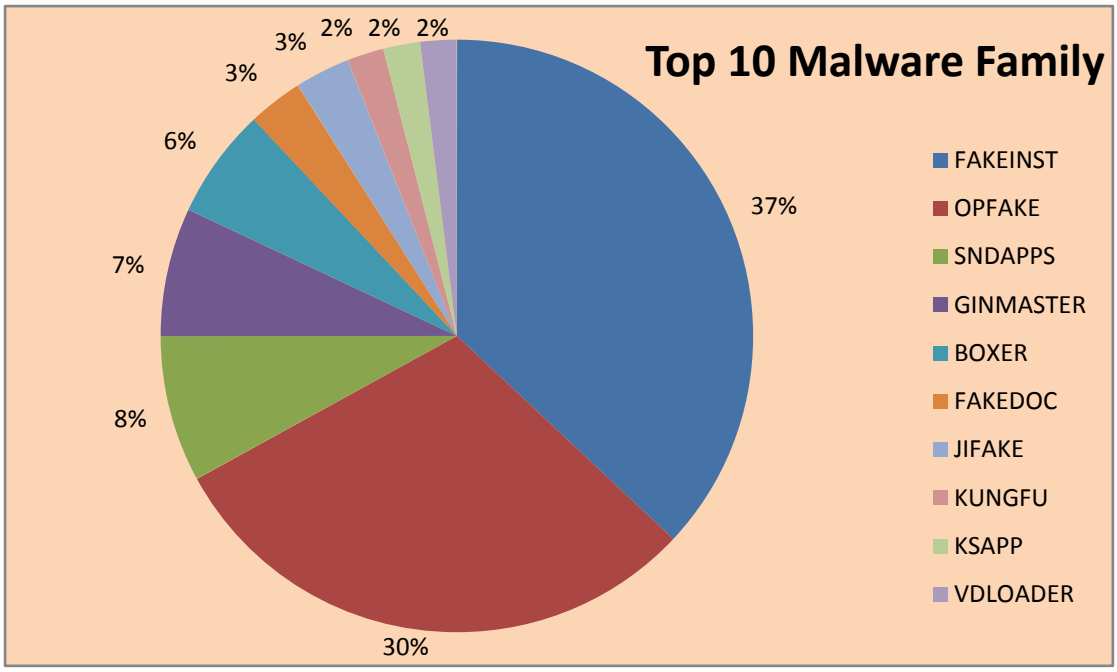
趋势科技移动客户端病毒报告

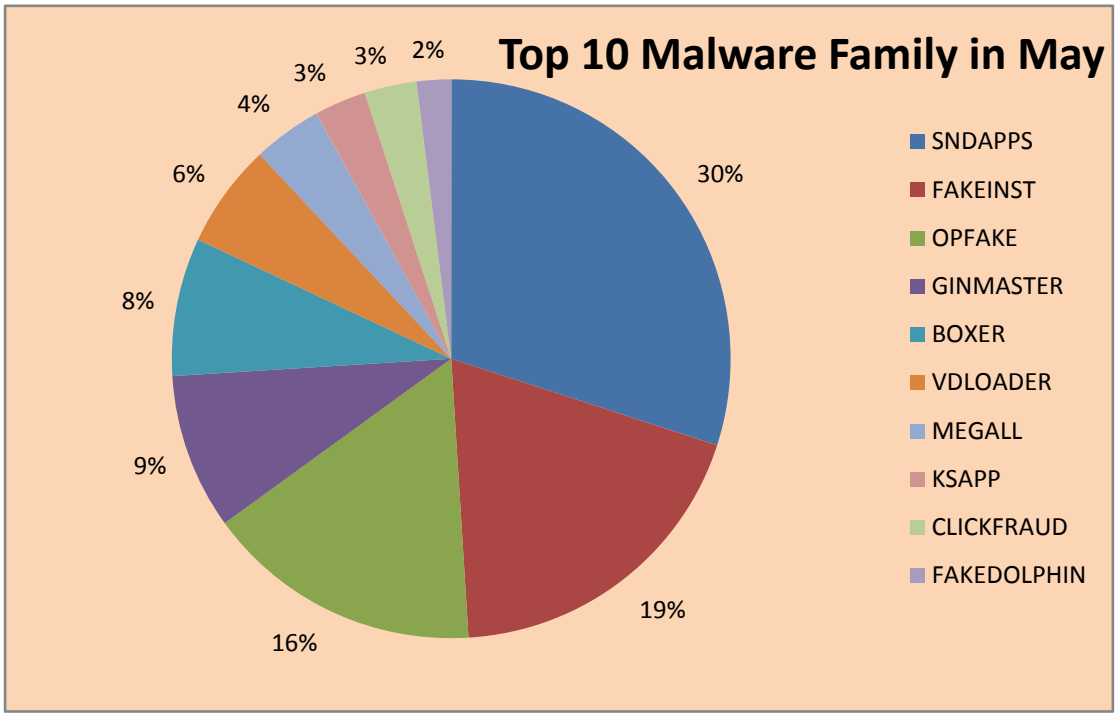
2013年5月移动客户端安全威胁概况

本月趋势科技移动客户端病毒码约为88,284条。截止2013.5.31日中国区移动客户端病毒码1.481.00，大小1,024,882字节, 可以检测病毒约61万个。 本月趋势科技新发现移动客户端病毒约5万个。

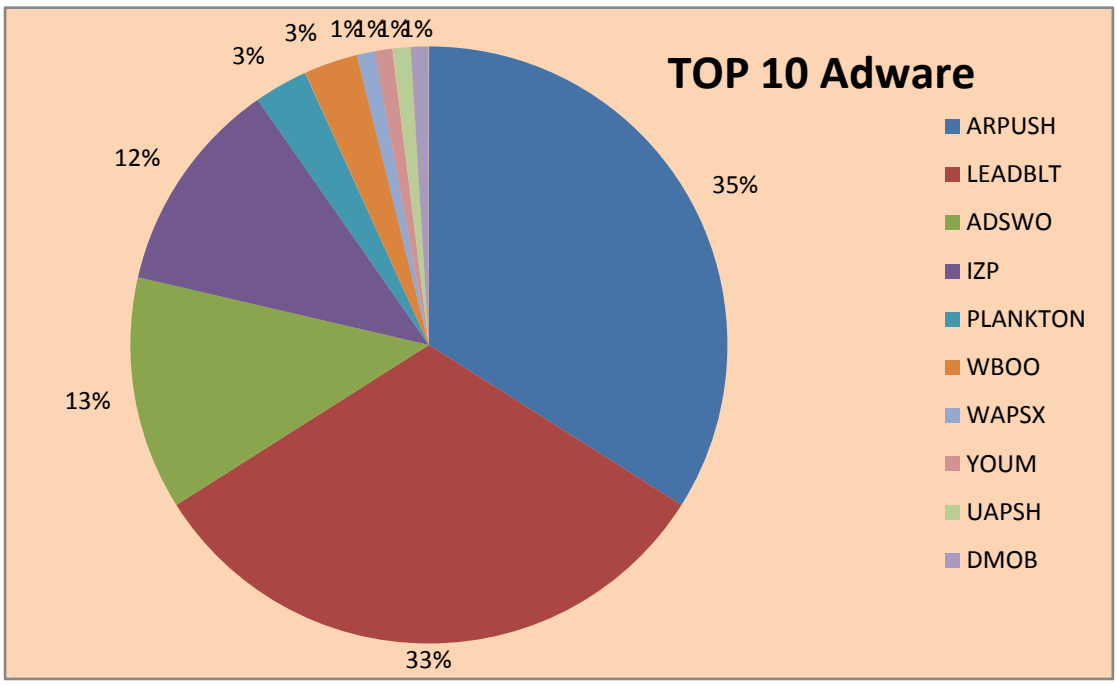
趋势科技移动客户端病毒码中排名前十的病毒家族：



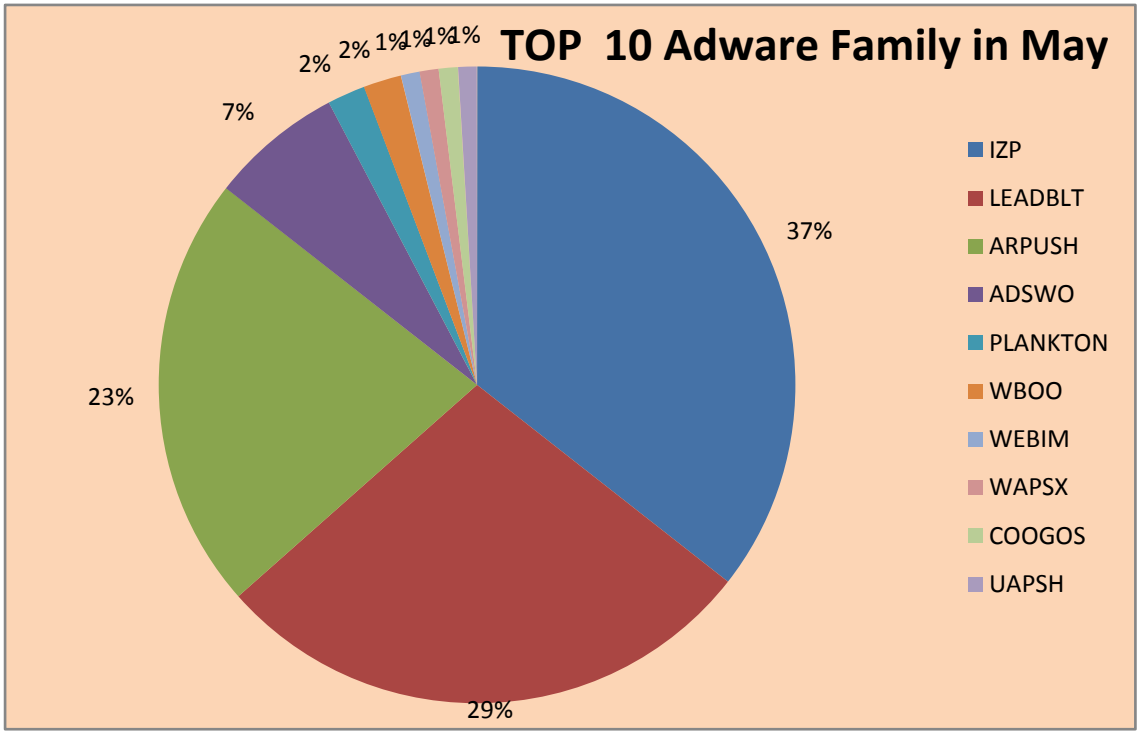
趋势科技移动客户端 5 月新增病毒码中排名前十的病毒家族：



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：



移动设备的“安全”：远程锁定被盗手机所带来的问题

由于移动设备的被盗案件形势严峻，立法者开始决定出台相关法案来应对此事。上周，美国参议员Charles Schumer重新提交了2013移动设备反盗窃行动（Mobile Device Theft Deterrence Act of 2013）草案，其中将修改设备IMEI号的行为定为犯罪，并将受到最长达5年的监禁。理论上，这将会使得被盗手机重新使用变得更加困难，也会使得相关诉讼案件数量减少。CTIA，一个代表无线通信业的商贸组织，已经表示支持该草案。

丢失移动设备着实会带来很大的损失。更换手机需要花几百美元，并且，手机上所有的数据会都会丢失。企业高度重视后者所带来的的问题。

即使该法案通过，它所能带来的影响的大小也是未知的，因为许多被盗设备会被销往国外。（赃物被销往国外的案例不仅局限在电气设备，比如被盗的汽车就一直会被销赃至阿尔巴尼亚，非洲等其他欠发达国家和地区。）

更大的问题是，对于该问题的其他解决办法反倒会降低移动设备的安全性。人们建议将远程锁定功能加入新设备。然而，从安全的角度看，这样做是很有问题的：这意味着远程管控设备的功能将会被加入其中，也就不排除攻击者会以此功能为目标，获得相应权限从而做任何能做的事。

有一个很棘手的问题是谁掌握了这样的关键能力，用户和组织都可能遭到社会工程学攻击，从而被黑客锁定设备。我们应该让设备更安全，而不是削弱其安全性；一个能被远程锁定的系统，存在诸多现实的安全隐患。也许我们更应该关注手机被盗后的定位，而这样的功能已经内置在了除Android之外的iOS和Windows Phone系统中。

设备被盗的问题应该被当做是警方的问题，而不是一定要寻求一个技术解决方案。任何解决设备被盗问题的方案都应该兼顾整体安全性，而政策所带来的负面效应不容忽视。

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。