2016 年第 15 题

大家好，我是胡一米。这期视频是关于 2016 年看雪 CTF 第 15 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 15 题主要参看了 HHHso、风间仁以及 QuiZow 的 Writeup，链接如下：
HHHso:
https://bbs.pediy.com/thread-214338.htm
风间仁：
https://bbs.pediy.com/thread-214316.htm
QuiZow:
https://bbs.pediy.com/thread-214464.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. MFC 程序分析
b. 8 种反调试方法
c. 错位洗牌和异或加密

二、视频操作

2.1 静态分析反调试

a. MFC 程序分析
b. 8 种反调试方法
(1) sub_402450 : rdtsc：将时间标签计数器读入 EDX:EAX

(2) sub_402DE0: 对比 od 特征码：0x00404000 处，特征码内容为：

```
debug043:01DDFDE8 db    55h ; U
debug043:01DDFDE9 db 0F0h
debug043:01DDFDEA db    33h ; 3
debug043:01DDFDEB db 0C9h
debug043:01DDFDEC db    89h
debug043:01DDFDED db    4Bh ; K
debug043:01DDFDEE db       4
debug043:01DDFDEF db    89h
debug043:01DDFDF0 db    0Bh
debug043:01DDFDF1 db    6Ah ; j
debug043:01DDFDF2 db       0
debug043:01DDFDF3 db 0E8h
debug043:01DDFDF4 db    40h ; @
debug043:01DDFDF5 db 0D1h
debug043:01DDFDF6 db 0FFh
debug043:01DDFDF7 db 0FFh
debug043:01DDFDF8 db    59h ; Y
debug043:01DDFDF9 db 0E9h
debug043:01DDFDFA db    83h
debug043:01DDFDFB db 0FDh
debug043:01DDFDFC db 0FFh
debug043:01DDFDFD db 0FFh
debug043:01DDFDFE db    83h
debug043:01DDFDFF db    7Dh ; }
debug043:01DDFE00 db 0FCh
debug043:01DDFE01 db       0
debug043:01DDFE02 db    75h ; u
debug043:01DDFE03 db    0Eh
debug043:01DDFE04 db    83h
debug043:01DDFE05 db    7Dh ; }
debug043:01DDFE06 db 0F8h
debug043:01DDFE07 db       0
```

(3) sub_402280 : FindWindowA(ClassName = Progman)
判断父进程是否为 explorer.exe

(4) sub_402150 : OpenProcess(csrss.exe): SeDebugPrivilege 权限可以打开 csrss.exe

(5) sub_402390 : PEB.NtGlobalFlag 调试堆创建标志。

Ring 3 中，
Fs 指向 GDT 中的 0x3B 段，为 TEB 基址
ntdll!_TEB
+0x000 NtTib : _NT_TIB
+0x01c EnvironmentPointer : Ptr32 Void
+0x018 Self : Ptr32 //TEB
+0x020 ClientId : _CLIENT_ID
+0x028 ActiveRpcHandle : Ptr32 Void
+0x02c ThreadLocalStoragePointer : Ptr32 Void
+0x030 ProcessEnvironmentBlock : Ptr32 _PEB
+0x034 LastErrorValue : Uint4B
+0x038 CountOfOwnedCriticalSections : Uint4B
+0x03c CsrClientThread : Ptr32 Void
+0x040 Win32ThreadInfo : Ptr32 Void
+0x044 User32Reserved : [26] Uint4B
+0x0ac UserReserved : [5] Uint4B
+0x0c0 WOW32Reserved : Pt32 Void
+0x0c4 CurrentLocale : Uint4B
+0x0c8 FpSoftwareStatusRegister : Uint4B
+0x0cc SystemReserved1 : [54] Ptr32 Void
+0x1a4 ExceptionCode : Int4B
+0x1a8 ActivationContextStack : _ACTIVATION_CONTEXT_STACK
+0x1bc SpareBytes1 : [24] UChar
+0x1d4 GdiTebBatch : _GDI_TEB_BATCH
+0x6b4 RealClientId : _CLIENT_ID
+0x6bc GdiCachedProcessHandle : Ptr32 Void
+0x6c0 GdiClientPID : Uint4B
+0x6c4 GdiClientTID : Uint4B
+0x6c8 GdiThreadLocalInfo : Ptr32 Void
+0x6cc Win32ClientInfo : [62] Uint4B
+0x7c4 glDispatchTable : [233] Ptr32 Void
+0xb68 glReserved1 : [29] Uint4B
+0xbdc glReserved2 : Ptr32 Void
+0xbe0 glSectionInfo : Ptr32 Void
+0xbe4 glSection : Ptr32 Vod

```
   +0xbe8 glTable                  : Ptr32 Voi
   +0xbec glCurrentRC              : Ptr32 Void
   +0xbf0 glContext                : Ptr32 Void
   +0xbf4 LastStatusValue    : Uint4B
   +0xbf8 StaticUnicodeString : _UNICODE_STRING
   +0xc00 StaticUnicodeBuffer : [261] Uint2B
   +0xe0c DeallocationStack : Ptr32 Void
   +0xe10 TlsSlots                 : [64] Ptr32 Void
   +0xf10 TlsLinks                 : _LIST_ENTRY
   +0xf18 Vdm                      : Ptr32 Void
   +0xf1c ReservedForNtRpc : Ptr32 Void
   +0xf20 DbgSsReserved        : [2] Ptr32 Void
   +0xf28 HardErrorsAreDisabled : Uint4B
   +0xf2c Instrumentation    : [16] Ptr32 Void
   +0xf6c WinSockData              : Ptr32 Void
   +0xf70 GdiBatchCount        : Uint4B
   +0xf74 InDbgPrint               : UChar
   +0xf75 FreeStackOnTermination : UChar
   +0xf76 HasFiberData             : UChar
   +0xf77 IdealProcessor      : UChar
   +0xf78 Spare3                   : Uint4
   +0xf7c ReservedForPerf    : Ptr32 Void
   +0xf80 ReservedForOle      : Ptr32 Void
   +0xf84 WaitingOnLoaderLock : Uint4B
   +0xf88 Wx86Thread               : _Wx86ThreadState
   +0xf94 TlsExpansionSlots : Ptr32 Ptr32 Void
   +0xf98 ImpersonationLocale : Uint4B
   +0xf9c IsImpersonating    : Uint4B
   +0xfa0 NlsCache                 : Ptr32 Void
   +0xfa4 pShimData                : Ptr32 Void
   +0xfa8 HeapVirtualAffinity : Uint4B
   +0xfac CurrentTransactionHandle : Ptr32 Void
   +0xfb0 ActiveFrame              : Ptr32 _TEB_ACTIVE_FRAME
   +0xfb4 SafeThunkCall        : UChar
   +0xfb5 BooleanSpare             : [3] UChar

ntdll!_PEB
   +0x000 InheritedAddressSpace : UChar
   +0x001 ReadImageFileExecOptions : UChar
   +0x002 BeingDebugged        : UChar
   +0x003 SpareBool                : UChar
   +0x004 Mutant                   : Ptr32 Void
   +0x008 ImageBaseAddress : Ptr32 Void
   +0x00c Ldr                      : Ptr32 _PEB_LDR_DATA
```

+0x010 ProcessParameters : Ptr32 _RTL_USER_PROCESS_PARAMETERS
+0x014 SubSystemData : Ptr32 Void
+0x018 ProcessHeap : Ptr32 Void
+0x01c FastPebLock : Ptr32 _RT_CRITICAL_SECTION
+0x020 FastPebLockRoutine : Ptr32 Void
+0x024 FastPebUnlockRoutine : Ptr32 Void
+0x028 EnvironmentUpdateCount : Uint4B
+0x02c KernelCallbackTable : Ptr32 Void
+0x030 SystemReserved : [1] Uint4B
+0x034 AtlThunkSListPtr32 : Uint4B
+0x038 FreeList : Ptr32 _PEB_FREE_BLOCK
+0x03c TlsExpansionCounter : Uint4B
+0x040 TlsBitmap : Ptr32 Void
+0x044 TlsBitmapBits : [2] Uint4B
+0x04c ReadOnlySharedMemoryBase : Ptr32 Void
+0x050 ReadOnlySharedMemoryHeap : Ptr32 Void
+0x054 ReadOnlyStaticServerData : Ptr32 Ptr32 Void
+0x058 AnsiCodePageData : Ptr32 Void
+0x05c OemCodePageData : Ptr32 Void
+0x060 UnicodeCaseTableData : Ptr32 Void
+0x064 NumberOfProcessors : Uint4B
+0x068 NtGlobalFlag : Uint4B
+0x070 CriticalSectionTimeout : _LARGE_INTEGER
+0x078 HeapSegmentReserve : Uint4B
+0x07c HeapSegmentCommit : Uint4
+0x080 HeapDeCommitTotalFreeThreshold : Uint4B
+0x084 HeapDeCommitFreeBlockThreshold : Uint4B
+0x088 NumberOfHeaps : Uint4B
+0x08c MaximumNumberOfHeaps : Uint4B
+0x090 ProcessHeaps : Ptr32 Ptr32 Void
+0x094 GdiSharedHandleTable : Ptr32 Void
+0x098 ProcessStarterHelper : Ptr32 Void
+0x09c GdiDCAttributeList : Uint4B
+0x0a0 LoaderLock : Ptr32 Void
+0x0a4 OSMajorVersion : Uint4B
+0x0a8 OSMinorVersion : Uint4B
+0x0ac OSBuildNumber : Uint2B
+0x0ae OSCSDVersion : Uint2B
+0x0b0 OSPlatformId : Uint4B
+0x0b4 ImageSubsystem : Uint4B
+0x0b8 ImageSubsystemMajorVersion : Uint4B
+0x0bc ImageSubsystemMinorVersion : Uint4B
+0x0c0 ImageProcessAffinityMask : Uint4B
+0x0c4 GdiHandleBuffer : [34] Uint4B

+0x14c PostProcessInitRoutine : Ptr32 void
+0x150 TlsExpansionBitmap : Ptr32 Void
+0x154 TlsExpansionBitmapBits : [32] Uint4B
+0x1d4 SessionId : Uint4B
+0x1d8 AppCompatFlags : _ULARGE_INTEGER
+0x1e0 AppCompatFlagsUser : _ULARE_INTEGER
+0x1e8 pShimData : Ptr32 Void
+0x1ec AppCompatInfo : Ptr32 Void
+0x1f0 CSDVersion : _UNICODE_STRING
+0x1f8 ActivationContextData : Ptr32 Void
+0x1fc ProcessAssemblyStorageMap : Ptr32 Void
+0x200 SystemDefaultActivationContextData : Ptr32 Void
+0x204 SystemAssemblyStorageMap : Ptr32 Void
+0x208 MinimumStackCommit : Uint4B

(6) sub_402410 : NtSetInformationThread(threadInformationClass = ThreadHideFromDebugger)
线程脱离调试器

(7) sub_4023A0 : 检测断点寄存器 dr0 ~ dr3

(8) sub_4027C0 : 检测辅助调试的驱动程序。

```
0244FD20  5C 5C 2E 5C 50 52 4F 43  45 58 50 31 35 32 00 00  \\.\PROCEXP152..
0244FD30  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0244FD40  5C 5C 2E 5C 45 58 54 52  45 4D 00 00 00 00 00 00  \\.\EXTREM......
0244FD50  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0244FD60  5C 5C 2E 5C 46 49 4C 45  4D 00 00 00 00 00 00 00  \\.\FILEM.......
0244FD70  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0244FD80  5C 5C 2E 5C 46 49 4C 45  56 58 47 00 00 00 00 00  \\.\FILEVXG.....
0244FD90  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0244FDA0  5C 5C 2E 5C 49 43 45 45  58 54 00 00 00 00 00 00  \\.\ICEEXT......
0244FDB0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0244FDC0  5C 5C 2E 5C 4E 44 42 47  4D 53 47 2E 56 58 44 00  \\.\NDBGMSG.VXD.
0244FDD0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0244FDE0  5C 5C 2E 5C 4E 54 49 43  45 00 00 00 00 00 00 00  \\.\NTICE.......
0244FDF0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0244FE00  5C 5C 2E 5C 52 45 47 53  59 53 00 00 00 00 00 00  \\.\REGSYS......
0244FE10  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0244FE20  5C 5C 2E 5C 52 45 47 56  58 47 00 00 00 00 00 00  \\.\REGVXG......
0244FE30  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0244FE40  5C 5C 2E 5C 52 49 4E 47  30 00 00 00 00 00 00 00  \\.\RING0.......
0244FE50  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

```
0244FE60    5C 5C 2E 5C 53 49 43 45    00 00 00 00 00 00 00 00    \\.\SICE........
0244FE70    00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00    ................
0244FE80    5C 5C 2E 5C 53 49 57 56    49 44 00 00 00 00 00 00    \\.\SIWVID......
0244FE90    00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00    ................
0244FEA0    5C 5C 2E 5C 54 52 57 00    00 00 00 00 00 00 00 00    \\.\TRW.........
0244FEB0    00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00    ................
0244FEC0    5C 5C 2E 5C 53 50 43 4F    4D 4D 41 4E 44 00 00 00    \\.\SPCOMMAND...
0244FED0    00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00    ................
0244FEE0    5C 5C 2E 5C 53 59 53 45    52 00 00 00 00 00 00 00    \\.\SYSER.......
0244FEF0    00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00    ................
0244FF00    5C 5C 2E 5C 53 59 53 45    52 42 4F 4F 54 00 00 00    \\.\SYSERBOOT...
0244FF10    00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00    ................
0244FF20    5C 5C 2E 5C 53 59 53 45    52 44 42 47 4D 53 47 00    \\.\SYSERDBGMSG.
0244FF30    00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00    ................
0244FF40    5C 5C 2E 5C 53 59 53 45    52 4C 41 4E 47 55 41 47    \\.\SYSERLANGUAG
```

2.2 动态调试程序逻辑

a. 奇偶洗牌和异或加密

输入→填充为 0x4D，并奇偶洗牌 3 次→异或加密→分段存储

分段存储→填充为 77，奇偶洗牌 1 次→异或加密→比较

CR22QIBennetDWelcomYou

2.3 完成分析

这里直接使用 HHHso 大佬提供的脚本。

三、小结

题目很好。

附录：

录制顺序：29-28-7-19-22-16-15-?