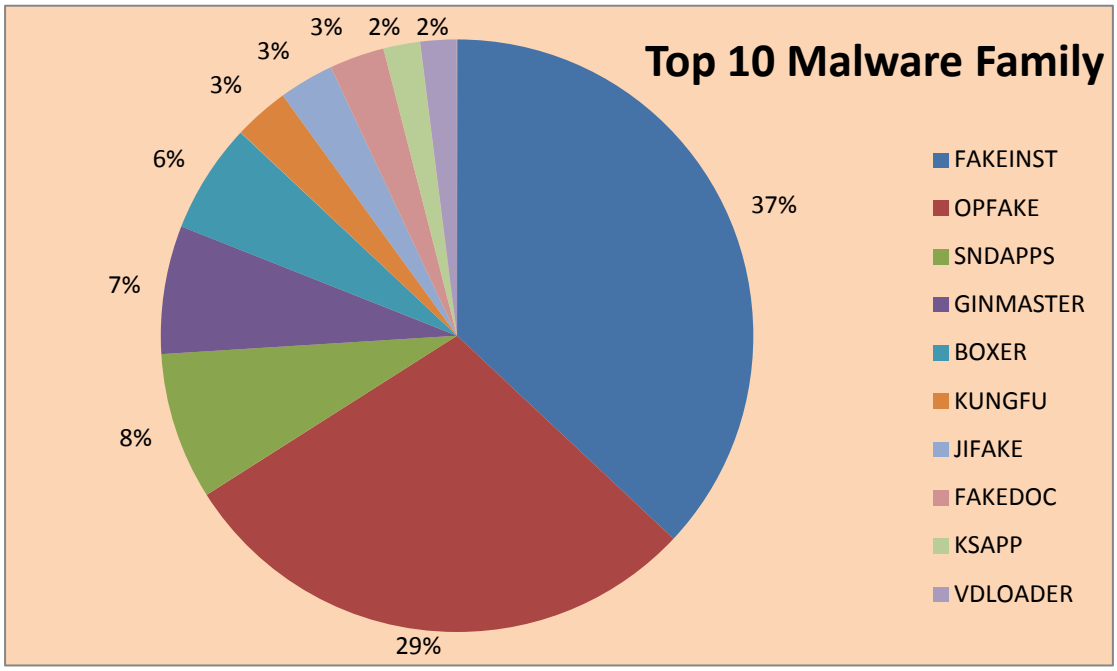
趋势科技移动客户端病毒报告

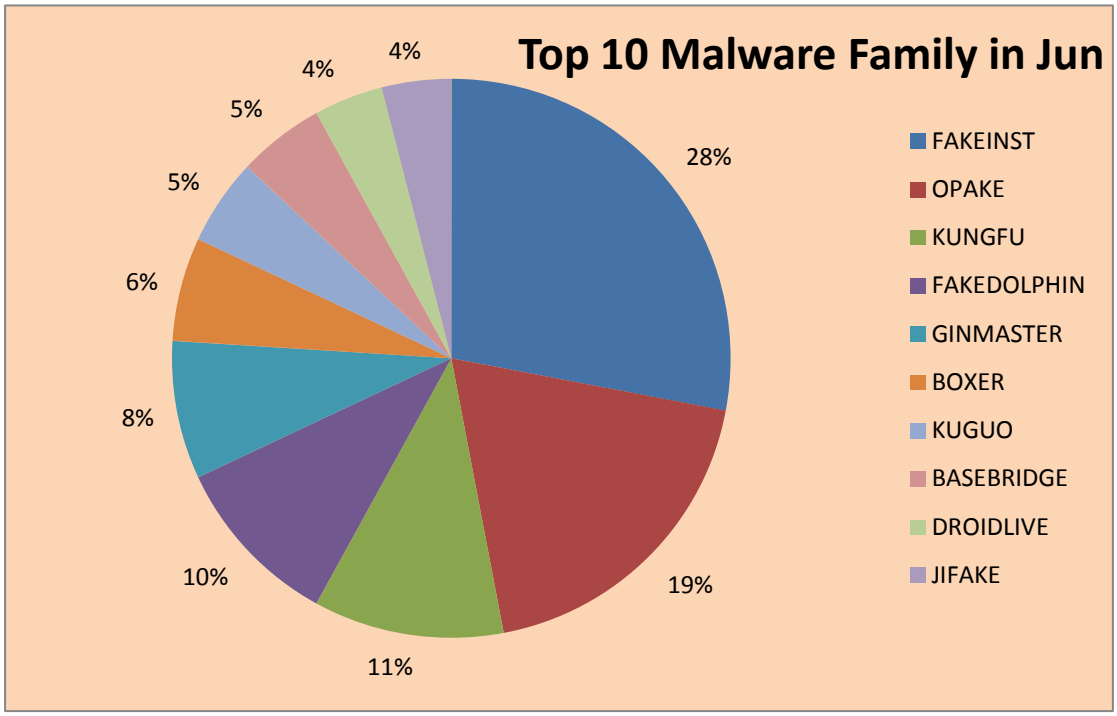
2013年6月移动客户端安全威胁概况

本月趋势科技移动客户端病毒码约为116,912条。截止2013.6.30日中国区移动客户端病毒码1.499.00，大小1,1092,475字节,可以检测病毒约69万个。 本月趋势科技新发现移动客户端病毒约8万个。

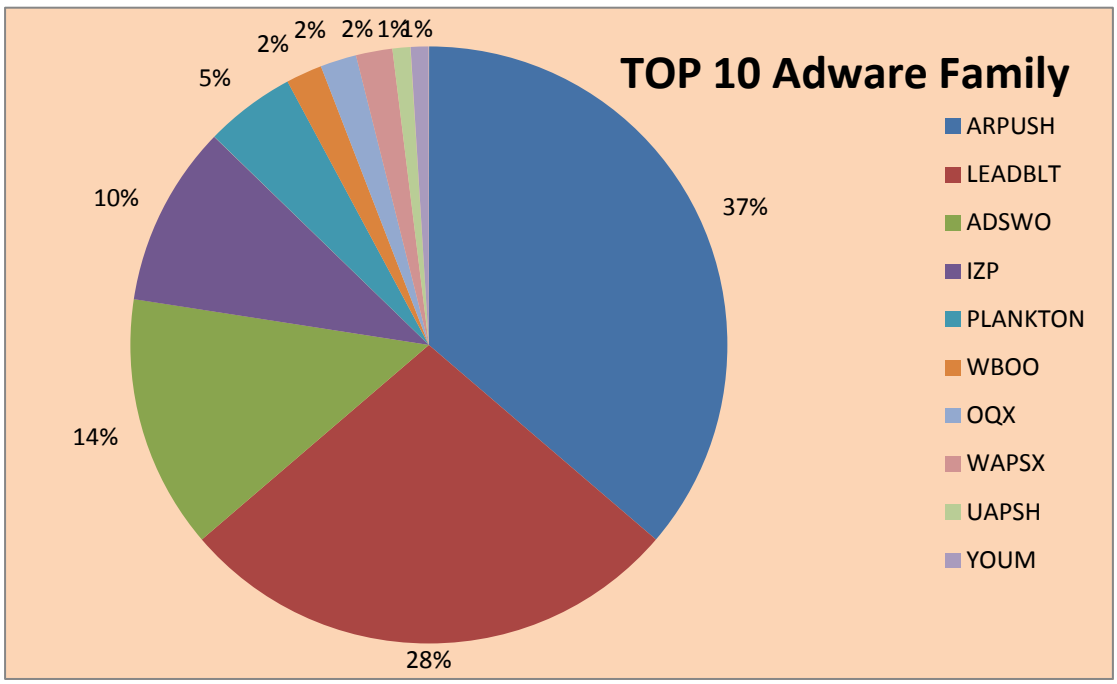
趋势科技移动客户端病毒码中排名前十的病毒家族：



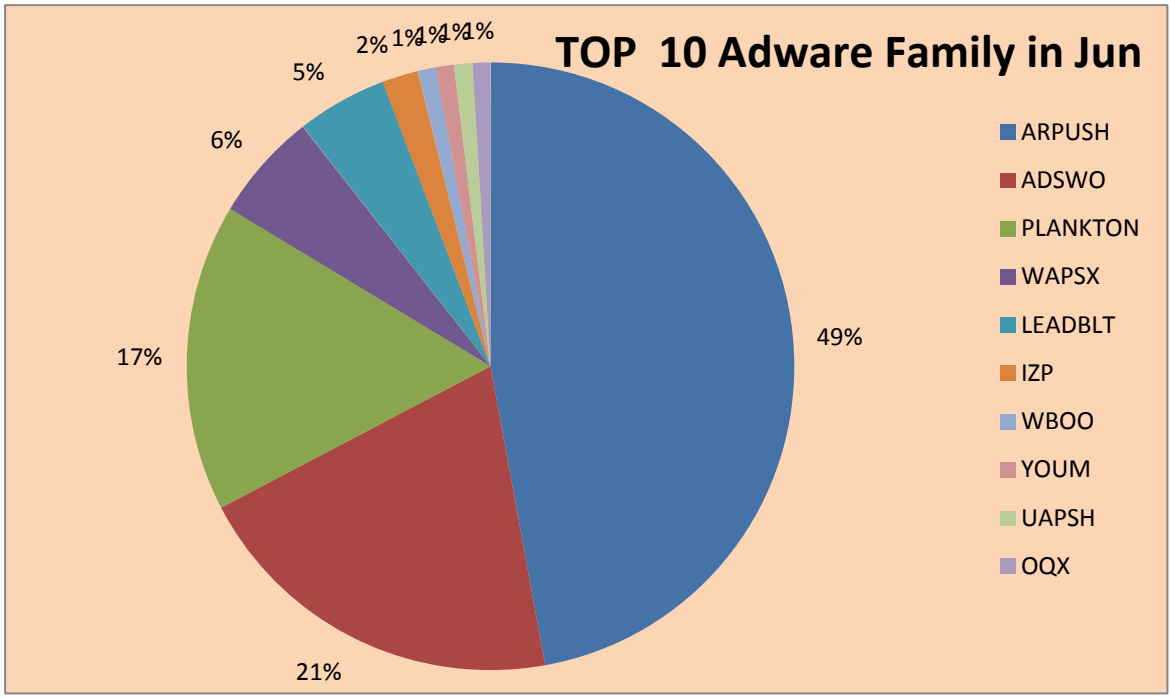
趋势科技移动客户端 6 月新增病毒码中排名前十的病毒家族：



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 6 月新增病毒码中排名前十的广告软件家族：



黑客改进了 OBAD 中的隐藏函数

我们曾接触过攻击 Android 系统漏洞的应用程序，这些程序大多会请求更高的系统权限。最近，一个名字叫 ANDROID_OBAD 的更加高级的 Android 恶意程序进入了人们的视线。它与 ANDROID_JIFAKE 都来源于同一作者，该程序不能被正常卸载，并能够触发更多的恶意代码。

新型高级隐藏功能

这一病毒家族具有完整的隐藏和反编译功能。安装后，它会请求 root 权限并激活管理员功能。因为它能获得 root 权限，该病毒能完全控制设备并能展开进一步的攻击。

如果用户没有按软件要求激活，程序重新启动时会频繁弹出提示框。并且，如果用户点击返回或直接按 home 键，弹框会重新出现。

当用户终于有机会卸载掉它时，由于管理员已经激活，程序会转向隐藏模式继续运行。

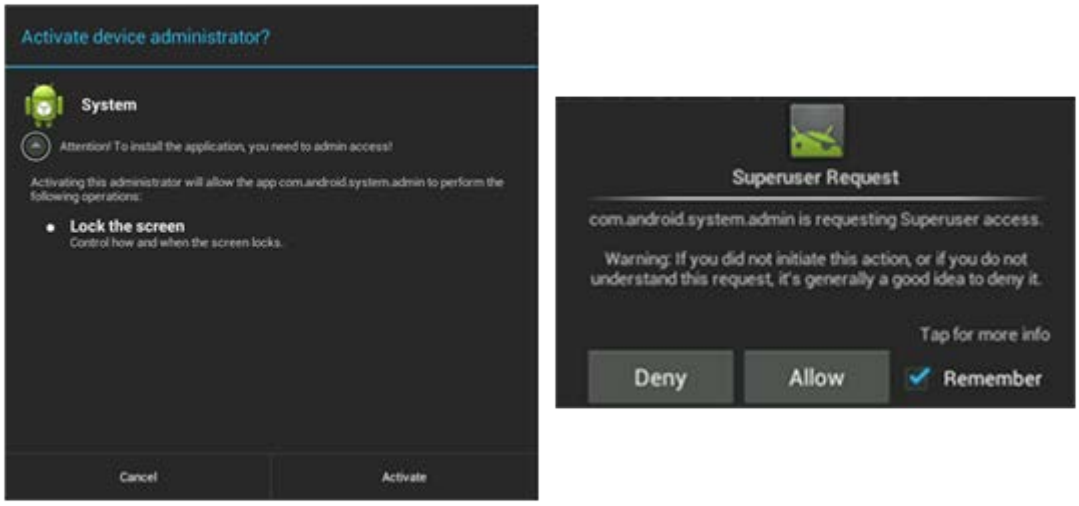


图 1

此时虽然你能将在程序管理中将该恶意软件识别出来，然而你却没办法卸载它，因为它是一个设备管理程序。

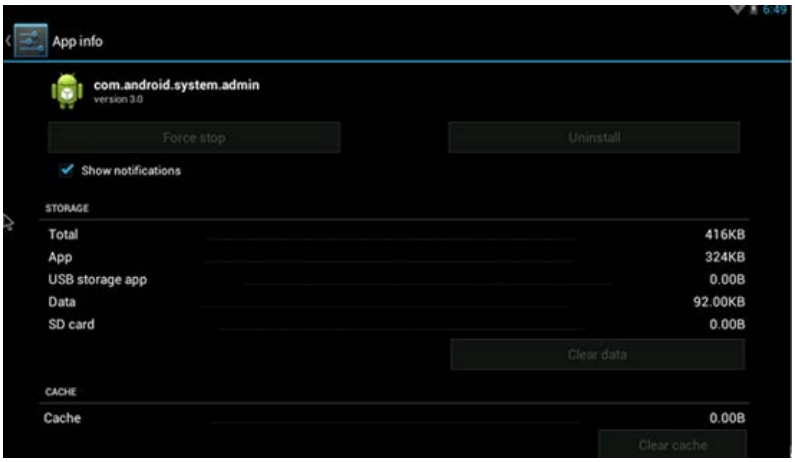


图 2

这种反卸载功能也被应用到了在设备管理列表中进行隐藏。

图3

从安全研究者的角度看，这是 ANDROID_OBAD 对抗传统分析工具的方法。

系统能够正确识别 AndroidManifest.xml,但主流解码工具却不能正确解析。多数 sanbox 在加载 ANDROID_OBAD 时会出错，因为该病毒能够检测 sanbox。

新型代码混淆技术

该程序的 Dalvik code 用了新方法进行混淆。几乎每一个类文件都对应一个不同的加密函数。每一个用到的字符串和函数都必须在程序运行时先被解密。程序的一些部分，如字符串常量，还被加密了多次。目前的反编译工具在跟踪这一执行过程时都会出错。

下面是一个解密函数的代码片段：

```
private static String cOIcOOo(int p6, int p7, int p8)
{
    p7 = (p7 + 72);
    p8 = (p8 + 91);
    v5 = 0;
    v4 = com.android.system.admin.CIlOCClc.ooCclcC;
    v1 = new byte[p7];
    // if(v4 == 0) {
    //     v2 = p7;
    //     v3 = p6;
    while (true)
    {
    // p6 = (p6 + 1);
    // p8 = ((v2 + v3) - 4);
    // }
        v1[v5] = ((byte) p8);
        v5 = (v5 + 1);
        if (v5 < p7) {
            v2 = p8;
            v3 = v4[p6];
            p6 = (p6 + 1);
            p8 = ((v2 + v3) - 4);
        } else {
            return new String(v1);
        }
    }
}
```

图4

当我们对代码进行解密后分析，可以发现该病毒有如下行为：

1. 隐藏 launcher，以后台服务的形式用最高权限运行
2. 自动打开 Wi-Fi 连接并且连接到远程服务器(http://www.{BLOCKED}ofox.com/load.php)
3. 收集用户的通讯录，拨号记录，短信，和已安装程序等信息
4. 下载、安装、卸载其他软件（由于有 root 权限，这些可以静默进行）
5. 通过蓝牙向其他手机分发恶意软件

ANDROIDOS_OBAD vs. ANDROIDOS_JIFAKE

ANDROIDOS_OBAD 和它之前出现的 ANDROIDOS_JIFAKE 有相似之处。后者是一个伪装的 App 安装包，欺骗用户安装并执行后，会注册为服务并连接到远程服务器上等候指令。远程命令包括发送扣费短信和启用反卸载功能。

反卸载（anti-uninstall）功能是利用了 Android 设备管理的漏洞。如果一个程序被安装并被指定为设备管理程序，它就被授予更多的权限并能够限制设备功能，包括强制执行安全策略、锁定设备或销毁用户数据，并且不能被正常卸载。

想要卸载这样的设备管理程序，用户需要关闭设置->安全->设备管理中的选项。利用一个未公布的 Android 漏洞，可以将关闭选项隐藏起来。用户就会被迫将恶意软件注册为设备管理程序并且无法禁用它们。

Trend Micro Mobile Security 已经能够检测这类病毒。

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。