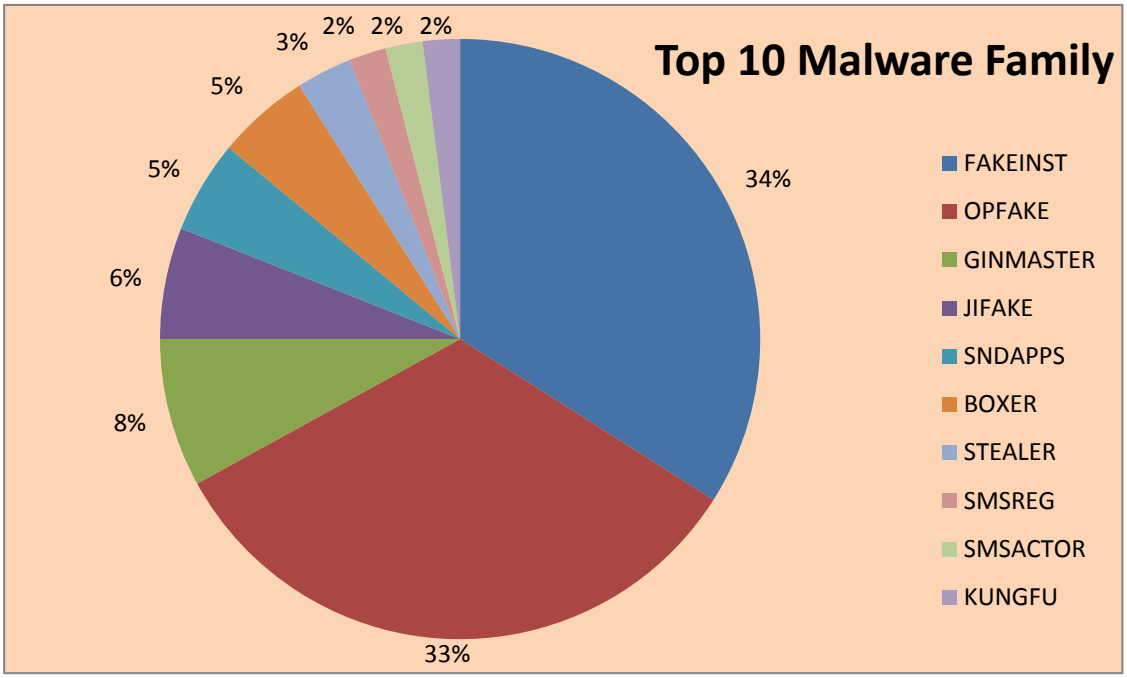
趋势科技移动客户端病毒报告

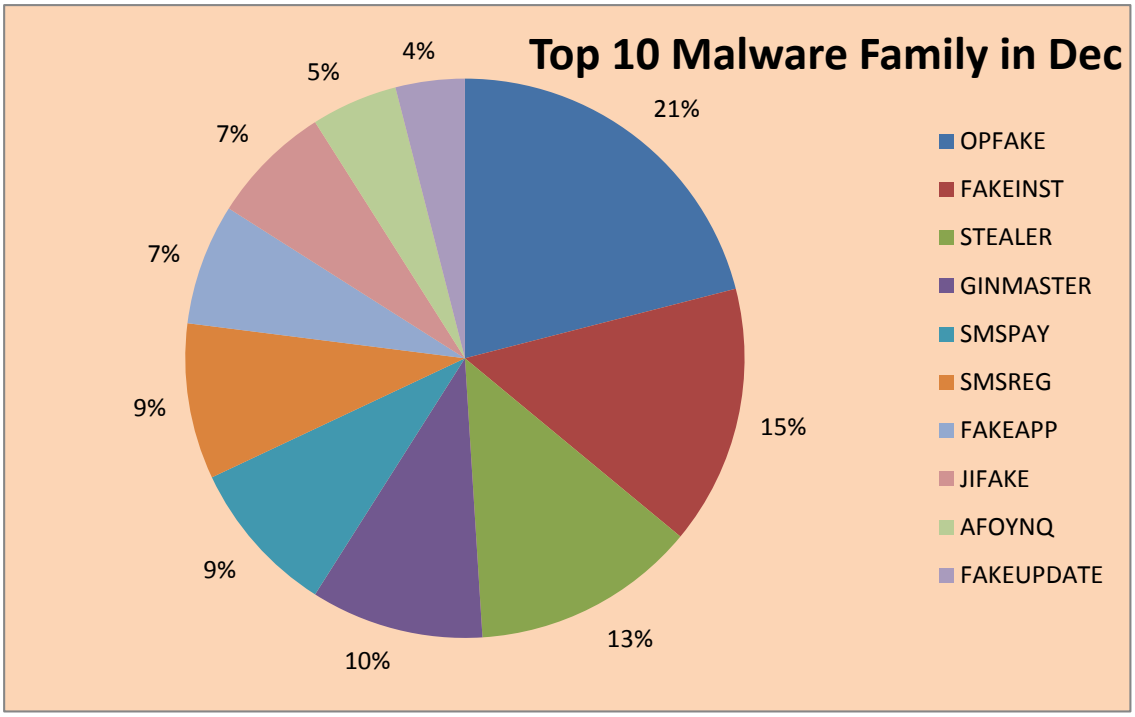
2013年12月移动客户端安全威胁概况

本月趋势科技移动客户端病毒码约为384,010条。截止2013.12.31日中国区移动客户端病毒码1.603.00，大小8,201,241字节,可以检测病毒约138万个。 本月趋势科技新发现移动客户端病毒约12万个。

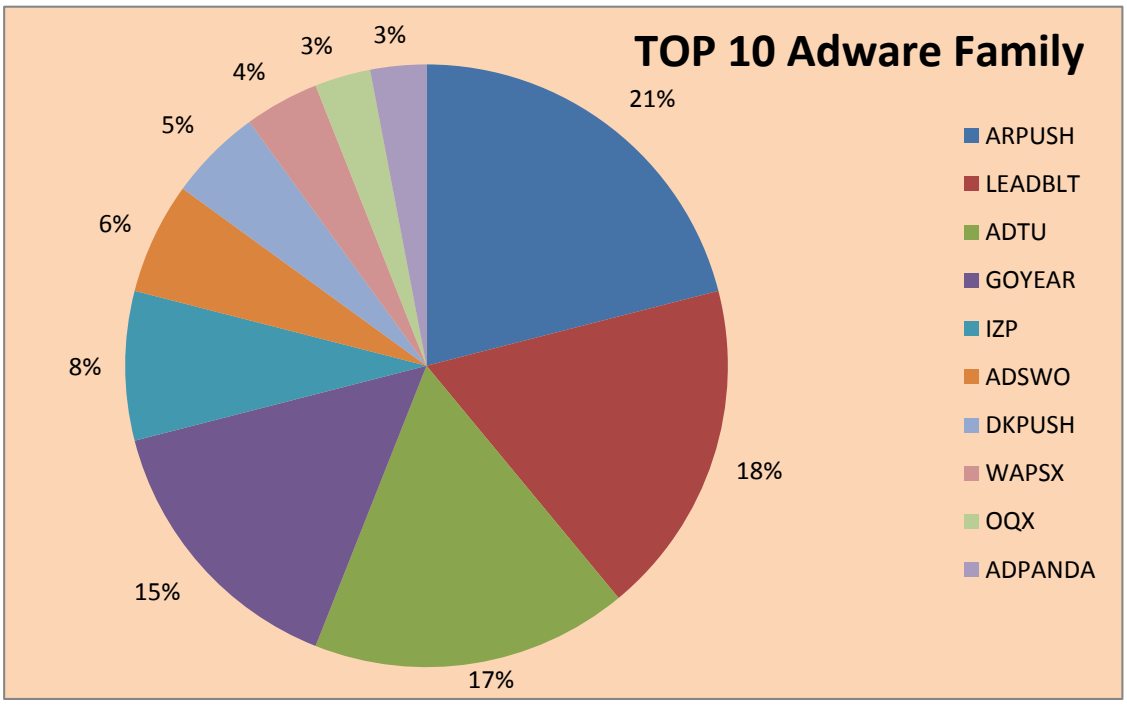
趋势科技移动客户端病毒码中排名前十的病毒家族：



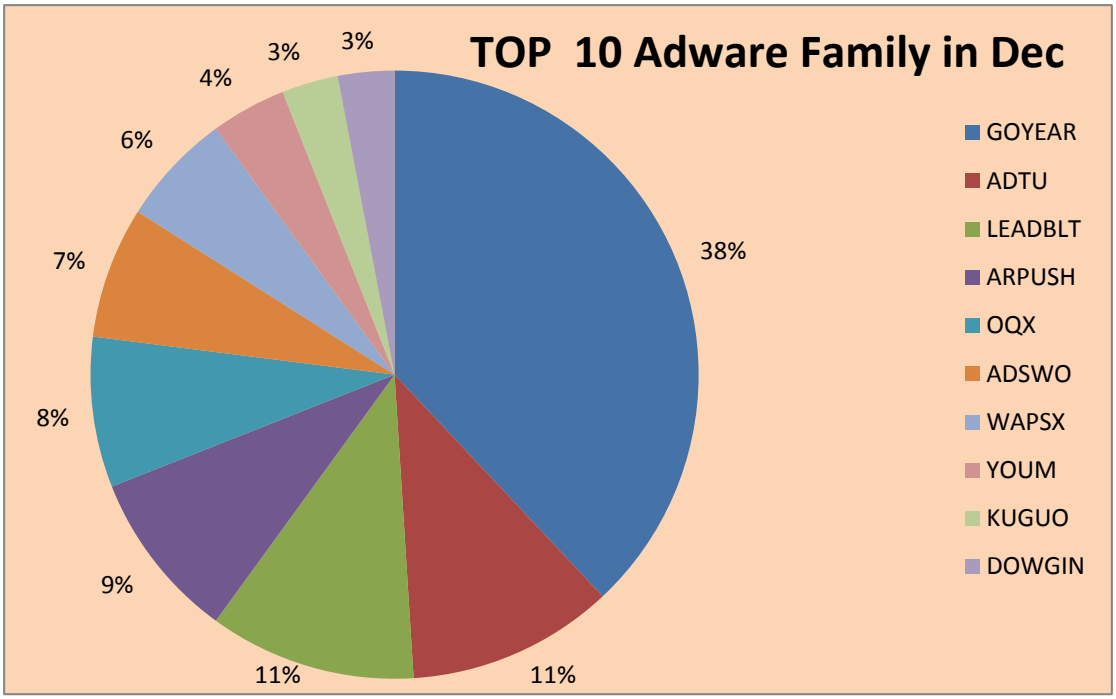
趋势科技移动客户端 12 月新增病毒码中排名前十的病毒家族：



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 12 月新增病毒码中排名前十的广告软件家族：



个人化设备以及一些不切实际的期望

最近，有一个非常火热的话题，是关于部署平板设备的。据洛杉矶时报报道，洛杉矶联合学区(Los Angeles Unified School District, LAUSD)被强制暂停了一项向学生提供 iPad 的计划，因为几个学生发现了能够突破学校管理者设置的安全限制的方法。

原来，LAUSD 并没有充分地管理好它们的 iPad。他们仅是使用了 ActiveSync 账户，而学生们可以随便将其从 iPad 中删除。这使得他们可以控制自己的 iOS 设备并用其下载音乐，访问社交媒体网站等。（这些学校因此收回了所有已发放的 iPad）

这个案例显示了在大范围内系统地部署移动设备所带来的弊端。这就亟需更为成熟的管理方案，但这样会增加成本。（包括前期投入和长期成本）所以，他们采取了相对简单且易维护的解决方案，但是这样很容易被攻破。从纯技术的角度来看，解决问题的方法不是没有，但并没有被采用。

然而，值得我们注意的是为什么不采用。技术的问题可以轻易解决。为什么学生们要去破解他们手里的设备呢？一名学生回答的好：他们把设备带回家，但是用它却什么都干不了。

一言以蔽之，学生们把这些 iPad 当成个人设备 ，用它存储自己的数据，做自己的想做的事。由此，那些想保护员工设备的企业可以得到一些启发。

尽管企业消费端化迅速兴起，“个人设备”和“工作设备”之间仍然存在着差异。移动设备的管理试图踏平这些差异，但是这样会增加成本和复杂性。重要的是，用户关于“个人”和“工作”的思维差异仍然存在。这意味着企业数据可能因为暴露在个人设备上而面临安全风险。

比技术方案更重要的是理解和改变用户的思维方式。理解用“个人”设备处理“工作”信息即意味着需要改变使用习惯这一命题，是解决企业消费端化的策略中的一部分。比如，你不能把存放工作邮件的平板电脑给孩子去玩游戏，那就太愚蠢了。员工需要理解安全除了受到技术制约，也受到使用习惯的制约。

反过来，企业需要明白在个人设备上施加的限制措施要足够合理。像上面那个例子，由于限制太过严格导致学生已经想要突破这些限制了。同时企业需要注意他们设置的限制不能被轻易绕过。

处理企业消费端化，我们需要策略上的支持。很明显，不同机构根据他们不同的需求，能力，和潜在威胁会有不同策略。这个案例告诉我们的是，这些策略需要合理，更重要的是需要具有可实施性。

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。