APK分析工具

1. 安装到手机之前，分析下这个APK有没有恶意行为
2. 反汇编这个文件

**一、腾讯哈勃分析系统、免费**

**1. 支持的文件格式：**

**APK**、EXE、BAT、JS、VBS、PDF、HTML + 各种压缩包 + office文档

1. **支持的文件大小：**

普通用户**（QQ用户）**30MB，高级用户**（申请即可）**100MB

1. **优势：**

1）极速响应：**海量数据**解决方案，实时输出文件分析结论

2）精准鉴定：独有集群智能系统，**深度挖掘**病毒恶意行为

3）用户上传分析后，哈勃会自动收集样本的**静态属性**和运行时产生的**动态行为**

4）版本众多：APP + PC端 + 在线的 [腾讯哈勃分析系统](https://habo.qq.com/)

**4. 分析报告：**

[RespondCode.apk实例](https://habo.qq.com/file/showdetail?pk=ADEGY11oB2AIPls%2F) 包含以下内容

基本信息：文件名称、大小、包名、最低运行环境等

**危险函数：具有潜在风险**的函数，如“ContentResolver -- 读取联系人、短信等数据库”

其他行为：？？？

文件列表：获得DEX（源码打包后的可执行文件）+ 各种XML（配置、布局文件）

Acticities：活动名 + 类型

**漏洞风险列表：**具有的**潜在风险**，如“允许应用被调试”

1. **爱加密APP漏洞分析平台、免费**

**1. 优势：**

1）快速分析：一键上传即可检测APP，快速分析找出漏洞

2）漏洞检测：多达100 + 项深度检测项目

3）专业报告：人工 + 自动化渗透分析

4）修复意见：给出针对性安全修复建议

**2. 检测方式：**

1）静态检测：利用**apktool、dex2jar、jd-gui、smail2dex**等静态工具对应用进行**反编译**

扫描分析，并将搜索到的隐患代码进行摘录存入到监测平台后台

1. 动态监测：通过**沙箱模型、虚拟机**等方对应用的安装、运行过程进行行为的**检测**

**分析**、从外界**观察应用程序的执行过程**，进而激励应用程序所表现出来的恶意行为

3）人工渗透分析：由资深测试人员进行检测分析，通过人工安装运行及试用来圈定检测重点，在基础检测和深度检测的同时，兼顾侧重点检测。