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/whklhhhh/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：

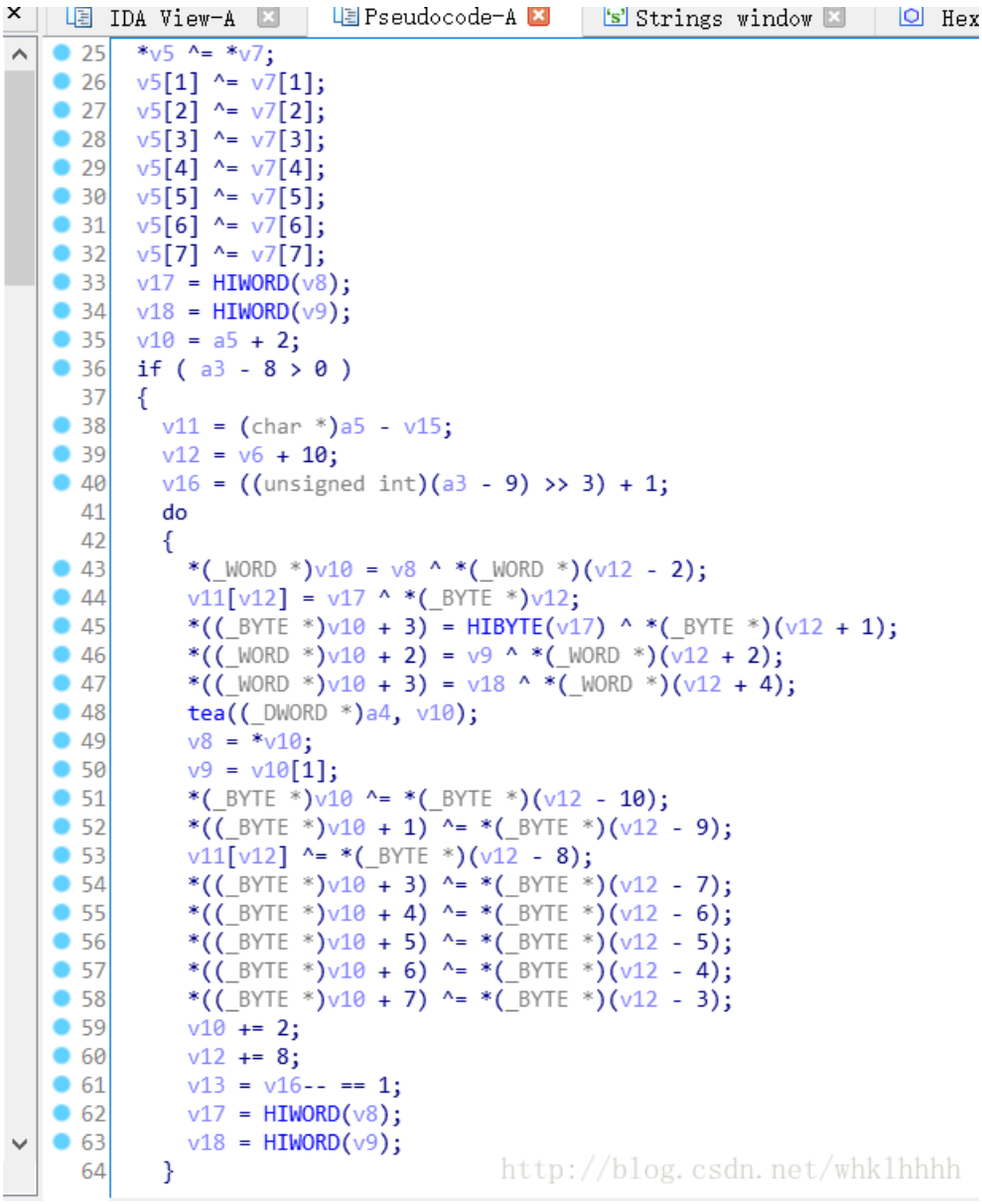
```
v12 -= 0x61C88647;
```

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



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