# 介绍

Dexsim 是赖老师写的一款android字符串解密工具，其原理使用动态加载执行需要解密的方法，然后将解密结果替换对应的smali代码，本文主要介绍该工具的使用，如果对其实现感兴趣可以看对应的代码。

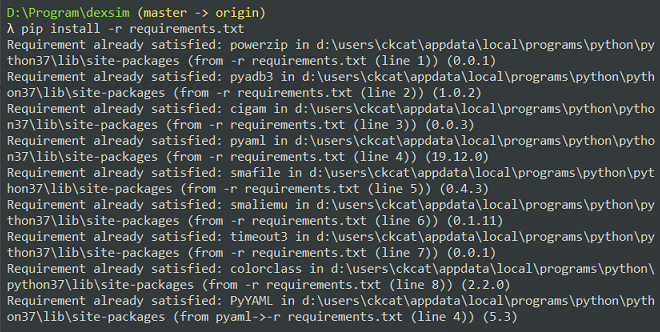
# 使用

该工具需要python3环境，其中dss和dexsim中部分源码已经被我改动过，主要改动为将

/data/local/dss和/data/local/dss\_data 改为对应的 /sdcard /dss 和 /sdcard/dss\_data，这样不需要root权限应该也可以了，高版本的android系统（目前测试支持android 8.1真机）应该也兼容了，第一次运行是给一个权限就可以了。

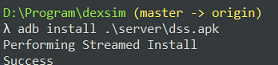
## 安装依赖库

pip install -r requirements.txt



## 安装dss.apk

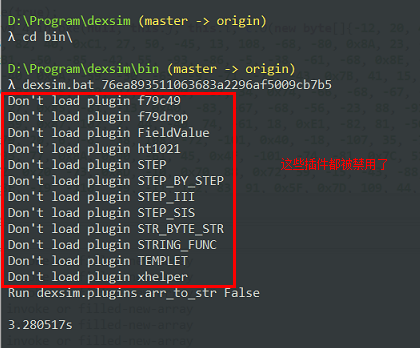
adb install ./server/dss.apk



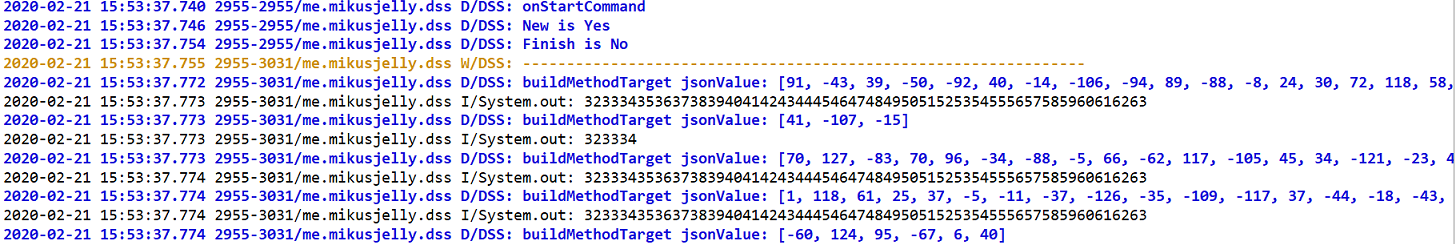
## 开始解密

cd bin

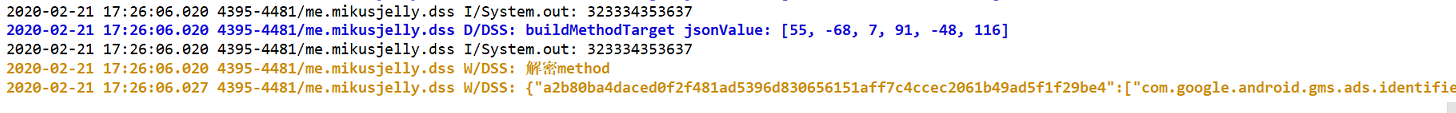
dexsim.bat apk或dex

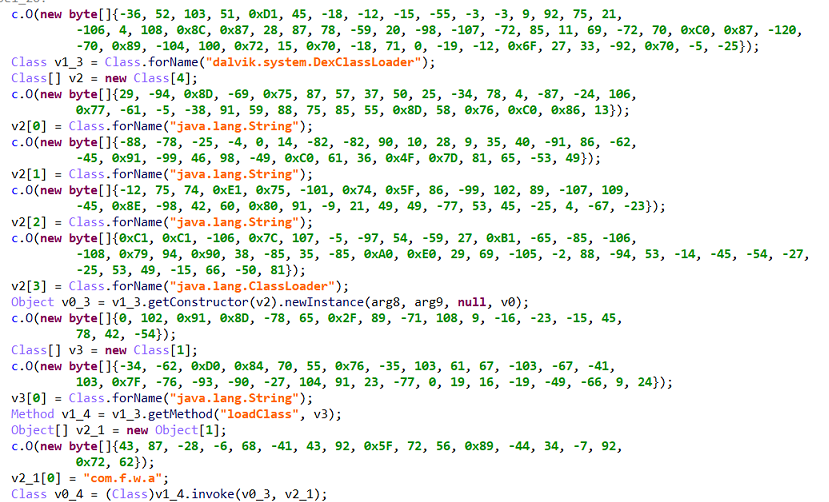


对应的需要解密的内容



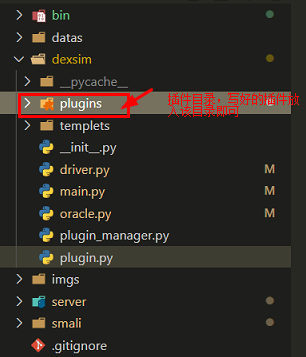
解密后的结果

解密后的dex



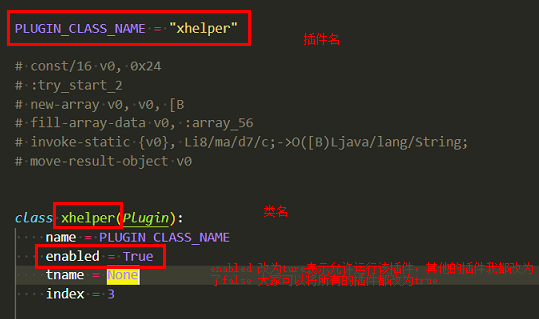
# 添加自己的解插件

插件已经支持一些常见的加密方式，当我们遇到dexsim 不能解密的时候，需要添加自己的揭秘插件，下面简单的讲解一下最近解密xhelper样本时添加的xhelper 插件，下图为整个项目的代码结构。



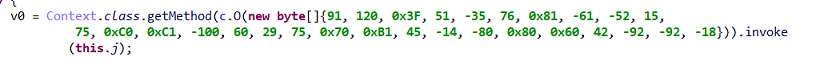
## 添加插件

在plugins目录中创建xhelper.py文件，将ht1021.py中的内容复制进去，修改如下图

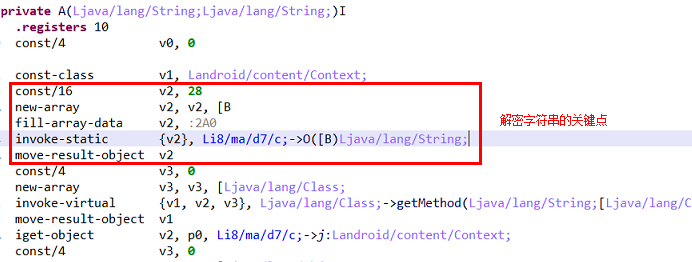


## 寻找解密函数的规律

可以发现dex中的字符串都被加密了，如下图

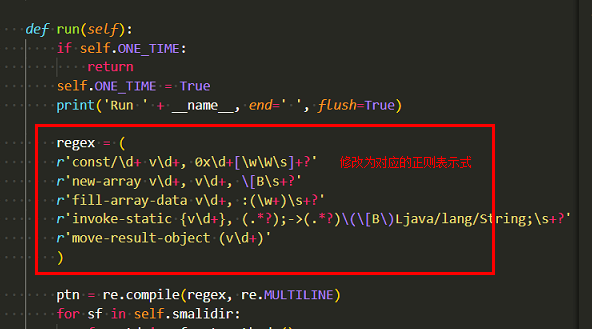


转换为smali代码如下图，可以发现解密字符串的关键点。

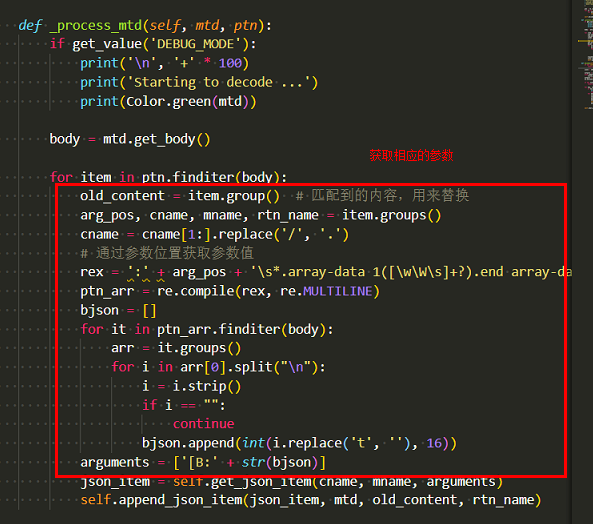


|  |
| --- |
| const/16 v0, 0x24  :try\_start\_2  new-array v0, v0, [B  fill-array-data v0, :array\_56  invoke-static {v0}, Li8/ma/d7/c;->O([B)Ljava/lang/String;  move-result-object v0 |

我们需要获取的内容为解密函数，返回值，参数值，类名，将其转化为对应的正则表达式，并修改xhelper.py的代码



此正则表达式只能获取参数的位置，需要进一步获取参数的值，即通过下列方法获取参数值，修改对应xhelper.py代码：



至此整个插件就修改完成了，执行完成后就可以获得上面解密后的结果。

如果解密过程中遇到什么问题可以问我或者赖老师。