2016 年第 2 题

大家好，我是胡一米。这期视频是关于 2016 年看雪 CTF 第 2 题解题资料。

一、简介

1.1 录制说明

视频是基于其他大佬文字 Writeup 录制的，所以在视频操作之前就已知了该题中的各种坑，如反调试等，所以不再演示踩坑过程。

1.2 录制参考

第 2 题主要参看了库洛洛、HighHand、风间仁和 HHHso 的 Writeup，链接如下：
库洛洛：
https://bbs.pediy.com/thread-213702.htm
HighHand:
https://bbs.pediy.com/thread-213697.htm
风间仁：
https://bbs.pediy.com/thread-213698.htm
HHHso:
https://bbs.pediy.com/thread-213712.htm

1.3 内容简介

在本期中，主要讨论 3 个问题。这 3 个问题可能与最终的 Key 没有太大的联系，但题目中既然出现了，还是说一说。此 3 个问题分别是：
a. RC6 算法
b. 变形的 AES 算法
c. Lua.dll 相关的杂项

二、视频操作

2.1 静态分析

a. Lua.dll 相关的杂项

log(32) / log(2) == log2 (32) = 5

2.2 动态调试程序逻辑

a. RC6 算法
b. 变形的 AES 算法

stK5CKpBsw7TPF45

2.3 完成分析

借用程序本身的代码，计算序列号。

ConstantStr -> AES -> RC6

```
.rdata:0042D244 unk_42D244 db 0A4h    ; DATA XREF: fnGetRegSnToVerify+10 ↑ o
.rdata:0042D245 db    47h ; G
.rdata:0042D246 db    98h
.rdata:0042D247 db    0Ch
.rdata:0042D248 db    9Eh
.rdata:0042D249 db    40h ; @
.rdata:0042D24A db 0D7h
.rdata:0042D24B db 0F6h
.rdata:0042D24C db 0EBh
.rdata:0042D24D db    76h ; v
.rdata:0042D24E db    6Eh ; n
.rdata:0042D24F db    6Dh ; m
.rdata:0042D250 db    7Eh ; ~
.rdata:0042D251 db 0A3h
.rdata:0042D252 db    3Eh ; >
.rdata:0042D253 db 0EBh
```

```
.rdata:0042D254 db 0D5h
.rdata:0042D255 db    51h ; Q
.rdata:0042D256 db    30h ; 0
.rdata:0042D257 db       6
.rdata:0042D258 db    7Dh ; }
.rdata:0042D259 db 0C0h
.rdata:0042D25A db 0FBh
.rdata:0042D25B db    6Ch ; l
.rdata:0042D25C db 0C2h
.rdata:0042D25D db    7Ah ; z
.rdata:0042D25E db    43h ; C
.rdata:0042D25F db 0C5h
.rdata:0042D260 db 0A4h
.rdata:0042D261 db 0C9h
.rdata:0042D262 db 0B1h
.rdata:0042D263 db 0FDh
```

4B 7D 6F 22 BD EA 61 C3 0B E7 B2 D9 2C 6B 41 88
5D 71 27 85 BA 71 F0 B9 23 77 28 6C FC 36 A6 D0

三、小结

题目很好。

附录：

录制顺序：29-28-7-19-22-16-15-14-11-2