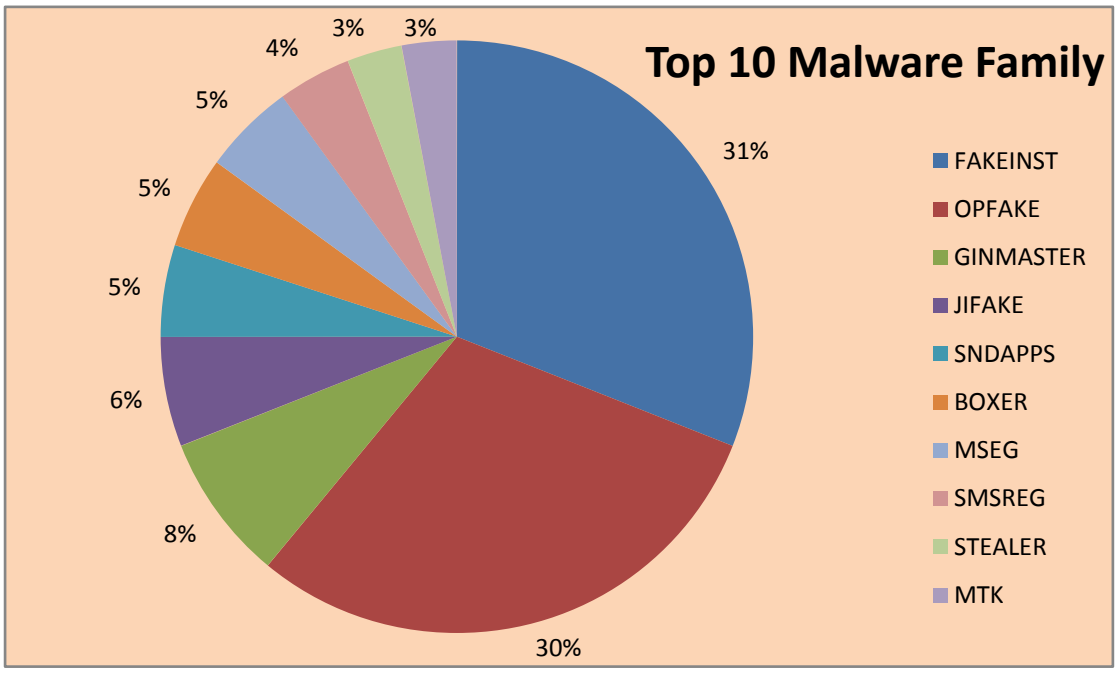
趋势科技移动客户端病毒报告

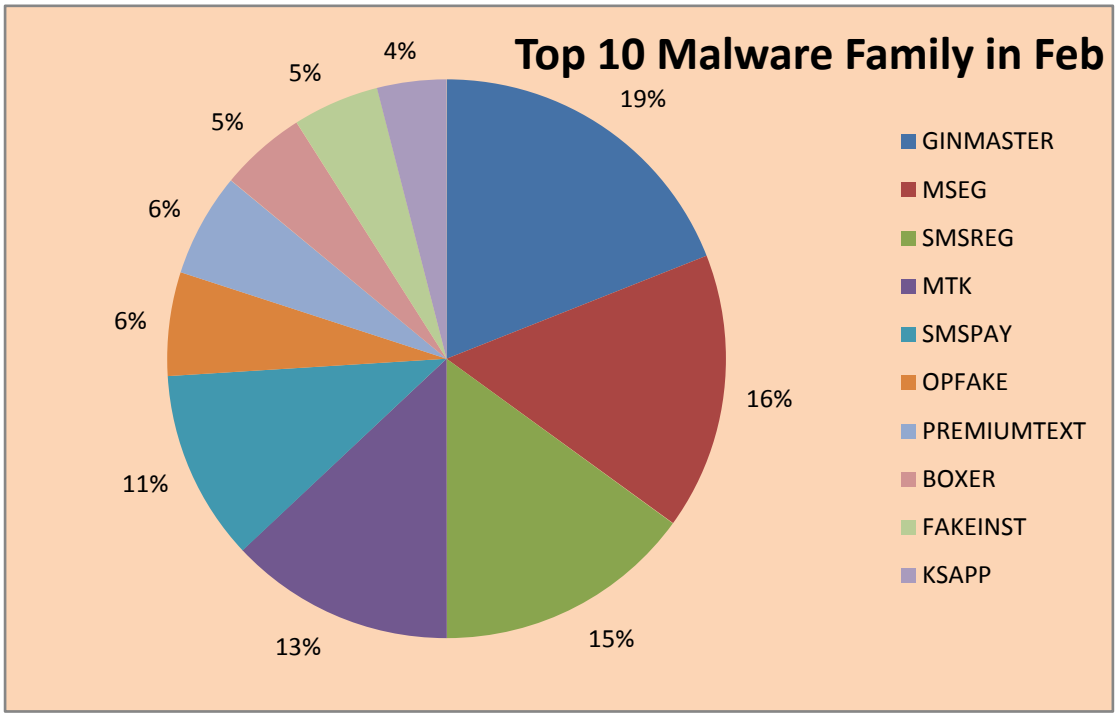
2014年2月移动客户端安全威胁概况

本月，截止 2014.2.28 日中国区移动客户端病毒码 1.635.00，大小 10,313,758 字节,可以检测病毒约 182 万个。本月趋势科技新发现移动客户端病毒约 27 万个。

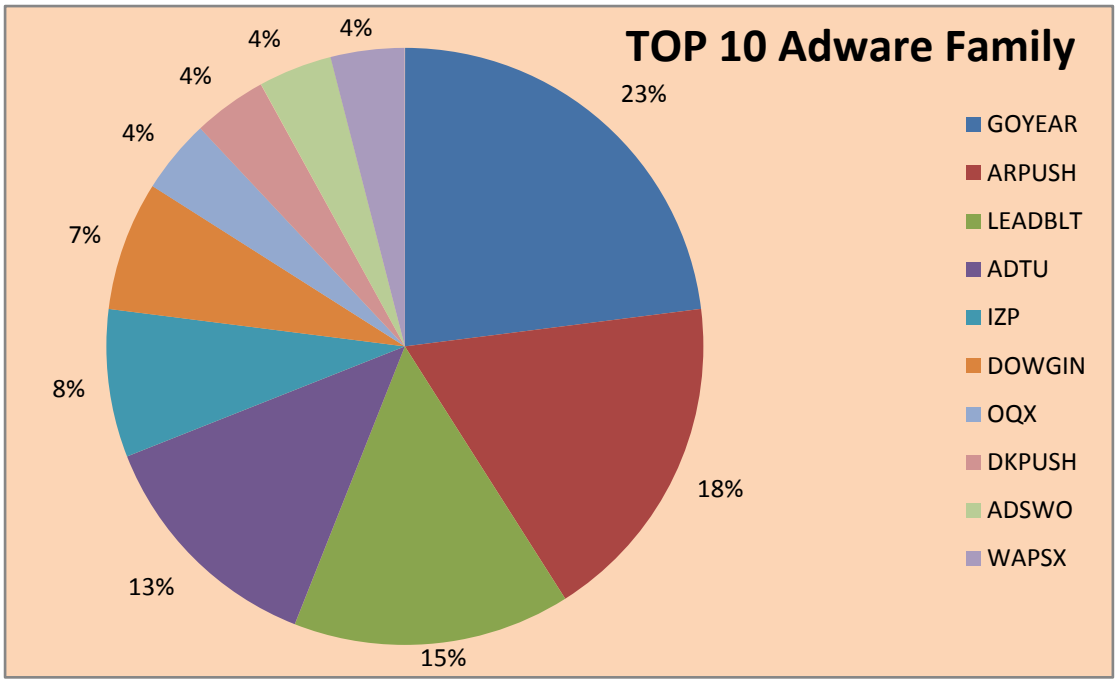
趋势科技移动客户端病毒码中排名前十的病毒家族：



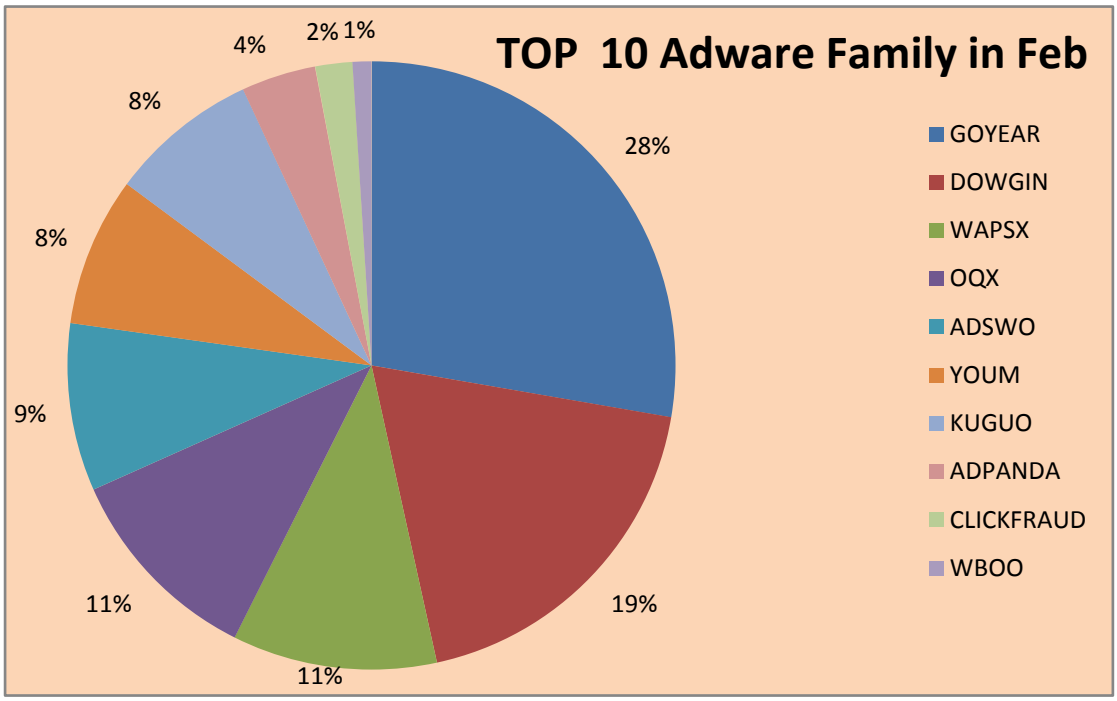
趋势科技移动客户端 2 月新增病毒码中排名前十的病毒家族：



趋势科技移动客户端病毒码中排名前十的广告软件家族：



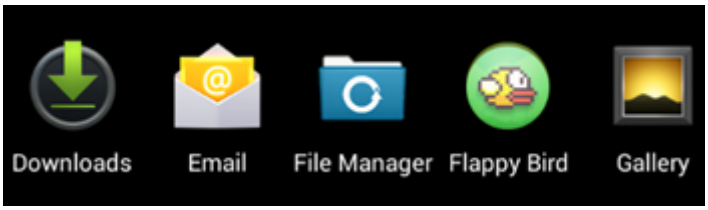
趋势科技移动客户端 2 月新增病毒码中排名前十的广告软件家族：



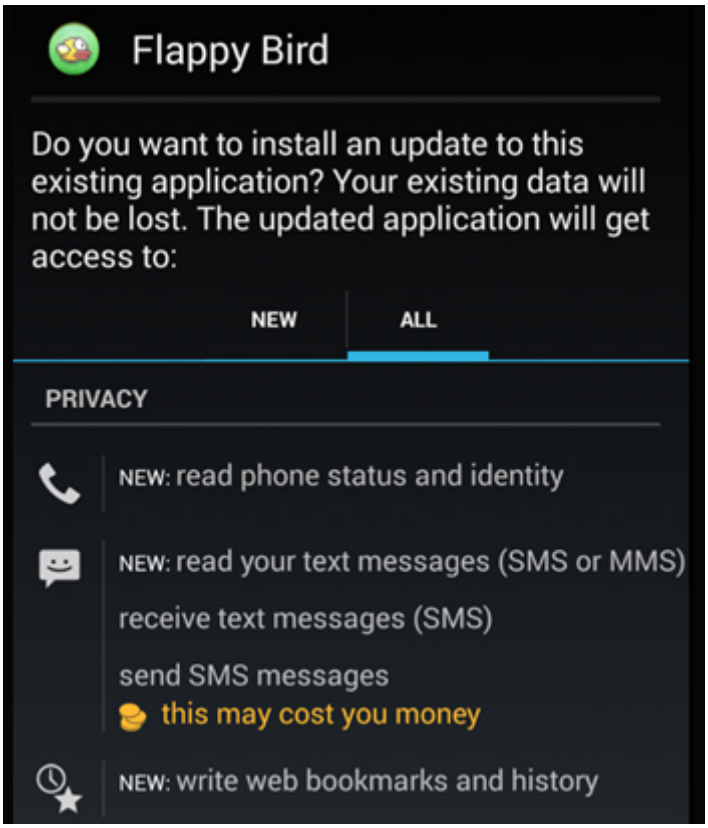
带木马的 Flappy Bird 来袭

关于 Flappy Bird 游戏的相关事件已经在网络上引起了巨大的关注：在成为了一款相当受欢迎的游戏之后(其下载量已超过 5 千万)，它的开发者突然宣布将从应用商店中将此游戏撤下，后来他的确这么做了。这个决定让大家对这款游戏的兴趣不减反增。应用商店中出现了类似的游戏，甚至有人拍卖安装了这款游戏的手机。

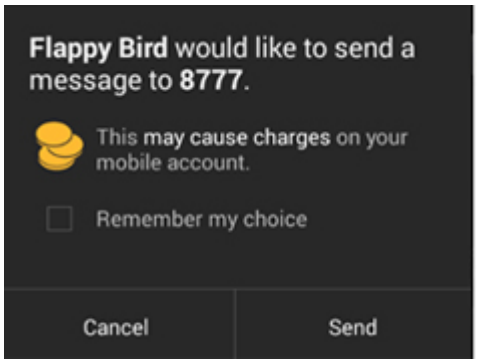
然而，另外一个方面的进展却是我们不想看到的：在安卓平台上，我们发现大量的假冒 Flappy Bird。这种现象在俄罗斯和越南的应用商店中尤其猖獗，假冒程序数量几乎已经和正常程序数量相当。

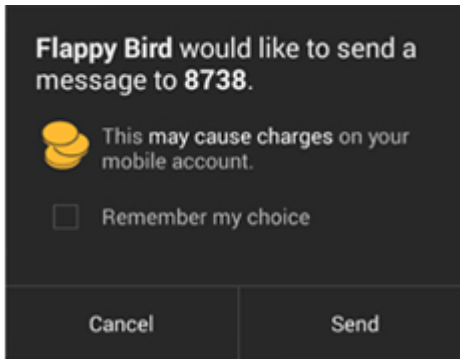


目前我们发现的假冒版本基本都是扣费类型的恶意程序，它们会在用户不知情的情况下，向固定号码发送扣费短信，造成用户账户费用损失。如下图所示，这个假冒的 Flappy Bird 向用户请求短信读取和发送的权限，但是正常程序是不需要这项权限的。



一旦游戏安装完成并运行，程序就开始向固定号码发送短信：





当程序运行时，它会在后台偷偷通过 Google 的云消息服务连接到 C&C 服务器来获取指令。通过我们对该程序的分析，发现它能够发送短信并且拦截含有特定内容的短信通知。

除了恶意扣费，这个程序还会泄露用户的信息，包括手机号码，运营商，Gmail 地址等。

其他的假冒程序会在原来的免费版本中添加收费功能，运行时弹出对话框让用户付费才能继续，否则游戏就会退出。

这些假冒的 Flappy Bird 现在被检测为 ANDROIDOS_AGENT.HBTF ，ANDROIDOS_OPFAKE.HATC 和 ANDROIDOS_SMSREG.HAT。

我们建议安卓用户，尤其是那些热衷下载 Flappy Bird 的用户，安装这些程序时要小心。网络犯罪者通常会利用热门游戏获取不义之财（例如 Candy Crush, 愤怒的小鸟，神庙逃亡 2 等），制造安全威胁。在我们发布的 *Checking the Legitimacy of Android Apps* 一文中，介绍了几种预防恶意程序的方法。用户可以安装趋势科技移动客户端（Trend Micro Mobile Security）来检测程序的安全性。

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。