

[原创] 键盘过滤之i8042prt!I8042KeyboardInterruptService深层hook

ALwalker

极客

2023-5-9 20:45

举报

3705

当我在参考《寒江独钓 Windows内核安全编程》的键盘过滤部分时，涉及到Hook i8042prt!I8042KeyboardInterruptService 底层函数。

在查找该函数的地址时，书中推荐的方法是同时遍历 driver_object->device_object->DeviceExtension（此结构未公开）中的地址，只要该地址合法且存在于 Kbdclass 模块中即可。

本机环境为win10，可能存在差异？

经过测试发现，i8042prt!I8042KeyboardInterruptService 函数位于 i8042prt 模块中（通过加载调试符号号表得到的），且在 driver_object->device_object->DeviceExtension 中无法获取。。。

遂采用特征码搜索，搜先获取 i8042prt 模块的基址，然后搜索特征码得到。

```
kd> u I8042KeyboardInterruptService
i8042prt!I8042KeyboardInterruptService:
fffff805`7c256820 488bc4      mov     rax, rsp
fffff805`7c256823 48895010     mov     qword ptr [rax+10h], rdx
fffff805`7c256827 53          push    rbx
fffff805`7c256828 56          push    rsi
fffff805`7c256829 57          push    rdi
fffff805`7c25682a 4154        push    r12
fffff805`7c25682c 4155        push    r13
fffff805`7c25682e 4156        push    r14
kd> s fffff805`7c250000 110000 53 56 57 41 54 41 55 41 56
fffff805`7c256827 53 56 57 41 54 41 55 41-56 41 57 48 83 ec 50 48 SVWATAUAVAWH..PH
```

(二) i8042prt!I8042KeyboardInterruptService 函数的深层 hook

通过分析该函数，发现其内部调用了 I8xQueueCurrentKeyboardInput 函数，跟进其内部发现又调用了 I8xWriteDataToKeyboardQueue。

I8xWriteDataToKeyboardQueue，顾名思义，即将 KEYBOARD_INPUT_DATA 结构写入队列中，其参数 rcx 应指向队列，rdx 指向 KEYBOARD_INPUT_DATA 结构。因此，只要修改 KEYBOARD_INPUT_DATA 结构中的参数即可实现深层hook。

```
i8042prt!I8042KeyboardInterruptService+0x6c0:
fffff805`7c256ee0 488b8c2498000000 mov     rcx, qword ptr [rsp+98h]
fffff805`7c256ee8 e8f3050000      call    i8042prt!I8xQueueCurrentKeyboardInput (fffff805`7c2574e0)
fffff805`7c256eed e9f2000000      jmp     i8042prt!I8042KeyboardInterruptService+0x7c4 (fffff805`7c256fe4) Branch
```

```
i8042prt!I8xQueueCurrentKeyboardInput+0x21:
fffff805`7c257501 488d9388030000 lea     rdx, [rbx+388h]
fffff805`7c257508 488bcb         mov     rcx, rbx
fffff805`7c25750b e8a8f0ffff     call    i8042prt!I8xWriteDataToKeyboardQueue (fffff805`7c2565b8)
fffff805`7c257510 84c0          test    al, al
fffff805`7c257512 7561          jne     i8042prt!I8xQueueCurrentKeyboardInput+0x95 (fffff805`7c257575) Branch
```

其中，rdx 如下：

☆

4

👍

¥

```
kd> g
Breakpoint 2 hit
i8042prt!I8xQueueCurrentKeyboardInput+0x2b:
fffff805`7c25750b e8a8f0ffff call i8042prt!I8xWriteDataToKeyboardQueue (fffff805`7c2565b8)
kd> r
rax=ffffce0ea8ab8774 rbx=ffffce0ea8ab83e0 rcx=ffffce0ea8ab83e0
rdx=ffffce0ea8ab8768 rsi=0000000000000000 rdi=ffffce0ea8ab8290
rip=fffff8057c25750b rsp=fffff8057b359e70 rbp=ffffce0ea8ab83f0
r8=0000000000000194 r9=ffffce0ea8aaf6ac r10=ffffce0ea8aaf000
r11=000000000000001c r12=fffff8057c25eb38 r13=000000000000001b
r14=fffff8057c260000 r15=0000000000000001
iop1=0 nv up ei pl nz na pe nc
cs=0010 ss=0000 ds=002b es=002b fs=0053 gs=002b efl=00000202
i8042prt!I8xQueueCurrentKeyboardInput+0x2b:
fffff805`7c25750b e8a8f0ffff call i8042prt!I8xWriteDataToKeyboardQueue (fffff805`7c2565b8)
```

```
kd> dq fffffce0ea8ab8768
ffffce0e`a8ab8768 00000000`001f0000 00000000`00000000
```

```
kd> eq fffffce0e`a8ab8768 00000000`00200000 # down
kd> eq fffffce0e`a8ab8768 00000001`00210000 # up
```

效果图如下：

```
kd> g
回调函数执行. 4
[Down] 0x20
[up] 0x21
[Down] 0x1f
[up] 0x1f
irp派发.
```

[零基础网络安全攻防-研修见习班](#)

☆

👍

¥

↶


收藏 · 4

点赞

打赏

分享

最新回复 (1)



秋狸

2023-5-10 09:12


2楼

👍 1

...

感谢分享

极客



R0g

内容

回帖

表情

高级回复

返回