2016 年第 22 题

大家好，我是胡一米。这期视频是关于 2016 年看雪 CTF 第 22 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 22 题主要参看了 tgjarwl、风间仁以及 HighHand 的 Writeup，链接如下：

风间仁：
https://bbs.pediy.com/thread-214606.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. c++ EH
b. 调试与异常
c. context 结构
d. 双进程调试方法

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. c++ EH
b. 调试与异常

CREATE_PROCESS_DEBUG_EVENT 3
CREATE_THREAD_DEBUG_EVENT 2
EXCEPTION_DEBUG_EVENT 1
EXIT_PROCESS_DEBUG_EVENT 5

#define EXCEPTION_BREAKPOINT ((DWORD)0x80000003)
#define EXCEPTION_SINGLE_STEP ((DWORD)0x80000004)
#define EXCEPTION_ACCESS_VIOLATION ((DWORD)0xC0000005)
#define EXCEPTION_INT_DIVIDE_BY_ZERO ((DWORD)0xC0000094)

2.2 动态调试其加密过程

通过动态调试，理解程序内存加载过程。
a. 双进程调试方法
b. context 结构

ACCESS_VIOLATION
BREAKPOINT A * 7 + 1
BREAKPOINT 1 change order
BREAKPOINT 2 compare first
BREAKPOINT A
BREAKPOINT 3 compare second
BREAKPOINT 2
BREAKPOINT 3 compare third
BREAKPOINT A * 4
BREAKPOINT C
BREAKPOINT D
SingleStep 0x12
ACCESSVIOLATION 0x8
….
….
….
….

+0x08c SegGs
+0x090 SegFs
+0x094 SegEs
+0x098 SegDs
+0x09c Edi
+0x0a0 Esi
+0x0a4 Ebx
+0x0a8 Edx
+0x0ac Ecx
+0x0b0 Eax
+0x0b4 Ebp
+0x0b8 Eip
+0x0bc SegCs
+0x0c0 EFlags
+0x0c4 Esp
+0x0c8 SegSs

2.3 计算某一个验证码

这里直接使用风间仁大佬贴出的代码。

三、小结

题目很好。

附录：

录制顺序：29 – 28 – 7 – 19 – 22 - ？