



Reliable enumerating the Windows processes in ring3

Tombkeeper@xfocus.org



- Psapi
 - EnumProcesses()
- ToolHelp32
 - Process32First()
 - Process32Next()
- NtQuerySystemInformation()
 - SystemProcessInformation = 5
 - à ExpGetProcessInformation()
 - à Travel the ActiveProcessLinks
 - à Locate the EPROCESS
 - à Obtain the information of process

- A snip of EPROCESS structure:

```
.....  
DWORD UniqueProcessId  
LIST_ENTRY ActiveProcessLinks
```

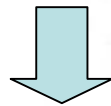
```
.....  
Char ImageFileName[16]
```

- A snip of ETHREAD structure:

```
.....  
PEPROCESS ThreadsProcess
```

```
kd> da poi(PsInitialSystemProcess) + 1fc
81a2fc5c "System"
kd> da poi(poi(PsInitialSystemProcess)+a0) -a0 + 1fc
8132af5c "SMSS.EXE"
kd> da poi(poi(poi(PsInitialSystemProcess)+a0)) -a0 + 1fc
8134af5c "CSRSS.EXE"
kd> da poi(poi(poi(poi(PsInitialSystemProcess)+a0))) -a0 + 1fc
8119375c "WINLOGON.EXE"
```

Locate all EPROCESS



Normal method of



Obtain the process information



Compare and find the hidden processes

Core problem: Locating the EPROCESS

- Hook NtQuerySystemInformation()
 - Hook SDT
 - SystemProcessInformation=5
SystemHandleInformation=16
 - Implement:
 - Hacker Defender (holy_father@phreaker.net)
- Travel the ActiveProcessLinks directly and enumerate the processes
 - Can detective Hook NtQuerySystemInformation()
 - Implement:
 - KProcCheck (chewkeong@security.org.sg)

- Unlink itself from ActiveProcessLinks
 - Implement:
 - [FU_Rootkit \(fuzen_op@yahoo.com\)](mailto:fuzen_op@yahoo.com)
- Utilize the thread schedule list detect the hidden processes
 - KiWaitInListHead, KiWaitOutListhead, KiDispatcherReadyListHead
 - Can detect Hook NtQuerySystemInformation()
 - Can detect unlink from ActiveProcessLinks
 - Can't implement on Windows XP and Windows 2003
 - Implement
 - [Klister \(joanna@mailsnare.net\)](mailto:joanna@mailsnare.net)
 - [KProcCheck \(chewkeong@security.org.sg\)](mailto:chewkeong@security.org.sg)

- Defeat processes detective method base on kernel schedule link
 - <http://www.xfocus.net/articles/200404/693.html>
(Kinsephi@hotmail.com)

- Hook SwapContext()

Original SwapContext() function:

```
__fastcall SwapContext  
(  
    PETHREAD SwapIn,  
    PETHREAD SwapOut  
)
```


- Support Windows 2000/XP/2003
- CONTEXT SWAP level detective more reliable
- Can detect all know process hidden method
- SwapContext() is not Exported function

- Reliable
- May cause system crash

- Implement:

- http://www.rootkit.com/newsread_print.php?newsid=170

70

(kkasslin@cc.hut.fi)

- Windows NT 5.0、 5.1
 - EPROCESS.SessionProcessLinks
 - Not include System和smss.exe
 - EPROCESS.Vm.WorkingSetExpansionLinks

- Windows NT 5.2
 - EPROCESS.MmProcessLinks

```
kd> dt _EPROCESS ImageFileName poi(MmProcessList)-238  
+0x154 ImageFileName : [16] "Idle"
```

```
kd> dt _EPROCESS ImageFileName poi(poi(MmProcessList))-238  
+0x154 ImageFileName : [16] "System"
```

- Export PsInitialSystemProcess Ntoskrnl.exe

```
kd> dt _EPROCESS ImageFileName  
poi(PsInitialSystemProcess)  
+0x1fc ImageFileName : [16] "System"
```

- NtQuerySystemInformation()
 - SystemHandleInformation = 16
 - SYSTEM_HANDLE_INFORMATION.Object

- Utilizing KPCR

```
kd> dt _KPCR PrcbData.CurrentThread ffdff000
```

```
+0x120 PrcbData :
```

```
+0x004 CurrentThread : 0xff91e740
```

```
kd> dt _ETHREAD ThreadsProcess 0xff91e740
```

```
+0x22c ThreadsProcess : 0xff9011c0
```

```
kd> dt _EPROCESS ImageFileName 0xff9011c0
```

```
+0x1fc ImageFileName : [16] "kd.exe"
```

- Read physical memory

```
RtlInitUnicodeString (  
    &PhyMemString,  
    L\\Device\\PhysicalMemory  
);
```

```
ZwOpenSection (  
    &hPhyMem, SECTION_MAP_READ,  
    &PhyMemAttribs
```

```
);  
MapAddress = MapViewOfFile (  
    hPhyMem, FILE_MAP_READ, 0, ReadAddress,  
    ReadLength + GetPageSize()  
);
```

- Virtual address → Physical address

```
PVOID __stdcall LameGetPhysicalAddress( PVOID KernelAddress )
{
    PVOID PhysAddress = 0;

    if((DWORD)KernelAddress < 0x80000000L ||
        (DWORD)KernelAddress >= 0xA0000000L)
        (DWORD)PhysAddress = (DWORD)KernelAddress & 0x0FFFFFFF;
    else
        (DWORD)PhysAddress = (DWORD)KernelAddress & 0x1FFFFFFF;
    return PhysAddress;
}
```

– Flier Lu (flier_AT_nsfocus.com)

“Aintegrality of Windows NT system dispatch list”

- ZwSystemDebugControl()

```
NTSTATUS ZwSystemDebugControl (  
    IN SYSDBG_COMMAND Command,  
    IN PVOID InputBuffer,  
    IN ULONG InputBufferLength,  
    OUT PVOID OutputBuffer,  
    IN ULONG OutputBufferLength,  
    OUT PULONG ReturnLength  
);
```

```
typedef struct _MEMORY_CHUNKS {  
    ULONG Address;  
    PVOID Data;  
    ULONG Length;  
}MEMORY_CHUNKS, *PMEMORY_CHUNKS;  
MEMORY_CHUNKS QueryBuff;
```

```
ZwSystemDebugControl (  
    SysDbgReadKernelMemory,  
    &QueryBuff,  
    sizeof(MEMORY_CHUNKS),  
    NULL,  
    0,  
    &ReturnLength  
);
```


- Windows NT 5.0

```
kd> dt _EPROCESS plmageFileName  
poi(poi(PsInitialSystemProcess)+a0)-a0  
+0x284 plmageFileName : 0x81363fb8 "\WINNT\system32\SMSS.EXE"
```

- Windows NT 5.1/5.2

```
lkd> dt _eprocess SeAuditProcessCreationInfo.ImageFileName->Name  
0ff894218  
nt!_EPROCESS  
+0x1d4 SeAuditProcessCreationInfo :  
+0x000 ImageFileName :  
+0x000 Name : _UNICODE_STRING  
"\Device\HarddiskVolume1\WINDOWS\system32\cmd.exe"
```

- Can't unlink the EPROCESS properly After process end
- Other members of EPROCESS are corrupted
 - Check validity
- MmProcessLinks can enumerate all the remains of EPROCESS

[1] Hacker Defender

Holy_Father(holy_father_AT_phreaker.net)

- <http://rootkit.host.sk/>

[2] KprocCheck Tan Chew

Keong(chewkeong_AT_security.org.sg)

- <http://www.security.org.sg/code/kproccheck.html>

[3] FU_Rootkit fuzen_op(fuzen_op_AT_yahoo.com)

- https://www.rootkit.com/vault/fuzen_op/FU_Rootkit.zip

[4] Klister Joanna Rutkowska(joanna_AT_mailsnare.net)

- <http://www.rootkit.com/vault/joanna/klister-0.4.zip>

[5] 绕过内核调度链表进程检测

SoBelt(Kinsephi_AT_hotmail.com)

- <http://www.xfocus.net/articles/200404/693.html>

[6] Detecting Hidden Processes by Hooking the

SwapContext Function kkasslin(kkasslin_AT_cc.hut.fi)

- http://www.rootkit.com/newsread_print.php?newsid=170

[7] Playing with Windows /dev/(k)mem crazylord

(razylord_AT_thins.net)

- <http://www.phrack.org/phrack/59/p59-0x10.txt>

[8] 自动验证 Windows NT 系统服务描述表的完整性 Flier Lu (flier_AT_nsfocus.com)

- <http://www.nsfocus.net/index.php?act=magazine&do=view&mid=2119>

[9] 对 Native API NtSystemDebugControl 的分析 tombkeeper (tombkeeper_AT_xfocus.org)

- <http://www.xfocus.net/articles/200408/721.html>

[10] 获取 Windows 系统的内核变量 tombkeeper (tombkeeper_AT_xfocus.org)

- <http://www.xfocus.net/articles/200408/724.html>