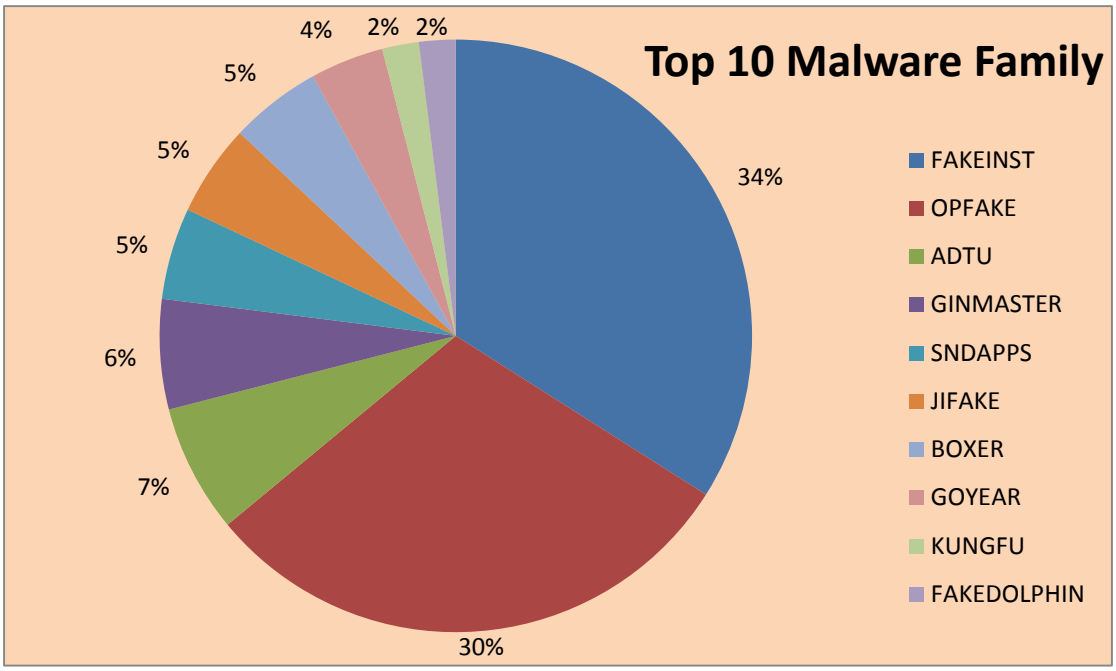
趋势科技移动客户端病毒报告

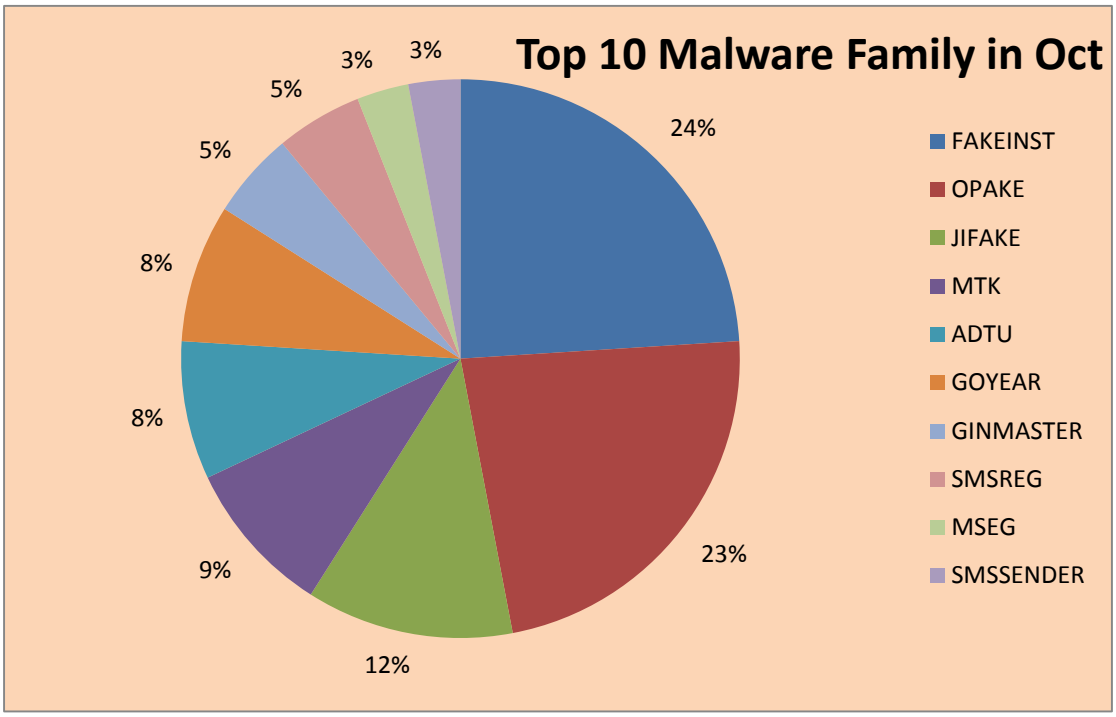
2013年10月移动客户端安全威胁概况

本月趋势科技移动客户端病毒码约为210,100条。截止2013.10.31日中国区移动客户端病毒码1.587.00，大小2,322,004字节,可以检测病毒约110万个。 本月趋势科技新发现移动客户端病毒约10万个。

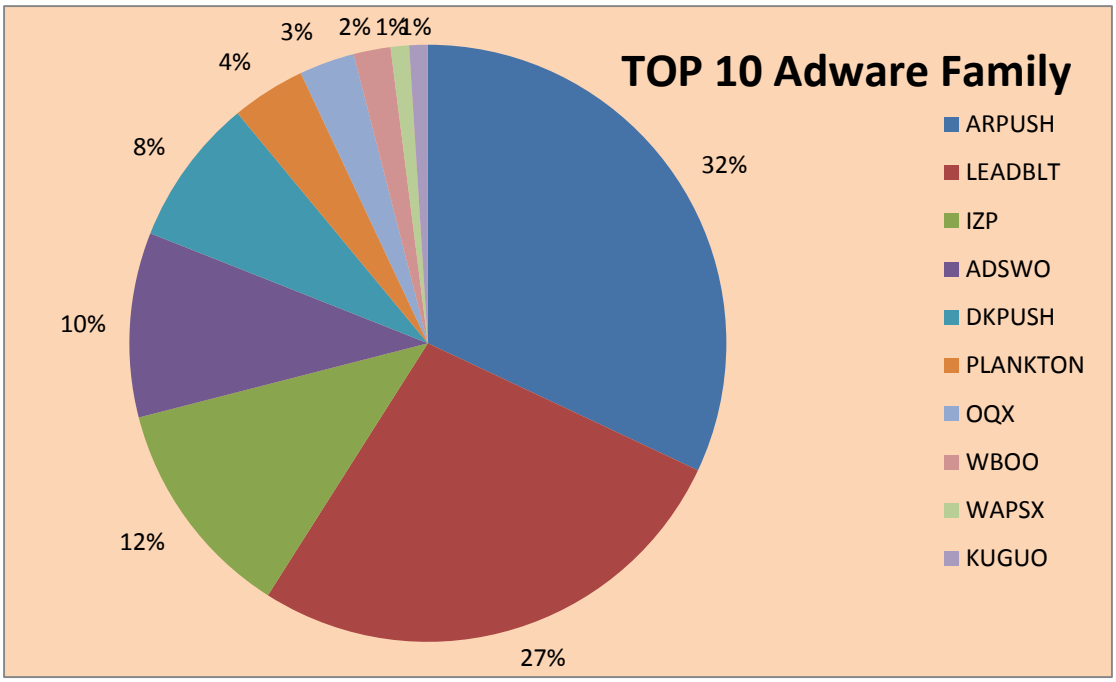
趋势科技移动客户端病毒码中排名前十的病毒家族：



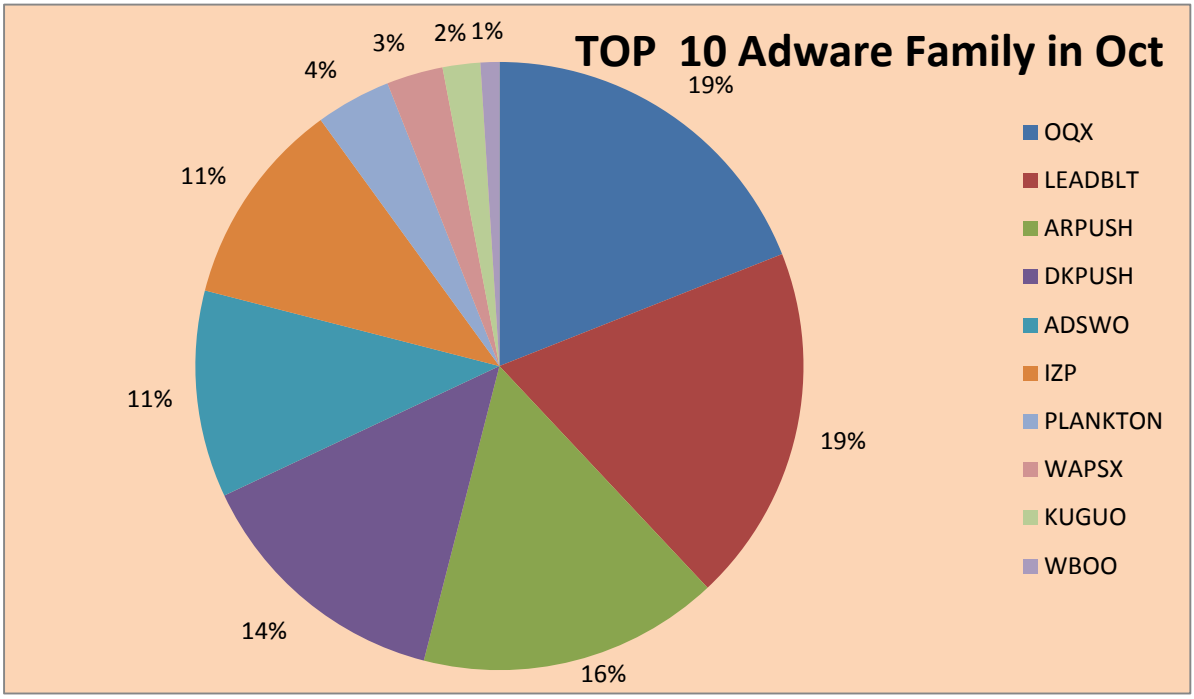
趋势科技移动客户端 10 月新增病毒码中排名前十的病毒家族：



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 10 月新增病毒码中排名前十的广告软件家族：



黑客利用虚假 Facebook 登录页面盗取信用卡信息

最近我们发现了一个和 Facebook 官方移动页面非常像的网络钓鱼页面。然而仔细观察就能发现，钓鱼页面的 URL 和官方页面的明显不同。真正的 Facebook 页面位于 https://m.facebook.com/login 并且地址栏会出现一个锁形标志，代表该页面采用加密连接。

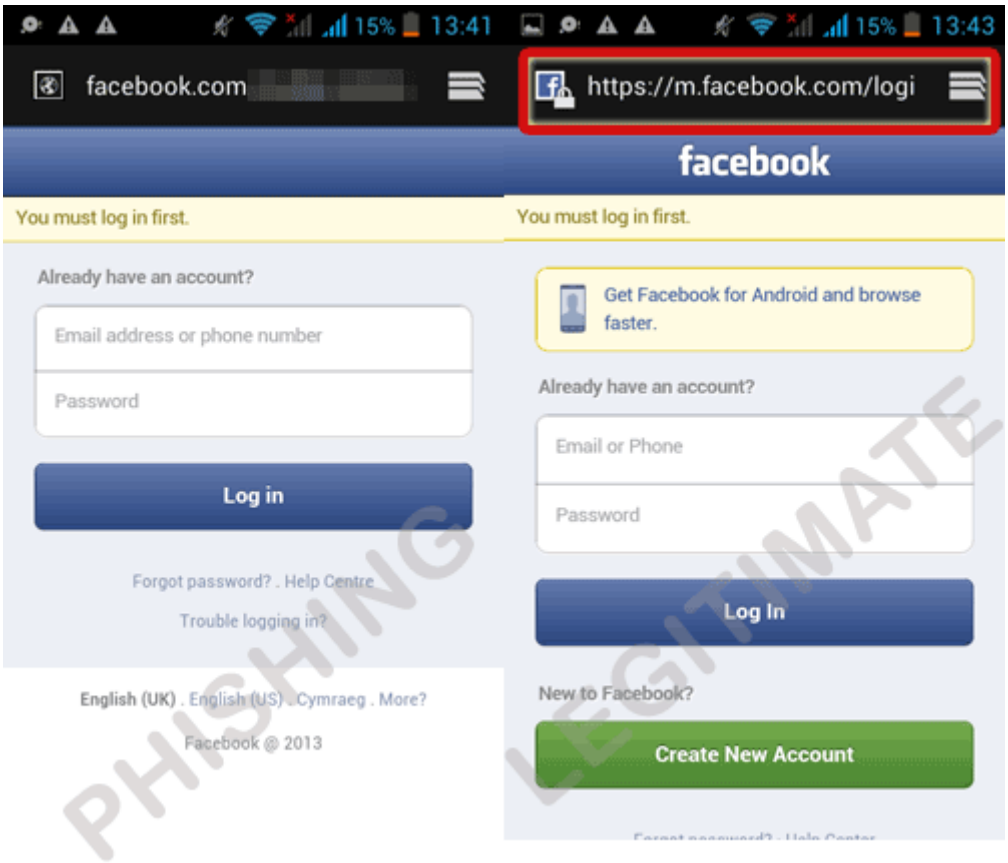


图 1. 假冒页面 vs. 官方页面

该页面不仅仅会盗取 Facebook 账户，一旦用户登入，就会弹出如下页面让用户选择安全问题。这听起来没什么，但是这些安全问题有可能被用于其他网站，这就带来了安全风险。

图2. 假冒安全问题页面

这一步完成后，用户会被带到下面的页面，这次需要提供信用卡信息。

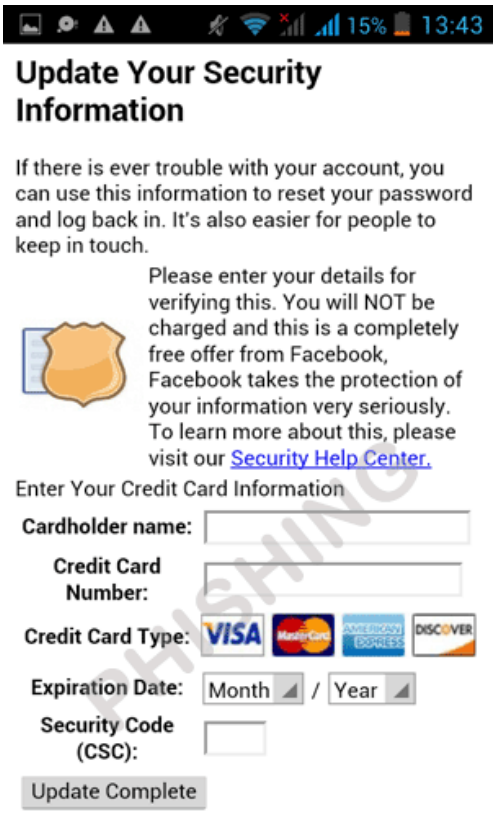


图3. 骗取信用卡信息的页面

对于类似的钓鱼网站，用户应当时刻保持警惕，并在输入任何个人信息之前再次检查网站的URL，尤其是那些声称其为特定服务的网页。Facebook 不会要求用户填写信用卡信息，除非他们需要在线购物。

今年的早些时候，我们已经确认移动设备成为了钓鱼攻击的平台。诸多备受瞩目的事件，如针对摩根大通银行客户的钓鱼攻击，作为跨平台安全威胁的假冒 WhatsApp 消息通知，Android 主秘钥漏洞，以及与日俱增的移动网银交易规模，这些都说明了针对移动平台的安全威胁正变得像 PC 平台上的那样严重。

通过正确的防护，用户可以避免成为此类威胁的受害者。Trend Micro 通过网站信誉服务（Web Reputation Service）拦截相关恶意网站，保护用户信息安全。

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。