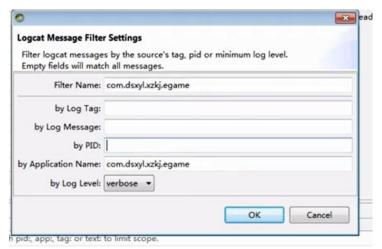
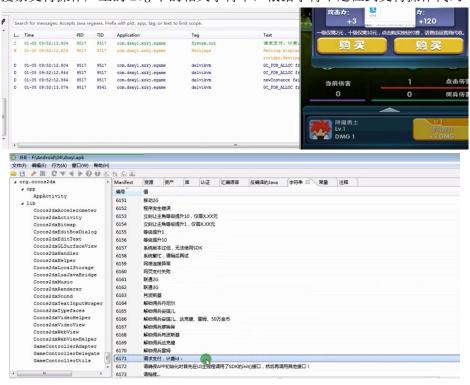
## 内付破解

- 1. 工具: jeb、Android Monitor、Android Killer
- 2. 步骤:
  - (1) 通过 Monitor 查看 app 的相关 Log, 根据 app 的 packageName 过滤 Log



(2) 搜索支付操作产生的 Log 中的相关字符串,根据字符串定位到支付操作代码



```
public void order_internal() {
    Object v9 = this.valueNap.get(Integer.valueOf(this.mOrgID));
    this.mMMID = Long.parseLong(((Map)v9).get("Id"));
    System.out.println("海宋文村, 计数d: " + this.mMMID);
    this.mOrderID = "orderID-" + SystemClock.elapsedRealtime();
    LSGAVirtualCurrency.onChargeRequest(this.mOrderID, ((Map)v9).get("tradeName"), ((double)(((( float)Integer.parseInt(((Map)v9).get("money")))) / 1f)), "CNY", ((double)((((float)Integer .parseInt(((Map)v9).get("money")))) / 1f)), "爱演戏");
    HashMap v8 = new HashMap();
    v8.put("toolsAlias", ((Map)v9).get("alias"));
    EgamePay.pay(((Activicy)this), ((Map)v8), new EgamePayListener() {
        public void payCancel(Map arg3) {
            AppActivity.onResult(AppActivity.this.mOrgID, -1);
        }
        public void payFailed(Map arg3, int arg1) {
            AppActivity.onResult(AppActivity.this.mOrgID, -1);
        }
        public void paySuccess(Map arg3) {
            AppActivity.onResult(AppActivity.this.mOrgID, 0);
        }
    });
}
```

(3) 可以看出当 onResult 第二个参数为 0 时,支付成功。定位到 onResult 函数的位置

```
public static void onResult(int id, int success) {
    if(success == 0) {
        LSGAVirtualCurrency.onChargeSuccess(AppActivity.context.mOrderID);
}

AppActivity.context.runOnGLThread(New Runnable() {
        public void run() {
              AppActivity.onResultNative(this.valSid, this.valSsuccess);
        }
        ));
}
```

修改 success==0 的跳转或者使得 success 恒等于 0

```
Cocos2dxLuaJavaBridge
                Cocos2dxMusic
                                                                             public static void onResult(int id, int success) (
                                                                                     if(success == 0) {
    LSGAVirtualCurrency.onChargeSuccess(AppActivity.context.mOrderID);
                Cocos2dxRenderer
                Cocos2dxSound
Cocos2dxTextInputWraper
                Cocos2dxTypefaces
                                                                                     AppActivity.context.runOnGLThread(new Runnable() {
                Cocos2dxVideoHelper
Cocos2dxVideoView
                                                                                             public void run() (
                                                                                                    AppActivity.onResultNative(this.valSid, this.valSsuccess);
                Cocos2dxWebView
                Cocos2dxWebViewHelper
GameControllerAdapter
               GameControllerAdapte_
GameControllerDelegate
                                                                             static native void onResultNative(AppActivity this, int arg1, int arg2) (
 显示内部类

    思示的時
    仮論译方法 Lorg/cocos2dx/cpp/AppActivity$2;-><init>(Lorg/cocos2dx/cpp/AppActivity;)V
反論译方法 Lorg/cocos2dx/cpp/AppActivity$4;
反論译方法 Lorg/cocos2dx/cpp/AppActivity$4;
反論译方法 Lorg/cocos2dx/cpp/AppActivity$4;
反論译方法 Lorg/cocos2dx/cpp/AppActivity$4;-><init>(II)V
反論译英 Lorg/cocos2dx/cpp/AppActivity$4;->run()V
反编译英 Lorg/cocos2dx/cpp/AppActivity$3;
反编译方法 Lorg/cocos2dx/cpp/AppActivity$3;-><init>(Lorg/cocos2dx/cpp/AppActivity$3;->kg/AppActivity$3;->kg/AppActivity$3;->payCancel(Ljava/util/Map;)V
反编译方法 Lorg/cocos2dx/cpp/AppActivity$3;->payFailed(Ljava/util/Map;)V
反编译方法 Lorg/cocos2dx/cpp/AppActivity$3;->paySuccess(Ljava/util/Map;)V
232:26 | Lorg/cocos2dx/cpp/AppActivity:->onResult(II)V | FFFFFFE
```

可以在最下面看到 onResult 函数所在的文件位置

(4)在 smali 文件中对 success 参数的值进行修改, 使该参数恒等于 0

```
AndroidManifestxml AppActivity.small

AppActivity.small

AppActivity.small

AppActivity.small

AppActivity.small

AppActivity.small

AppActivity.small

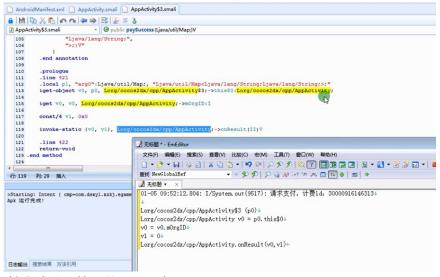
AppActivity.small

AppActivity.small

But appare apple app
```

```
AndroidManifest.xml AppActivity.smali
 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
  AppActivity.smali
             99 .method public static onResult (II) V
                                     .locals 2
.param p0, "id" # I
.param p1, "success"
          101
          102
          103
                                     .prologue
          105
                                       const/4 pl, 0
                                     if-nez pl, :cond 0
          108
          109
                                      sget-object v0, Lorg/cocos2dx/cpp/AppActivity;->context:Lorg/cocos2dx/cpp/AppActivity;
          111
                                      iget-object v0, v0, Lorg/cocos2dx/cpp/AppActivity;->mOrderID:Ljava/lang/String;
          114
          115
                                      invoke-static (v0), Lcom/lotuseed/android/LSGAVirtualCurrency; ->onChargeSuccess(Ljava/
          117
                                       .line 440
```

(5)直接在 order internal()的开始处调用支付成功处理操作



支付成功处理情况的 smali 代码

找到这段代码需要放置的位置

```
AndroidManifest.xml AppActivity.smali AppActivity$3.smali
.prologue
const/high16 v6, 0x3f800000
         .line 395
iget-object v0, p0, Lorg/cocos2dx/cpp/AppActivity;->valueMap:Ljava/util/Map;
         iget v1, p0, Lorg/cocos2dx/cpp/AppActivity;->mOrgID:I
         invoke-static {vl}, Ljava/lang/Integer;->valueOf(I)Ljava/lang/Integer;
         invoke-interface {v0, v1}, Ljava/util/Map;->get(Ljava/lang/Object;)Ljava/lang/Object;
AndroidManifest.xml AppActivity.smali* AppActivity$3.smali
 1335 .method public order_internal() V
  1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
          .prologue iget-object v0, p0, Lorg/cocos2dx/cpp/AppActivity$3;->this$0:Lorg/cocos2dx/cpp/AppActivity;
          iget v0, v0, Lorg/cocos2dx/cpp/AppActivity;->mOrgID:I
          invoke-static (v0, v1), Lorg/cocos2dx/cpp/AppActivity;->onResult(II)V
          const/high16 v6, 0x3f800000 # 1.0f
          .line 395 iget-object v0, p0, Lorg/cocos2dx/cpp/AppActivity;->valueMap:Ljava/util/Map;
  1353
```

将这段代码插入到选择的位置上,不过在 app 运行时会产生错误,原因是在 1339 行中 p0 是类 AppActivity\$3 的指针而不是 AppActivity 的,所以将该句删掉

```
AndroidManifest.xml AppActivity.smali AppActivity$3.smali

    AppActivity.smali

                          → Opublic order_internal ()V
 1334
 1335 .method public order_internal()V
1336 .locals 10
 1337
  1338
  1339
        iget v0, p0, Lorg/cocos2dx/cpp/AppActivity;->mCrgID:1
  1341
         const/4 v1, 0x0
  1342
  1343
         invoke-static (v0, v1), Lorg/cocos2dx/cpp/AppActivity;->onResult(II)V
  1344
  1345
  1346
 1347
1348
         return-void
         const/high16 v6, 0x3f800000 # 1.0f
  1349
  1351
          .line 395
  1352
          iget-object v0, p0, Lorg/cocos2dx/cpp/AppActivity;->valueMap:Ljava/util/Map;
  1353
行: 1340 列: 63 插入
```

重新编译并安装后,可以完成内付破解