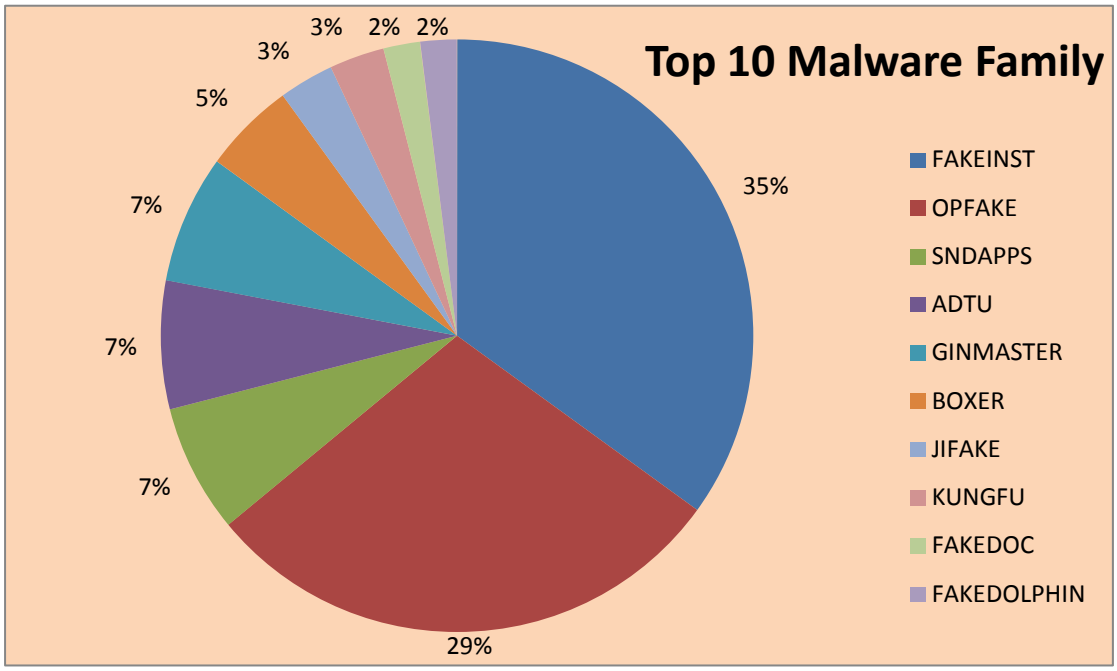
趋势科技移动客户端病毒报告

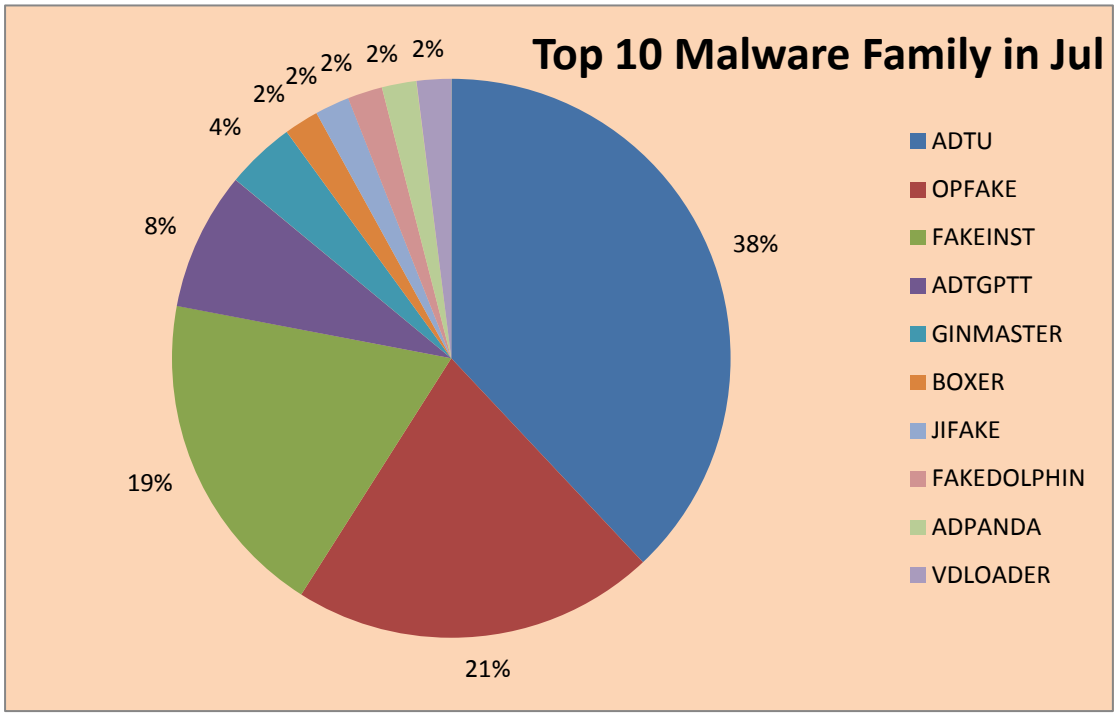
2013年7月移动客户端安全威胁概况

本月趋势科技移动客户端病毒码约为125,070条。截止2013.7.31日中国区移动客户端病毒码1.525.00，大小1,389,384字节,可以检测病毒约80万个。 本月趋势科技新发现移动客户端病毒约11万个。

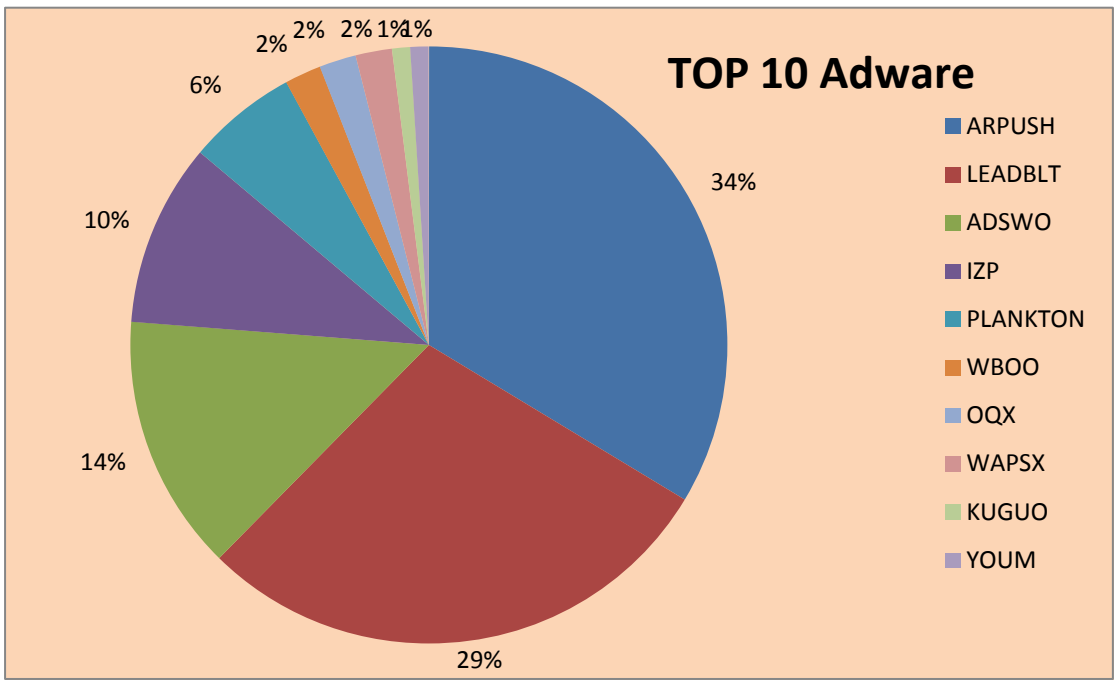
趋势科技移动客户端病毒码中排名前十的病毒家族：



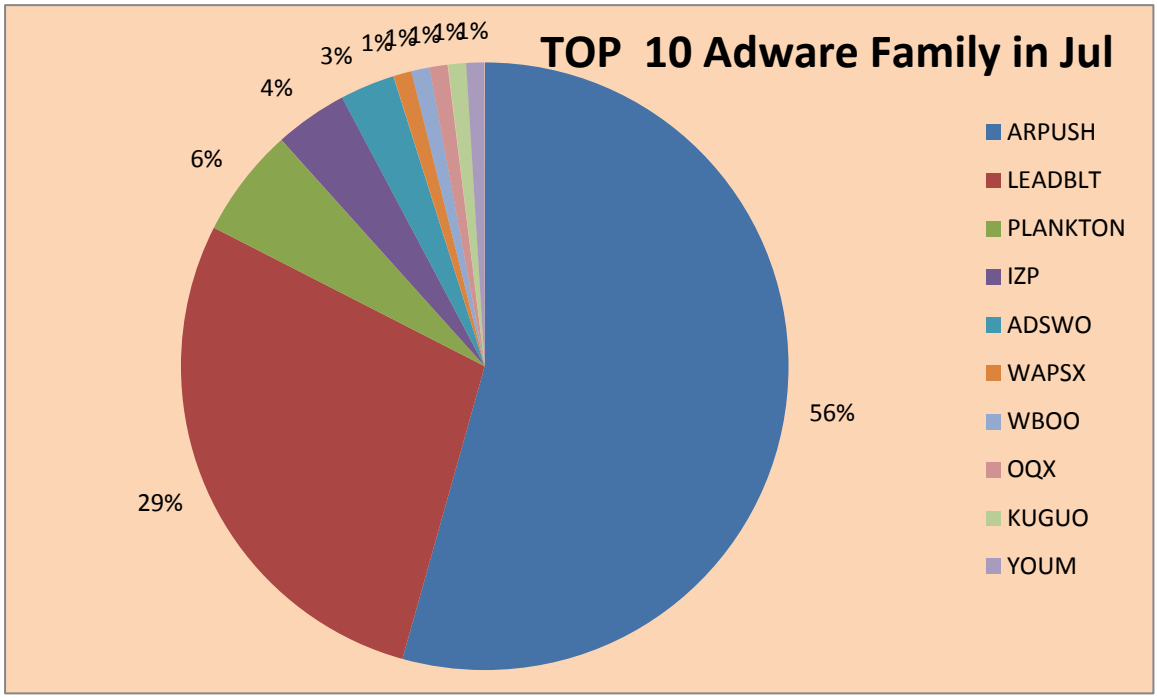
趋势科技移动客户端 7 月新增病毒码中排名前十的病毒家族：



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 7 月新增病毒码中排名前十的广告软件家族：

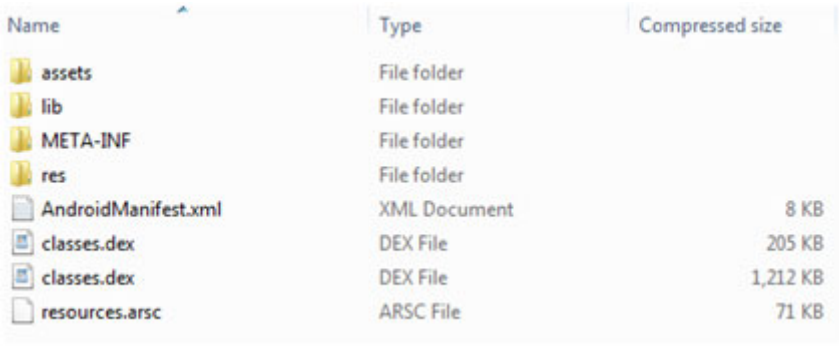


Android 签名漏洞被利用，网银软件被插入恶意代码

最近被曝出的 Android 签名漏洞，能够使黑客将恶意代码插入到已安装的程序中而不改变程序的签名。我们持续监测了利用这一漏洞进行攻击的恶意程序，目前，我们已经发现了一款以韩国农协银行（NH Nonghyup Bank）网银软件为目标的恶意程序。

韩国农协银行（NH Nonghyup Bank）是韩国最大的金融机构。他们的网上银行软件在手机用户中的安装量非常大，总计已经被安装近 500 万到 1000 万次。

黑客利用了该软件的高普及率，在第三方网站上提供一个可下载的更新。该更新含有恶意代码。它利用 Android 签名漏洞将恶意代码插入正常的网银程序，从而使其变为木马。



被插入代码的文件中，classes.dex 文件大小会变为 205kb，比正常程序的要小。

黑客还提供了一个已经被插好代码的网银程序，以防有的用户并没有安装网银程序。执行这个恶意程序会触发显示一个欺诈页面，用来骗取用户输入的账户信息。

当用户执行程序时会显示图示页面

如果用户输入了真实的信息，他们的账号密码等信息会通过服务器回传给黑客。

这一发现，充分显示了 Android 签名漏洞被利用对用户来讲是非常大的一个安全风险。被插入恶意代码的网银软件在危险程度上，可以与以往针对网银的恶意程序相比拟，因为它不仅导致个人信息泄露，而且会造成经济损失。

并且，它是去篡改已经被安装到手机中的程序，用户可能都毫无察觉，直到大事已晚。

所以我们建议用户从正规渠道下载程序和更新，最好是从官方网站或者应用商店下载。趋势科技用户能够通过我们的 Trend Micro Mobile Security App 防范这一安全风险，针对 Android 签名漏洞的利用程序已经能被检测。

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。