

Windows Process Injection - Process Hollowing

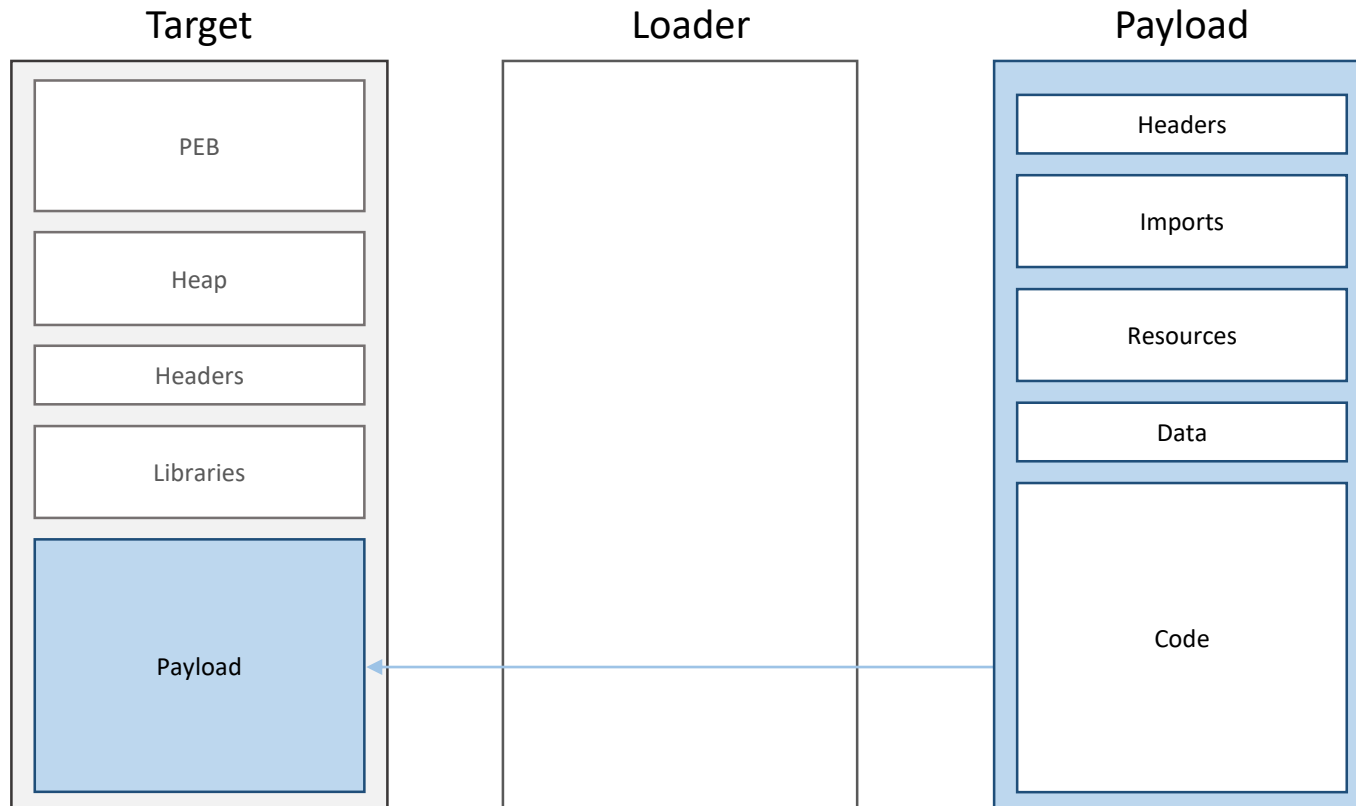
January, 2021

Marc Ochsenmeier

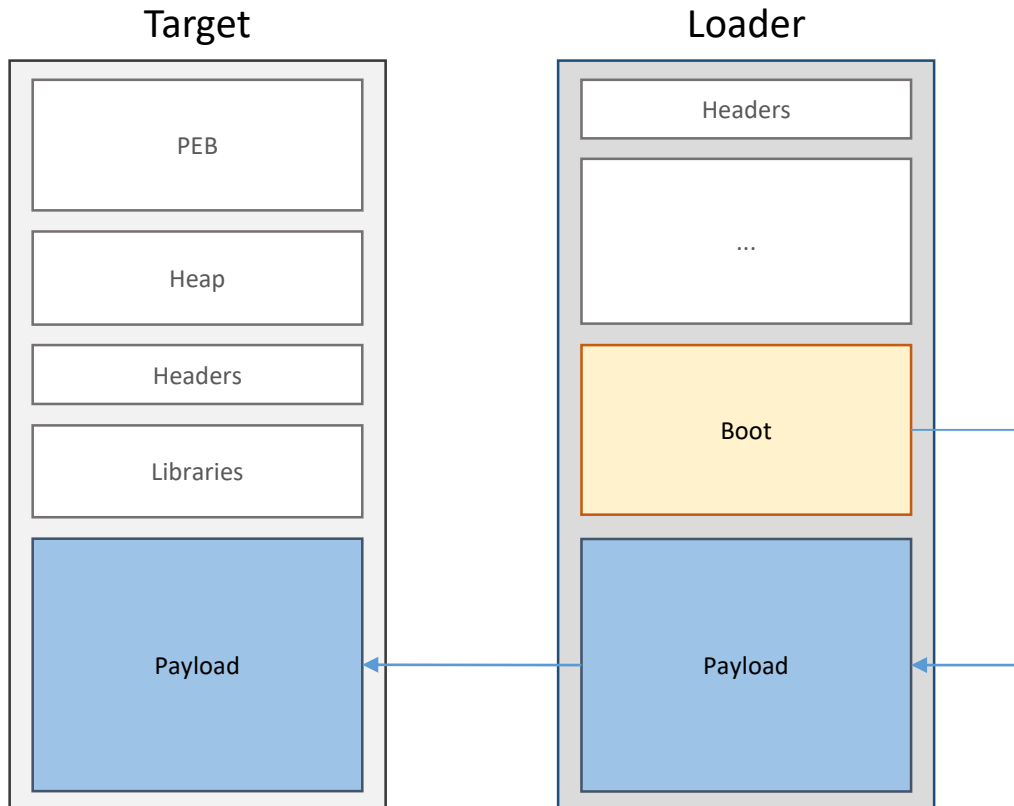
@ochsenmeier

www.winitor.com

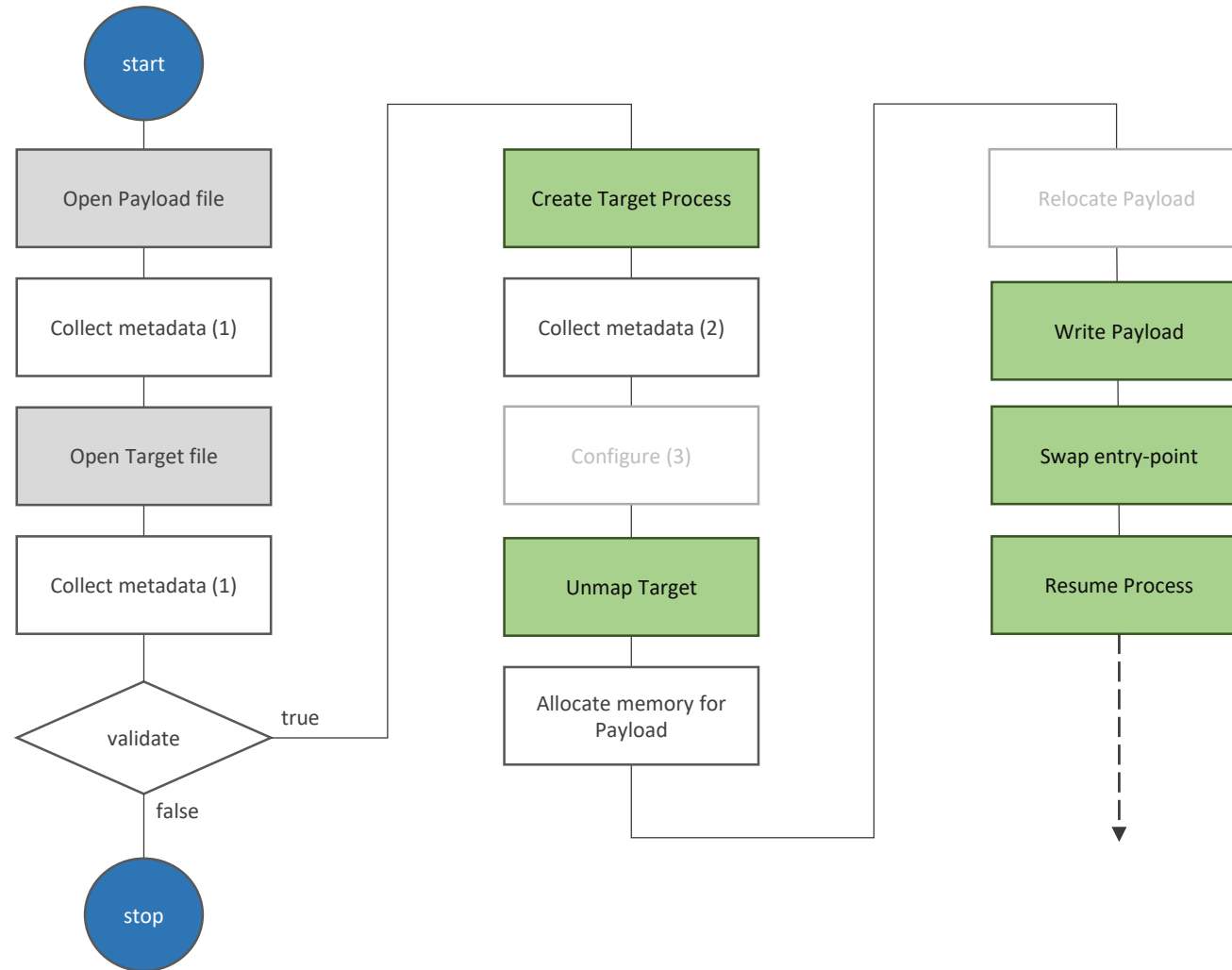
- Actors



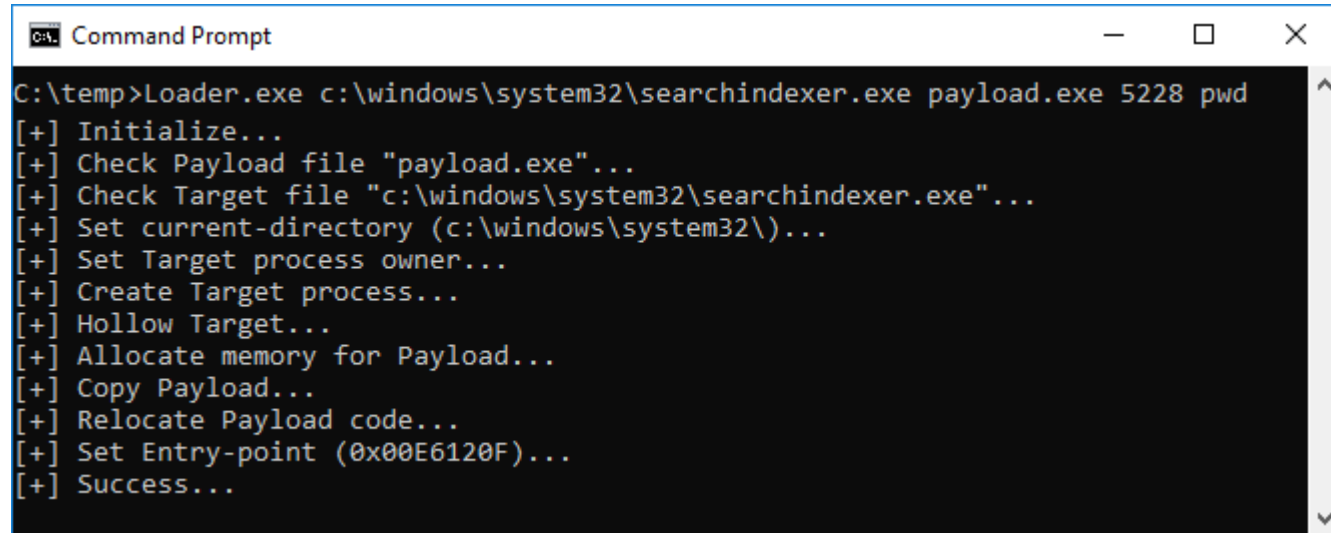
- Actors



- Logical Steps



- Demo



```
Command Prompt
C:\temp>Loader.exe c:\windows\system32\searchindexer.exe payload.exe 5228 pwd
[+] Initialize...
[+] Check Payload file "payload.exe"...
[+] Check Target file "c:\windows\system32\searchindexer.exe"...
[+] Set current-directory (c:\windows\system32\)...
[+] Set Target process owner...
[+] Create Target process...
[+] Hollow Target...
[+] Allocate memory for Payload...
[+] Copy Payload...
[+] Relocate Payload code...
[+] Set Entry-point (0x00E6120F)...
[+] Success...
```

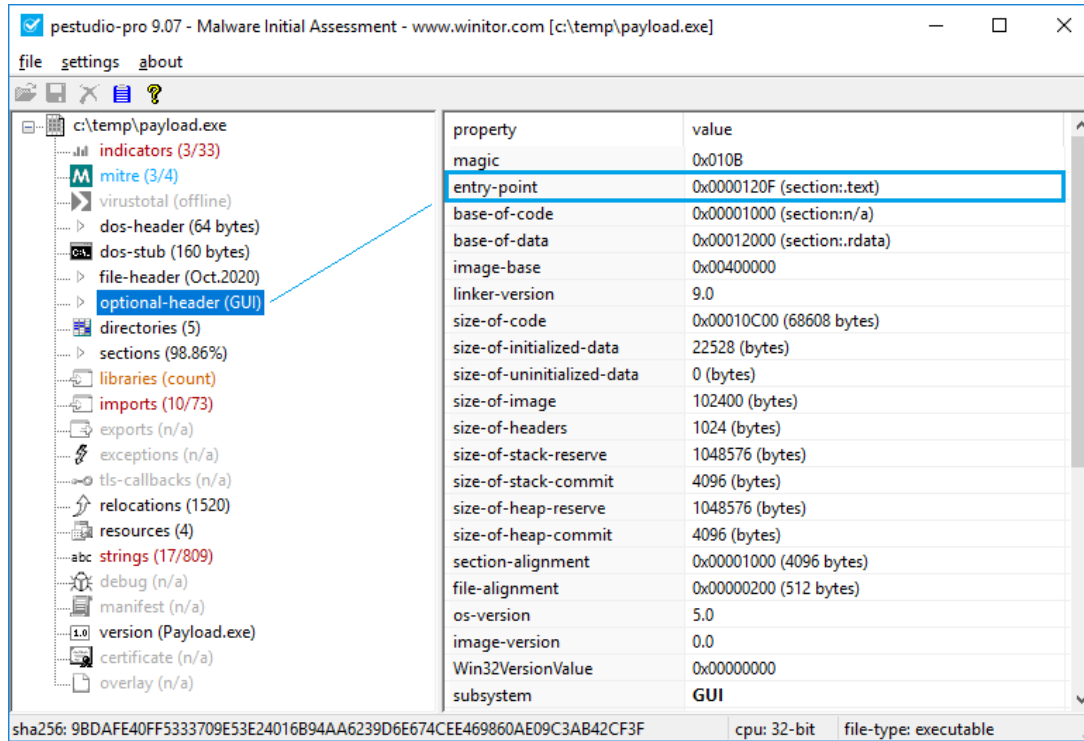
- Prerequisites > Environment

- CPU width
- Subsystem
- Relocation Support
- Integrity Level

	Target 32bit	Target 64 bit
Payload 32bit	x	x
Payload 64bit	-	x

	NATIVE	GUI	CUI	EFI
NATIVE	-	-	-	-
GUI	-	x	-	-
CUI	-	x	x	-
EFI	-	-	-	-

- Prerequisites > Entry-point



The screenshot shows the PEStudio Pro 9.07 interface. The left pane displays the file structure, with 'optional-header (GUI)' selected. The right pane shows the corresponding PE header fields. A blue box highlights the 'entry-point' field, which is set to '0x0000120F (section:.text)'. A blue arrow points from this field to the 'optional-header (GUI)' entry in the left pane.

property	value
magic	0x010B
entry-point	0x0000120F (section:.text)
base-of-code	0x00001000 (section:n/a)
base-of-data	0x00012000 (section:.rdata)
image-base	0x00400000
linker-version	9.0
size-of-code	0x00010C00 (68608 bytes)
size-of-initialized-data	22528 (bytes)
size-of-uninitialized-data	0 (bytes)
size-of-image	102400 (bytes)
size-of-Headers	1024 (bytes)
size-of-stack-reserve	1048576 (bytes)
size-of-stack-commit	4096 (bytes)
size-of-heap-reserve	1048576 (bytes)
size-of-heap-commit	4096 (bytes)
section-alignment	0x00001000 (4096 bytes)
file-alignment	0x00000200 (512 bytes)
os-version	5.0
image-version	0.0
Win32VersionValue	0x00000000
subsystem	GUI

sha256: 9BDAFE40FF5333709E53E24016B94AA6239D6E674CEE469860AE09C3AB42CF3F cpu: 32-bit file-type: executable

- Detection > Static Indicators > API

```
if ( Buffer == lpAddress )
{
    v15 = GetModuleHandleA("ntdll.dll");
    NtUnmapViewOfSection = GetProcAddress(v15, "NtUnmapViewOfSection");
    ((void (__stdcall *))(HANDLE, LPVOID))NtUnmapViewOfSection(hProcess[0], Buffer);
    v14 = lpAddress;
}
v17 = VirtualAllocEx(hProcess[0], v14, 0xE8000u, 0x3000u, 0x40u);
v23 = (int)v17;
if ( v17 )
{
    WriteProcessMemory(hProcess[0], v17, &unk_4160D0, 0x1000u, &NumberOfBytesWritten);
    v18 = v23;
    for ( i = 0; i < 12; i += 4 )
        WriteProcessMemory(
            hProcess[0],
            (LPVOID)(v18 + *(int *)((char *)&v38 + i)),
            (char *)&unk_4160D0 + *(int *)((char *)&v32 + i),
            *(SIZE_T *)((char *)&nSize + i),
            &NumberOfBytesWritten);
    v13 = lpContext;
    WriteProcessMemory(hProcess[0], (LPVOID)(lpContext->Ebx + 8), &lpAddress, 4u, &NumberOfBytesWritten);
    v13->Eax = v23 + 942800;
    SetThreadContext(hProcess[1], v13);
    ResumeThread(hProcess[1]);
}
```

md5,0580896027E9B92E00887E57202E27A8

API	Process-Hollowing
CreateProcess	X
GetFileSize	X
GetThreadContext	X
NtQueryInformationProcess	X
NtUnmapViewOfSection	X
ReadProcessMemory	X
ResumeThread	X
SetThreadContext	X
VirtualAllocEx	X
WriteProcessMemory	X

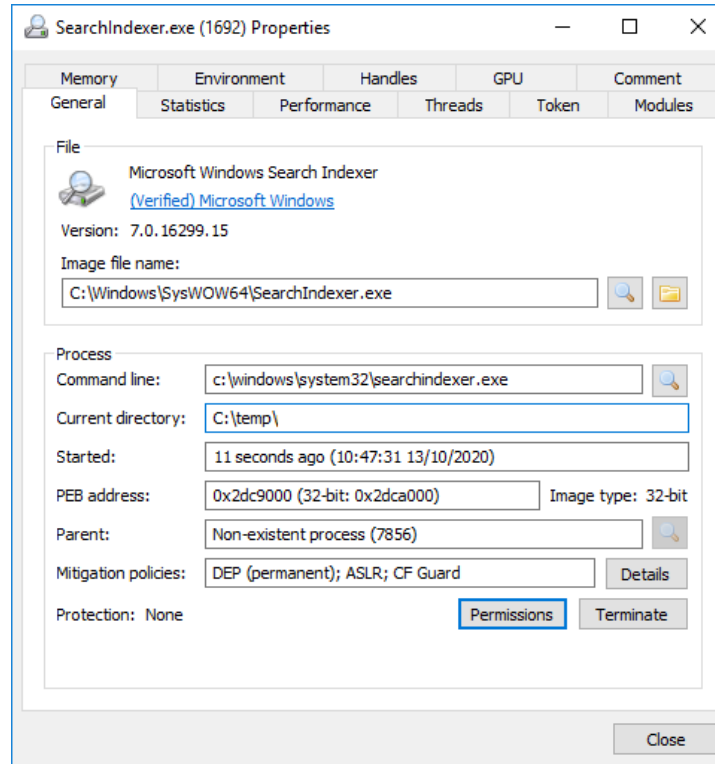
- Hunting > YARA

```
rule Windows_Injection_ProcessHollowing
{
  meta:
    description = "Detect Windows Process Injection using Process-Hollowing"
    author      = "Marc Ochsenmeier"
    creation    = "2021-01-13"
    update     = "2021-01-13"
    sha256     = "65d92f949d9cf4f5f7b26dbf92683ce4b1624fb5ce3c53594685d7e135a95d3"
    sha256     = "c6a148ac7cb2db26eb6686ce36e56bd40aabfe6b1ee6c6565eb468837c9b382d"
    sha256     = "d1622f834e2ef69448867ee29c57f1e4b96b7e8149b28beb90b46082114c7c44"
    sha256     = "45bfa1327c2c0118c152c7192ada429c6d4ae03b8164ebe36ab5ba9a84f5d7aa"
    sha256     = "14751672beb4bf7ac190c278f23926c428dfd26849676b34656e9a41b9032fbd"

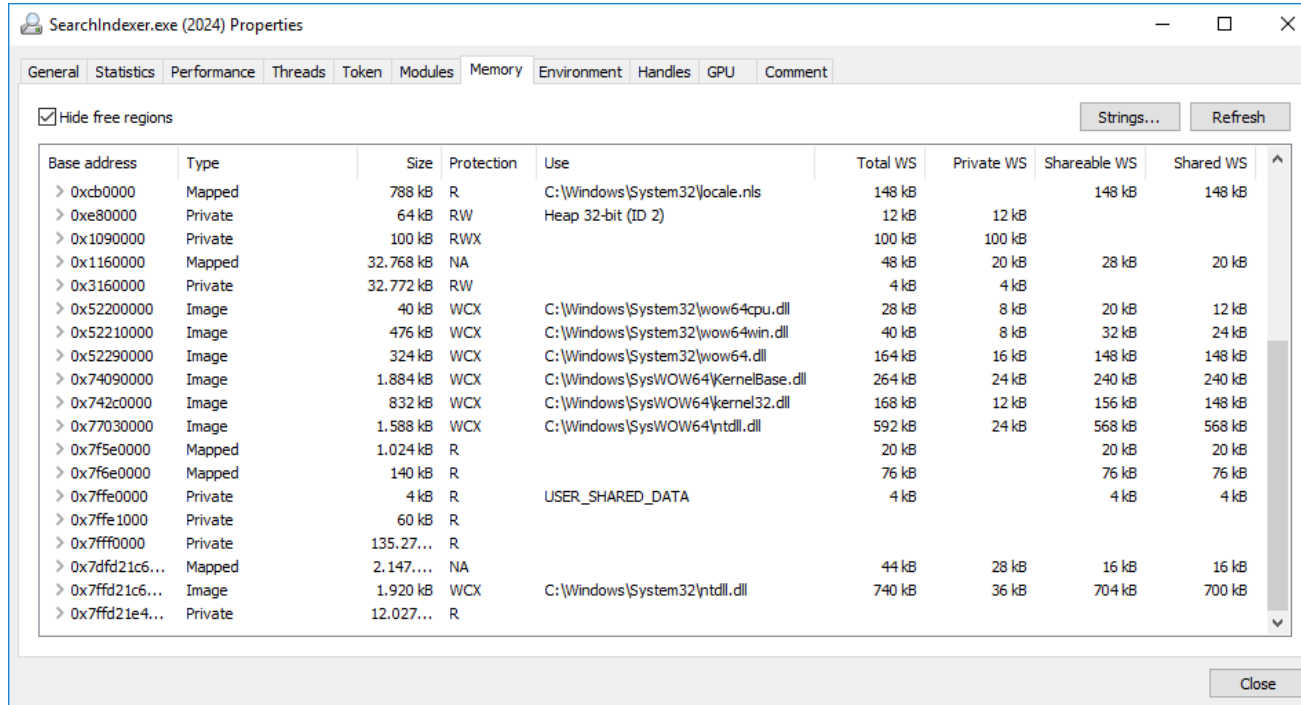
  strings:
    $ = "CreateProcess"  ascii wide nocase
    $ = "NtUnmapViewOfSection"  ascii wide nocase
    $ = "ReadProcessMemory"  ascii wide nocase
    $ = "WriteProcessMemory"  ascii wide nocase
    $ = "VirtualAlloc"  ascii wide nocase
    $ = "GetThreadContext"  ascii wide nocase
    $ = "SetThreadContext"  ascii wide nocase
    $ = "ResumeThread"  ascii wide nocase

  condition:
    FILE_PE and 7 of them
}
```

- Characteristics
 - Orphan legit process
 - Current directory
 - Memory regions
 - Memory content
 - Size



- Characteristics > Memory regions



SearchIndexer.exe (2024) Properties

General Statistics Performance Threads Token Modules Memory Environment Handles GPU Comment

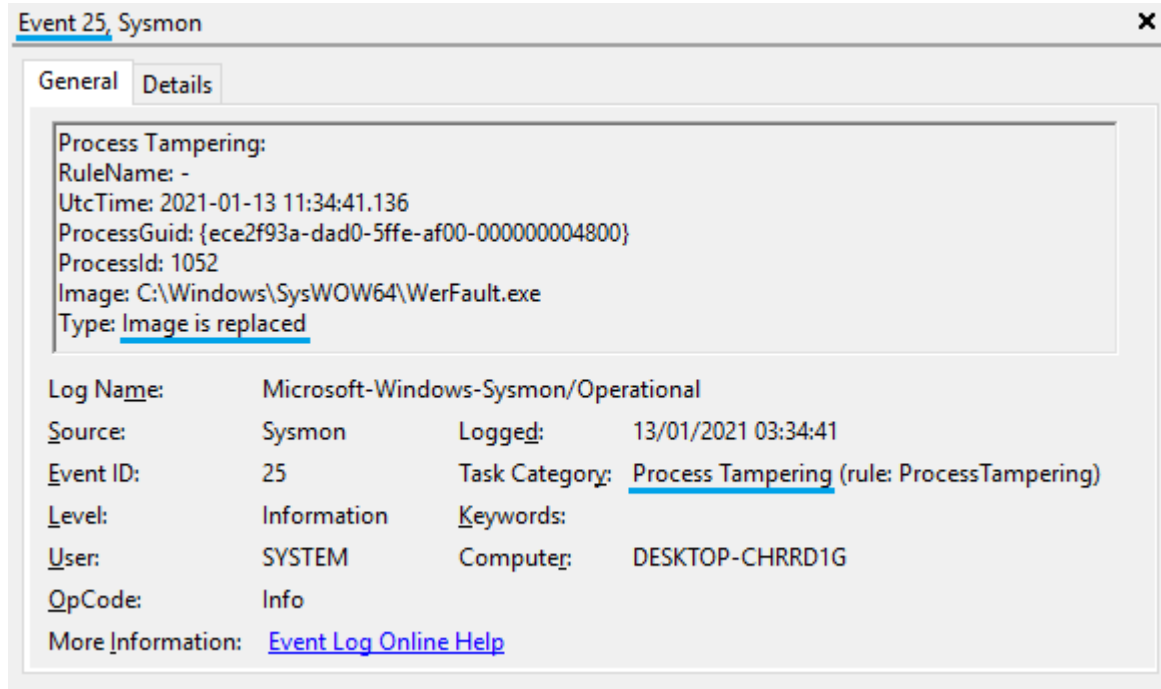
Hide free regions

Strings... Refresh

Base address	Type	Size	Protection	Use	Total WS	Private WS	Shareable WS	Shared WS
> 0xcb0000	Mapped	788 kB	R	C:\Windows\System32\locale.nls	148 kB		148 kB	148 kB
> 0xe80000	Private	64 kB	RW	Heap 32-bit (ID 2)	12 kB	12 kB		
> 0x1090000	Private	100 kB	RWX		100 kB	100 kB		
> 0x1160000	Mapped	32,768 kB	NA		48 kB	20 kB	28 kB	20 kB
> 0x3160000	Private	32,772 kB	RW		4 kB	4 kB		
> 0x52200000	Image	40 kB	WCX	C:\Windows\System32\wow64cpu.dll	28 kB	8 kB	20 kB	12 kB
> 0x52210000	Image	476 kB	WCX	C:\Windows\System32\wow64win.dll	40 kB	8 kB	32 kB	24 kB
> 0x52290000	Image	324 kB	WCX	C:\Windows\System32\wow64.dll	164 kB	16 kB	148 kB	148 kB
> 0x74090000	Image	1,884 kB	WCX	C:\Windows\SysWOW64\KernelBase.dll	264 kB	24 kB	240 kB	240 kB
> 0x742c0000	Image	832 kB	WCX	C:\Windows\SysWOW64\kernel32.dll	168 kB	12 kB	156 kB	148 kB
> 0x77030000	Image	1,588 kB	WCX	C:\Windows\SysWOW64\ntdll.dll	592 kB	24 kB	568 kB	568 kB
> 0x7f5e0000	Mapped	1,024 kB	R		20 kB		20 kB	20 kB
> 0x7f6e0000	Mapped	140 kB	R		76 kB		76 kB	76 kB
> 0x7ffe0000	Private	4 kB	R	USER_SHARED_DATA	4 kB		4 kB	4 kB
> 0x7ffe1000	Private	60 kB	R					
> 0x7fff0000	Private	135,27...	R					
> 0x7dfd21c6...	Mapped	2,147,...	NA		44 kB	28 kB	16 kB	16 kB
> 0x7ffd21c6...	Image	1,920 kB	WCX	C:\Windows\System32\ntdll.dll	740 kB	36 kB	704 kB	700 kB
> 0x7ffd21e4...	Private	12,027,...	R					

Close

- Detection > Tools > Sysmon

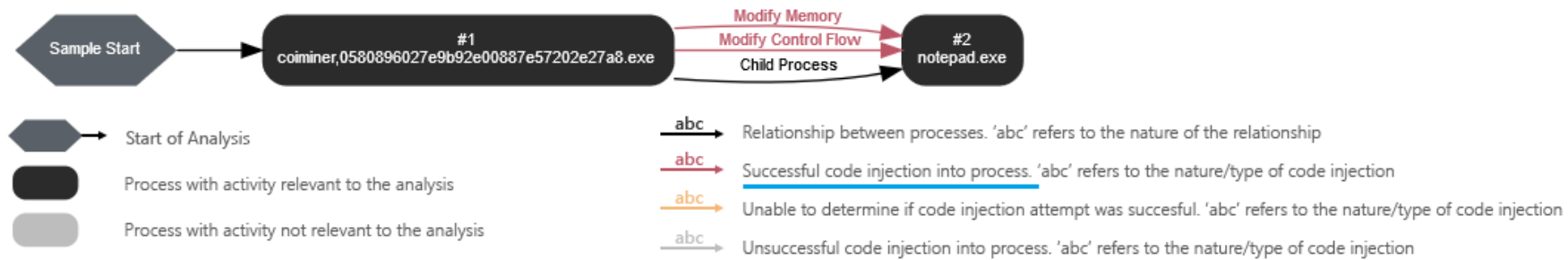


- Analysis > Tools > Sanbox

Screenshots



Monitored Processes



- Samples
 - <https://attack.mitre.org/techniques/T1055/012/>

• References

- Process Hollowing, John Leitch
 - www.autosectools.com/Process-Hollowing.pdf
- process-hollowing - poc
 - <https://code.google.com/archive/p/process-hollowing/downloads>
- The return of the spoof part 1: Parent process ID spoofing
 - blog.nviso.eu/2020/01/31/the-return-of-the-spoof-part-1-parent-process-id-spoofing/
- Ten process injection techniques: Survey of common and trending process injection techniques
 - www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
- SpiderLabs Blog - Analyzing Malware Hollow Processes
 - www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/analyzing-malware-hollow-processes
- Running a (32-bit) Process in the Context of Another
 - www.blog.codereversing.com/runasproc.pdf
- Sysmon - Process tampering detection
 - <https://medium.com/falconforce/sysmon-13-process-tampering-detection-820366138a6c>