Windows驱动开发学习记录-遍历内核已加载模块之二(使用ZwQuerySystemInformation)

原创

禁锢在时空之中的灵魂 于 2021-10-14 11:36:11 发布 102 收藏
分类专栏： Windows内核 文章标签： windows c++ 驱动程序

附另两种方法链接：

Windows驱动开发学习记录-遍历内核已加载模块之一(使用DriverSection)

Windows驱动开发学习记录-遍历内核已加载模块之三(使用 AuxKlib)

1.原型

```
NTSTATUS  ZwQuerySystemInformation(
        IN SYSTEM_INFORMATION_CLASS SystemInformationClass,
        OUT PVOID SystemInformation,
        IN ULONG SystemInformationLength,
        OUT PULONG ReturnLength);
```

- **SystemInformationClass** 查询的系统信息类型,之后给出。遍历模块为 SystemModuleInformation,值11
- **SystemInformation** 返回结果的缓冲区
- **SystemInformationLength** 第二个参数缓冲区的大小
- **ReturnLength** 实际返回的大小

使用时调用两次该函数，第一次SystemInformationLength传0,返回的ReturnLength为结果大小，再根据此大小分配内存空间，再次调用。

2.SYSTEM_INFORMATION_CLASS类型

```
typedef enum _SYSTEM_INFORMATION_CLASS
{
        SystemBasicInformation,        //  0
        SystemProcessorInformation,        //  1
        SystemPerformanceInformation,        //  2
        SystemTimeOfDayInformation,        //  3
        SystemPathInformation,        //  4
        SystemProcessInformation,                //5
        SystemCallCountInformation,        //  6
        SystemDeviceInformation,        //  7
```

```
    SystemProcessorPerformanceInformation,        //  8
    SystemFlagsInformation,        //  9
    SystemCallTimeInformation,        //  10
    SystemModuleInformation,        //  11
    SystemLocksInformation,        //  12
    SystemStackTraceInformation,        //  13
    SystemPagedPoolInformation,        //  14
    SystemNonPagedPoolInformation,        //  15
    SystemHandleInformation,        //  16
    SystemObjectInformation,        //  17
    SystemPageFileInformation,        //  18
    SystemVdmInstemulInformation,        //  19
    SystemVdmBopInformation,        //  20
    SystemFileCacheInformation,        //  21
    SystemPoolTagInformation,        //  22
    SystemInterruptInformation,        //  23
    SystemDpcBehaviorInformation,        //  24
    SystemFullMemoryInformation,        //  25
    SystemLoadGdiDriverInformation,        //  26
    SystemUnloadGdiDriverInformation,        //  27
    SystemTimeAdjustmentInformation,        //  28
    SystemSummaryMemoryInformation,        //  29
    SystemMirrorMemoryInformation,        //  30
    SystemPerformanceTraceInformation,        //  31
    SystemObsolete0,        //  32
    SystemExceptionInformation,        //  33
    SystemCrashDumpStateInformation,        //  34
    SystemKernelDebuggerInformation,        //  35
    SystemContextSwitchInformation,        //  36
    SystemRegistryQuotaInformation,        //  37
    SystemExtendServiceTableInformation,        //  38
    SystemPrioritySeperation,        //  39
    SystemVerifierAddDriverInformation,        //  40
    SystemVerifierRemoveDriverInformation,        //  41
    SystemProcessorIdleInformation,        //  42
    SystemLegacyDriverInformation,        //  43
    SystemCurrentTimeZoneInformation,        //  44
    SystemLookasideInformation,        //  45
    SystemTimeSlipNotification,        //  46
    SystemSessionCreate,        //  47
    SystemSessionDetach,        //  48
    SystemSessionInformation,        //  49
    SystemRangeStartInformation,        //  50
    SystemVerifierInformation,        //  51
    SystemVerifierThunkExtend,        //  52
    SystemSessionProcessInformation,        //  53
    SystemLoadGdiDriverInSystemSpace,        //  54
    SystemNumaProcessorMap,        //  55
    SystemPrefetcherInformation,        //  56
    SystemExtendedProcessInformation,        //  57
    SystemRecommendedSharedDataAlignment,        //  58
    SystemComPlusPackage,        //  59
    SystemNumaAvailableMemory,        //  60
    SystemProcessorPowerInformation,        //  61
    SystemEmulationBasicInformation,        //  62
    SystemEmulationProcessorInformation,        //  63
    SystemExtendedHandleInformation,        //  64
    SystemLostDelayedWriteInformation,        //  65
    SystemBigPoolInformation,        //  66
    SystemSessionPoolTagInformation,        //  67
```

```
        SystemSessionMappedViewInformation,        //  68
        SystemHotpatchInformation,        //  69
        SystemObjectSecurityMode,        //  70
        SystemWatchdogTimerHandler,        //  71
        SystemWatchdogTimerInformation,        //  72
        SystemLogicalProcessorInformation,        //  73
        SystemWow64SharedInformation,        //  74
        SystemRegisterFirmwareTableInformationHandler,        //  75
        SystemFirmwareTableInformation,        //  76
        SystemModuleInformationEx,        //  77
        SystemVerifierTriageInformation,        //  78
        SystemSuperfetchInformation,        //  79
        SystemMemoryListInformation,        //  80
        SystemFileCacheInformationEx,        //  81
        MaxSystemInfoClass                        //82

} SYSTEM_INFORMATION_CLASS;
```

我们使用的是第11号功能SystemModuleInformation。

3.返回数据类型 _SYSTEM_MODULE_INFORMATION

64位环境下和32位环境下结构体不一样。

```
typedef struct _SYSTEM_MODULE_INFORMATION_ENTRY64 {
        ULONG Reserved[4];
        PVOID Base;
        ULONG Size;
        ULONG Flags;
        USHORT Index;
        USHORT Unknown;
        USHORT LoadCount;
        USHORT ModuleNameOffset;
        CHAR ImageName[256];
} SYSTEM_MODULE_INFORMATION_ENTRY64, *PSYSTEM_MODULE_INFORMATION_ENTRY64;


typedef struct _SYSTEM_MODULE_INFORMATION_ENTRY32 {
        ULONG Reserved[2];
        PVOID Base;
        ULONG Size;
        ULONG Flags;
        USHORT Index;
        USHORT Unknown;
        USHORT LoadCount;
        USHORT ModuleNameOffset;
        CHAR ImageName[256];
} SYSTEM_MODULE_INFORMATION_ENTRY32, * PSYSTEM_MODULE_INFORMATION_ENTRY32;

typedef struct _SYSTEM_MODULE_INFORMATION
{
        ULONG Count;//内核中以加载的模块的个数
#ifdef _AMD64_
        SYSTEM_MODULE_INFORMATION_ENTRY64 Module[1];
#else
        SYSTEM_MODULE_INFORMATION_ENTRY32 Module[1];
#endif

} SYSTEM_MODULE_INFORMATION, * PSYSTEM_MODULE_INFORMATION;
```

4.实现

- .h文件

```
typedef enum
{
	MmTagTypeZQSI = 'ISQZ',		//ZwQuerySystemInformation
}MmTagType;

typedef enum _SYSTEM_INFORMATION_CLASS
{
	SystemModuleInformation =  11
} SYSTEM_INFORMATION_CLASS;

typedef struct _SYSTEM_MODULE_INFORMATION_ENTRY64 {
	ULONG Reserved[4];
	PVOID Base;
	ULONG Size;
	ULONG Flags;
	USHORT Index;
	USHORT Unknown;
	USHORT LoadCount;
	USHORT ModuleNameOffset;
	CHAR ImageName[256];
} SYSTEM_MODULE_INFORMATION_ENTRY64, *PSYSTEM_MODULE_INFORMATION_ENTRY64;


typedef struct _SYSTEM_MODULE_INFORMATION_ENTRY32 {
	ULONG Reserved[2];
	PVOID Base;
	ULONG Size;
	ULONG Flags;
	USHORT Index;
	USHORT Unknown;
	USHORT LoadCount;
	USHORT ModuleNameOffset;
	CHAR ImageName[256];
} SYSTEM_MODULE_INFORMATION_ENTRY32, * PSYSTEM_MODULE_INFORMATION_ENTRY32;

typedef struct _SYSTEM_MODULE_INFORMATION
{
	ULONG Count;//内核中以加载的模块的个数
#ifdef _AMD64_
	SYSTEM_MODULE_INFORMATION_ENTRY64 Module[1];
#else
	SYSTEM_MODULE_INFORMATION_ENTRY32 Module[1];
#endif

} SYSTEM_MODULE_INFORMATION, * PSYSTEM_MODULE_INFORMATION;
```

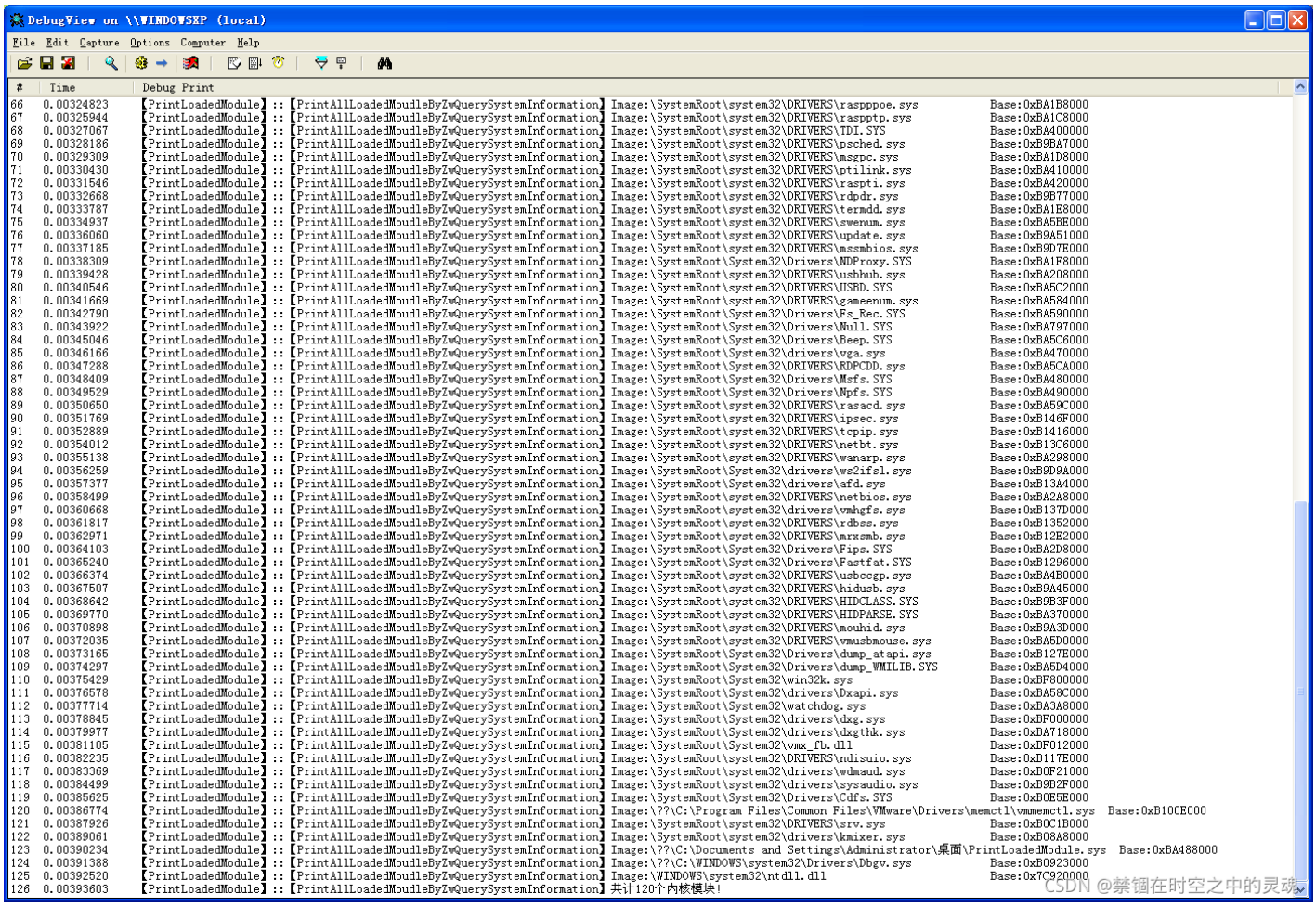
- .C文件

```
NTSTATUS PrintAllLoadedMoudleByZwQuerySystemInformation()
{
	ULONG ulInfoLength = 0;
	PVOID pBuffer = NULL;
	NTSTATUS ntStatus = STATUS_UNSUCCESSFUL;
	KDPRINT("【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Enter.....\r\n");
	do
	{
		ntStatus = ZwQuerySystemInformation(SystemModuleInformation,
```

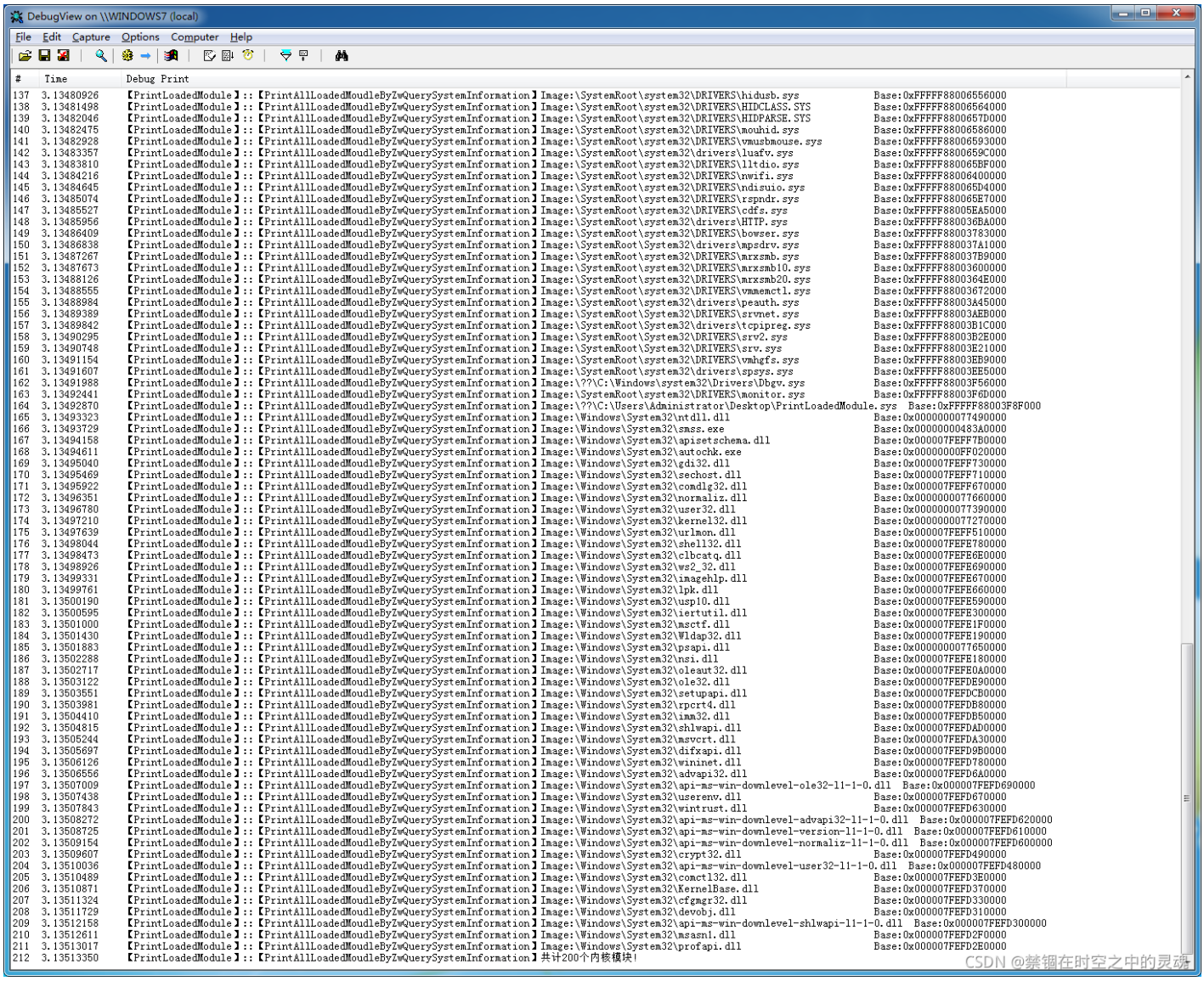
```
                        NULL,
                        NULL,
                        &ulInfoLength);
                if ((ntStatus == STATUS_INFO_LENGTH_MISMATCH))
                {
                        pBuffer = ExAllocatePoolWithTag(PagedPool, ulInfoLength, MmTagTypeZQSI);
                        if (pBuffer == NULL)
                        {
                                KDPRINT("【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInforma
                                break;
                        }
                        ntStatus = ZwQuerySystemInformation(SystemModuleInformation,
                                pBuffer,
                                ulInfoLength,
                                &ulInfoLength);
                        if (!NT_SUCCESS(ntStatus))
                        {
                                KDPRINT("【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInforma
                                break;
                        }

                        PSYSTEM_MODULE_INFORMATION pModuleInformation = (PSYSTEM_MODULE_INFORMATION)pBuffer
                        if(pModuleInformation)
                        {
                                for (ULONG i = 0; i < pModuleInformation->Count; i++)
                                {
                                        KDPRINT("【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySyste
                                                pModuleInformation->Module[i].ImageName, pModuleInformation
                                }
                                KDPRINT("【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInforma
                        }

                        ntStatus = STATUS_SUCCESS;
                }
        } while (false);

        if (pBuffer)
        {
                ExFreePoolWithTag(pBuffer, MmTagTypeZQSI);
        }

        return ntStatus;
}

NTSTATUS  DriverEntry(PDRIVER_OBJECT pDriverObject,
        PUNICODE_STRING pRegistryPath)
{
        UNREFERENCED_PARAMETER(pDriverObject);
        UNREFERENCED_PARAMETER(pRegistryPath);
        PrintAllLoadedMoudleByZwQuerySystemInformation();
        return STATUS_SUCCESS;
}
```

5.运行结果

XP 32位：


DebugView on \\WINDOWSXP (local)
File Edit Capture Options Computer Help
Time Debug Print
66 0.00324823 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\raspppoe.sys Base:0xBA1B8000
67 0.00325944 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\raspptp.sys Base:0xBA1C8000
68 0.00327067 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\TDI.SYS Base:0xBA400000
69 0.00328186 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\psched.sys Base:0xB9BA7000
70 0.00329309 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\msgpc.sys Base:0xBA1D8000
71 0.00330430 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\ptilink.sys Base:0xBA410000
72 0.00331546 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\raspti.sys Base:0xBA420000
73 0.00332668 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\rdpdr.sys Base:0xB9B77000
74 0.00333787 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\termdd.sys Base:0xBA1E8000
75 0.00334937 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\swenum.sys Base:0xBA5BE000
76 0.00336060 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\update.sys Base:0xB9A51000
77 0.00337185 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\mssmbios.sys Base:0xB9D7E000
78 0.00338309 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\Drivers\NDProxy.SYS Base:0xBA1F8000
79 0.00339428 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\usbhub.sys Base:0xBA208000
80 0.00340546 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\USBD.SYS Base:0xBA5C2000
81 0.00341669 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\gameenum.sys Base:0xBA584000
82 0.00342790 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\Drivers\Fs_Rec.SYS Base:0xBA590000
83 0.00343922 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\Drivers\Null.SYS Base:0xBA797000
84 0.00345046 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\Drivers\Beep.SYS Base:0xBA5C6000
85 0.00346166 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\drivers\vga.sys Base:0xBA470000
86 0.00347288 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\DRIVERS\RDPCDD.sys Base:0xBA5CA000
87 0.00348409 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\Drivers\Msfs.SYS Base:0xBA480000
88 0.00349529 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\Drivers\Npfs.SYS Base:0xBA490000
89 0.00350650 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\rasacd.sys Base:0xBA59C000
90 0.00351769 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\ipsec.sys Base:0xB146F000
91 0.00352889 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\tcpip.sys Base:0xB1416000
92 0.00354012 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\netbt.sys Base:0xB13C6000
93 0.00355138 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\wanarp.sys Base:0xBA298000
94 0.00356259 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\drivers\ws2ifsl.sys Base:0xB9D9A000
95 0.00357377 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\drivers\afd.sys Base:0xB13A4000
96 0.00358499 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\netbios.sys Base:0xBA2A8000
97 0.00360668 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\drivers\vmhgfs.sys Base:0xB137D000
98 0.00361817 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\rdbss.sys Base:0xB1352000
99 0.00362971 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\mrxsmb.sys Base:0xB12E2000
100 0.00364103 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\Drivers\Fips.SYS Base:0xBA2D8000
101 0.00365240 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\Drivers\Fastfat.SYS Base:0xB1296000
102 0.00366374 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\usbccgp.sys Base:0xBA4B0000
103 0.00367507 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\hidusb.sys Base:0xB9A45000
104 0.00368642 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\HIDCLASS.SYS Base:0xB9B3F000
105 0.00369770 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\HIDPARSE.SYS Base:0xBA370000
106 0.00370898 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\mouhid.sys Base:0xB9A3D000
107 0.00372035 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\vmusbmouse.sys Base:0xBA5D0000
108 0.00373165 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\Drivers\dump_atapi.sys Base:0xB127E000
109 0.00374297 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\Drivers\dump_WMILIB.SYS Base:0xBA5D4000
110 0.00375429 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\win32k.sys Base:0xBF800000
111 0.00376578 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\Dxapi.sys Base:0xBA58C000
112 0.00377714 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\watchdog.sys Base:0xBA3A8000
113 0.00378845 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\drivers\dxg.sys Base:0xBF000000
114 0.00379977 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\drivers\dxgthk.sys Base:0xBA718000
115 0.00381105 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\vmx_fb.dll Base:0xBF012000
116 0.00382235 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\ndisuio.sys Base:0xB117E000
117 0.00383369 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\drivers\wdmaud.sys Base:0xB0F21000
118 0.00384499 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\drivers\sysaudio.sys Base:0xB9B2F000
119 0.00385625 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\Drivers\Cdfs.SYS Base:0xB0E5E000
120 0.00386774 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\??\C:\Program Files\Common Files\VMware\Drivers\memctl\vmmemctl.sys Base:0xB100E000
121 0.00387926 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\srv.sys Base:0xB0C1B000
122 0.00389061 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\drivers\kmixer.sys Base:0xB08A8000
123 0.00390234 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\??\C:\Documents and Settings\Administrator\桌面\PrintLoadedModule.sys Base:0xBA488000
124 0.00391388 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\??\C:\WINDOWS\system32\Drivers\Dbgv.sys Base:0xB0923000
125 0.00392520 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\WINDOWS\system32\ntdll.dll Base:0x7C920000
126 0.00393603 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】共计120个内核模块!
CSDN @禁锢在时空之中的灵魂

Win7 64位:


DebugView on \\WINDOWS7 (local)
File Edit Capture Options Computer Help
Time Debug Print
137 3.13480926 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\hidusb.sys Base:0xFFFFF88006556000
138 3.13481498 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\HIDCLASS.SYS Base:0xFFFFF88006564000
139 3.13482046 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\HIDPARSE.SYS Base:0xFFFFF880065D000
140 3.13482475 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\mouhid.sys Base:0xFFFFF88006586000
141 3.13482928 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\vmusbmouse.sys Base:0xFFFFF88006593000
142 3.13483357 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\drivers\luafv.sys Base:0xFFFFF8800659C000
143 3.13483810 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\lltdio.sys Base:0xFFFFF880065BF000
144 3.13484216 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\nwifi.sys Base:0xFFFFF88006400000
145 3.13484645 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\ndisuio.sys Base:0xFFFFF880065D4000
146 3.13485074 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\rspndr.sys Base:0xFFFFF880065E7000
147 3.13485527 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\cdfs.sys Base:0xFFFFF88005EA5000
148 3.13485956 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\drivers\HTTP.sys Base:0xFFFFF880036BA000
149 3.13486409 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\bowser.sys Base:0xFFFFF88003783000
150 3.13486838 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\drivers\mpsdrv.sys Base:0xFFFFF880037A1000
151 3.13487267 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\mrxsmb.sys Base:0xFFFFF880037B9000
152 3.13487673 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\mrxsmb10.sys Base:0xFFFFF88003600000
153 3.13488126 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\mrxsmb20.sys Base:0xFFFFF88003640E000
154 3.13488555 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\vmmemctl.sys Base:0xFFFFF88003672000
155 3.13488984 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\drivers\peauth.sys Base:0xFFFFF88003A45000
156 3.13489389 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\DRIVERS\srvnet.sys Base:0xFFFFF88003AEB000
157 3.13489842 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\drivers\tcpipreg.sys Base:0xFFFFF88003B1C000
158 3.13490295 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\DRIVERS\srv2.sys Base:0xFFFFF88003B2E000
159 3.13490748 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\System32\DRIVERS\srv.sys Base:0xFFFFF88003E21000
160 3.13491154 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\vmhgfs.sys Base:0xFFFFF88003EB9000
161 3.13491607 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\drivers\spsys.sys Base:0xFFFFF88003EE5000
162 3.13491988 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\??\C:\Windows\system32\Drivers\Dbgv.sys Base:0xFFFFF88003F56000
163 3.13492441 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\SystemRoot\system32\DRIVERS\monitor.sys Base:0xFFFFF88003F6D000
164 3.13492870 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\??\C:\Users\Administrator\Desktop\PrintLoadedModule.sys Base:0xFFFFF88003F8F000
165 3.13493323 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\ntdll.dll Base:0x0000000077490000
166 3.13493729 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\smss.exe Base:0x00000000483A0000
167 3.13494158 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\apisetschema.dll Base:0x000007FEFF7B0000
168 3.13494611 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\autochk.exe Base:0x00000000FF020000
169 3.13495040 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\gdi32.dll Base:0x000007FEFF730000
170 3.13495469 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\sechost.dll Base:0x000007FEFF710000
171 3.13495922 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\comdlg32.dll Base:0x000007FEFF670000
172 3.13496351 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\normaliz.dll Base:0x0000000077660000
173 3.13496780 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\user32.dll Base:0x0000000077390000
174 3.13497210 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\kernel32.dll Base:0x0000000077270000
175 3.13497639 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\urlmon.dll Base:0x000007FEFF510000
176 3.13498044 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\shell32.dll Base:0x000007FEFE780000
177 3.13498473 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\clbcatq.dll Base:0x000007FEFE6E0000
178 3.13498926 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\ws2_32.dll Base:0x000007FEFE690000
179 3.13499331 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\imagehlp.dll Base:0x000007FEFE670000
180 3.13499761 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\lpk.dll Base:0x000007FEFE660000
181 3.13500190 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\usp10.dll Base:0x000007FEFE590000
182 3.13500595 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\iertutil.dll Base:0x000007FEFE300000
183 3.13501000 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\msctf.dll Base:0x000007FEFE1F0000
184 3.13501430 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\Wldap32.dll Base:0x000007FEFE190000
185 3.13501883 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\psapi.dll Base:0x0000000077650000
186 3.13502288 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\nsi.dll Base:0x000007FEFE180000
187 3.13502717 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\oleaut32.dll Base:0x000007FEFE0A0000
188 3.13503122 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\ole32.dll Base:0x000007FEFDE90000
189 3.13503551 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\setupapi.dll Base:0x000007FEFDCB0000
190 3.13503981 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\rpcrt4.dll Base:0x000007FEFDB80000
191 3.13504410 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\imm32.dll Base:0x000007FEFDB50000
192 3.13504815 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\shlwapi.dll Base:0x000007FEFDAD0000
193 3.13505244 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\msvcrt.dll Base:0x000007FEFDA30000
194 3.13505697 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\difxapi.dll Base:0x000007FEFD9B0000
195 3.13506126 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\wininet.dll Base:0x000007FEFD780000
196 3.13506556 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\advapi32.dll Base:0x000007FEFD6A0000
197 3.13507009 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\api-ms-win-downlevel-ole32-l1-1-0.dll Base:0x000007FEFD690000
198 3.13507438 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\userenv.dll Base:0x000007FEFD670000
199 3.13507843 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\wintrust.dll Base:0x000007FEFD630000
200 3.13508272 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\api-ms-win-downlevel-advapi32-l1-1-0.dll Base:0x000007FEFD620000
201 3.13508725 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\api-ms-win-downlevel-version-l1-1-0.dll Base:0x000007FEFD610000
202 3.13509154 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\api-ms-win-downlevel-normaliz-l1-1-0.dll Base:0x000007FEFD600000
203 3.13509607 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\crypt32.dll Base:0x000007FEFD490000
204 3.13510036 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\api-ms-win-downlevel-user32-l1-1-0.dll Base:0x000007FEFD480000
205 3.13510489 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\comctl32.dll Base:0x000007FEFD3E0000
206 3.13510871 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\KernelBase.dll Base:0x000007FEFD370000
207 3.13511324 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\cfgmgr32.dll Base:0x000007FEFD330000
208 3.13511729 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\devobj.dll Base:0x000007FEFD310000
209 3.13512158 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\api-ms-win-downlevel-shlwapi-l1-1-0.dll Base:0x000007FEFD300000
210 3.13512611 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\msasn1.dll Base:0x000007FEFD2F0000
211 3.13513017 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】Image:\Windows\System32\profapi.dll Base:0x000007FEFD2E0000
212 3.13513350 【PrintLoadedModule】::【PrintAllLoadedMoudleByZwQuerySystemInformation】共计200个内核模块!
CSDN @禁锢在时空之中的灵魂