# 简介

1. 使用Python语言编写的工具。
2. 静态检测APP的Dalvik字节码（.dex文件，smali语法）。
3. 主要检测APP中潜在的恶意行为，

* Telephony identifiers exfiltration：

IMEI：国际移动设备身份码。每台手机的IMEI都是唯一的。

IMSI：国际移动用户识别码。储存在SIM卡中，可用于区别移动用户的有效信息。

MCC：移动信号国家码。唯一识别移动用户所属的国家（IMSI中包括此项）。

MNC：移动网络号码。识别移动客户所属的移动网络（IMSI中包括此项）。

LAC：位置区码。标识不同的位置区。

CID：手机的平台版本。紧跟IMEI存储在手机的OTP（One Time Programmable）芯片中。

操作者姓名

……

* Device Settings exfiltration：软件版本、使用数据、系统设置、日志……
* Geolocation information leakage：GPS/WIFI定位……
* Connection interfaces information exfiltration：WIFI认证信息、蓝牙MAC地址……
* Telephony services abuse：发送短信、拨打号码……
* Audio/video flow interception：通话记录（语音）、视频刻录……
* Remote connection establishment：蓝牙匹配、APN设置编辑……
* PIM data leakage：联系人、日历、短信、邮件……
* External memory operations：访问SD卡……
* PIM data modification：添加/删除联系人、日历日程……
* Arbitrary code execution：本地代码（使用JNI，Java本地接口）、UNIX命令、权限增加……
* Denial of Service：关闭事件通知、文件删除、杀死进程、隐藏虚拟键盘、关闭/重启终端……

1. 会自动生成txt或html格式的报告，且分析可分为三个等级：初级（适用初学者），高级以及专家级。在结果部分会详细说明
2. 然而只停留在了5年前。。。

# 来源

https://github.com/maaaaz/androwarn/

# 使用步骤&结果

依赖

* Python >= 2.6
* Jinja2 : http://pypi.python.org/pypi/Jinja2/
* Chilkat : https://www.chilkatsoft.com/python.asp

安装 （<https://github.com/maaaaz/androwarn/wiki/Installation>）

直接下载Androwarn源码

$ git clone https://github.com/maaaaz/androwarn.git

使用

安装成功后，可以查看所有可选命令

$ python androwarn.py -h

Usage: androwarn.py [options]

Options:

-h, --help show this help message and exit

-i INPUT, --input=INPUT

APK file to analyze

-v VERBOSE, --verbose=VERBOSE

Verbosity level { 1-3 } (ESSENTIAL, ADVANCED, EXPERT)

-r REPORT, --report=REPORT

Report type { txt, html }

-d, --display-report Display analysis results to stdout

-L LOG\_LEVEL, --log-level=LOG\_LEVEL

Log level { DEBUG, INFO, WARN, ERROR, CRITICAL }

-n, --no-connection Disable lookups on Google Play

使用分析时一条命令如下：

$ python androwarn.py -i SampleApplication/bin/SampleApplication.apk -v 3

-r html -n

[+] Analysis successfully completed and HTML file report available './Report/com.androwarn.sampleapplication.html'

之后会自动生成报告，保存在Report目录下。

结果

1. 初级

初级的分析报告包括应用程序信息、分析结果、APK文件以及安卓manifest.xml配置文件四个模块。

应用程序信息包括：应用程序名称、版本、package名称以及应用程序的描述四个部分，其中应用程序名称和描述无法显示（可能是中文问题？需要通过源码发现）。

分析结果包括：检测出的简介中的所有可能的恶意行为。

APK文件包括：输入的apk文件名、文件的fingerprint。

Manifest.xml文件包括：APP所申请的权限列表。

1. 高级

高级建立于初级的基础上，在APK文件部分增加了2个内容：文件列表（并不是所有文件）、认证信息。

1. 专家级

专家级建立于高级的基础上，首先在manifest.xml文件部分增加了以下几个内容：应用程序的Main Activity（APP入口activity）、应用程序暴露出来的所有activity、Receiver、Provider等。

其次新增了第5个模块—APIS的使用情况，主要包括：类列表、内部的类列表、外部的类列表、内部的包列表、外部的包列表等。

注：同目录下附有样板APP以及对应报告。

# 注意事项&问题

1. 待分析的APK文件名称不能为中文，否则会报错（编码问题），可以生成txt格式的报告，但无法生成html格式的报告。
2. 对同一个APK进行不同级别的分析时，分析所产生的报告会覆盖，均以APK的主包名命名。
3. 所有分析结果只客观列出名称或行为，不进行任何可能产生危害的分析。
4. 中文的无法显示或编码问题？