19th Asian Games Hangzhou 2022

杭州2022年第19届亚运会官方合作伙伴
Official Prestige Partner of the 19th Asian Games Hangzhou 2022

服务中心
Service Center

Sysmon驱动保护

——深度剖析进程隐藏的实现原理

www.dbappsecurity.com.cn　400-6059-110

目录
CONTENTS

什么是Sysmon

Sysmon是微软的一款轻量级的系统监控工具，它通过系统服务和驱动程序实现记录进程创建、文件访问以及网络信息的记录，并把相关的信息写入并展示在windows的日志事件里。主要用于记录和分析系统进程的活动来识别恶意或者异常活动。

事件ID 1：进程创建 - 提供有关新创建进程的扩展信息。
事件ID 2：进程更改文件创建时间 - 当进程显式修改文件创建时间时，会注册此事件。
事件ID 3：网络连接 - 记录机器上的TCP/UDP连接。
事件ID 4：Sysmon服务状态更改 - 报告Sysmon服务的状态（启动或停止）。
事件ID 5：进程终止 - 报告进程何时终止。
事件ID 6：驱动程序加载 - 提供有关在系统上加载驱动程序的信息。
事件ID 7：模块加载 - 当在特定进程中加载模块时，记录日志。
事件ID 8：CreateRemoteThread - 检测到进程在另一个进程中创建线程。
事件ID 9：RawAccessRead - 检测到进程从驱动器进行原始读取操作。
……

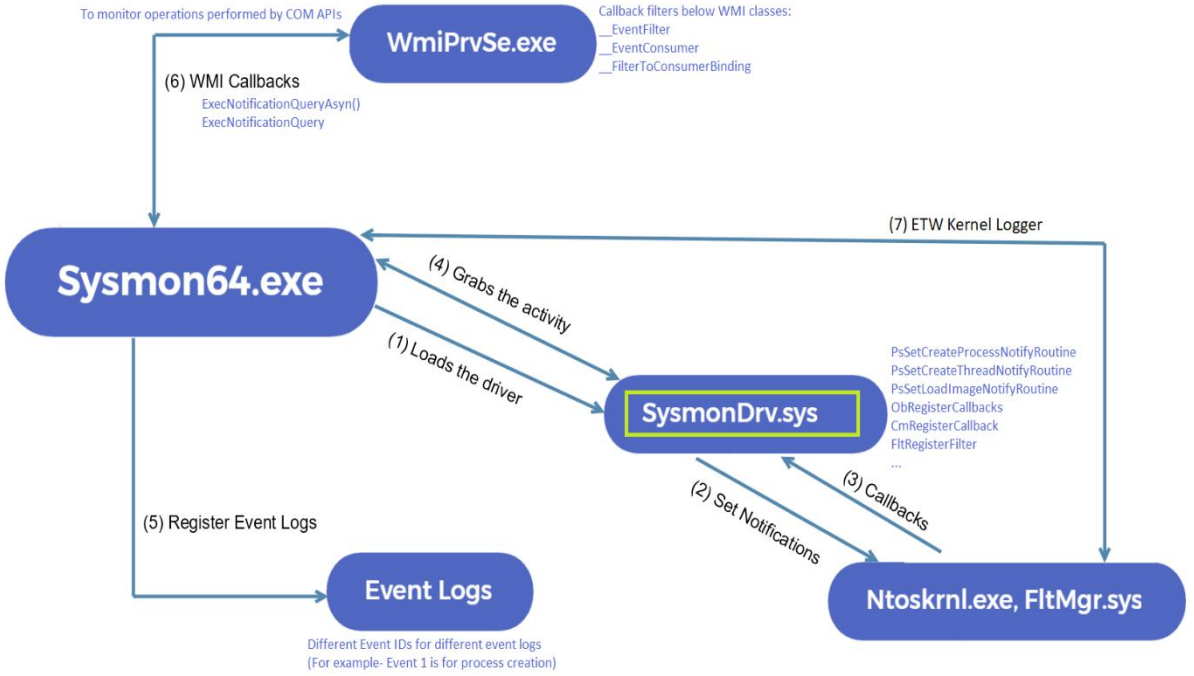
Sysmon的组成

SYSMON 主体可以分为三个部分

驱动程序：驱动程序 SysmonDrv.sys 在内核中利用回调函数搜集进程相关信息，并通过注册 minifilter 文件过滤驱动实现记录文件、注册表操作日志。

服务进程：注册为系统服务，利用ETW(Event Tracing for Windows) 实现对网络数据记录，负责将驱动捕获到的事件写入Windows日志。

管理工具：通过命令行实现安装、卸载Sysmon，以及修改、更新配置。



如何检测 Sysmon的存在

枚举进程

```
PS C:\Users\admin> Get-Process | Where-Object { $_.ProcessName -eq "Sysmon64" }
Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    381      16    15212      22308                3472   0 Sysmon64
    151      10     1932      12036       0.08     5604   2 Sysmon64
```

枚举服务

```
PS C:\Users\admin> Get-CimInstance win32_service -Filter "Description = 'System Monitor service'"

ProcessId Name      StartMode State   Status ExitCode
--------- ----      --------- -----   ------ --------
3472      Sysmon64 Auto      Running OK     0
```

minifilter altitude

```
PS C:\Users\admin> fltmc.exe

筛选器名称                     数字实例        高度           框架
------------------------------  -------------  ------------  -----
bindflt                             1       409800         0
SysmonDrv                           4       385201         0
WdFilter                            6       328010         0
storqosflt                          0       244000         0
wcifs                               0       189900         0
CldFlt                              0       180451         0
FileCrypt                           0       141100         0
luafv                               1       135000         0
npsvctrig                           1        46000         0
Wof                                 4        40700         0
FileInfo                            6        40500         0
```

如何检测 Sysmon的存在

枚举注册表	PS C:\Users\admin> ls HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels | Where-Object {$_.name -like "*sysmon*"} Hive: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels Name Property ---- -------- Microsoft-Windows-Sysmon/Operational OwningPublisher : {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Enabled : 1

注册表路径
HKLM\System\CurrentControlSet\Services\SysmonDrv\
HKLM\System\CurrentControlSet\Services\Sysmon\
HKCU\Software\Sysinternals\System Monitor\
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-Sysmon/

枚举文件	PS C:\Users\admin> ls C:\Windows | Where-Object {$_.Name -match "Sysmon*"} 目录: C:\Windows Mode LastWriteTime Length Name ---- ------------- ------ ---- -a---- 2022/11/28 17:37 4421432 Sysmon64.exe -a---- 2023/3/23 17:00 169848 SysmonDrv.sys

文件路径
C:\Windows\SysmonDrv.sys
C:\Windows\Sysmon*.exe
%UserSysmonPath%/Sysmon*.exe
%UserSysmonPath%/config.xml C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx

如何攻击Sysmon

攻击方案

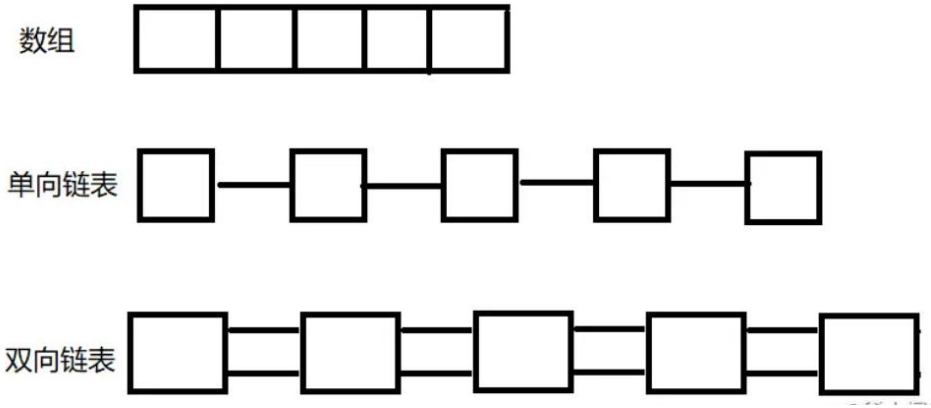
序号	攻击方法	检测方法
1	卸载Sysmon驱动程序	可通过 Sysmon 事件 ID 255（内部错误事件）、Windows 安全事件 ID 4672（特权服务审核事件） 检测到。
2	通过自定义驱动程序进行的攻击	可通过 Sysmon 事件 ID 6 （驱动程序已加载）检测到。
3	终止 Sysmon 服务进程	可通过 Sysmon 事件 ID 10 （进程访问事件）检测到。
4	修改注册表规则	可通过 Sysmon 事件 ID 16（服务配置更改）检测到。
5	Sysmon 服务内存补丁	可通过 Sysmon 事件 ID 10 （进程访问事件）检测到。
6	终止 Sysmon 进程	可通过 Sysmon 事件 ID 5（进程终止）检测到。

防御方案

序号	攻击方法	防御思路
1	卸载Sysmon驱动程序	1. 驱动文件隐藏、驱动Altitude隐藏 2. 驱动进程断链隐藏
2	通过自定义驱动程序进行的攻击	1. 驱动文件隐藏、驱动Altitude隐藏 2. 驱动进程断链隐藏
3	终止 Sysmon 服务	1. 驱动文件隐藏、驱动Altitude隐藏 2. 驱动进程断链隐藏
4	修改注册表规则	注册 Minifilter 过滤，隐藏注册表键值。
5	Sysmon 服务内存补丁	1. MiniFilter 过滤实现本地文件隐藏。 2. MiniFilter 过滤实现进程句柄表保护，避免进程被OpenProcess。 3. 基于 SDDL 语句的服务名称隐藏
6	终止 Sysmon 进程	1. MiniFilter 过滤实现本地文件隐藏。 2. MiniFilter 过滤实现进程句柄表保护，避免进程被OpenProcess。

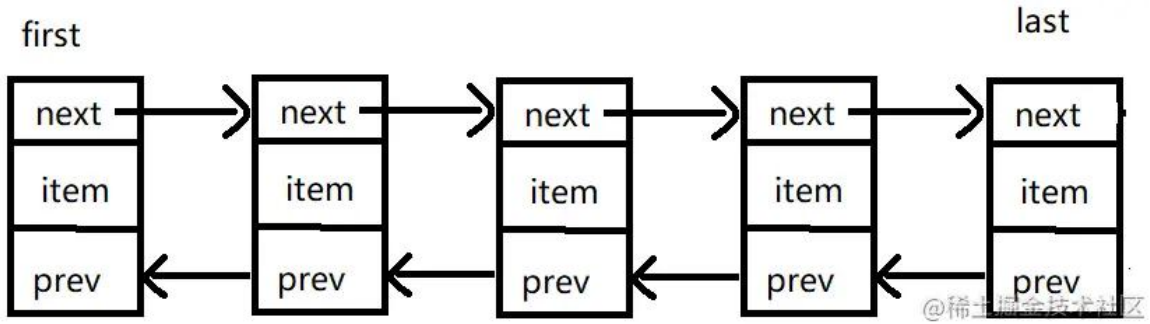
什么是双向链表

链表和数组一样也是数据结构之一，只不过因为链表中的数据“链接”在一起所以叫链表

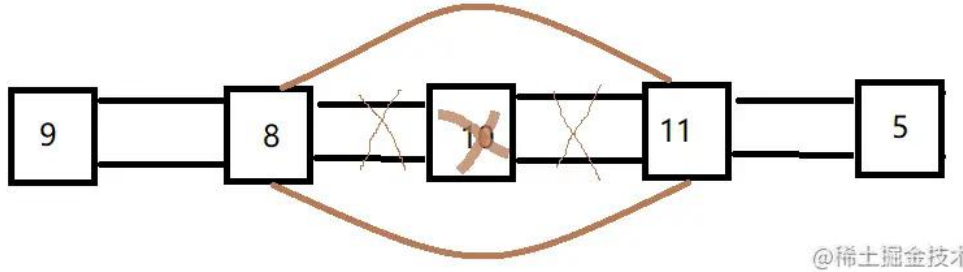


单向链表：只有一个方向的链表，比如前面的元素指向后面的元素），即只能前一个数据指向后一个数据。想要查询某个数据时，必须知道它前面的数据，也就是只能顺序查找。

双向链表：有两个方向的链表，即前一个元素指向后一个元素，后一个元素也指向前一个元素。



双向链表中每个结点都维护了两个指针，分别指向下一个结点和上一个结点。



进程隐藏


```
calc.exe    nt!_EPROCESS  0x00401000
               +0x000 Pcb              :
            _KPROCESS
               +0x438 ProcessLock      : _EX_PUSH_LOCK
               +0x440 UniqueProcessId  : Ptr64 Void
               +0x448 ActiveProcessLinks : _LIST_ENTRY  0x401448
                  +0x000 Flink            : Ptr64                0x401448    0x402448
下一个结构      _LIST_ENTRY
                  +0x008 Blink            : Ptr64                0x401450    …
上一个结构      _LIST_ENTRY
               +0x460 Flags2           :
            Uint4B
               …
               +0x5a8 ImageFileName    : [15]
            "calc.exe"
               …


Notepad.ex  nt!_EPROCESS  0x00402000
e
               +0x000 Pcb              :
            _KPROCESS
               +0x438 ProcessLock      : _EX_PUSH_LOCK
               +0x440 UniqueProcessId  : Ptr64 Void
               +0x448 ActiveProcessLinks : _LIST_ENTRY  0x402448
                  +0x000 Flink            : Ptr64                0x402448    0x403448
下一个结构      _LIST_ENTRY
                  +0x008 Blink            : Ptr64                0x402450    0x401448
上一个结构      _LIST_ENTRY
               +0x460 Flags2           :
            Uint4B
               …
               +0x5a8 ImageFileName    : [15]
            "notepad.exe"
               …


cmd.exe     nt!_EPROCESS  0x00403000
               +0x000 Pcb              :
            _KPROCESS
               +0x438 ProcessLock      : _EX_PUSH_LOCK
```

微软用 EPROCESS 结构体表示每一个进程，其中结构体里的成员 ActiveProcessLinks 把其所属的 EPROCESS 结构连接成双向链表，使得 ZwQuerysystemInformation函数可以沿着这条链表枚举系统中每一个存活的进程。

该链表除了用来记录进程以外，几乎没有其他用途，所以断开此链表并不会影响进程的执行和系统的正常工作，却能达到进程隐藏的目的

当一个新的进程创建时，父进程负责构造 EPROCESS 结构，

然后将 ActiveProcessLinks 插入全局内核变量 PsActiveProcessHead 链表中。

内核在进程创建时（PspCreateProcess）会插入链表：

InsertTailList(&PsActiveProcessHead,&Process->AvtiveProcessLinks);

在进程结束时（ PspExitProcess ）则会删除链表：

RemoveEntryList(&Process->ActiveProcessLinks);

手动修改链表

将进程的 Flink 修改为 cmd.exe 的 ActiveProcessLinks 地址；
将进程的 Blink 修改为 calc.exe 的 ActiveProcessLinks 地址；

```
eq 0x402000+448 0x403448
eq 0x402000+448+8 0x401448
```

进程隐藏 方法2

Windows 中每个进程都有对应的句柄（PID），
所有进程的句柄都保存在一张表里（PspCidTable 句柄表）
系统在创建一个新进程时，会将新进程的句柄复制到句柄中

通过遍历这个双向链表，可以把所有进程的句柄表连接起来

所以只要将目标进程的句柄从这个链表中删除，就可以实现隐藏进程句柄（PID）的效果

NextFreeTableEntry 字段被指向一个空闲句柄表的链表

当一个句柄被关闭并且对应的句柄表不再使用时，这个条目可以被加入到空闲链表中

当进程创建一个新的句柄时，Windows 会使用 NextFreeTableEntry 字段找到一个可用的句柄表项，并把新句柄的信息存储在那里。

```
typedef struct _HANDLE_TABLE_ENTRY {
    union {
        VOID* Object;
        ULONG_PTR Value;
    } u1;
    union {
        ULONG GrantedAccess;
        ULONG_PTR NextFreeTableEntry;
    } u2;
} HANDLE_TABLE_ENTRY, *PHANDLE_TABLE_ENTRY;
```

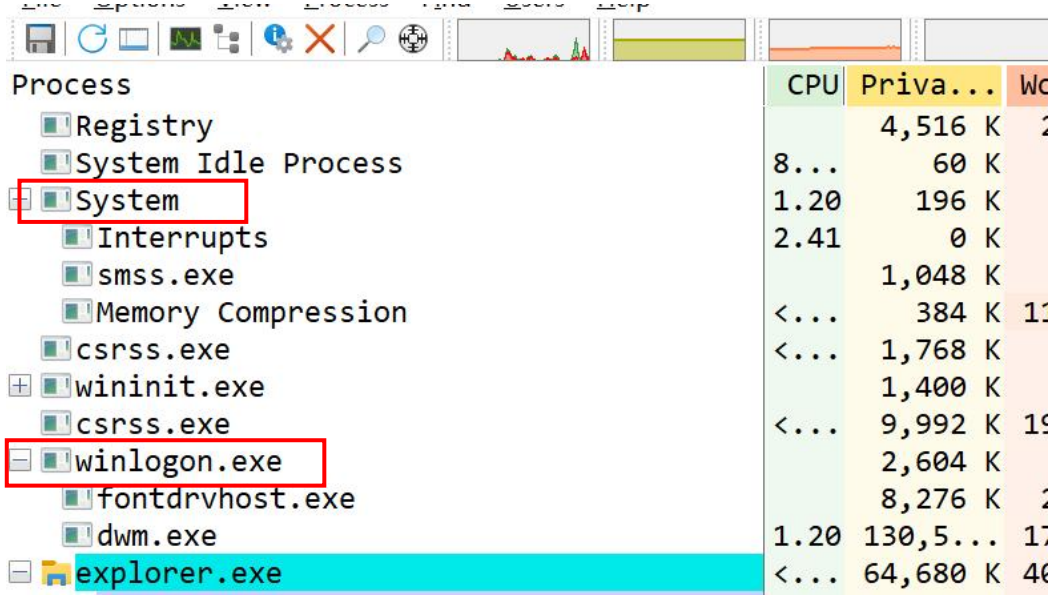
```
nt!_HANDLE_TABLE
   +0x000 NextHandleNeedingPool : Uint4B
   +0x004 ExtraInfoPages    : Int4B
   +0x008 TableCode         : Uint8B                    // 句柄表
   +0x010 QuotaProcess      : Ptr64 _EPROCESS           // 所属进程的EPROCESS
   +0x018 HandleTableList   : _LIST_ENTRY               // 句柄表的双向链表
   +0x028 UniqueProcessId   : Uint4B                    // 进程PID
   +0x02c Flags             : Uint4B
   +0x02c StrictFIFO        : Pos 0, 1 Bit
   +0x02c EnableHandleExceptions : Pos 1, 1 Bit
   +0x02c Rundown           : Pos 2, 1 Bit
   +0x02c Duplicated        : Pos 3, 1 Bit
   +0x02c RaiseUMExceptionOnInvalidHandleClose : Pos 4,
1 Bit
   +0x030 HandleContentionEvent : _EX_PUSH_LOCK
   +0x038 HandleTableLock   : _EX_PUSH_LOCK             // 句柄锁
   +0x040 FreeLists         : [1]
_HANDLE_TABLE_FREE_LIST
   +0x040 ActualEntry       : [32] UChar
   +0x060 DebugInfo         : Ptr64
_HANDLE_TRACE_DEBUG_INFO
```

如果 u1->Object 有效，则 u2 使用 GrantedAccess 为访问权限
如果 u1->Object == 0，则 u2 可能使用 NextFreeTableEntry 指向下一个可分配的句柄表项

```
HANDLE_TABLE_ENTRY HandleTableEntry
HandleTableEntry->u1.Object = 0;
HandleTableEntry->u2.NextFreeTableEntry = (ULONG_PTR)HandleTableEntry;
```

进程隐藏 方法3


```
nt!_EPROCESS
   +0x000 Pcb             : _KPROCESS
   +0x438 ProcessLock     : _EX_PUSH_LOCK
   +0x440 UniqueProcessId : Ptr64 Void                    // 进程 PID
   +0x448 ActiveProcessLinks : _LIST_ENTRY                // 进程链表
   ...
   +0x538 Win32WindowStation : Ptr64 Void
   +0x540 InheritedFromUniqueProcessId : Ptr64 Void       // 父进程 PID
   +0x548 OwnerProcessId  : Uint8B
   +0x550 Peb             : Ptr64 _PEB
   +0x558 Session         : Ptr64 _MM_SESSION_SPACE
```




```
.text:00000001402084B0
.text:00000001402084B0                                  public
PsGetProcessInheritedFromUniqueProcessId
.text:00000001402084B0
PsGetProcessInheritedFromUniqueProcessId proc near
.text:00000001402084B
0                                                       ; CODE
XREF: PsChargeProcessWakeCounter+1F↓p
.text:00000001402084B
0                                                       ; DATA
XREF: .pdata:00000001400C9780↑o
.text:00000001402084B0 48 8B 81 40 05       mov     rax, [rcx+540h]
.text:00000001402084B7 C3                     retn
.text:00000001402084B7
.text:00000001402084B7
PsGetProcessInheritedFromUniqueProcessId endp
```

PsGetProcessInheritedFromUniqueProcessId

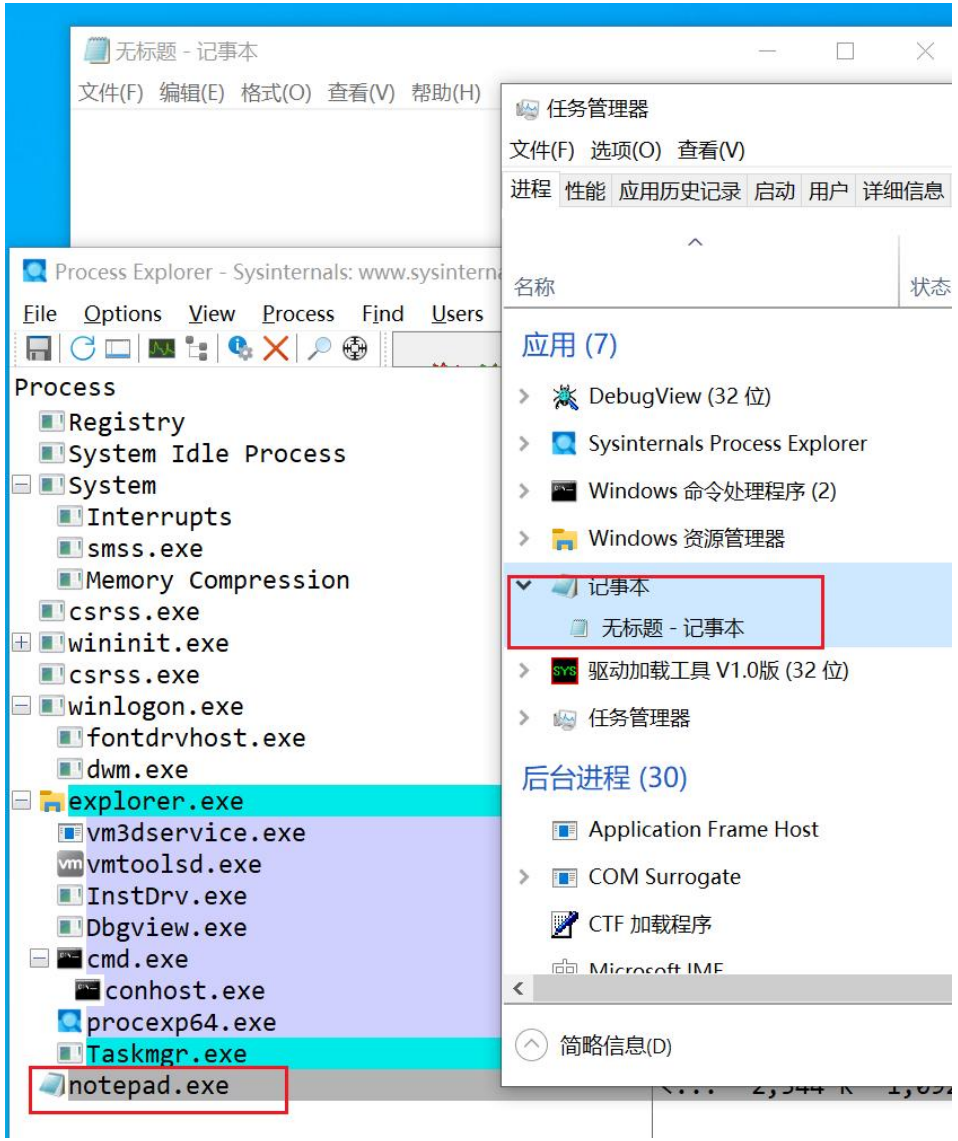
获取父进程PID的API
参数为EPROCESS结构指针

将 EPROCESS->InheritedFromUniqueProcessId 修改为 4 (System 进程)
将 EPROCESS->UniqueProcessId 修改为其它系统进程PID (例如 winlogon.exe)

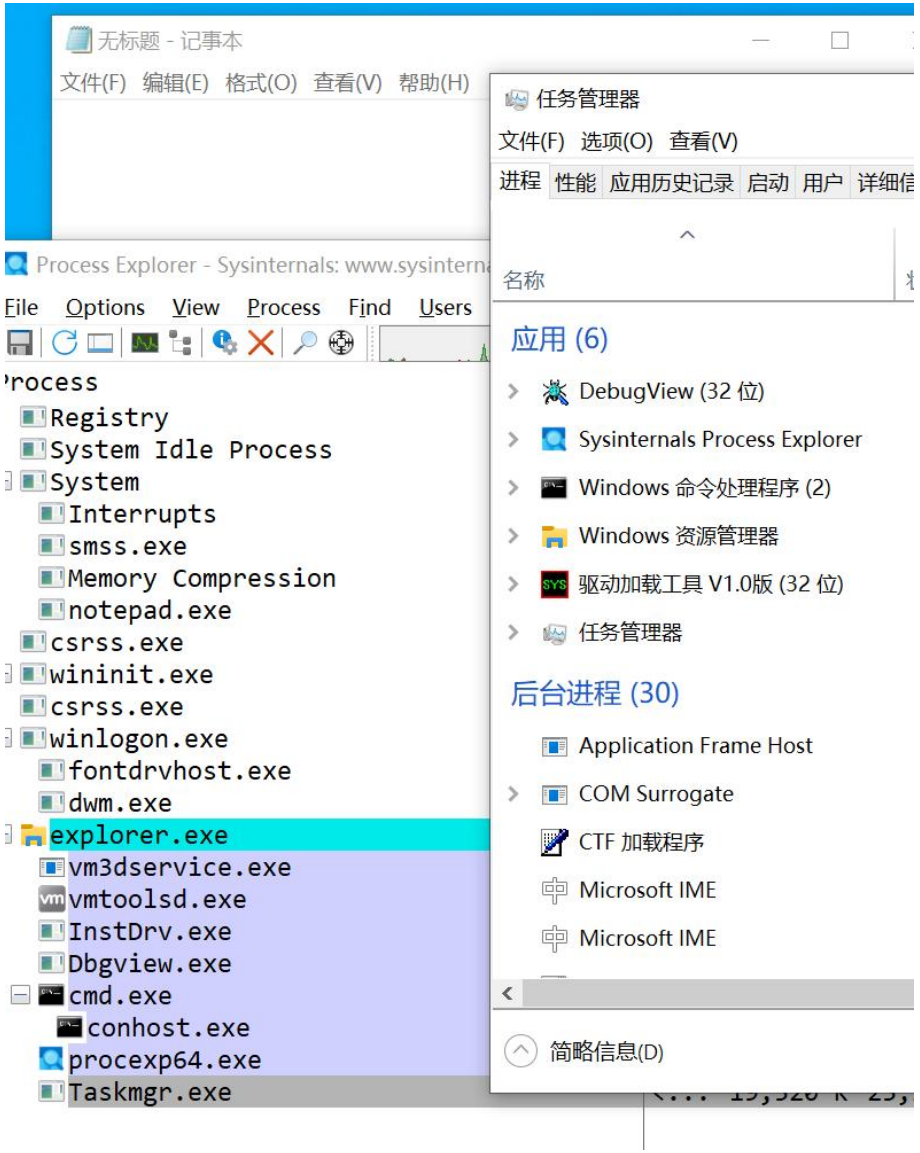
System下的系统进程很多都是隐藏不可见

进程隐藏 方法3

修改前



修改后



注册表管理API

API	描述
RegCreateKeyEx	用于创建新的注册表键，或打开现有的键。
RegOpenKeyEx	用于打开指定的注册表键。
RegCloseKey	用于关闭注册表键。当完成对键的所有操作后，必须关闭该键。
RegDeleteKey	用于删除注册表键。
RegDeleteValue	用于删除指定的注册表键的值。
RegSetValueEx	用于设置指定注册表键的值。
RegQueryValueEx	用于查询指定注册表键的值。
RegEnumKeyEx	用于枚举子键。它提供了读取注册表键的子键名称的功能。
RegEnumValue	用于枚举键值。它提供了读取注册表键的值的功能。
RegLoadKey	用于加载指定的注册表键。
RegUnLoadKey	用于卸载已加载的注册表键。
RegSaveKey	用于保存指定的注册表键及其子键和值。
RegRestoreKey	用于从磁盘文件恢复保存的注册表键及其子键和值。

minifilter 注册表过滤回调函数

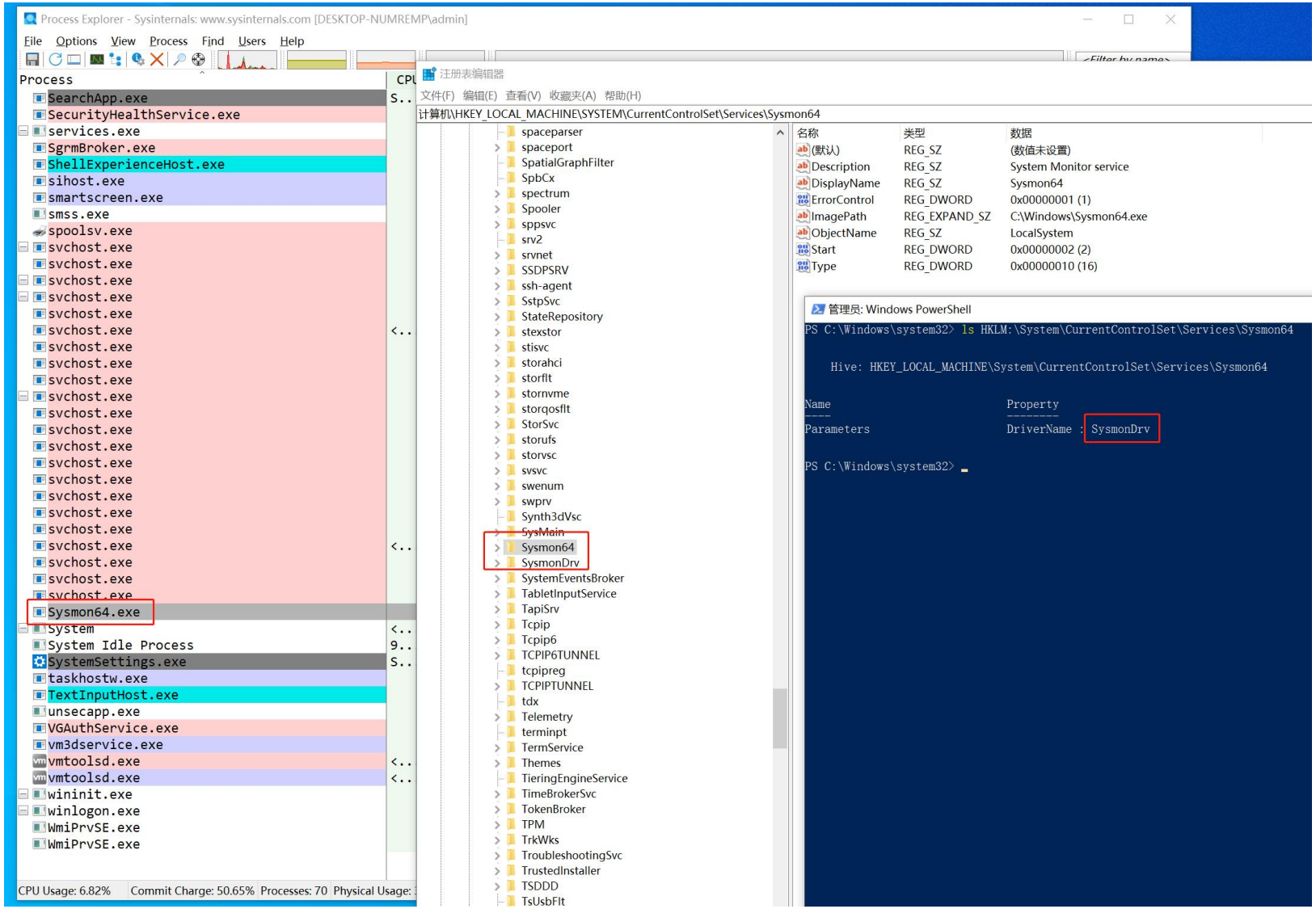
```
NTSTATUS RegistryFilterCallback(PVOID CallbackContext, PVOID
Argument1, PVOID Argument2)
{
    switch (Argument1)
    {
    case RegNtPreCreateKey:                STATUS_ACCESS_DENIED
    case RegNtPreCreateKeyEx:              STATUS_ACCESS_DENIED
    case RegNtPreOpenKey:                  STATUS_ACCESS_DENIED
    case RegNtPreOpenKeyEx:                STATUS_ACCESS_DENIED
    case RegNtPostEnumerateKey:            特殊处理
    case RegNtPostEnumerateValueKey:       特殊处理
    case RegNtSetValueKey:                 STATUS_ACCESS_DENIED
    case RegNtPreDeleteValueKey:           STATUS_ACCESS_DENIED
    case RegNtPreQueryValueKey:            STATUS_ACCESS_DENIED
    case RegNtPreQueryMultipleValueKey:    STATUS_ACCESS_DENIED
    default:
        status = STATUS_SUCCESS;
        break;
    }
}
```

前置回调（Pre-Callback）：这个回调函数在实际的I/O操作开始之前执行，可以修改或审查该操作。

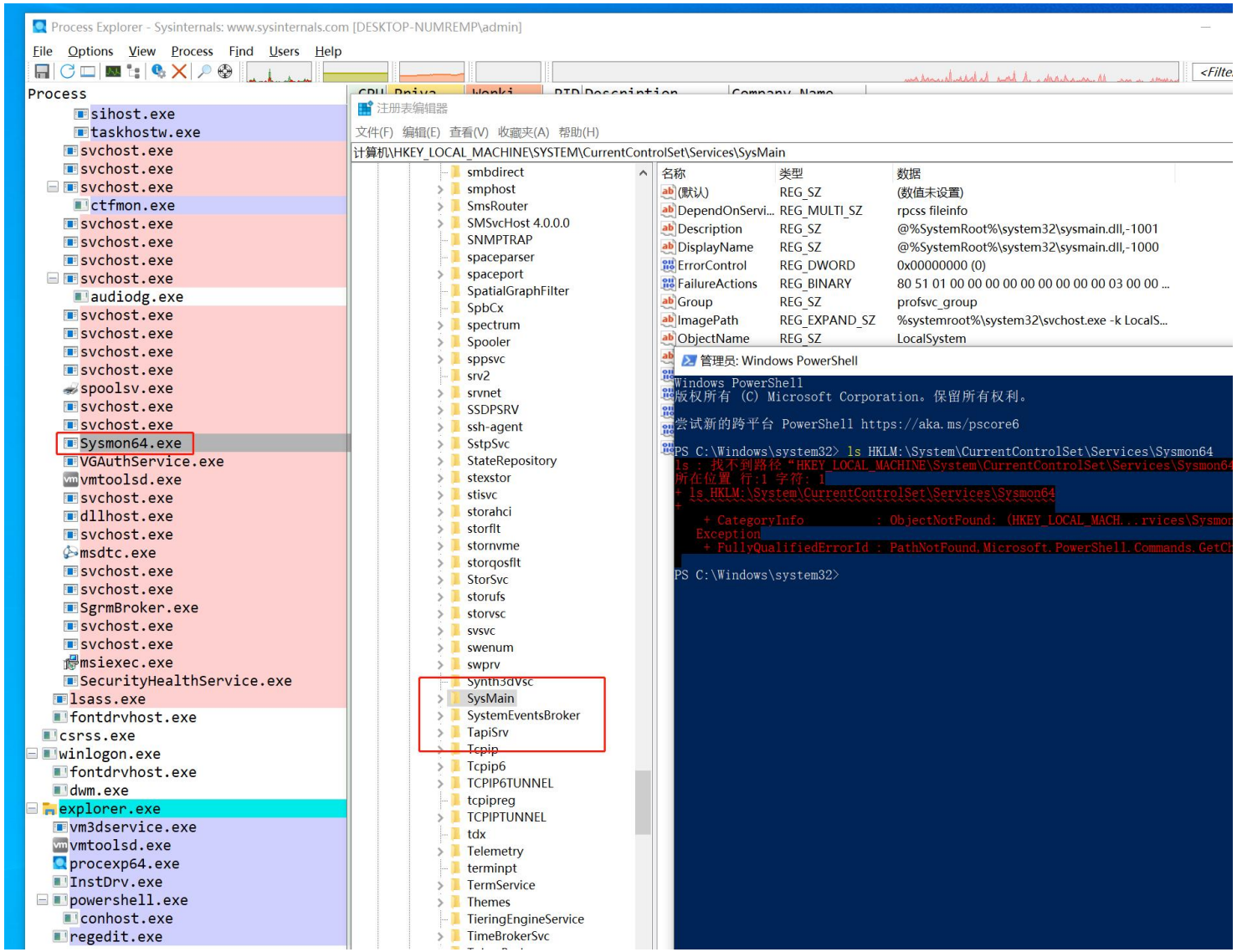
后置回调（Post-Callback）：在实际的I/O操作完成之后执行，可以查看操作结果，或进行一些后处理工作。

注册表隐藏

过滤前


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-NUMREMP\admin]
File Options View Process Find Users Help
Process
SearchApp.exe
SecurityHealthService.exe
services.exe
SgrmBroker.exe
ShellExperienceHost.exe
sihost.exe
smartscreen.exe
smss.exe
spoolsv.exe
svchost.exe
Sysmon64.exe
System
System Idle Process
SystemSettings.exe
taskhostw.exe
TextInputHost.exe
unsecapp.exe
VGAuthService.exe
vm3dservice.exe
vmtoolsd.exe
wininit.exe
winlogon.exe
WmiPrvSE.exe
CPU Usage: 6.82% Commit Charge: 50.65% Processes: 70 Physical Usage:
注册表编辑器
文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)
计算机\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sysmon64
spaceparser
spaceport
SpatialGraphFilter
SpbCx
spectrum
Spooler
sppsvc
srv2
srvnet
SSDPSRV
ssh-agent
SstpSvc
StateRepository
stexstor
stisvc
storahci
storflt
stornvme
storqosflt
StorSvc
storufs
storvsc
svsvc
swenum
swprv
Synth3dVsc
SysMain
Sysmon64
SysmonDrv
SystemEventsBroker
TabletInputService
TapiSrv
Tcpip
Tcpip6
TCPIP6TUNNEL
tcpipreg
TCPIPTUNNEL
tdx
Telemetry
terminpt
TermService
Themes
TieringEngineService
TimeBrokerSvc
TokenBroker
TPM
TrkWks
TroubleshootingSvc
TrustedInstaller
TSDDD
TsUsbFlt
名称 类型 数据
(默认) REG_SZ (数值未设置)
Description REG_SZ System Monitor service
DisplayName REG_SZ Sysmon64
ErrorControl REG_DWORD 0x00000001 (1)
ImagePath REG_EXPAND_SZ C:\Windows\Sysmon64.exe
ObjectName REG_SZ LocalSystem
Start REG_DWORD 0x00000002 (2)
Type REG_DWORD 0x00000010 (16)
管理员: Windows PowerShell
PS C:\Windows\system32> ls HKLM:\System\CurrentControlSet\Services\Sysmon64
Hive: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Sysmon64
Name Property
Parameters DriverName : SysmonDrv
PS C:\Windows\system32>

注册表隐藏


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-NUMREMP\admin]
File Options View Process Find Users Help
Process
sihost.exe
taskhostw.exe
svchost.exe
ctfmon.exe
audiodg.exe
Sysmon64.exe
VGAuthService.exe
vmtoolsd.exe
dllhost.exe
msdtc.exe
SgrmBroker.exe
msiexec.exe
SecurityHealthService.exe
lsass.exe
fontdrvhost.exe
csrss.exe
winlogon.exe
dwm.exe
explorer.exe
vm3dservice.exe
procexp64.exe
InstDrv.exe
powershell.exe
conhost.exe
regedit.exe
注册表编辑器
文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)
计算机\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SysMain
smbdirect
smphost
SmsRouter
SMSvcHost 4.0.0.0
SNMPTRAP
spaceparser
spaceport
SpatialGraphFilter
SpbCx
spectrum
Spooler
sppsvc
srv2
srvnet
SSDPSRV
ssh-agent
SstpSvc
StateRepository
stexstor
stisvc
storahci
storflt
stornvme
storqosflt
StorSvc
storufs
storvsc
svsvc
swenum
swprv
Synth3dVsc
SysMain
SystemEventsBroker
TapiSrv
Tcpip
Tcpip6
TCPIP6TUNNEL
tcpipreg
TCPIPTUNNEL
tdx
Telemetry
terminpt
TermService
Themes
TieringEngineService
TimeBrokerSvc
名称 类型 数据
(默认) REG_SZ (数值未设置)
DependOnServi... REG_MULTI_SZ rpcss fileinfo
Description REG_SZ @%SystemRoot%\system32\sysmain.dll,-1001
DisplayName REG_SZ @%SystemRoot%\system32\sysmain.dll,-1000
ErrorControl REG_DWORD 0x00000000 (0)
FailureActions REG_BINARY 80 51 01 00 00 00 00 00 00 00 00 00 03 00 00 ...
Group REG_SZ profsvc_group
ImagePath REG_EXPAND_SZ %systemroot%\system32\svchost.exe -k LocalS...
ObjectName REG_SZ LocalSystem
管理员: Windows PowerShell
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。
尝试新的跨平台 PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> ls HKLM:\System\CurrentControlSet\Services\Sysmon64
ls : 找不到路径“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Sysmon64
所在位置 行:1 字符: 1
+ ls HKLM:\System\CurrentControlSet\Services\Sysmon64
+ CategoryInfo : ObjectNotFound: (HKEY_LOCAL_MACH...rvices\Sysmon
Exception
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetCh
PS C:\Windows\system32>

过滤后

文件隐藏

```
typedef struct _FLT_OPERATION_REGISTRATION {

    UCHAR MajorFunction;                                    // 操作的类型
    FLT_OPERATION_REGISTRATION_FLAGS Flags;
    PFLT_PRE_OPERATION_CALLBACK PreOperation;               // 操作前的回调
    PFLT_POST_OPERATION_CALLBACK PostOperation;             // 操作后的回调

    PVOID Reserved1;

} FLT_OPERATION_REGISTRATION, *PFLT_OPERATION_REGISTRATION;
```

Create	IRP_MJ_CREATE
CreatePipe	IRP_MJ_CREATE_NAMED_PIPE
CreateMailslot	IRP_MJ_CREATE_MAILSLOT
Read	IRP_MJ_READ
Write	IRP_MJ_WRITE
QueryFileInformation	IRP_MJ_QUERY_INFORMATION
SetFileInformation	IRP_MJ_SET_INFORMATION
QueryEa	IRP_MJ_QUERY_EA
SetEa	IRP_MJ_SET_EA
QueryVolumeInformation	IRP_MJ_QUERY_VOLUME_INFORMATION
SetVolumeInformation	IRP_MJ_SET_VOLUME_INFORMATION
DirectoryControl	IRP_MJ_DIRECTORY_CONTROL

IRP_MJ_CREATE

判断创建的文件或目录是否为需要隐藏的文件或目录

如果是直接返回 STATUS_NO_SUCH_FILE（不存在）

```
FLT_PREOP_CALLBACK_STATUS FltCreatePreOperation(
    _Inout_ PFLT_CALLBACK_DATA Data,
    _In_ PCFLT_RELATED_OBJECTS FltObjects,
    _Flt_CompletionContext_Outptr_ PVOID* CompletionContext)
{
    PFLT_FILE_NAME_INFORMATION fltName;

    FltGetFileNameInformation(Data, FLT_FILE_NAME_NORMALIZED, &fltName);

    if (RtlCompareUnicodeString(&fltName->Name, sysmonName, TRUE) == 0)
    {
        Data->IoStatus.Status = STATUS_NO_SUCH_FILE;
        return FLT_PREOP_COMPLETE;
    }
    FltReleaseFileNameInformation(fltName);

    return FLT_PREOP_SUCCESS_NO_CALLBACK;
}
```

文件隐藏

```
IRP_MJ_DIRECTORY_CONTROL

switch (params->DirectoryControl.QueryDirectory.FileInformationClass)
{
    case FileFullDirectoryInformation:
    case FileBothDirectoryInformation:
    case FileDirectoryInformation:
    case FileIdFullDirectoryInformation:
    case FileIdBothDirectoryInformation:
    case FileNamesInformation:
}
```

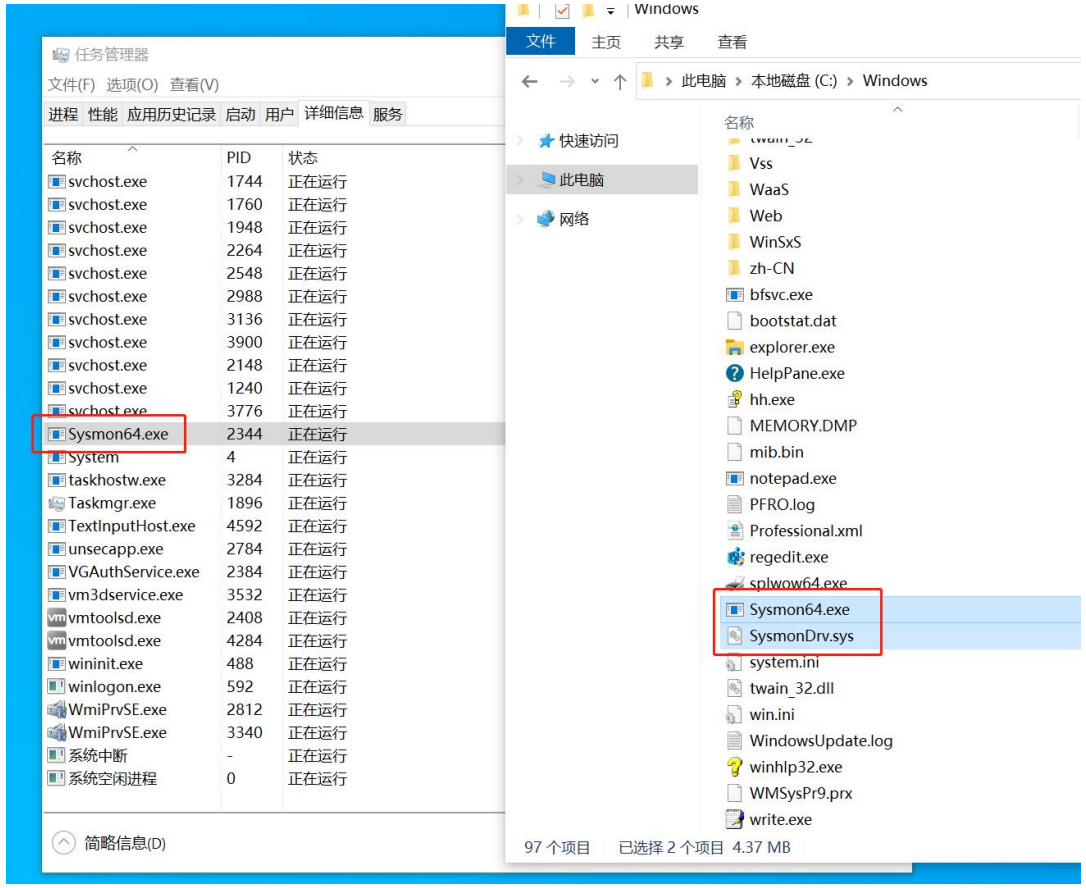
```
typedef struct _FILE_FULL_DIR_INFORMATION {
    ULONG NextEntryOffset;
    ULONG FileIndex;
    LARGE_INTEGER CreationTime;
    LARGE_INTEGER LastAccessTime;
    LARGE_INTEGER LastWriteTime;
    LARGE_INTEGER ChangeTime;
    LARGE_INTEGER EndOfFile;
    LARGE_INTEGER AllocationSize;
    ULONG FileAttributes;
    ULONG FileNameLength;
    ULONG EaSize;
    WCHAR FileName[1];
} FILE_FULL_DIR_INFORMATION,
*PFILE_FULL_DIR_INFORMATION;
```

1. 修改上一个条目的NextEntryOffset指向下一个条目,跳过当前条目
2. 用0填充当前条目的信息

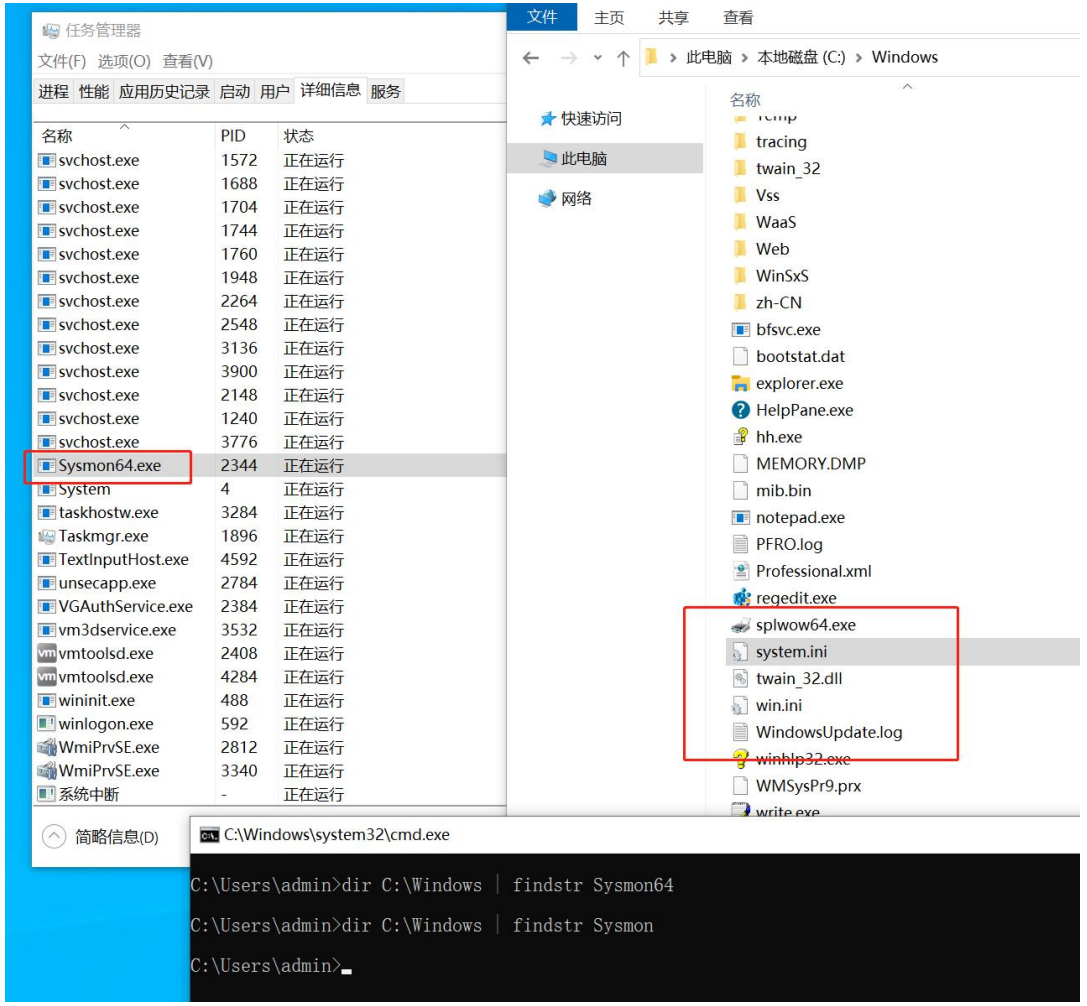
```
if (info->NextEntryOffset != 0)
{
    prevInfo->NextEntryOffset += info->NextEntryOffset;
}
else
{
    prevInfo->NextEntryOffset = 0;
    status = STATUS_SUCCESS;
}
RtlFillMemory(info, sizeof(FILE_FULL_DIR_INFORMATION), 0);
```

文件隐藏

隐藏前

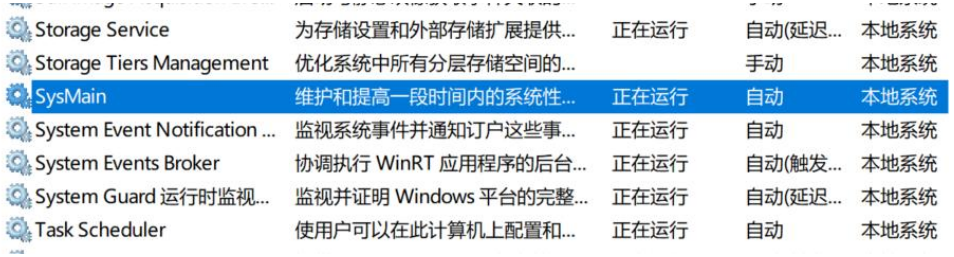

任务管理器
文件(F) 选项(O) 查看(V)
进程 性能 应用历史记录 启动 用户 详细信息 服务
名称 PID 状态
svchost.exe 1744 正在运行
svchost.exe 1760 正在运行
svchost.exe 1948 正在运行
svchost.exe 2264 正在运行
svchost.exe 2548 正在运行
svchost.exe 2988 正在运行
svchost.exe 3136 正在运行
svchost.exe 3900 正在运行
svchost.exe 2148 正在运行
svchost.exe 1240 正在运行
svchost.exe 3776 正在运行
Sysmon64.exe 2344 正在运行
System 4 正在运行
taskhostw.exe 3284 正在运行
Taskmgr.exe 1896 正在运行
TextInputHost.exe 4592 正在运行
unsecapp.exe 2784 正在运行
VGAuthService.exe 2384 正在运行
vm3dservice.exe 3532 正在运行
vmtoolsd.exe 2408 正在运行
vmtoolsd.exe 4284 正在运行
wininit.exe 488 正在运行
winlogon.exe 592 正在运行
WmiPrvSE.exe 2812 正在运行
WmiPrvSE.exe 3340 正在运行
系统中断 - 正在运行
系统空闲进程 0 正在运行
简略信息(D)
Windows
文件 主页 共享 查看
此电脑 › 本地磁盘 (C:) › Windows
快速访问
此电脑
网络
名称
Vss
WaaS
Web
WinSxS
zh-CN
bfsvc.exe
bootstat.dat
explorer.exe
HelpPane.exe
hh.exe
MEMORY.DMP
mib.bin
notepad.exe
PFRO.log
Professional.xml
regedit.exe
splwow64.exe
Sysmon64.exe
SysmonDrv.sys
system.ini
twain_32.dll
win.ini
WindowsUpdate.log
winhlp32.exe
WMSysPr9.prx
write.exe
97 个项目 已选择 2 个项目 4.37 MB

隐藏后


任务管理器
文件(F) 选项(O) 查看(V)
进程 性能 应用历史记录 启动 用户 详细信息 服务
名称 PID 状态
svchost.exe 1572 正在运行
svchost.exe 1688 正在运行
svchost.exe 1704 正在运行
svchost.exe 1744 正在运行
svchost.exe 1760 正在运行
svchost.exe 1948 正在运行
svchost.exe 2264 正在运行
svchost.exe 2548 正在运行
svchost.exe 3136 正在运行
svchost.exe 3900 正在运行
svchost.exe 2148 正在运行
svchost.exe 1240 正在运行
svchost.exe 3776 正在运行
Sysmon64.exe 2344 正在运行
System 4 正在运行
taskhostw.exe 3284 正在运行
Taskmgr.exe 1896 正在运行
TextInputHost.exe 4592 正在运行
unsecapp.exe 2784 正在运行
VGAuthService.exe 2384 正在运行
vm3dservice.exe 3532 正在运行
vmtoolsd.exe 2408 正在运行
vmtoolsd.exe 4284 正在运行
wininit.exe 488 正在运行
winlogon.exe 592 正在运行
WmiPrvSE.exe 2812 正在运行
WmiPrvSE.exe 3340 正在运行
系统中断 - 正在运行
简略信息(D)
文件 主页 共享 查看
此电脑 › 本地磁盘 (C:) › Windows
快速访问
此电脑
网络
名称
tracing
twain_32
Vss
WaaS
Web
WinSxS
zh-CN
bfsvc.exe
bootstat.dat
explorer.exe
HelpPane.exe
hh.exe
MEMORY.DMP
mib.bin
notepad.exe
PFRO.log
Professional.xml
regedit.exe
splwow64.exe
system.ini
twain_32.dll
win.ini
WindowsUpdate.log
winhlp32.exe
WMSysPr9.prx
write.exe
C:\Windows\system32\cmd.exe
C:\Users\admin>dir C:\Windows | findstr Sysmon64
C:\Users\admin>dir C:\Windows | findstr Sysmon
C:\Users\admin>

服务隐藏

Windows服务支持使用安全描述符定义语言（Security Descriptor Definition Language | SDDL）控制服务权限的功能。通过修改SDDL可以修改对象（文件或者服务）的DACL（自主访问控制列表），从而修改用户对对象的访问控制。通过对服务的SDDL进行编辑，拒绝所有用户对该服务的读取权限，即实现服务隐藏的效果。



隐藏

```
& $env:SystemRoot\System32\sc.exe sdset Sysmon64
"D:(D;;DCLCWPDTSD;;;IU)(D;;DCLCWPDTSD;;;SU)(D;;DCLCW
PDTSD;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;
SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOC
RSDRCWDWO;;;BA)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;
WD)"
```

恢复

```
& $env:SystemRoot\System32\sc.exe sdset Sysmon64
"D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOC
RSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRR
C;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```

minifilter Altitude 隐藏

```
FLTMGR!_FLT_FILTER
   +0x000 Base              : _FLT_OBJECT
      +0x000 Flags             : _FLT_OBJECT_FLAGS
      +0x004 PointerCount      : Uint4B
      +0x008 RundownRef        : _EX_RUNDOWN_REF
      +0x010 PrimaryLink       : _LIST_ENTRY
      +0x020 UniqueIdentifier : _GUID
   +0x030 Frame             : Ptr64 _FLTP_FRAME
      +0x000 Type              : _FLT_TYPE
      +0x008 Links             : _LIST_ENTRY
      +0x018 FrameID           : Uint4B
      +0x020 AltitudeIntervalLow : _UNICODE_STRING
      +0x030 AltitudeIntervalHigh : _UNICODE_STRING
      +0x040 LargeIrpCtrlStackSize : UChar
      +0x041 SmallIrpCtrlStackSize : UChar
      +0x048 RegisteredFilters : _FLT_RESOURCE_LIST_HEAD
      +0x0c8 AttachedVolumes   : _FLT_RESOURCE_LIST_HEAD
      +0x148 MountingVolumes   : _LIST_ENTRY
```

```
C:\Windows\system32>fltmc

筛选器名称                     数字实例    高度         框架
------------------------------ ----------  -----------  -----
bindflt                             0      409800         0
SysmonDrv                           3      385201         0
storqosflt                          0      244000         0
wcifs                               0      189900         0
CldFlt                              0      180451         0
FileCrypt                           0      141100         0
luafv                               1      135000         0
npsvctrig                           1       46000         0
Wof                                 1       40700         0
FileInfo                            3       40500         0

C:\Windows\system32>fltmc

筛选器名称                     数字实例    高度         框架
------------------------------ ----------  -----------  -----
bindflt                             0      409800         0
storqosflt                          0      244000         0
wcifs                               0      189900         0
CldFlt                              0      180451         0
FileCrypt                           0      141100         0
luafv                               1      135000         0
npsvctrig                           1       46000         0
Wof                                 1       40700         0
FileInfo                            3       40500         0

C:\Windows\system32>
```

PrimaryLink 指针指向双向链表中的下一个 FLT_FILTER 结构地址

19th Asian Games Hangzhou 2022

杭州2022年第19届亚运会官方合作伙伴
Official Prestige Partner of the 19th Asian Games Hangzhou 2022

联系我们

Contact Us

浙江省杭州市滨江区西兴街道联慧街188号安恒大厦
www.dbappsecurity.com.cn
400-6059-110

安恒信息官方服务号
网安人的干货充电站