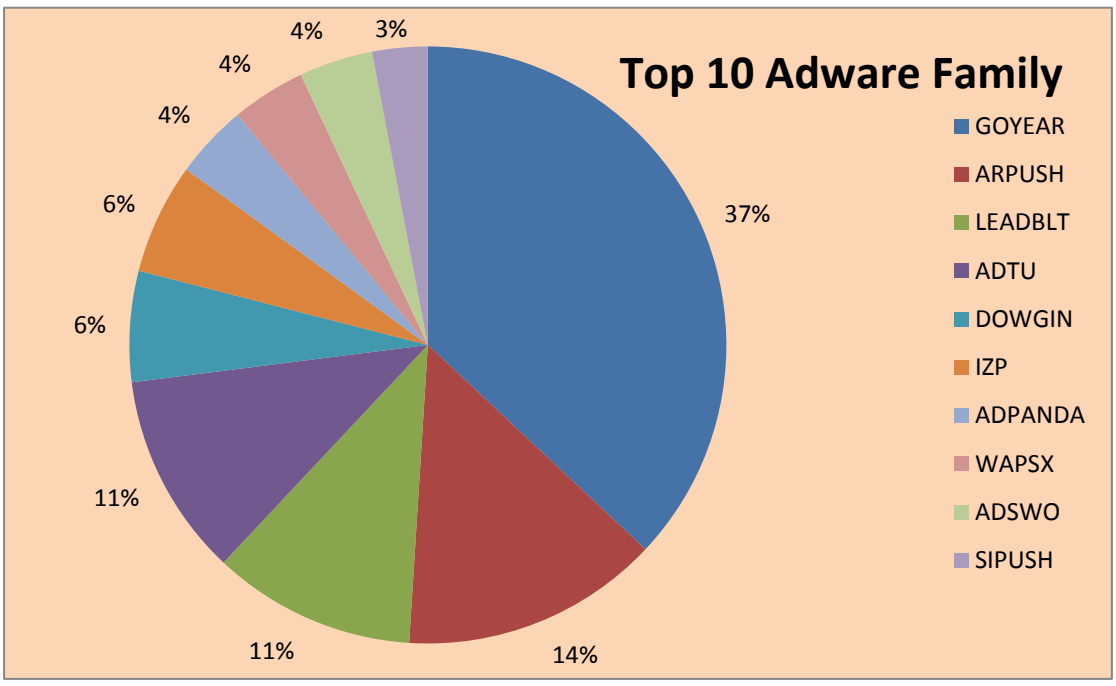
趋势科技移动客户端病毒码中排名前十的病毒家族：



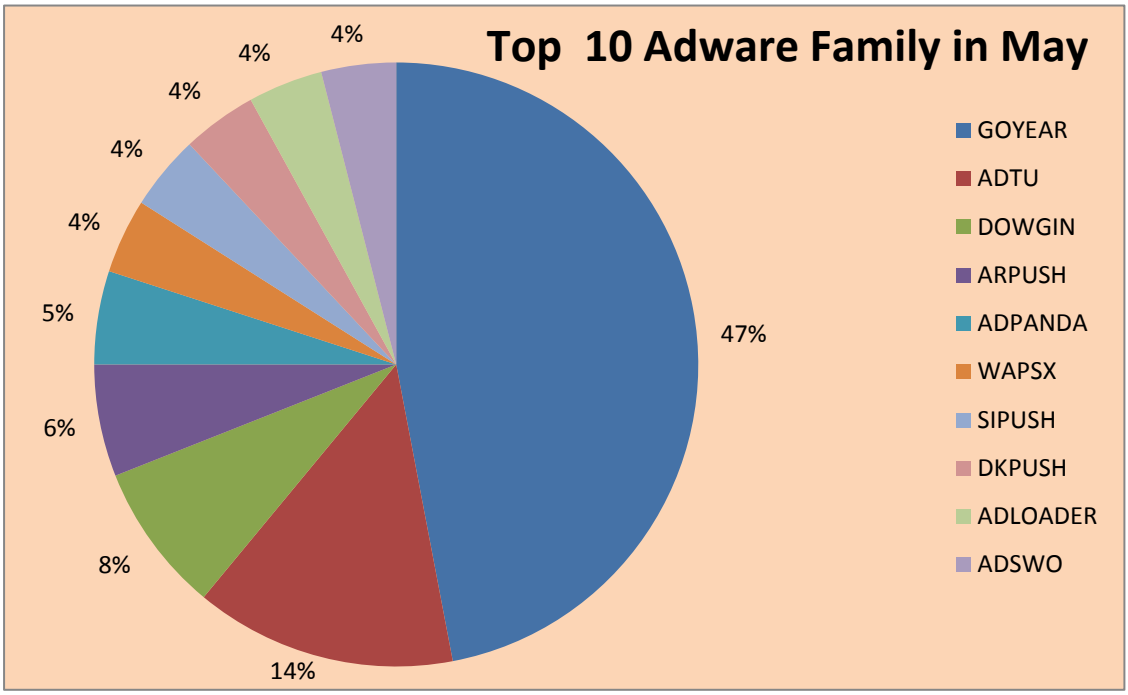
趋势科技移动客户端 5 月新增病毒码中排名前十的病毒家族：



趋势科技移动客户端病毒码中排名前十的广告软件家族：



趋势科技移动客户端 5 月新增病毒码中排名前十的广告软件家族：



Android 应用组件可以被恶意利用

最近我们发现一组包含漏洞的安卓程序可能导致用户数据被泄露或被利用，并以此来开展攻击。这两个受影响的应用都具有较高的知名度：

- 一款装机量超过 1 千万的笔记软件，其下载页面有近 10 万的评论量
- 一款装机量超过 100 万的购物类软件，其下载页面有几千的评论量

这个漏洞存在于一个安卓系统中用来执行程序功能的特定组件。该组件有一个名为“android:exported”的属性，当该属性被设置为“true”时，就允许其他程序访问或执行该组件。这意味着安装好的程序可以触发其他程序的特定功能。显然，对于软件开发者和供应商来讲，这样可以更方便地与其他厂商的程序协作和通信。但是，从安全的角度来讲，这也为黑客攻击提供了便利。

利用 Activities 开展攻击

根据攻击者的目的和程序本身的差异，利用这个漏洞的方式可能多种多样。例如，根据我们的分析，在某购物类应用中，一个与购物时弹框提示有关的 Activity 可以被其他程序触发和利用。也就是说恶意程序可以在这个购物应用中弹出窗口，开展攻击。攻击者可以设计一个指向恶意链接或者其他恶意程序的弹框提示来诱骗用户。

利用 Content Provider 窃取信息

另外一种可能的利用方式是以控制重要信息的 Content Provider 为目标，获取和收集信息。与存储用户输入的笔记软件相关的 Content Provider 有可能被用来获取用户数据。

这些重要的 Content Provider 可以用定义权限的方式加以保护。然而，权限保护等级设置不合理同样会导致漏洞被利用。在我们上边提到的笔记应用里，存储用户输入的 Content Provider 被设为 READ 和 WRITE 权限。但是，这两个权限的保护等级都被设置为“normal”，即所有安装在该设备上的程序都被授予了这两个权限。

如何应对

对于开发者，这个案例说明了对程序不同模块设置合理限制的重要性。那些被证实了可能被利用的组件需要通过权限来保护，并设置正确的保护等级。上文提到的这种做法尽管不能做到百分之百的安全，但还是能提供较高等级的安全性。

我们强烈建议开发者检测一下程序中用的的组件并确保相关访问权限得到合理的限制。我们已经通知了上文提到的相关程序的开发者，告知了程序存在的安全问题。据估计还可能有更多的软件受到该漏洞的影响，届时我们会及时通知相关厂商。

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。