顶象Android加固保护

一、产品简介

顶象Android应用加固保护是一套纵深防御体系，分别从代码安全、资源文件安全、数据安全和运行时环境安全维度提供安全保护,同时针对每个维度又进行了不同层次的划分，加固策略可依据实际场景进行定制化调配，安全和性能达到完美平衡。

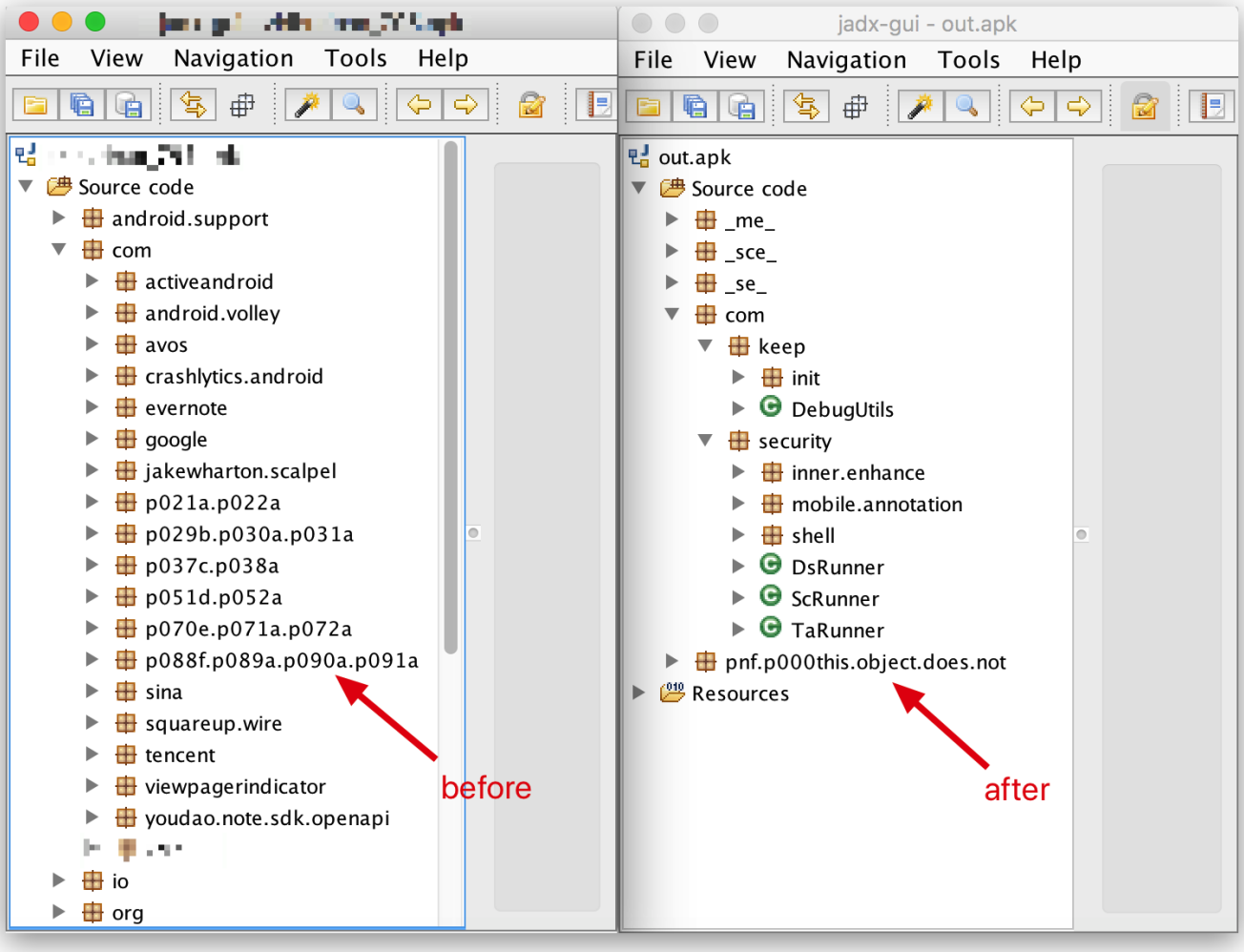
二、产品功能

目前Android加固主要包含dex文件整体保护、java代码虚拟化保护、so文件保护、html/js保护、游戏相关脚本保护、本地数据保护、运行时保护这几大类功能。

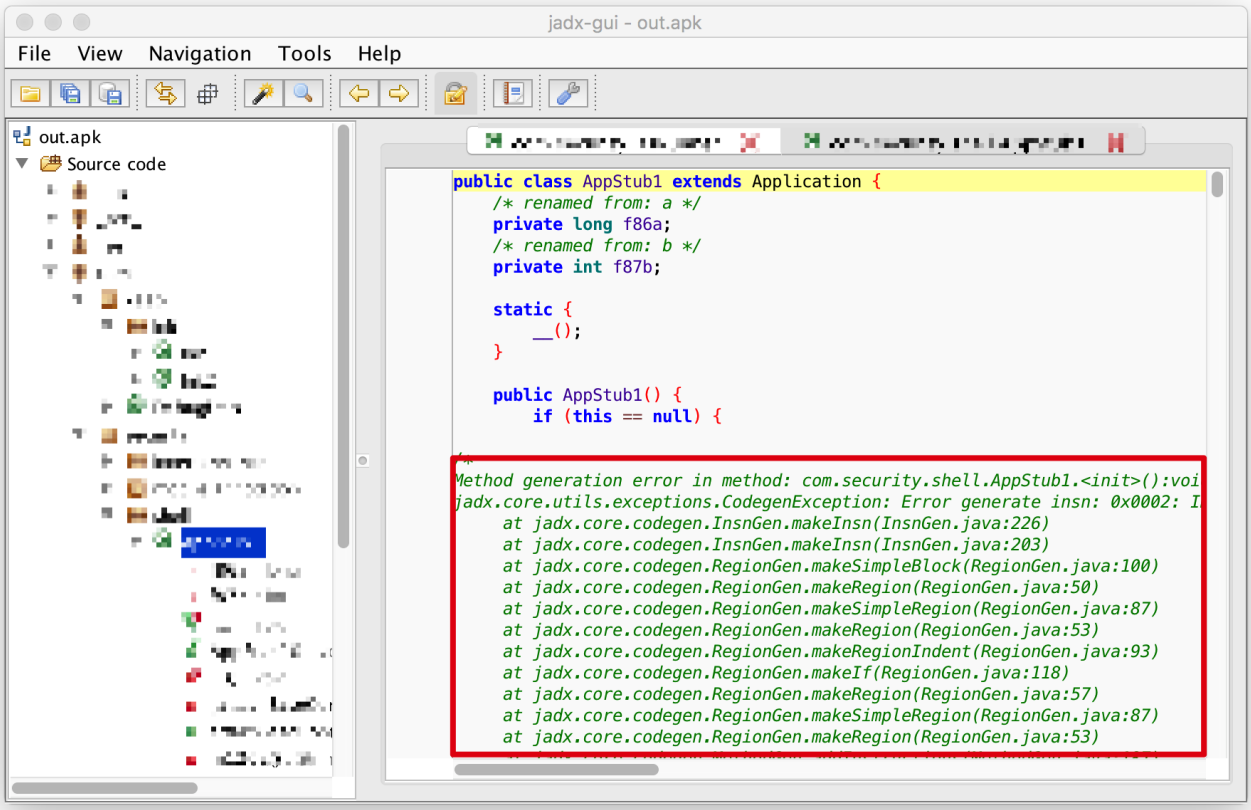
2.1 dex文件整体保护

通过将原dex文件加密隐藏，并使用防JAVA代码反编译、JAVA字符常量加密等技术对DEX文件进行全面性保护。

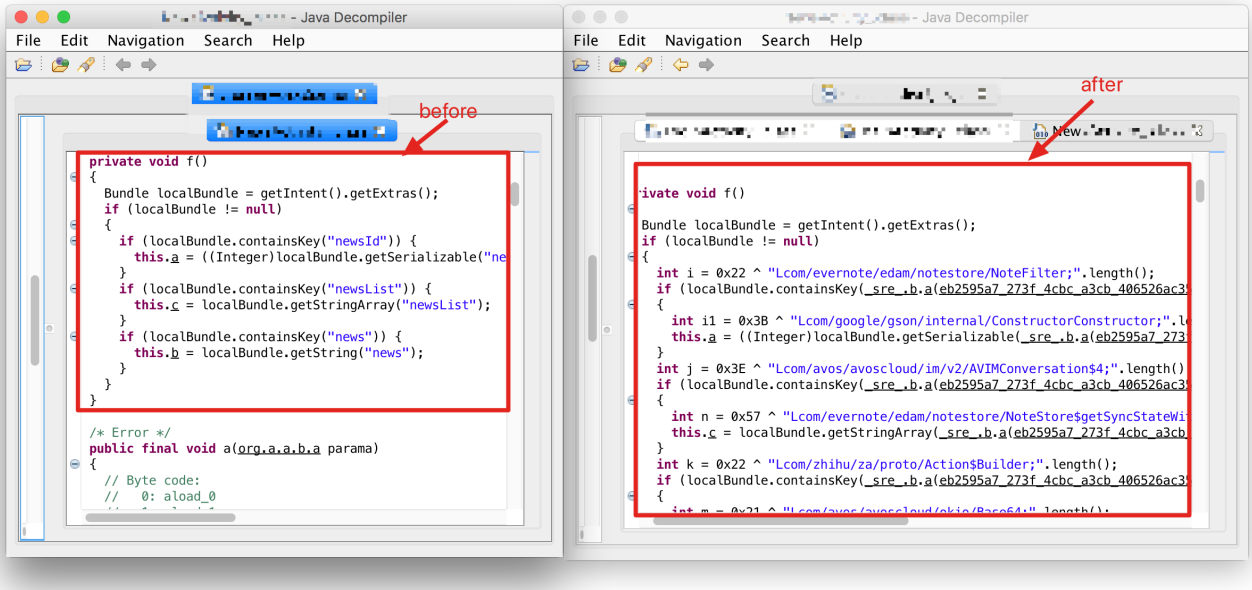
使用dex文件整体保护后，原dex文件代码被隐藏，使用逆向工具打开也无法找到原dex内容:



防java反编译，可以使反编译工具无法直接把代码反编译为java，提高逆向分析难度，包括但不限于（JEB、jd-gui、jadx）：



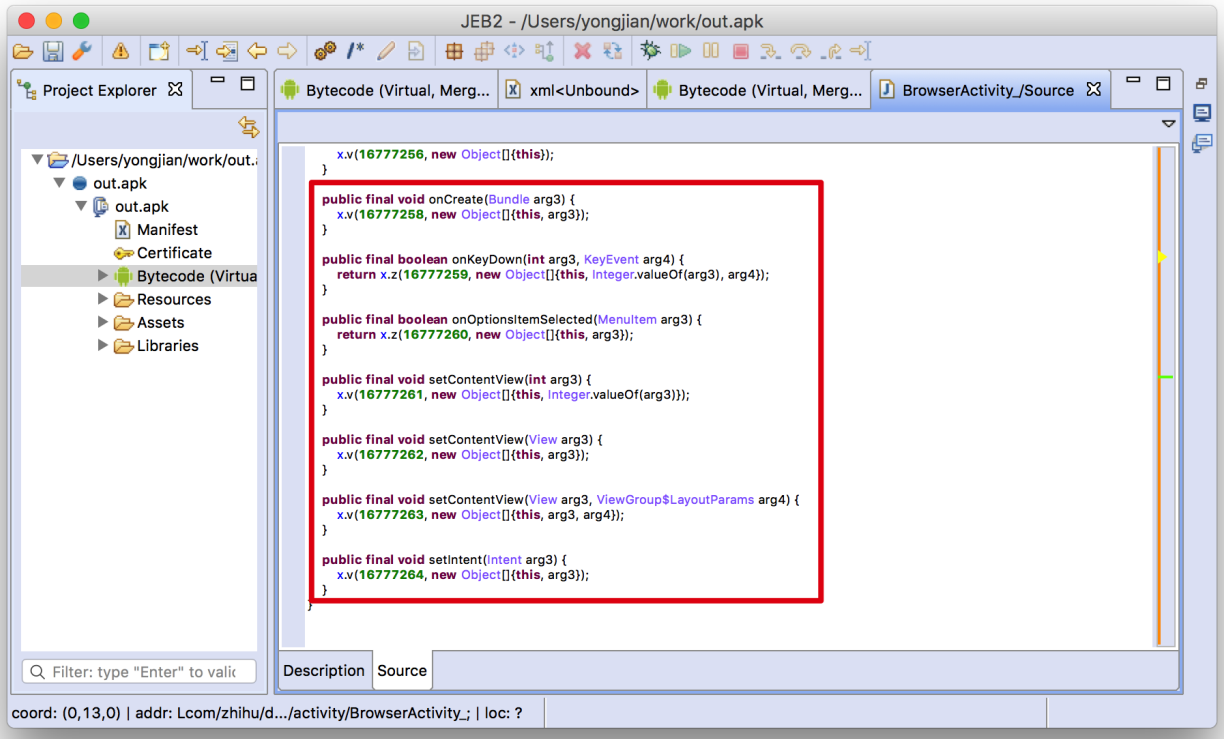
JAVA常量字符串加密，会隐藏代码中明文的常量字符串，增加逆向难度:



2.2 java代码虚拟化保护

通过将原java代码指令转换为DX-VM虚拟机指令，运行在DX虚拟机之上，无法被反编译回可读的源代码，任何工具均无法直接反编译虚拟机指令。

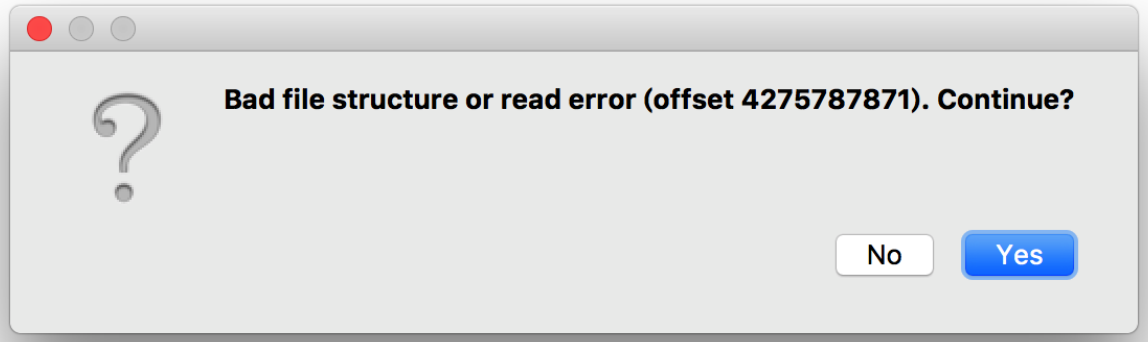
采用java代码虚拟化保护后，对源码反编译将无法看到任何与原代码相似的内容，函数体中只有对虚拟机子系统的调用:



2.3 so文件保护

通过对SO文件进行反编译、防篡改、防盗用、虚机保护、代码压缩等技术对SO文件进行全面性保护。

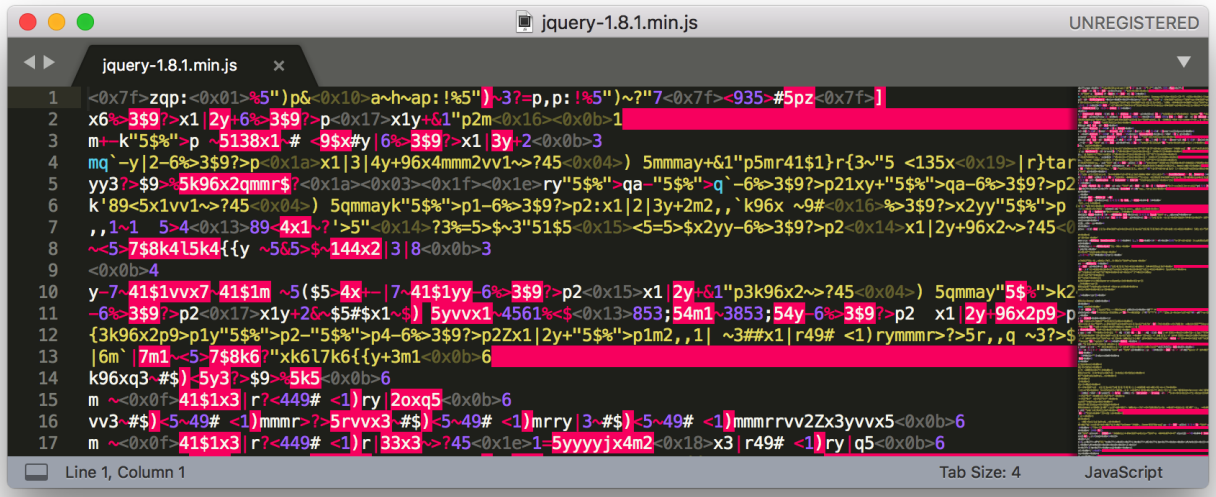
采用so文件保护后，主流反编译器都无法对被保护过的so进行正常分析:



2.4 html/js保护

通过对html/js文件进行防篡改，加密等技术对html/js进行全面保护。

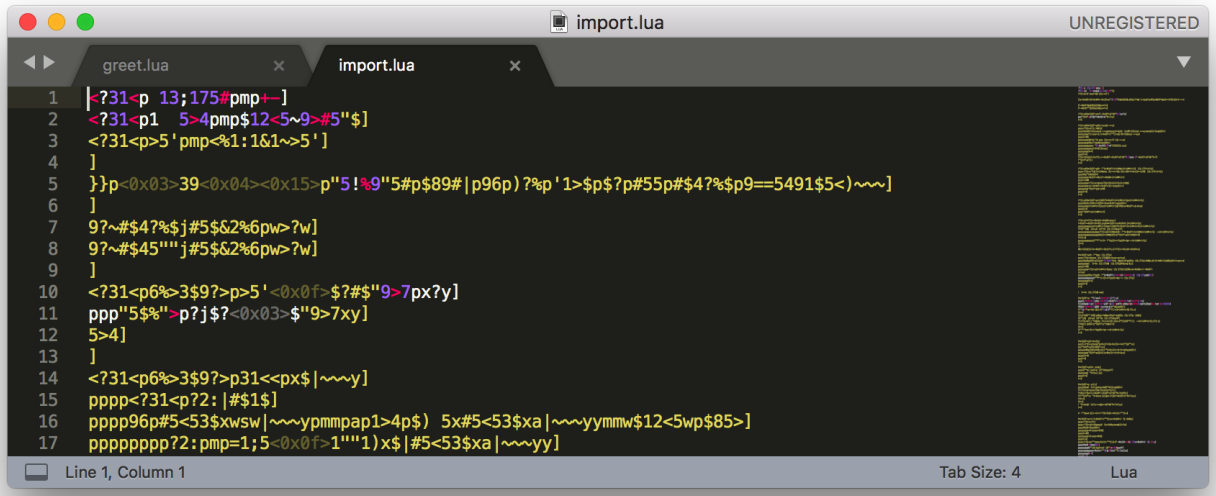
采用html/js保护后，无法直接获得明文的html/js文件:



2.5 游戏相关保护

通过对主流游戏引擎所用到的脚本/dll文件进行防篡改，加密等技术，进行全面保护。

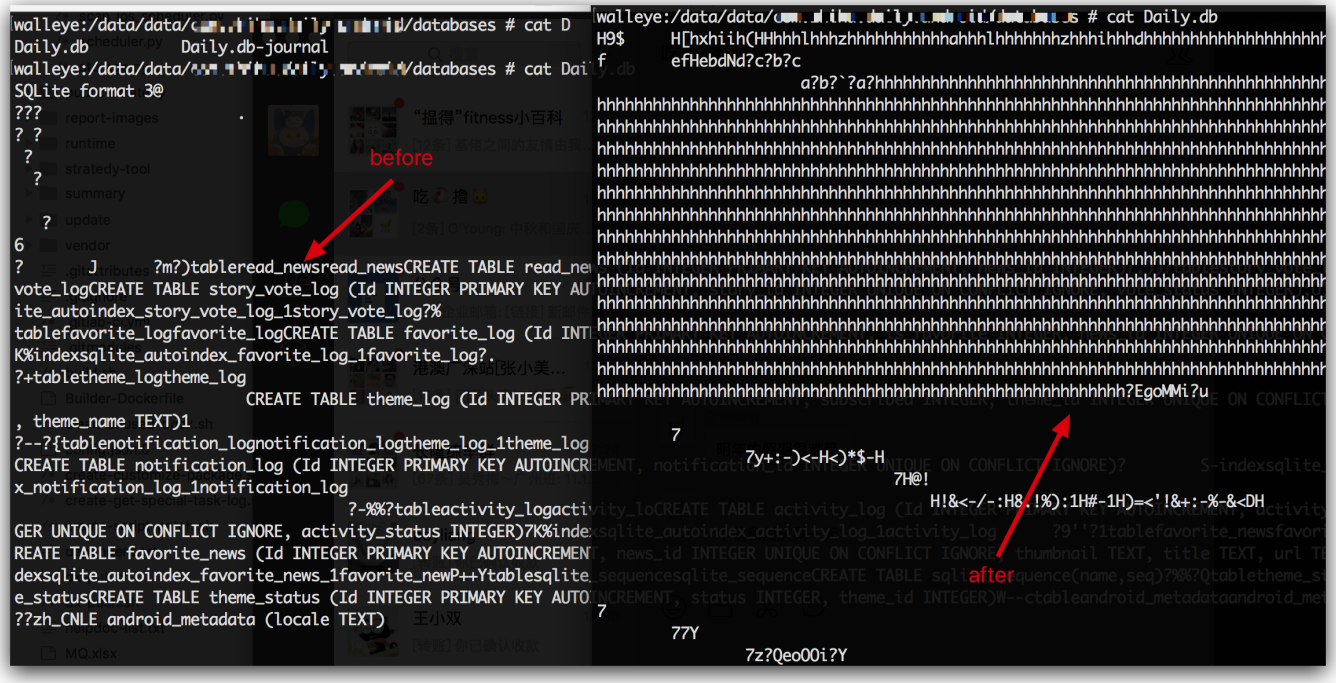
采用游戏相关保护后，无法直接获得明文脚本或明文的dll文件：

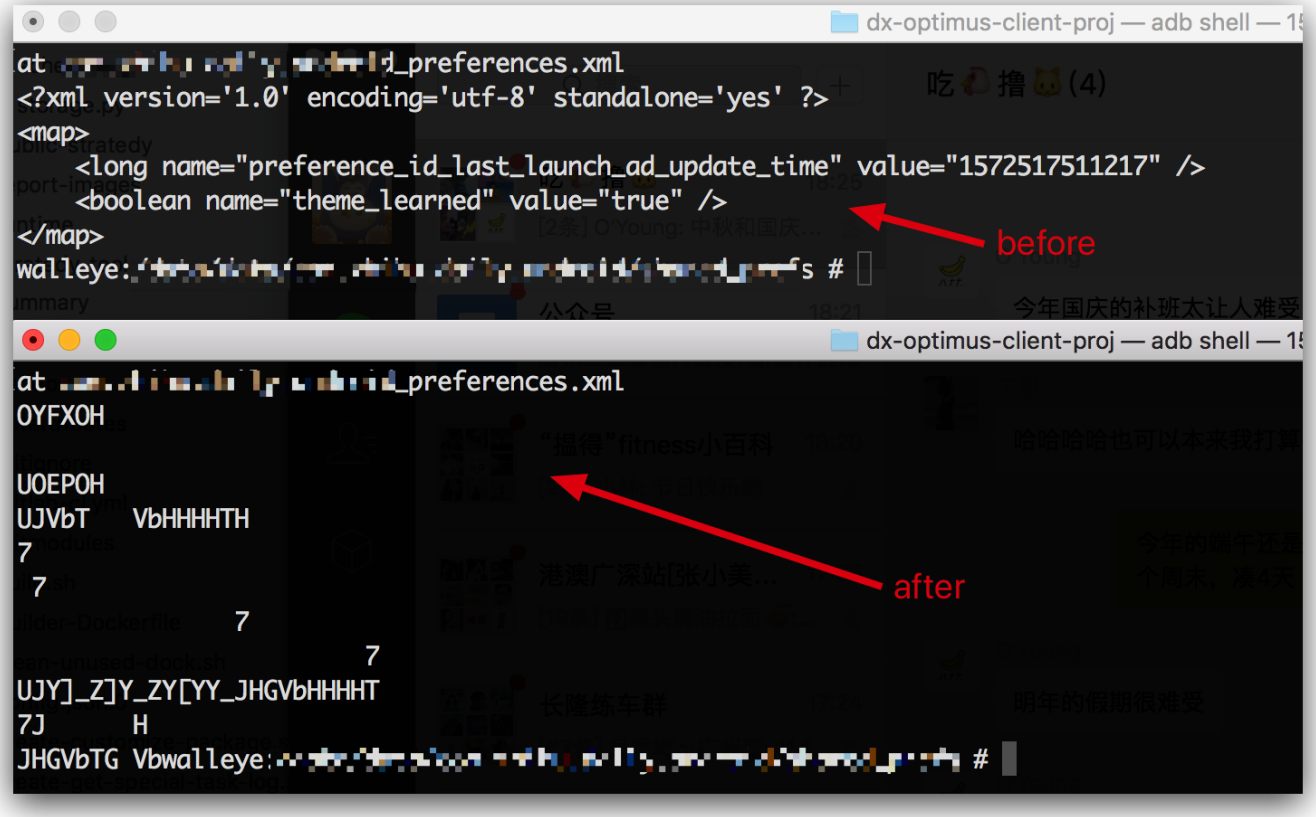


2.6 本地数据保护

通过对对本地数据文件进行防篡改，加密等技术进行全面保护。

采用本地数据保护后，无法直接明文查看db文件或sp文件:





2.7 运行时保护

通过运行时保护，可以有效防止被调试，内存dump，代码注入等行为。

三、适用范围

- **Android版本**：4.2 ~ 10
- **支持语言**：java
- **支持格式**：

    - App类型，支持`.apk`格式
    - sdk类型，支持`.aar`格式和`.jar`格式
- **其他要求**：
    - apk文件包必须包含签名
    - apk文件必须未经过加固
    - 压缩后体积在 `300M` 以内

四、使用指南

4.1 待加固文件准备

1. 准备好已经进行签名的待加固apk文件。

2. 准备好与待加固apk文件相同的签名key文件。

4.2 上传加固文件进行加固

4.2.1 基础版

1. 登录顶象控制台，并进入Android加固保护页面

2. 选择基础加固版本，并点击立即使用，弹出创建任务窗口，并上传待加固的apk

3. 点击确定，创建加固任务

4.2.2 标准版

1. 登录顶象控制台，并进入Android加固保护页面

2. 选择标准加固版本，并点击立即使用，弹出创建任务窗口，并上传待加固的apk

3. 根据需要自行选择加固策略

- **标准**：对常见的android应用进行保护，功能包括，dex文件加密隐藏，dexvmp，反篡改，反调试，防内存dump，防注入，app包签名校验。
- **html/js**：对html，js等文件进行加密，另外功能还包括反篡改，反调试，app包签名校验，防内存dump，防注入。
- **等保**：对等保类需求进行定制，以满足通过等保需求。
- **游戏**：对u3d，cocos2dx等游戏引擎脚本文件进行加密，另外还包括反篡改，反调试，防内存dump，防注入，app包签名校验。

4. 点击确定，创建加固任务

4.2.3 旗舰版

1. 登录顶象控制台，并进入Android加固保护页面

2. 联系客服人员，说明旗舰版的具体需求，并等待客服人员配置策略完成

3. 选择旗舰加固版本，并点击立即使用，弹出创建任务窗口，并上传待加固的apk

4. 点击确定，创建加固任务

4.3 下载加固包

1. 任务提交成功后，会进入加固等待队列，后台加固处理完成后可至任务列表进行下载。

2. 下载后得到未签名的加固包，格式与源包格式一致，为.apk。

3. 对加固的apk进行重签名即可安装使用，需要保证与加固前的签名一致。

4. 若加固失败，可点击任务列表右侧"查看失败原因"，查看具体原因。

五、Android签名工具

5.1.1 功能简介

本工具用于对android加固后的apk进行重新签名。

5.1.2 使用说明

1. 解压顶象签名工具.zip，并运行（windows运行run-win.bat， mac/linux运行run-mac-linux.sh）。

2. 选择签名的key文件，并输入key密码。

3. 选择alias名，并输入alias密码。

4. 点击"签名"按钮，等待即可签名完成。

六、常见问题

6.1 关于apk签名

Q: apk签名是什么?

A: 签名就是用于识别app开发者，并保证apk完整性的一个机制，谷歌要求每一个app都需要有签名。

Q: 为什么上传的apk需要有签名?

A: 加固有防二次打包的功能，需要提前apk原本的签名，供加固后验证签名正确性用。

Q: 在 androidstudio 中打出的debug版本包，可以加固吗?

A: 不建议用debug版本包加固，因为debug版本的包使用的是androidstudio的debug签名，可能导致加固后无法重签名，或者签错名的情况。导致无法正常运行。

6.2 关于加固后重签名

Q: 上传之前apk已经签过名了，为什么加固后又要重新签一次?

A: 加固之后会破坏apk原有的签名，所以需要重新签名，否则无法安装。

Q: 为什么重签名需要和加固前保持一致?

A: 如果不保持一致，则会触发加固的防二次打包功能，无法正常运行。

6.3 如何重新签名

Q: 该如何重新签名?

A: 根据以下步骤操作:

1.到 此链接 下载DX签名工具。

2.按照5.1.2步骤操作。

6.4 热更框架支持

Q: 加固目前支持哪些热更框架?

A: 目前加固支持阿里 sophix，腾讯 tinker两大主流热更框架。

Q: 使用热更框架的app，加固时需要什么特别操作吗?

A:

1. 如果使用tinker，请加固后在tinker中开启"加固模式"，详细见此链接,
2. 如果是sophix，则不需要特别操作。

6.5 加固对不同语言的支持:

Q: 加固支持 Kotlin 语言吗?

A: 支持

6.6 加固三个不同版本功能相关:

Q: 关于基础版功能?

A: 基础版包含最低程度的app保护，具体可以登陆后，参考此链接，可免费试用三次，不支持人工售后解决问题。

Q: 标准版有什么通用功能?

A: 标准版包含dex整体保护、java代码虚拟化、反dump、反调试、反重打包、代码防篡改，参考此链接，不支持试用，支持人工售后解决问题。

Q: 有什么特殊需求标准版可以满足?

A: 以下情况可以使用标准版解决:

1. 有 html/js 代码保护的app（适合Phonegap、RN、Cordova之类的跨平台框架）。
2. 有游戏保护需求的app（适合Xamarin、Flutter、u3d-mono、cocos2dx等框架、c#、lua）。
3. 有等保需求的app。

Q: 等保能不能保过?

A: 用户选择标准版，直接上传app加固后，拿到等保平台测试即可，如果不过再联系售后即可。

Q: 旗舰版可以满足什么需求?

A: 以下情况可以使用旗舰版:

1. 有so保护需求的app。
2. 有资源加密需求的（非html/js代码)。
3. 有上谷歌商店需求的。
4. 有反注入，反模拟器，反多开，反root需求的app。

Q: 如何给出旗舰版的java代码虚拟化保护范围?

A: 把需要特殊保护的重要类以列表形式列出完整类名，例如：（com.android.app.Activity）。

Q: 如何给出旗舰版资源加密保护范围?

A: 把需要保护的资源文件在apk中的路径以列表形式给出，例如：（assets/abc.png）。

Q: 如何给出旗舰版so保护范围?

A: 按照以下规则给出保护列表:

1. 如果需要保护的so在apk中lib文件夹下的话，给出完整文件名即可，如：libabcdef.so。
2. 如果需要保护的so在assets文件夹下，则给出完整路径，如：
   `assets/so/x86/libabcdef.so`,`assets/so/armeabi-v7a/libabcdef.so`

6.7 加固不能满足的需求:

Q: 加固支持 敏感数据防爬虫，签名算法升级，秘钥升级，敏感数据加密保护需求吗?

A: 不支持

Q: 加固能支持so vmp保护吗?

A: 不支持

Q: 加固如何防止抓包?

A: 加固不支持防抓包

Q: 游戏进行加固，可以防第三方外挂吗?

A: 加固不支持防外挂

Q: Android加固有aab保护方案么?

A: 没有

Q: 线上saas是否有sdk加固?

A: 没有

Q: android加固是否提供纯so保护功能?

A: 如果有apk的话，旗舰版可以提供次功能，把需要保护的so范围给出即可，如果没有apk则不支持。同样也不支持linux的so保护。

Q: 问加固能否设置在一定时间后自动crash

A: 不能

Q: 破解别人的/xposed插件能否正常加固

A: 破解别人的so不推荐加固，有可能会引起不知名问题。xposed插件不能被加固。

Q: android加固是否支持java代码.class文件?

A: 不支持

Q: android加固否支持.a加固

A: 不支持

Q: 加固dex039失败如何处理?

A: 目前dex039仅支持android9.0的机器，通用性太差，所以加固目前不支持。如果改app需要加固，请在androidstudio项目中，把minsdk版本调低。

6.8 android加固其他常见问题:

Q: 我的app加固后被杀毒软件报毒，该如何处理?

A: 请先确认未加固的app是否也会被报毒，如果不会，则反馈售后让技术人员处理。

Q: 我的app加固后运行会崩溃，如何处理?

A: 请先确保app未加固前所有功能均正常，如果崩溃现象仅在加固后出现，则反馈售后让技术人员处理。

Q: 我如何验证我的app被加固，并且功能正常?

A: 加固报告中，包含所有开启的保护功能描述，和检测方法。可以按照报告指示的步骤来操作验证功能是否生效。

Q: 加固后是否会影响我的app接受或发送广播?

A: 加固前后app所有功能不受影响，使用方式也不会改变。

Q: 加固后调用栈是否发生变化，定位是否方便?

A: 加固不会改变app调用栈。

Q: 加固后上传的到自己开发的市场，显示解析错误，该如何处理?

A: 加固后的app，只要重新签名成功，上传市面上任何一个应用市场都不会出错的，所以这种情况应该查看下自己开发的市场或者工具是否有bug。

Q: 我们的apk在模拟器中运行，被另一个apk记录下了所有操作，该如何处理?

A: 这种情况一般是被代码注入了，可以使用旗舰版，开启反注入功能和反模拟器功能。