

## 2021/05/31\_Windows64位内核\_第1课\_64位系统调用

笔记本: Windows64位内核  
创建时间: 2021/5/31 星期一 15:00  
作者: ileemi

---

- [课前会议](#)
- [DSE](#)
- [KPP](#)
- [64位系统调用](#)
- [64位SSDT保护](#)
- [回调函数 \(callbacks\)](#)
- [API使用](#)

## 课前会议

windows vista  
windows 7  
windows 8  
windows 10

## DSE

DSE (驱动强制签名): 驱动没有签名, 操作系统就不加载。

驱动签名的购买: 微软官网 --> 获取代码签名证书。EV 证书主要用来验证签名的身份。同时微软提供了测试签名, 供驱动开发者测试驱动程序。win7启动程序时按F8可以进入测试模式 (选择 --> 禁用驱动程序签名强制)。

若要禁止使用测试签名代码, 请使用以下 BCDEdit 命令行:

```
Bcdedit.exe -set TESTSIGNING OFF
```

三环程序 (驱动) 签名验证一般使用离线验证 (硬件驱动可能不需要连接网络)。使用过期签名 (正常、有效) 依然可以加载驱动。

## KPP

KPP (PG): 内核补丁保护, 禁止API hook 以及检测内核代码是否被修改 (内核代码被修改操作系统就蓝屏), 内核层会进行实时监控 (监控代码段即可, 数据段不需

要监控)。  
通过VT技术可以过PG保护。

## 64位系统调用

定位 SSDT表 的位置：可以从三环公开API进行分析，分析其如何进入系统调用 (ntdll.dll) 。

```
public ZwCreateFile
proc near                                ; CODE XREF: sub_18004BDA8+E31p
                                        ; sub_180056BD4+1071p ...
                                        ; NtCreateFile
mov     r10, rcx
mov     eax, 55h ; 'U'
test    byte ptr ds:7FFE0308h, 1
jnz     short loc_18009D8C5
syscall                                ; Low latency system call
retn
```

syscall --> sysenter  
sysret --> sysexit

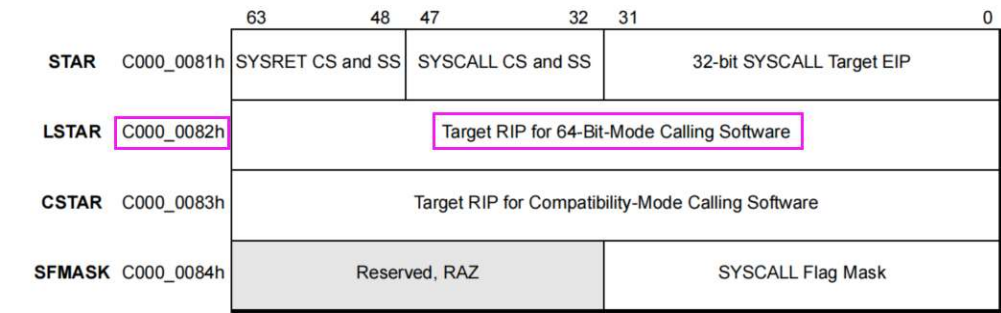


Figure 6-1. STAR, LSTAR, CSTAR, and MASK MSRs

```
windbg: rdmsr c0000082
```

系统调用API: KiSystemCall64

离内核模块的基地址一定会超过4GB (偏移大于4G) 。

分析 ntsokrnl.exe

## 64位SSDT保护

```

.text:000000140408534 KiSystemServiceRepeat: ; CODE XREF: KiSystemCall64+90E1j
.text:000000140408534     lea     r10, KeServiceDescriptorTable ; 查表
.text:000000140408538     lea     r11, KeServiceDescriptorTableShadow
.text:000000140408542     test    dword ptr [rbx+78h], 128
.text:000000140408549     jz      short loc_14040855E
.text:00000014040854B     test    dword ptr [rbx+78h], 200000h
.text:000000140408552     jz      short loc_140408558
.text:000000140408554     lea     r11, KeServiceDescriptorTableFilter
.text:000000140408558 loc_140408558: ; CODE XREF: KiSystemCall64+3921j
.text:000000140408558     mov     r10, r11
.text:00000014040855E loc_14040855E: ; CODE XREF: KiSystemCall64+3891j
.text:00000014040855E     cmp     eax, [r10+rdi+10h]
.text:000000140408563     jnb     loc_140408A95
.text:000000140408569     mov     r10, [r10+rdi]
.text:00000014040856D     movsxd  r11, dword ptr [r10+rax*4]
.text:000000140408571     mov     rax, r11
.text:000000140408574     sar     r11, 4
.text:000000140408578     add     r10, r11
.text:00000014040857B     cmp     edi, 20h ; ' '
.text:00000014040857E     jnz     short loc_1404085D0
.text:000000140408580     mov     r11, [rbx+0F0h]
.text:000000140408587 KiSystemServiceGdiTebAccess: ; DATA XREF: KiSystemServiceHandler+D10
.text:000000140408587     cmp     dword ptr [r11+1740h], 0

```

## 回调函数 (callbacks)

内核函数提供API帮助完成API hook。

提供以下监控：

进程、线程创建监控

对象操作监控

模块监控

注册表监控

开机、关机监控

网络监控

磁盘监控

## API使用

使用 Ex 后缀的API，驱动必须带有签名，否则会报STATUS\_ACCESS\_DENIED --> 0xC0000022L 错误。PE格式中必须要由该字段信息。通过CFF工具将其关闭（选项头 --> DllCharacteristics --> Code Integrity Image（打勾））或者通过vs在项目属性中添加链接选项（/INTEGRITYCHECK）