# HookPort.sys分析报告

目录

[HookPort.sys分析报告 1](#_Toc431896910)

[一、 驱动入口DriverEntry 2](#_Toc431896911)

[1.1 检测加载者是否为Ntos 2](#_Toc431896912)

## 驱动入口DriverEntry

### 1.1 检测加载者是否为Ntos

顺带保存IopLoadDriver

### 挂钩函数索引

SDTIndexArray[000] = ZwCreateKeyIndex;

SDTIndexArray[001] = ZwQueryValueKeyIndex;

SDTIndexArray[002] = ZwDeleteKeyIndex;

SDTIndexArray[003] = ZwDeleteValueKeyIndex;

SDTIndexArray[004] = ZwRenameKeyIndex;

SDTIndexArray[005] = ZwReplaceKeyIndex;

SDTIndexArray[006] = ZwRestoreKeyIndex;

SDTIndexArray[007] = ZwSetValueKeyIndex;

SDTIndexArray[008] = ZwCreateFileIndex;

SDTIndexArray[009] = ZwFsControlFileIndex;

SDTIndexArray[010] = ZwSetInformationFileIndex;

SDTIndexArray[011] = ZwWriteFileIndex;

SDTIndexArray[012] = ??

SDTIndexArray[013] = ZwCreateProcessIndex;

SDTIndexArray[014] = ZwCreateProcessExIndex;

SDTIndexArray[015] = ZwCreateUserProcessIndex;

SDTIndexArray[016] = ZwCreateThreadIndex;

SDTIndexArray[017] = ZwOpenThreadIndex;

SDTIndexArray[018] = ZwDeleteFileIndex;

SDTIndexArray[019] = ZwOpenFileIndex;

SDTIndexArray[020] = ZwReadVirtualMemoryIndex;

SDTIndexArray[021] = ZwTerminateProcessIndex;

SDTIndexArray[022] = ZwQueueApcThreadIndex;

SDTIndexArray[023] = ZwSetContextThreadIndex;

SDTIndexArray[024] = ZwSetInformationThreadIndex;

SDTIndexArray[025] = ZwProtectVirtualMemoryIndex;

SDTIndexArray[026] = ZwWriteVirtualMemoryIndex;

SDTIndexArray[027] = ZwAdjustGroupsTokenIndex;

SDTIndexArray[028] = ZwAdjustPrivilegesTokenIndex;

SDTIndexArray[029] = ZwRequestWaitReplyPortIndex;

SDTIndexArray[030] = ZwCreateSectionIndex;

SDTIndexArray[031] = ZwOpenSectionIndex;

SDTIndexArray[032] = ZwCreateSymbolicLinkObjectIndex;

SDTIndexArray[033] = ZwOpenSymbolicLinkObjectIndex;

SDTIndexArray[034] = ZwLoadDriverIndex;

SDTIndexArray[035] = ZwQuerySystemInformationIndex;

SDTIndexArray[036] = ZwSetSystemInformationIndex;

SDTIndexArray[037] = ZwSetSystemTimeIndex;

SDTIndexArray[038] = ZwSystemDebugControlIndex;

SDTIndexArray[039] = ZwUserBuildHwndListIndex;

SDTIndexArray[040] = ZwUserQueryWindowIndex;

SDTIndexArray[041] = ZwUserFindWindowExIndex;

SDTIndexArray[042] = ZwUserWindowFromPointIndex;

SDTIndexArray[043] = ZwUserMessageCallIndex;

SDTIndexArray[044] = ZwUserPostMessageIndex;

SDTIndexArray[045] = ZwUserSetWindowsHookExIndex;

SDTIndexArray[046] = ZwUserPostThreadMessageIndex;

SDTIndexArray[047] = ZwOpenProcessIndex;

SDTIndexArray[048] = ZwDeviceIoControlFileIndex;

SDTIndexArray[049] = ZwUserSetParentIndex;

SDTIndexArray[050] = ZwOpenKeyIndex;

SDTIndexArray[051] = ZwDuplicateObjectIndex;

SDTIndexArray[052] = ZwResumeThreadIndex;

SDTIndexArray[053] = ZwUserChildWindowFromPointExIndex;

SDTIndexArray[054] = ZwUserDestroyWindowIndex;

SDTIndexArray[055] = ZwUserInternalGetWindowTextIndex;

SDTIndexArray[056] = ZwUserMoveWindowIndex;

SDTIndexArray[057] = ZwUserRealChildWindowFromPointIndex;

SDTIndexArray[058] = ZwUserSetInformationThreadIndex;

SDTIndexArray[059] = ZwUserSetInternalWindowPosIndex;

SDTIndexArray[060] = ZwUserSetWindowLongIndex;

SDTIndexArray[061] = ZwUserSetWindowPlacementIndex;

SDTIndexArray[062] = ZwUserSetWindowPosIndex;

SDTIndexArray[063] = ZwUserSetWindowRgnIndex;

SDTIndexArray[064] = ZwUserShowWindowIndex;

SDTIndexArray[065] = ZwUserShowWindowAsyncIndex;

SDTIndexArray[066] = ZwQueryAttributesFileIndex;

SDTIndexArray[067] = ZwUserSendInputIndex;

SDTIndexArray[068] = ZwAlpcSendWaitReceivePortIndex;

SDTIndexArray[069] = 2000;

SDTIndexArray[070] = ZwUnmapViewOfSectionIndex;

SDTIndexArray[071] = ZwUserSetWinEventHookIndex;

SDTIndexArray[072] = ZwSetSecurityObjectIndex;

SDTIndexArray[073] = ZwUserCallHwndParamLockIndex;

SDTIndexArray[074] = ZwUserRegisterUserApiHookIndex;

SDTIndexArray[075] = 2000;

SDTIndexArray[076] = ZwUserRegisterWindowMessageIndex;

SDTIndexArray[077] = ZwUserCallNoParamIndex;

SDTIndexArray[078] = ZwAllocateVirtualMemoryIndex;

SDTIndexArray[079] = ZwUserCallOneParamIndex;

SDTIndexArray[080] = ZwCreateMutantIndex;

SDTIndexArray[081] = ZwOpenMutantIndex;

SDTIndexArray[082] = ZwVdmControlIndex;

SDTIndexArray[083] = ZwGetNextThreadIndex;

SDTIndexArray[084] = ZwGetNextProcessIndex;

SDTIndexArray[085] = ZwRequestPortIndex;

SDTIndexArray[086] = ZwFreeVirtualMemoryIndex;

SDTIndexArray[087] = ZwUserCallTwoParamIndex;

SDTIndexArray[088] = ZwUserCallHwndLockIndex;

SDTIndexArray[089] = ZwEnumerateValueKeyIndex;

SDTIndexArray[090] = ZwQueryKeyIndex;

SDTIndexArray[091] = ZwEnumerateKeyIndex;

SDTIndexArray[092] = ZwConnectPortIndex;

SDTIndexArray[093] = ZwSecureConnectPortIndex;

SDTIndexArray[094] = ZwAlpcConnectPortIndex;

SDTIndexArray[095] = ZwUserUnhookWindowsHookExIndex;

SDTIndexArray[096] = 2000;

SDTIndexArray[097] = 2000;

SDTIndexArray[098] = ZwSetTimerIndex;

SDTIndexArray[099] = ZwUserClipCursorIndex;

SDTIndexArray[100] = ZwSetInformationProcessIndex;

SDTIndexArray[101] = ZwUserGetKeyStateIndex;

SDTIndexArray[102] = ZwUserGetKeyboardStateIndex;

SDTIndexArray[103] = ZwUserGetAsyncKeyStateIndex;

SDTIndexArray[104] = ZwUserAttachThreadInputIndex;

SDTIndexArray[105] = ZwUserRegisterHotKeyIndex;

SDTIndexArray[106] = ZwUserRegisterRawInputDevicesIndex;

SDTIndexArray[107] = ZwGdiBitBltIndex;

SDTIndexArray[108] = ZwGdiStretchBltIndex;

SDTIndexArray[109] = ZwGdiMaskBltIndex;

SDTIndexArray[110] = ZwGdiPlgBltIndex;

SDTIndexArray[111] = ZwGdiTransparentBltIndex;

SDTIndexArray[112] = ZwGdiAlphaBlendIndex;

SDTIndexArray[113] = ZwGdiGetPixelIndex;

SDTIndexArray[114] = ZwMapViewOfSectionIndex;

SDTIndexArray[115] = ZwTerminateThreadIndex;

SDTIndexArray[116] = ZwAssignProcessToJobObjectIndex;

SDTIndexArray[117] = ZwTerminateJobObjectIndex;

SDTIndexArray[118] = ZwDebugActiveProcessIndex;

SDTIndexArray[119] = ZwSetInformationJobObjectIndex;

SDTIndexArray[120] = ZwUserGetRawInputBufferIndex;

SDTIndexArray[121] = ZwUserGetRawInputDataIndex;

SDTIndexArray[122] = 2000;

SDTIndexArray[123] = 2000;

SDTIndexArray[124] = ZwUserSetImeInfoExIndex;

SDTIndexArray[125] = ZwQueueApcThreadExIndex;

SDTIndexArray[126] = ZwAlpcConnectPortExIndex;

SDTIndexArray[127] = ZwMakeTemporaryObjectIndex;

SDTIndexArray[128] = ZwDisplayStringIndex;

SDTIndexArray[129] = 2000;

SDTIndexArray[130] = 2000;

SDTIndexArray[131] = ZwGdiOpenDCWIndex;

SDTIndexArray[132] = ZwGdiDeleteObjectAppIndex;

SDTIndexArray[133] = ZwUserBlockInputIndex;

SDTIndexArray[134] = 2000;

SDTIndexArray[135] = ZwContinueIndex;

SDTIndexArray[136] = dword\_1B8B0;

SDTIndexArray[137] = ZwAccessCheckAndAuditAlarmIndex;

SDTIndexArray[138] = ZwQueryInformationThreadIndex;

SDTIndexArray[139] = ZwQueryInformationProcessIndex;

SDTIndexArray[140] = ZwQueryIntervalProfileIndex;

SDTIndexArray[141] = ZwSetIntervalProfileIndex;

SDTIndexArray[142] = ZwCreateProfileIndex;

SDTIndexArray[143] = ZwUserLoadKeyboardLayoutExIndex;

SDTIndexArray[144] = ZwGdiAddFontResourceWIndex;

SDTIndexArray[145] = ZwGdiAddFontMemResourceExIndex;

SDTIndexArray[146] = ZwGdiAddRemoteFontToDCIndex;

SDTIndexArray[147] = ZwSuspendThreadIndex;

SDTIndexArray[148] = ZwSuspendProcessIndex;

SDTIndexArray[149] = ZwApphelpCacheControlIndex;

### 模块名加密算法

在ZwQuerySystemInformation => SystemModuleInformation得到模块文件名后，HookPort会将文件名经过加密与预先存储在程序中的加密过的模块名(一个4字节整数)作对比。

unsigned int \_\_declspec(naked) encode(char\* str)

{

\_asm

{

mov esi, [esp+4]

mov ebx, [esp+4]

mov edi, [esp+4]

xor al, al

loc\_17E37:

scasb

jnz short loc\_17E37

sub edi, ebx

cld

xor ecx, ecx

dec ecx

mov edx, ecx

loc\_17E42:

xor eax, eax

xor ebx, ebx

lodsb

xor al, cl

mov cl, ch

mov ch, dl

mov dl, dh

mov dh, 8

loc\_17E51:

shr bx, 1

rcr ax, 1

jnb short loc\_17E62

xor ax, 0xC6B4

xor bx, 0xCE96

loc\_17E62:

dec dh

jnz short loc\_17E51

xor ecx, eax

xor edx, ebx

dec edi

jnz short loc\_17E42

not edx

not ecx

mov eax, edx

rol eax, 10h

mov ax, cx

ret

}

}

穷举法得到：

0x07848DA1 knbdrv.sys 猎豹安全浏览器

0x42503C81 bd0001.sys 百度安全

0x4D71E020 tsfltmgr.sys qq管家

0xB8178767 kisknl.sys 金山毒霸