2016 年第 29 题

大家好，我是胡一米。这期视频是关于 2016 年看雪 CTF 第 29 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 29 题主要参看了 HighHand 和 HHHso 的 Writeup，链接如下：
HighHand:
https://bbs.pediy.com/thread-214953.htm
HHHso:
https://bbs.pediy.com/thread-214911.htm

还有部分其他人的 Writeup，链接如下：
yber:
https://bbs.pediy.com/thread-214949.htm
风间仁：
https://bbs.pediy.com/thread-214896.htm
Quizow:
https://bbs.pediy.com/thread-214918.htm

1.3 内容简介

在本期中，主要讨论 4 个问题。这 4 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 4 个问题分别是：
a. CM 中的查找函数的过程
b. CM 中的俄罗斯方块游戏
c. CM 中的各个验证步骤
d. 穷举得到最终的 Key

二、视频操作

2.1 静态分析定位关键点

结合其他大佬的分析过程，可以直接定位到关键点。
a. 查找函数的过程
b. patch 反调试
c. 俄罗斯方块
d. 各个验证步骤

```
typedef struct _IMAGE_EXPORT_DIRECTORY {
    DWORD   Characteristics;
    DWORD   TimeDateStamp;
    WORD    MajorVersion;
    WORD    MinorVersion;
    WORD   Name;
    DWORD   Base;
    DWORD   NumberOfFunctions;
    DWORD   NumberOfNames;
    DWORD   AddressOfFunctions;     // RVA from base of image
    DWORD   AddressOfNames;         // RVA from base of image, not FOA
    DWORD   AddressOfNameOrdinals;  // RVA from base of image
} IMAGE_EXPORT_DIRECTORY, *PIMAGE_EXPORT_DIRECTORY;
```

+0x18 NumberOfNames ;
+0x20 AddressOfNames;

401069 jz short loc_401072 >> jmp
401505 jz short loc_40150E >> jmp
401847 jz short loc_401850 >> jmp

？？？？
？？？？
？？？？
？？？？
****

*
*
*
*

8 位：x7 x6 x5 x4　x3 x2 x1 x0
0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

kahuSKey

条件一：0x325 < 0x3D0
条件二：int (x7 x6 x5 x4 ^ 0x66) +int(x3 x2 x1 x0 ^ 0x66) = 0x32113442
条件三：push 004032b5

2.2 动态调试其加密过程

通过动态调试，理解程序加解密过程。

2.3 穷举验证码

使用 visual studio，穷举验证码。这里直接使用 HighHand 大佬贴出的代码。

(无进位，不溢出)

三、小结

题目很好。