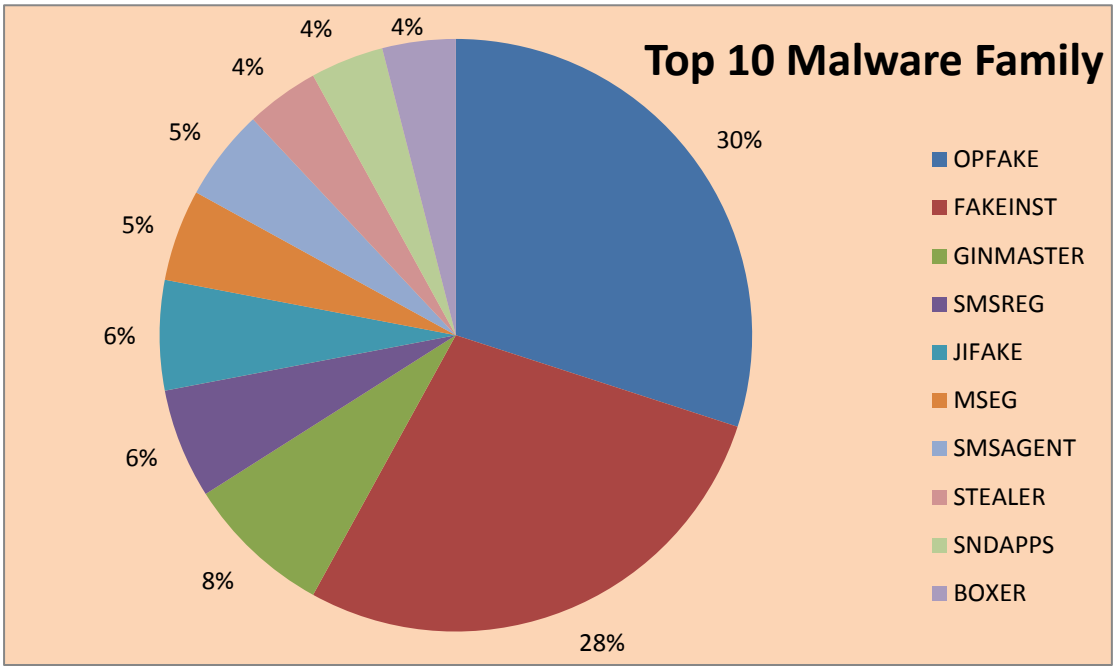
趋势科技移动客户端病毒报告

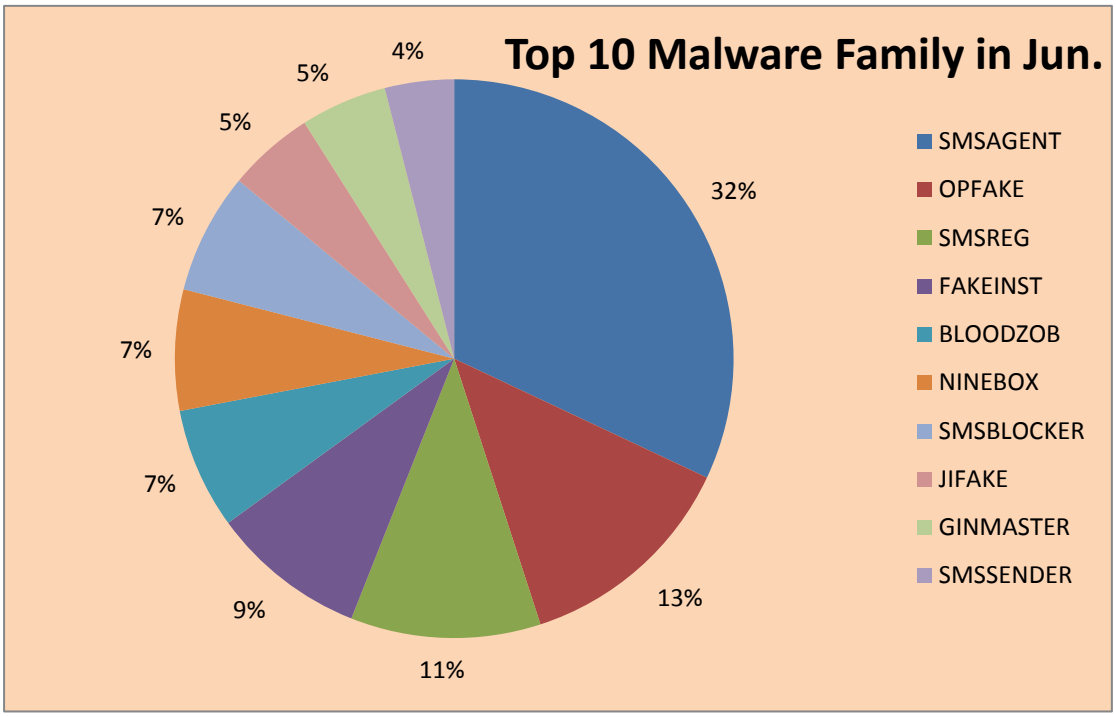
2014年6月移动客户端安全威胁概况

本月，截至 2014.6.30 日，发布中国区移动客户端病毒码 1.705.00，大小 18,272,458 字节。

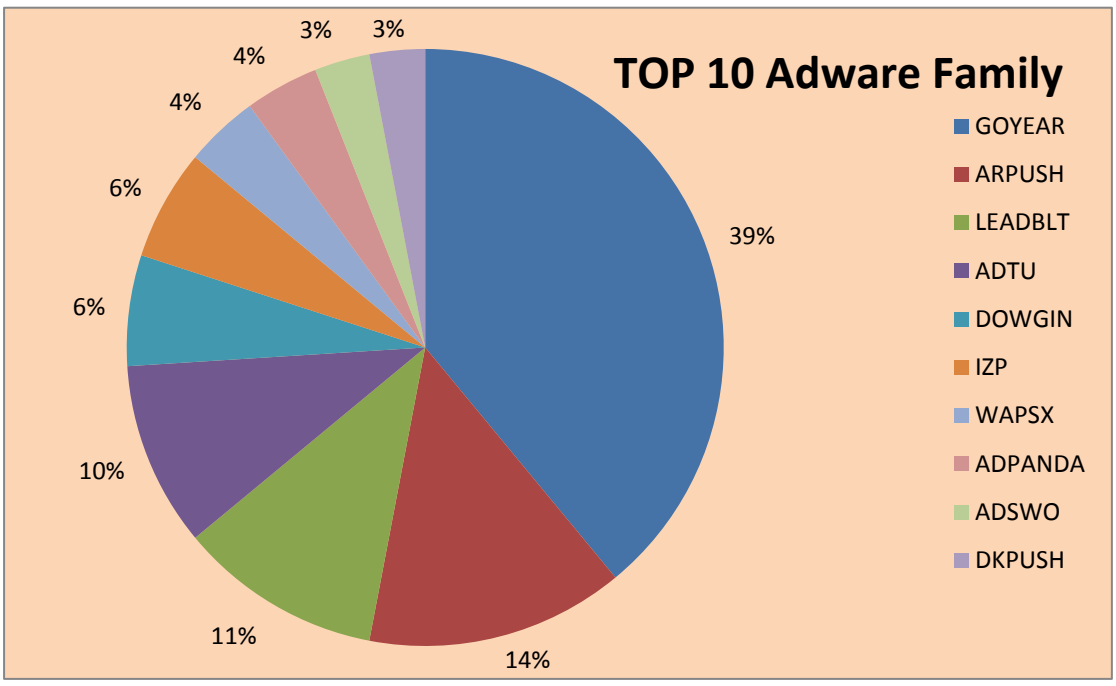
趋势科技移动客户端病毒码中排名前十的病毒家族：



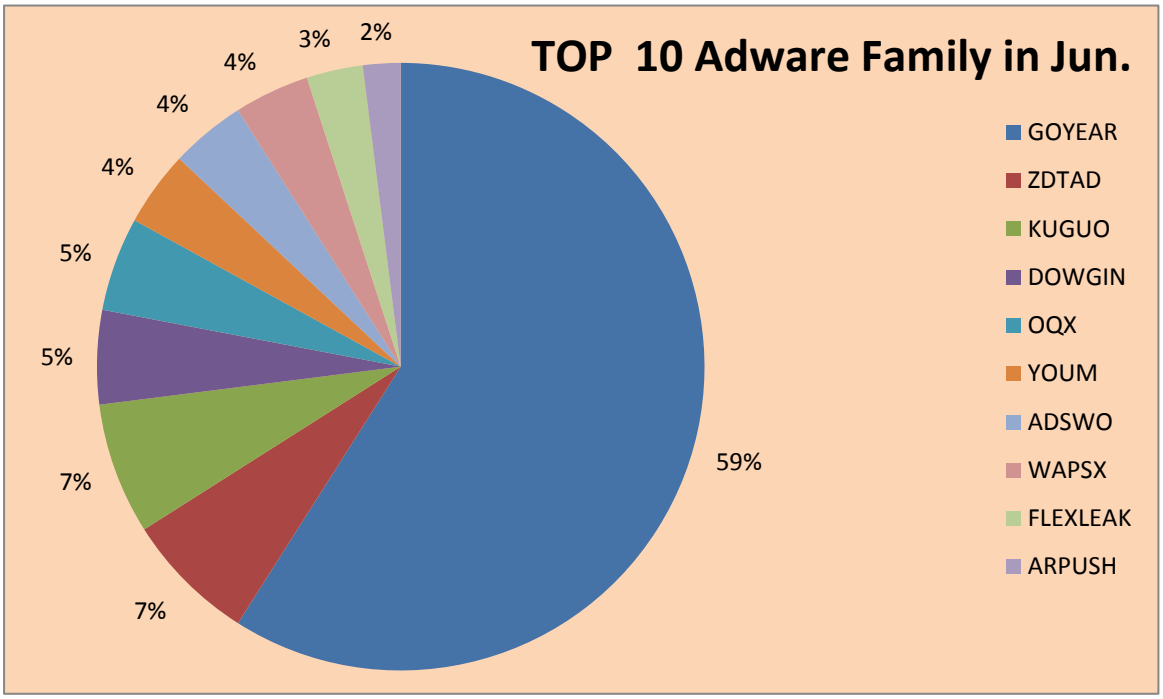
趋势科技移动客户端 6 月新增病毒码中排名前十的病毒家族：



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：



利用 TOR 的 Android 勒索软件

最近对移动平台上的勒索软件的报道又有了新的进展：它们开始利用 TOR 来隐藏与 C&C 服务器的通信。

这部分样本已经可以被检测为 AndroidOS_Locker.HBT。这只病毒会显示一个提示用户手机被锁定的界面，用户需要交 1000 卢布来解锁。提示还称如果不及时付费的话，会清除手机上的所有数据。被感染的 APP 多出现在第三方应用商店，应用名称可见 Sex xonix，Release，Locker， Vplayer，FLVplayer，DayWeekBar， Video Player。各类应用商店都有这些同名的、未被感染的正常应用。

下图是俄文的勒索提示。

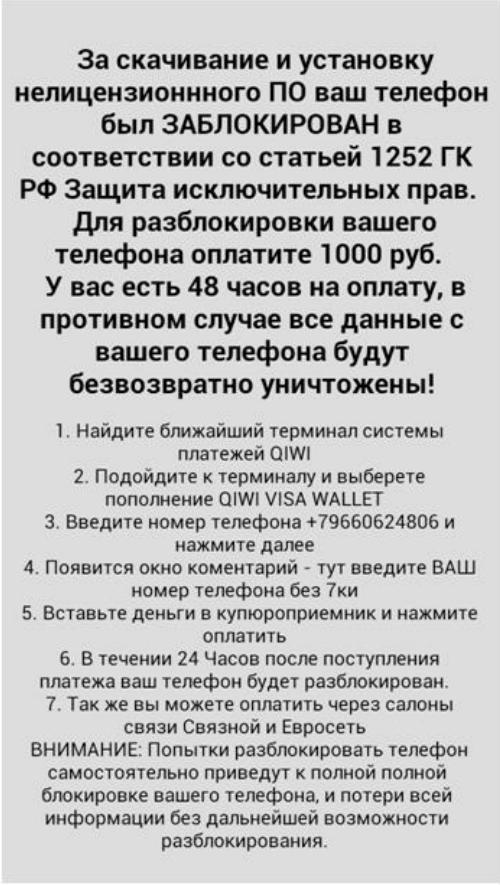


图 1，勒索软件的警告提示

大意是：
因为下载和安装 nelitsenzionnnogo 软件，依据俄罗斯联邦国防专有权法案第 1252 条之规定，您的手机已经被锁定。解锁你的手机需要支付 1000 卢布。
你有 48 小时的时间来完成支付，否则手机上的所有数据将被永久性破坏！

1. 找到最近的终端支付系统 Qiwi

2. 选择 QIWI VISA WALLET 方式
3. 输入电话号码 79660624806，按“下一步”
4. 在出现的窗口中输入您的电话号码
5. 把钱投入到机器并按支付
6. 收到付款后 24 小时内，你的手机将被解锁。
7. 你也可以通过移动商店和 Euronetwork 来支付。

注意：试图自己解锁手机将导致您的手机被彻底锁定，所有的信息都将丢失，并失去解锁的机会。

用户将被要求在 48 小时内通过 Qiwi 向 79660624806 / 79151611239 / 79295382310 或通过 Monexy 向 380982049193 这几个账户支付解锁费用。这个界面会不断弹出，导致用户无法正常使用手机。同时，手机上（内部和外部存储）以下格式的文件将被加密：

- jpeg
- jpg
- png
- bmp
- gif
- pdf
- doc
- docx
- txt
- avi
- mkv
- 3gp
- mp4

上述行为是典型的勒索，而且我们发现它与 C&C 服务器的通信是通过 TOR 的。虽然这不是我们第一次看到使用 TOR 的 Android 恶意软件，但这是首例使用 TOR 的勒索软件。考虑到现在用户存储在移动设备的数据量都比较大，我们预计这只是移动勒索软件不断发展的开始。

如何移除这种勒索软件？

感染了这种勒索软件的用户，可以通过 Android 调试连接手动删除它。ADB（Android Debug Bridge）是 Android SDK 的一部分，Android SDK 可以从 Android 的网站上下载到。
手动清除步骤如下：

1. 在 PC 上安装 Android SDK，包括 ADB 组件。
2. 将手机通过 USB 连接到 PC
3. 运行命令行并执行以下命令
   adb uninstall “org.simplelocker”

Android 版本低于 4.2.2 的用户都可以通过这几个步骤清除该病毒。4.2.2 或其以上版本的用

户会遇到些问题：设备会弹出对话框提示是否同意打开 USB 调试。但是勒索软件本身会一直占用屏幕窗口，导致用户很难使用 ADB。

请注意，在所有的情况下，用户都需要在被感染前已经打开了 USB 调试功能，打开的方法因设备的不同而不同。需要注意的是，打开 USB 调试功能本身是一种安全风险，因为这意味着获得物理访问权限的攻击者可以很容易地获得手机上的文件而不必输入 Android 的锁屏密码。

上面的步骤可以清除勒索软件，但不能恢复被锁定的文件。同 PC 上的勒索软件一样，恢复被锁定的文件是比较困难的。我们建议用户从备份中恢复文件。

相关样本的 SHA1 值如下：

- 3313e82160fe574b4d4d83ec157d96980c0e88c4
- 4824c957b7804d27c56002c93496182c8ec2840d
- 5a102f0e6238418d8c73173752e20a5914ec4958
- 725e9553040845d4b7ad2b0fd806597666d61605
- 808df267f38e095492ebd8aeb4b56671061b2f72
- 979020806f6fcb8a46a03bb4a4dcefcf26fa6e4c
- b4bc70e7f046894ef12b5836f70b0318ca7ad06f
- b5aab4bdb6bbb5914b1860c47080ccb558f07e5b
- c85e49e0e99c2c0e531f723bf14d84339919985d
- e6ee6dac2e6bd97c93a6a746442bfc0930e637af

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。