ROIS_BCTF2017_Re_writeup

原创

JasaLee 于 2017-04-19 17:07:27 发布 1037 收藏

分类专栏： 逆向学习笔记 移动安全

本文链接：https://blog.csdn.net/JasaLee/article/details/70242837

逆向学习笔记 同时被 2 个专栏收录

5 篇文章 1 订阅

订阅专栏

移动安全

5 篇文章 0 订阅

订阅专栏

pingpong

刚刚过去的BCTF-2017有一道Mobile逆向题，下面放出我的解题思路

题目链接: https://pan.baidu.com/s/1boUKogv 密码: 9b52

拿到题目用JEB打开

得到两个比较有用的函数

```
    public void onClick(View arg7) {
            if(MainActivity.this.tt % 2 == 1) {
                MainActivity.this.p = 0;
                MainActivity.this.num = 0;
                MainActivity.this.tt = MainActivity.this.ttt;
            }

            --MainActivity.this.tt;
            MainActivity.this.p = MainActivity.this.ping(MainActivity.this.p, MainActivity.this.num);
            ++MainActivity.this.num;
            if(MainActivity.this.num >= 7) {
                MainActivity.this.num = 0;
            }

            View v0 = MainActivity.this.findViewById(2131427414);
            ((TextView)v0).setText("PING");
            if(MainActivity.this.tt == 0) {
                ((TextView)v0).setText("FLAG: BCTF{MagicNum" + Integer.toString(MainActivity.this.p) +
            }
        }
    }


    public void onClick(View arg7) {
            if(MainActivity.this.tt % 2 == 0) {
                MainActivity.this.p = 0;
                MainActivity.this.num = 0;
                MainActivity.this.tt = MainActivity.this.ttt;
            }

            --MainActivity.this.tt;
            MainActivity.this.p = MainActivity.this.pong(MainActivity.this.p, MainActivity.this.num);
            ++MainActivity.this.num;
            if(MainActivity.this.num >= 7) {
                MainActivity.this.num = 0;
            }

            View v0 = MainActivity.this.findViewById(2131427414);
            ((TextView)v0).setText("PONG");
            if(MainActivity.this.tt == 0) {
                ((TextView)v0).setText("FLAG: BCTF{MagicNum" + Integer.toString(MainActivity.this.p) +
            }
        }
```

大概意思就是通过执行1000000次ping & pong 使得 tt = 0 输出 flag。ping（int，int）和pong（int，int）为native函数。

IDA打开发现，用了类似O-LLVM混淆，为了节省逆向时间，决定写个apk复用so文件。

其中有个坑点

```
.text:0000139C loc_139C                                 ; CODE XREF: Java_com_geekerchina_pingpongmachin
.text:0000139C                  LDR     R0, =0x18C23607
.text:0000139E                  CMP     R1, R0
.text:000013A0                  BNE     loc_1326
.text:000013A2                  MOV     R4, R6
.text:000013A4                  MOVS    R6, #1
.text:000013A6                  MOVS    R0, R6          ; seconds
.text:000013A8                  BL      j_j_sleep
.text:000013AC                  MVNS    R2, R6
.text:000013AE                  LDR     R3, [SP,#0x30+var_1C]
.text:000013B0                  EORS    R2, R3
.text:000013B2                  LDR     R1, =0xF4B872E4
.text:000013B4                  LDR     R0, =0xF10822ED
.text:000013B6                  TST     R2, R3
.text:000013B8                  BEQ     loc_13BC
.text:000013BA                  MOV     R1, R0
......
..text:000015A6 loc_15A6                                ; CODE XREF: Java_com_geekerchina_pingpongmachi
.text:000015A6                  LDR     R0, =0x74379DA2
.text:000015A8                  CMP     R1, R0
.text:000015AA                  BNE     loc_1582
.text:000015AC                  MOVS    R6, #1
.text:000015AE                  MOVS    R0, R6          ; seconds
.text:000015B0                  BL      j_j_sleep
.text:000015B4                  LDR     R1, =0xD44374E7
.text:000015B6                  LDR     R0, =0x2E3C981B
.text:000015B8                  TST     R4, R6
.text:000015BA                  BEQ     loc_1582
.text:000015BC                  B       loc_1580
```

由于过程中调用了sleep函数，我们要把它nop掉

这里只将 **MOVS R0, R6** 改成 **MOVS R0, #0**

然后贴上java代码

```
    public void flag(){
            check = num_1000000;
            while (true) {
                if (check % 2 == 1) {
                    --check;
                    beFlag = pong(beFlag,num);
                    ++num;
                    if(num >= 7) {
                        num = 0;
                    }
                } else {
                    --check;
                    beFlag = ping(beFlag,num);
                    ++num;
                    if(num >= 7){
                        num = 0;
                    }
                }
                if (check == 0) {
                    Log.d("FLAG : ", "BCTF{MagicNum" + Integer.toString(beFlag) + "}");
                    break;
                }
            }
        }
```

得到flag： BCTF{MagicNum4500009}