

171207 逆向-JarvisOJ（病毒数据分析）（2）

原创

奈沙夜影 于 2017-12-09 01:11:53 发布 235 收藏

分类专栏: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/whklhhh/article/details/78756787>

版权



[CTF 专栏收录该内容](#)

163 篇文章 4 订阅

订阅专栏

1625-5 王子昂 总结《2017年12月7日》【连续第433天总结】

A. JarvisOJ-Re-病毒数据分析（2）

B.

继续分析

加密算法的识别插件没有识别出来, 只能自己来查找了

核心函数sub_401AD0的算法中出现了一个特征常数:

```
v12 -= 0x61C88647;
```

百度其发现它可能是RC5、RC6、TEA加密算法, 常数通常为加法, 以下式出现

```
+0x9e3779b9;
```

RC算法中还有另外一个常数P, 这里没有, 所以估计是TEA算法

而在包装加密函数sub_401CB0中还进行了一些其他的处理，对input、key和output的异或换位等等，因此在解密的时候也需要对应操作

```
IDA View-A Pseudocode-A Strings window Hex
25 *v5 ^= *v7;
26 v5[1] ^= v7[1];
27 v5[2] ^= v7[2];
28 v5[3] ^= v7[3];
29 v5[4] ^= v7[4];
30 v5[5] ^= v7[5];
31 v5[6] ^= v7[6];
32 v5[7] ^= v7[7];
33 v17 = HIWORD(v8);
34 v18 = HIWORD(v9);
35 v10 = a5 + 2;
36 if ( a3 - 8 > 0 )
37 {
38     v11 = (char *)a5 - v15;
39     v12 = v6 + 10;
40     v16 = ((unsigned int)(a3 - 9) >> 3) + 1;
41     do
42     {
43         *(_WORD *)v10 = v8 ^ *(_WORD *)(v12 - 2);
44         v11[v12] = v17 ^ *(_BYTE *)v12;
45         *((_BYTE *)v10 + 3) = HIBYTE(v17) ^ *(_BYTE *)(v12 + 1);
46         *((_WORD *)v10 + 2) = v9 ^ *(_WORD *)(v12 + 2);
47         *((_WORD *)v10 + 3) = v18 ^ *(_WORD *)(v12 + 4);
48         tea((_DWORD *)a4, v10);
49         v8 = *v10;
50         v9 = v10[1];
51         *(_BYTE *)v10 ^= *(_BYTE *)(v12 - 10);
52         *((_BYTE *)v10 + 1) ^= *(_BYTE *)(v12 - 9);
53         v11[v12] ^= *(_BYTE *)(v12 - 8);
54         *((_BYTE *)v10 + 3) ^= *(_BYTE *)(v12 - 7);
55         *((_BYTE *)v10 + 4) ^= *(_BYTE *)(v12 - 6);
56         *((_BYTE *)v10 + 5) ^= *(_BYTE *)(v12 - 5);
57         *((_BYTE *)v10 + 6) ^= *(_BYTE *)(v12 - 4);
58         *((_BYTE *)v10 + 7) ^= *(_BYTE *)(v12 - 3);
59         v10 += 2;
60         v12 += 8;
61         v13 = v16-- == 1;
62         v17 = HIWORD(v8);
63         v18 = HIWORD(v9);
64     }
```

<http://blog.csdn.net/whklhxxx>

在这里查到了writeup: http://docs.ioin.in/writeup/blog.heysec.org/_archives_914/index.html

参考其可以写出解密代码

不过其中的prev_data和prev_tea_data提供了常数，猜测是前一次对key进行tea加密得到的数据通过动态调试可以获得

准备明天自己再试试，争取研究透这个程序

毕竟它相对而言很贴近实际的抽象了，不能仅仅满足于简单的CTF

C. 明日计划

JarvisOJ-Re-病毒数据分析