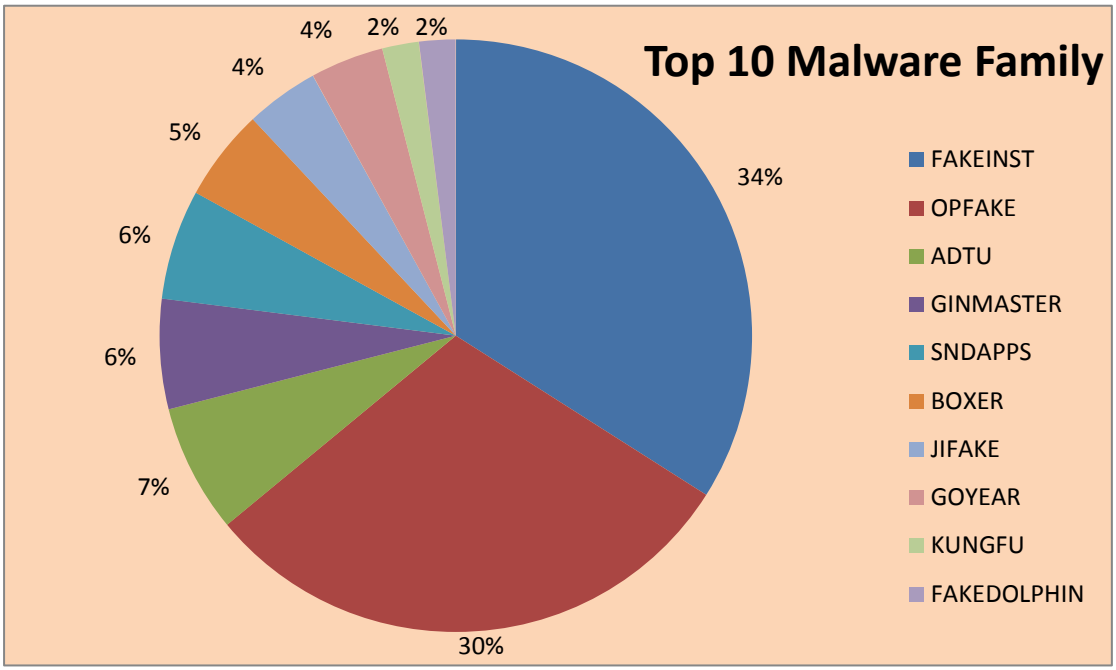
趋势科技移动客户端病毒报告

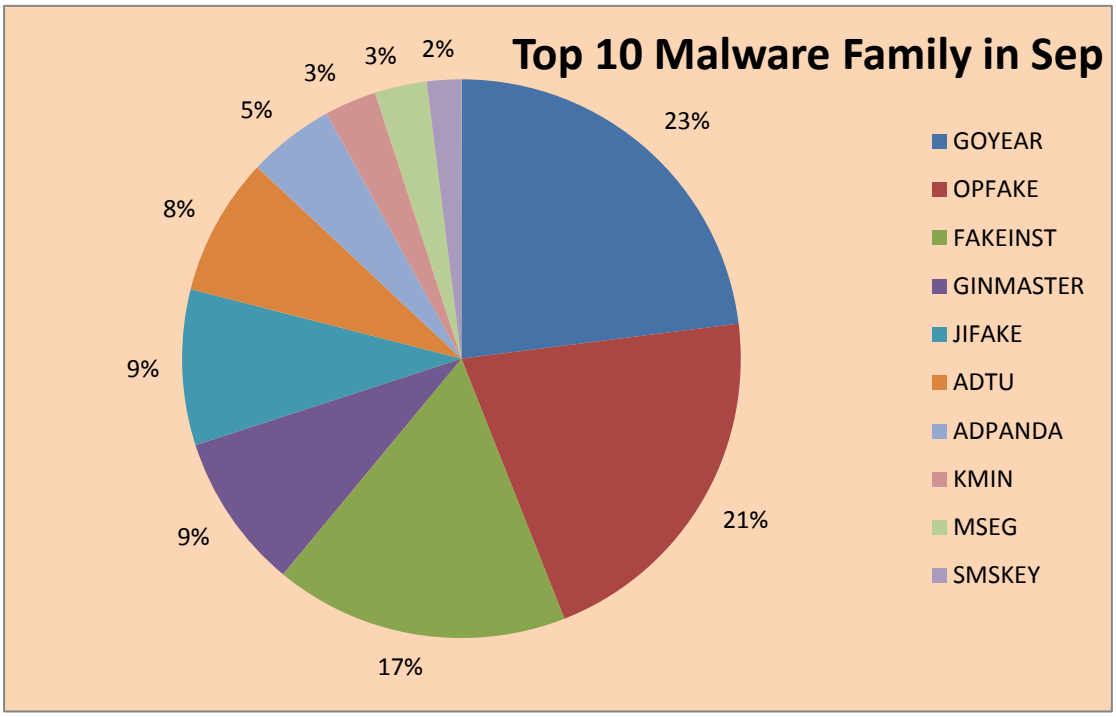
2013年9月移动客户端安全威胁概况

本月趋势科技移动客户端病毒码约为187,700条。截止2013.9.30日中国区移动客户端病毒码1.581.00，大小2,191,426字节,可以检测病毒约100万个。 本月趋势科技新发现移动客户端病毒约15万个。

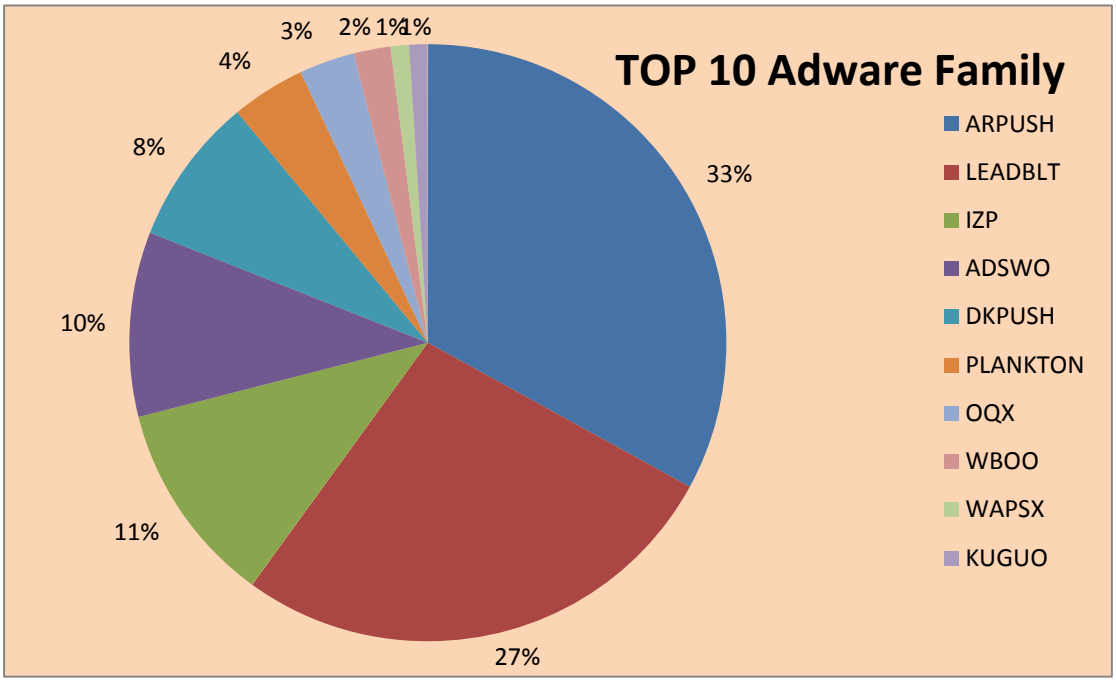
趋势科技移动客户端病毒码中排名前十的病毒家族：



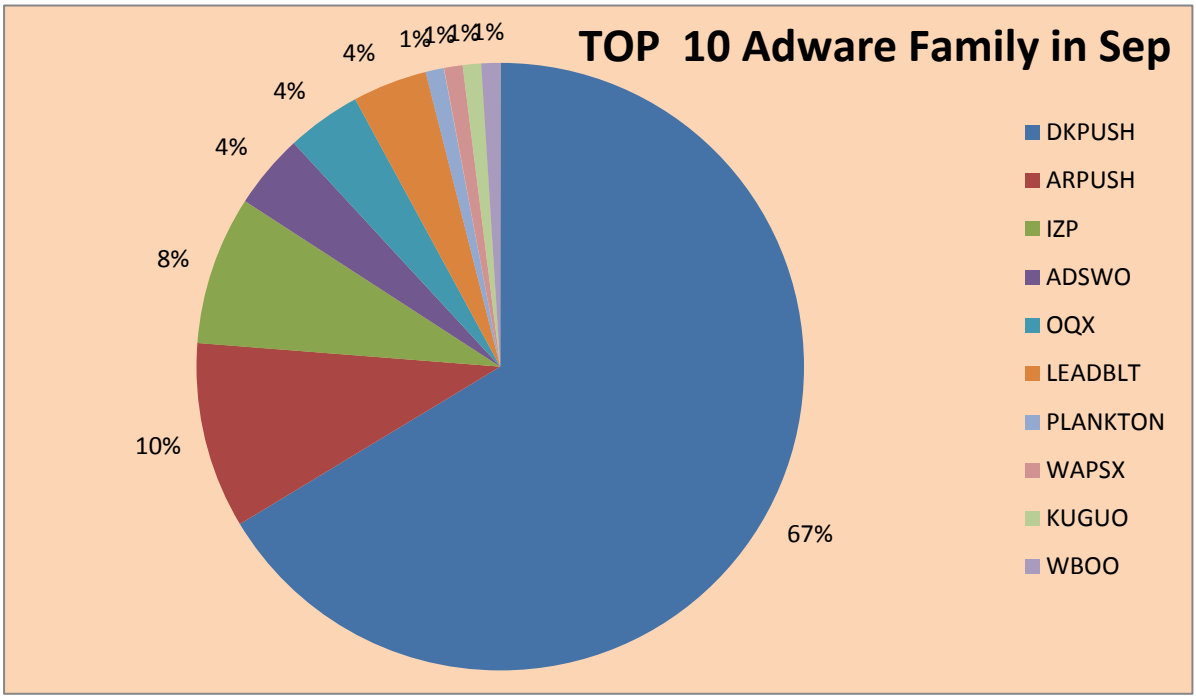
趋势科技移动客户端 9 月新增病毒码中排名前十的病毒家族：



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 9 月新增病毒码中排名前十的广告软件家族：



移动设备中的幽灵：保护移动网银安全

移动技术的发展使得网上银行等业务变得越来越方便。现在用户可以随时随地地购买商品、服务，理财和支付账单。然而，针对移动网银的安全威胁依然存在，需要我们提起重视并加以防范。

这些威胁包括：

- 移动钓鱼：恶意网站会伪装成银行或社交网络等正规机构网站的登录页面，以此欺骗用户输入登录信息。本季度，截至目前为止，将近一半的移动钓鱼网站是伪造的金融服务网站。
- 恶意程序：这类程序包含恶意代码，例如有些可以从宿主机上窃取信息。这类程序多来源于第三方应用商店或者恶意网站，而且多伪装成正常程序。
- 木马化程序（Trojanized apps ）：正常的应用也可能被木马插入恶意代码从而也变为恶意程序。这对用户来讲更具危险性，因为很难区分正常应用和这些“木马化”的程序。正因为如此，这类恶意程序能够在用户察觉之前潜伏运行相当长的时间。

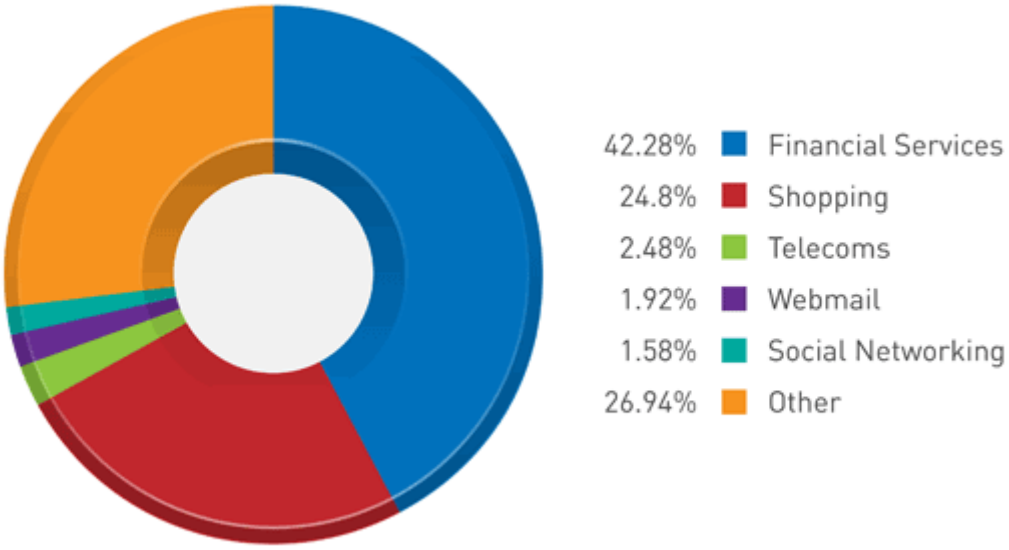


图1.移动钓鱼页面类型分布（2013 第三季度至今）

尽管银行已经采取相关措施来减少移动钓鱼带来的损失，对于用户来说，不论是个人还是企业，也应该采取一些自我保护措施。用户应该熟悉相关银行移动网银的流程，以便能察觉蛛丝马迹，防范钓鱼攻击。通常，好的使用习惯能够帮助保障用户的信息安全。

企业需要理解相关内容并就网上银行的安全风险对员工进行培训，确保安全的底线不受威胁。这些内容可以包括是否允许员工使用个人设备登录网银。企业还应该与相关银行合作研究必要的流程来降低已知的安全风险。

关于移动网银安全的防护的更多信息，我们最近发布了一份最新的移动安全月报 *Security in Mobile Banking*，其中我们探讨了移动网银防护的基本概念和技术。

关于趋势科技

趋势科技股份有限公司(TSE:4704)是全球云端安全的领导厂商，致力于保障企业与消费者数字信息交换环境的安全。趋势科技是业界的技术先驱，在服务器安全领域拥有超过 20 年的经验领先的整合式资安威胁管理技术能遏阻恶意程序、垃圾邮件、数据外泄以及最新的 Web 资安威胁，确保营运作业不中断，保障个人信息与财产的安全。请造访 TrendWatch 查询资安威胁详细信息，网址是：www.trendmicro.com/go/trendwatch。本公司弹性化的解决方案有多种型态可供选择，而且还有全球资安威胁情资专家提供 24 小时全年无休的支持服务。本公司许多解决方案均以 Trend Micro™ Smart Protection Network 为基础，这是涵盖网关外广大空间与客户端的新一代内容安全基础架构，专为协助客户防范 Web 资安威胁所设计。趋势科技是总部位于东京的跨国企业，其备受信赖的安全解决方案透过其业务合作伙伴营销全球。请造访 www.trendmicro.com。