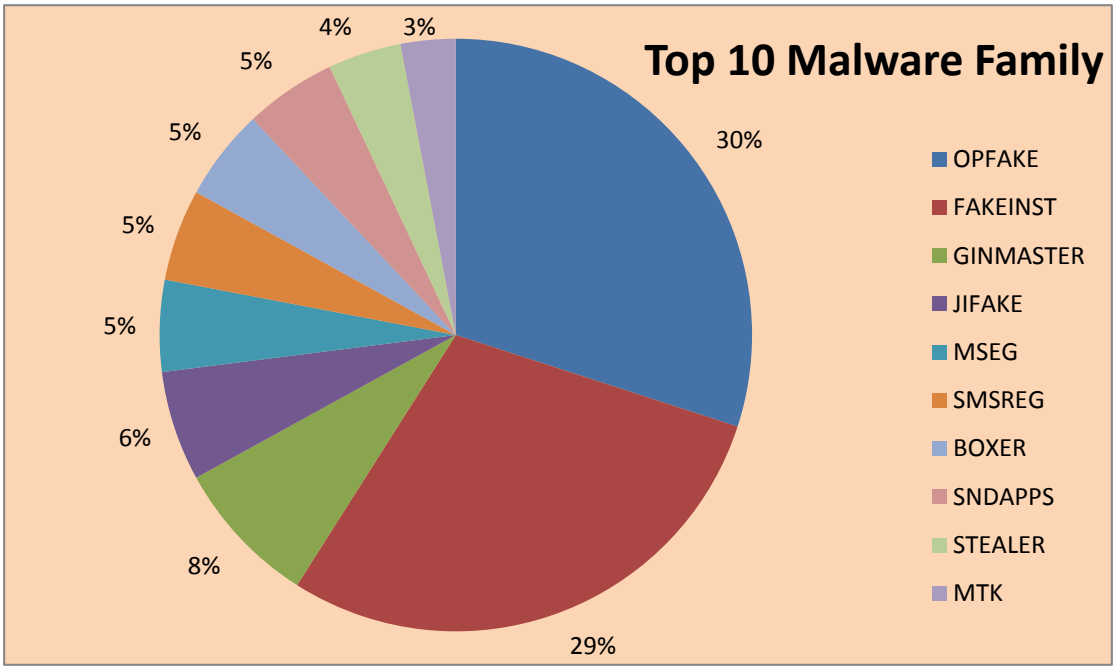
趋势科技移动客户端病毒报告

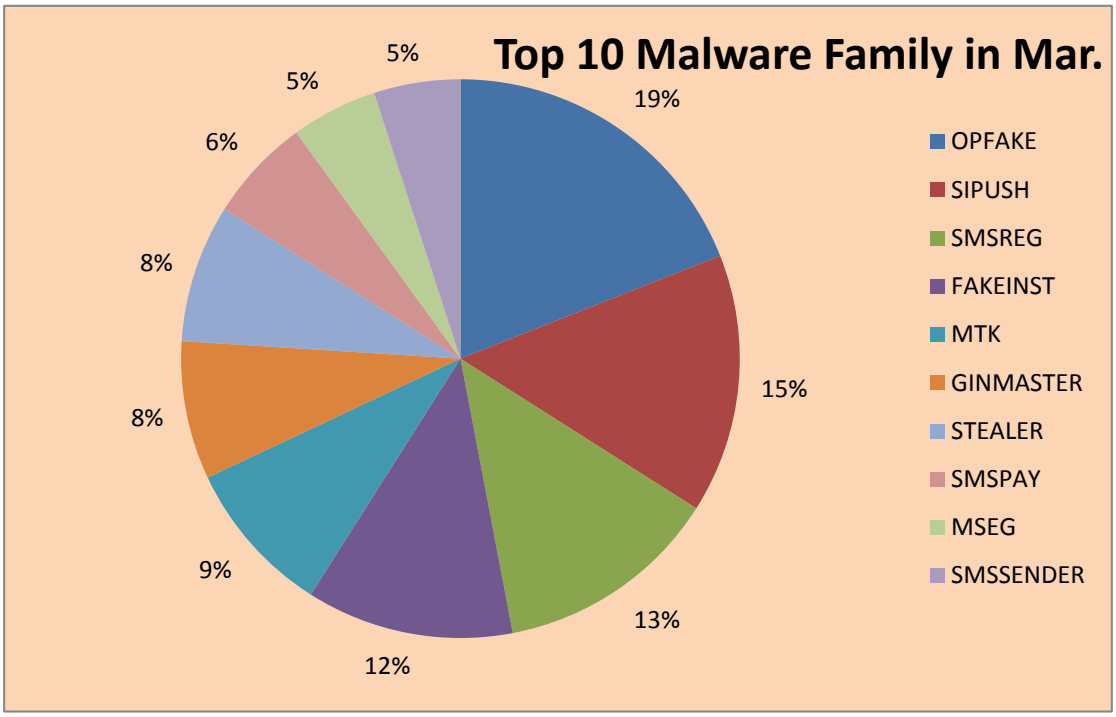
2014年3月移动客户端安全威胁概况

本月，截止 2014.3.31 日中国区移动客户端病毒码 1.649.00，大小 11,149,170 字节,可以检测病毒约 209 万个。本月趋势科技新发现移动客户端病毒约 27 万个。

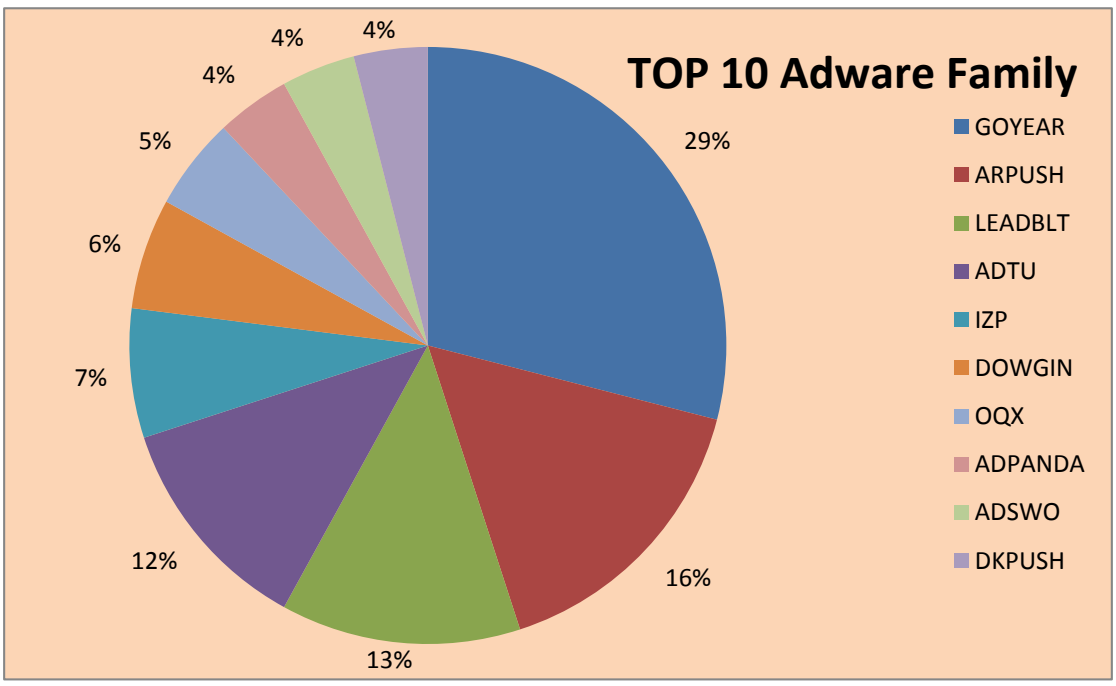
趋势科技移动客户端病毒码中排名前十的病毒家族：



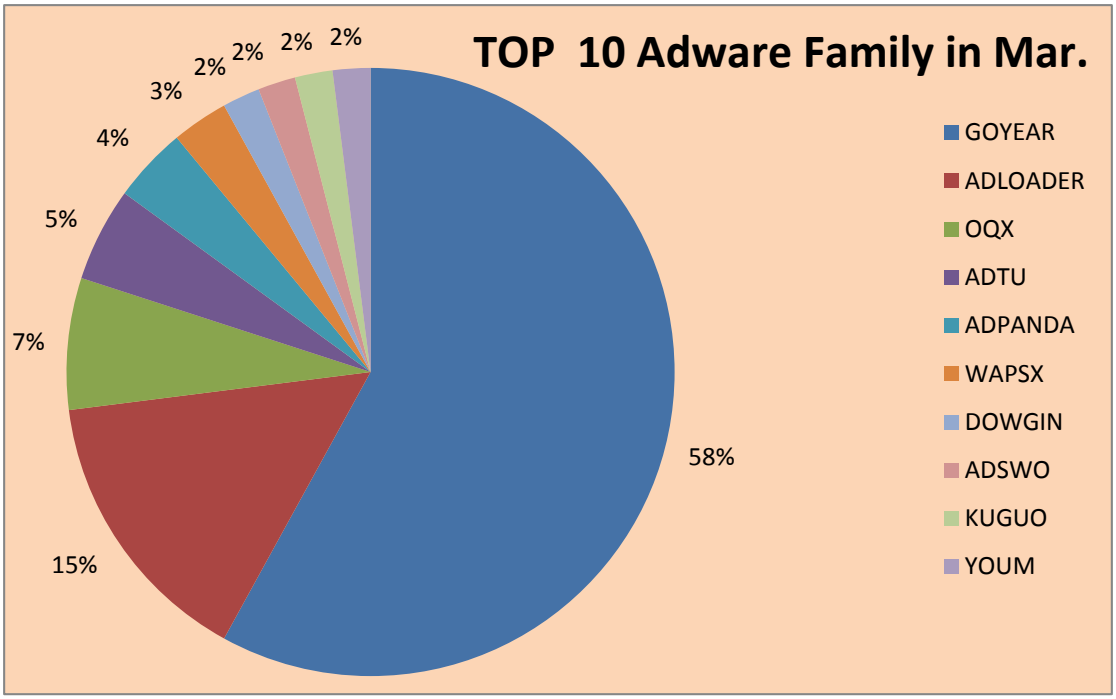
趋势科技移动客户端 3 月新增病毒码中排名前十的病毒家族：



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 3 月新增病毒码中排名前十的广告软件家族：



移动平台恶意和高危软件数量已达 200 万，增长迅猛

移动平台的恶意和高危软件数量在 6 个月之前已经达到 100 万个，短短数月之后的今天，这一数字已经翻了一番。

图 1.恶意和高危软件数量已经达到 200 万

紧随着移动恶意软件诞生 10 周年，即达到了这一里程碑式的数字。2004 年出现了第一个攻击 Nokia 塞班系统的 PoC，即 SYMBOS_CABIR。但是直到智能手机时代全面到来之前，移动恶意软件还没有成为重要的安全威胁。从相对无害的弹窗提示，移动恶意软件已经慢慢发展到具有扣费，信息窃取，后门甚至 rootkits 功能。

而且威胁仍在不断发展。数量达到 100 万后，我们注意到移动恶意软件开始转向比较前沿的领域。这类程序将在未来数月引领恶意软件技术。

TORBOT 的匿名技术

Onion Router(多称为 TOR)是用户用来在网络上匿名的工具。它也因为对地下网络的涉及而闻名。网络犯罪者现在经常用 TOR 隐藏他们的恶意程序。ANDROIDOS_TORBOT.A 是第一个利用 TOR 连接远程服务器的移动平台病毒。连接上服务器后，它会进行拨打电话，拦截并读取短信，向指定号码发送短信等恶意行为。对 TOR 网络的应用使得我们追踪它的行为以及 C&C 服务器地址变得更加困难。

DENDROID 的传播技术

我们经常谈论到移动平台恶意软件数量如何快速地增长。一个远程控制类的木马将大大地增加这一数量。ANDROIDOS_DENDROID.HBT 能够截屏，窃取照片、视频和音频记录，并且可以进行通话录音。值得一提的是 DENDROID 作为一款黑客工具出售，该软件在地下市

场里的售价已经达到 300 美元，承诺能够轻易将恶意代码插入正常程序。DENDROID 提供了一个 APK 捆绑工具，一个 APK 客户端，和一个能将这些应用重新打包的后台控制程序。更值得人们警惕的是 DENDROID 居然出现在 Google Play 商店，这款恶意软件能够绕过 Google Bouncer 的检测。

手机变成黑客的“挖矿”工具

网络犯罪者变本加厉，甚至把手机当成“挖矿”的工具。ANDROIDOS_KAGECOIN.HBT 能够挖掘 Bitcoin，Dogecoin，Litecoin 等电子货币。挖矿过程仅在设备充电的时候进行，因为这样电量的消耗不会引人注意。尽管恶意行为已经尽量地保持“低调”，但肯定会对设备造成影响。挖掘电子货币需要大量的运算，但是一般手机应付不了如此大的计算量，所以用户一般都会因为手机假死而选择重启。

移动安全新领域

需要指出的是我们在本文介绍的几个病毒都涉及了应用比较广泛的技术。TOR 因为涉及到了网上隐私保护，持续受到关注。电子货币如 Bitcoin 和 Dogecoin，随着它们货币价值的不断走高，也在大众中受到瞩目。由此可见，网络犯罪者会将一切可以触及到的利益纳入自己攻击的范畴。

随着移动平台的恶意和高危软件数量达到 200 万，用户们应该考虑如何防护自己的设备了。仔细辨别应用程序，防范不可信的 URL，删除可疑的短信和邮件，这些可以在一定程度增加安全性。密切关注已报告的软件漏洞，比如那些涉及用户权限和能使系统崩溃的漏洞，防止黑客攻击这些漏洞的可能。 Trend Micro Mobile Threat Hub 提供了与移动安全、智能手机和平板电脑安全防护方面相关的信息，欢迎访问。

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。