[原创] 某音国际版助手-TK助手分析 优

贝a塔 7 3

大牛

2019-3-18 00:52

抖音国际版，通常打不开，需要安装一些xposed插件，找到了个TK助手，分享一下

小白都会的东西，只是想分享下过程 高手略过

解包发现里面,这里有个收费的，很好奇，想研究一下

是个xposed插件，
1-列表通常搜索ListView RecycleView
2-类似操作找找Click时间或者CheckBox

1-Java层

来到在这个类的点击方法这里
  com.cowherd.up.M类;

```
        }
        case 2131230888: {
            this.bufPayType = "jp";
            StatService.onEvent(((Context)this), "jp", SzDevice.getDeviceId(), 1);
            if(!Config.getLocAble(this.bufPayType)) {
                if(!SzUtility.checkNull(Config.getCode(this.bufPayType))) {
                }
                else {
                    this.showPayCodeDia(this.jpTx.getText().toString(), this.bufPayType);
                    return;
                }
            }

            this.setCurrentSwitchOpen(this.jpSwitch, true);
            this.mFix.fixDevice(3);
            break;
        }
        case 2131230890: {
```

可以看到，对于日本的区域来了个检测，在Config.getLocAble里面

```
}

public static boolean getLocAble(String arg2) {
    SzCacheFileService v0 = SzCacheFileService.getInstance();
    StringBuilder v1 = new StringBuilder();
    v1.append(arg2);
    v1.append("_able");
    return v0.readData(v1.toString()).equalsIgnoreCase("1");
}

public static String getParam(String arg1) {
```

简单点直接return 对应的smali就是

const/4 v1, 0x1

return v1

2-JNI层

修改了发现启动崩溃，logcat找到是提示是在jni层，其实就是个签名验证

```
71          "signatures",
72          "[Landroid/content/pm/Signature;");
73  ((void (__fastcall *)(JNIEnv *, int))(*v2)->DeleteLocalRef)(v2, v12);
74  v14 = ((int (__fastcall *)(JNIEnv *, int, int))(*v2)->GetObjectField)(v2, v11, v13);
75  v15 = v14;
76  if ( !v14 )
77  {
78    v4 = "PackageInfo.signatures[] is null";
79    return j___android_log_print(6, &unk_241C, v4);
80  }
81  v17 = ((int (__fastcall *)(JNIEnv *, int, int))(*v2)->GetObjectArrayElement)(v2, v14, v26);
82  ((void (__fastcall *)(JNIEnv *, int))(*v2)->DeleteLocalRef)(v2, v11);
83  ((void (__fastcall *)(JNIEnv *, int))(*v2)->DeleteLocalRef)(v2, v15);
84  v18 = ((int (__fastcall *)(JNIEnv *, int))(*v2)->GetObjectClass)(v2, v17);
```

打开 IDA查看

```
.text:00000F40 20 1C                    MOVS    R0, R4
.text:00000F42 98 47                    BLX     R3
.text:00000F44 28 49                    LDR     R1, =(a3082032d308202 - 0xF4C)
.text:00000F46 05 1C                    MOVS    R5, R0
.text:00000F48 79 44                    ADD     R1, PC          ; "3082032d30820215a003020102020 41f93192
.text:00000F4A 01 F0 E5 F8              BL      j_strcmp        ; 比较签名是否正确
.text:00000F4E 23 68                    LDR     R3, [R4]
.text:00000F50 00 28                    CMP     R0, #0
.text:00000F52 0C D0                    BEQ     loc_F6E         ; 跳转到崩溃的地方
.text:00000F54 25 49                    LDR     R1, =(aJavaLangRuntim - 0xF5E)
.text:00000F56 9B 69                    LDR     R3, [R3,#0x18]
.text:00000F58 20 1C                    MOVS    R0, R4
.text:00000F5A 79 44                    ADD     R1, PC          ; "java/lang/RuntimeException"
.text:00000F5C 98 47                    BLX     R3              ; 主要是修改这个跳转分支
.text:00000F5E 23 68                    LDR     R3, [R4]
.text:00000F60 23 4A                    LDR     R2, =(aUnknowError - 0xF6C)
.text:00000F62 01 1C                    MOVS    R1, R0
.text:00000F64 9B 6B                    LDR     R3, [R3,#0x38]
.text:00000F66 20 1C                    MOVS    R0, R4          ; 手动抛出异常
.text:00000F68 7A 44                    ADD     R2, PC          ; "unknow error"
.text:00000F6A 98 47                    BLX     R3
.text:00000F6C 15 E0                    B       loc_F9A
.text:00000F6E          ; ---------------------------------------------------------------------------
```

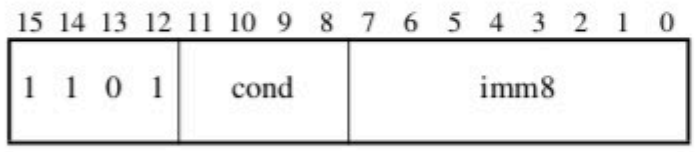
看ARM手册

A5.7.12 B

Branch causes a branch to a target address.

Encodings

T1 B<c> <label> Not allowed in IT block.




```
imm32 = SignExtend(imm8:'0', 32);
if cond == '1110' then SEE Permanently undefined space on page A4-37;
if cond == '1111' then SEE SVC (formerly SWI) on page A5-285;
if InITBlock() then UNPREDICTABLE;
```

T2 B<c> <label> Outside or last in IT block

修改机器码为BNE

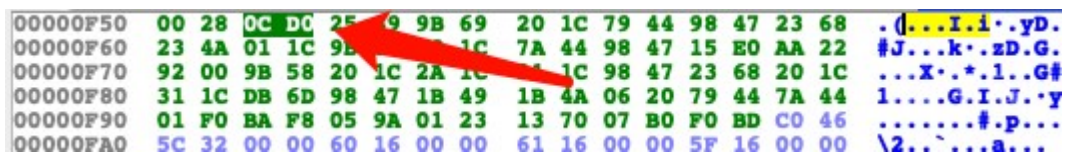
Opcode	Mnemonic extension	Meaning	Condition flag state
0000	EQ	Equal	Z set
0001	NE	Not equal	Z clear

也就是修改对应的cond

0XD00C 对应的二进制 1101 0000 0000 1100

修改为 1101 0001 0000 1100 就是0xd10c

然后写回去



上面的BEQ变成了BNE

然后打包安装，VIP就有了，来个图，好像是日本的吧大概可能

[培训]内核驱动高级班，冲击BAT一流互联网大厂工作，每周日13:00-18:00直播授课

最后于 2019-3-18 01:00 被贝a塔编辑，原因:

收藏 · 8 · 4 支持 分享

赞赏记录

参与人	雪币	留言	时间
PLEBFE		为你点赞~	2023-1-28 05:37
La0s		为你点赞~	2019-3-18 13:46
roysue		为你点赞~	2019-3-18 10:24
IamHuskar		为你点赞~	2019-3-18 09:35

最新回复 (11)

IamHuskar 4

专家

2 楼

tk看黄 指日可待

2019-3-18 09:35

0

小强!

极客

3 楼

TK看片，指日可待

2019-3-18 10:23

0

roysue 3

专家

4 楼

TK看片，指日可待

2019-3-18 10:24

0

blackcore

极客

5 楼

TK看片，指日可待

2019-3-19 08:59

0

anyehuyu

极客

6 楼

TK看片，指日可待

2019-3-19 18:49

0

Yougar

极客

7 楼

TK看片，指日可待

2019-3-21 15:51

0

皮豪

极客

8 楼

感谢分享

2019-3-22 10:29

0

烟油雾油

临时

9 楼

怎么下载啊 楼主

2019-4-1 18:09

0

nqxcwl

极客

10 楼

tk tk 雄起来~~~

2019-4-1 19:30

0

wx_保密

临时

11 楼

在哪里啊?

2020-2-24 00:08

0

首页 社区 课程 招聘 发现

最新回复 (11)

virjar 9 1

大侠

12 楼

TK看片，指日可待

2020-2-24 19:18

0 •••

贝a塔

3 年没回复的帖子已锁定，有问题请联系版主!

回帖 表情 高级回复

返回