Windows Process Injection - Process Hollowing

July 06, 2021

Marc Ochsenmeier

@ochsenmeier

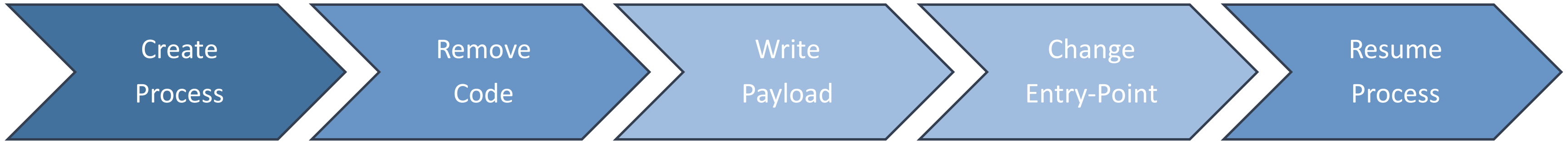
www.winitor.com

Windows Process Hollowing

- Definition
  - Is a kind of injection
  - Is a kind of cloaking|impersonation
  - Is also known as “RunPE”
- Goals
  - Evasion
  - Persistence
  - Escalation

Windows Process Hollowing

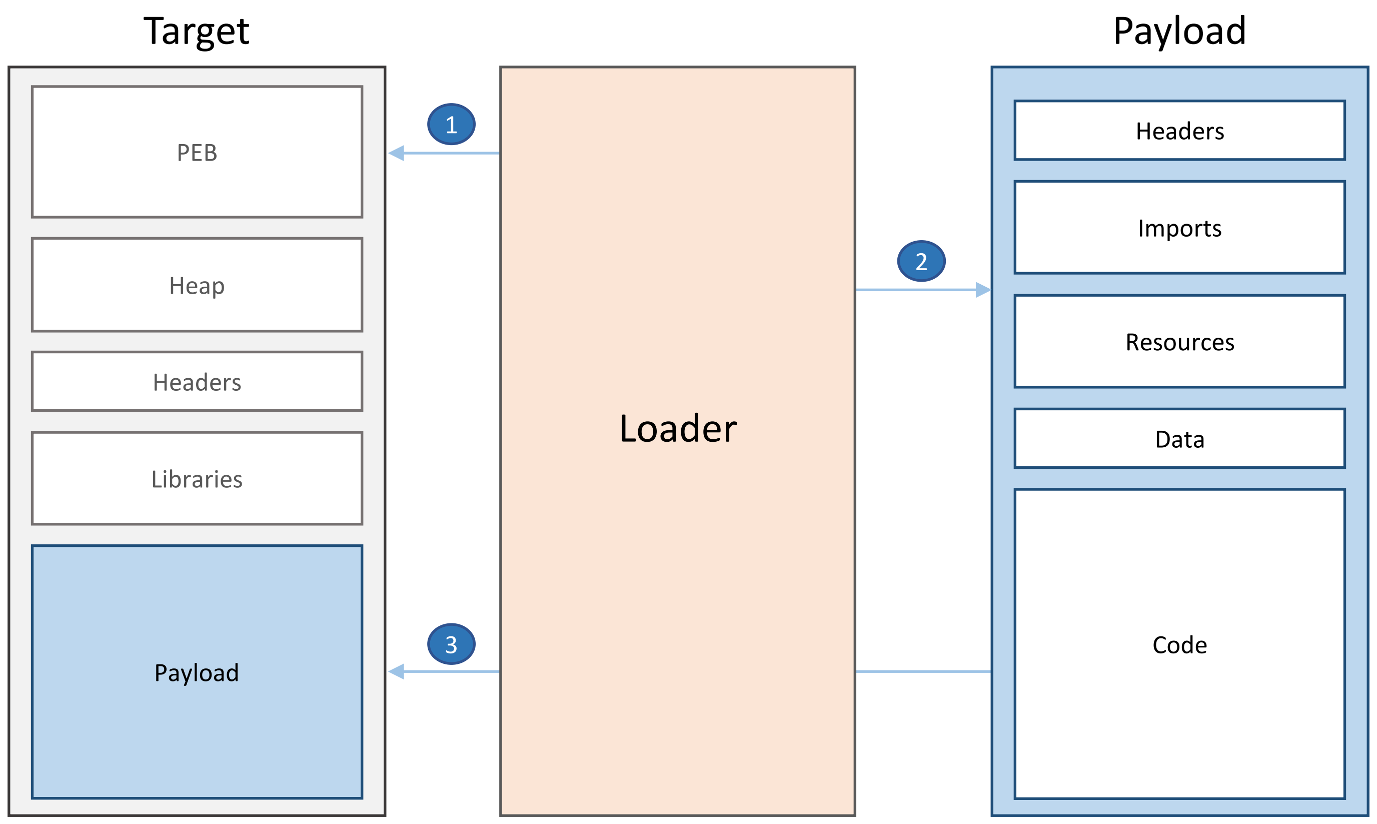
- Stages
  - A <u>new instance</u> of a (target) process is created
  - The code of the process is removed from memory
  - Memory is allocated in the process to put the content of a payload
  - The entry-point of the target process is swapped
  - The suspended thread of the target process is resumed



  - The (original, legit) Target process is never run
  - The (malicious) Payload process is never created

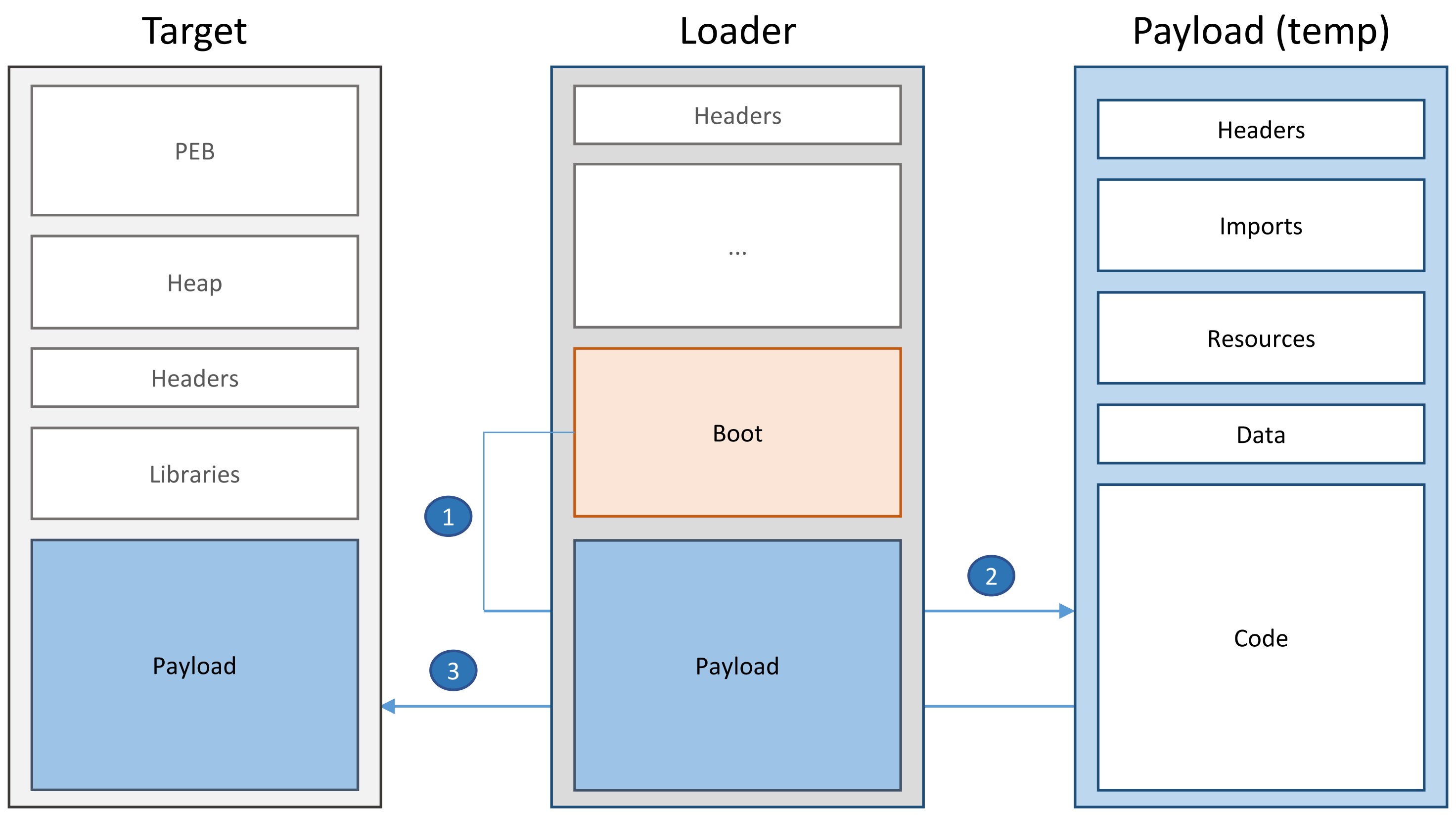
Windows Process Hollowing

- Actors > Scenario



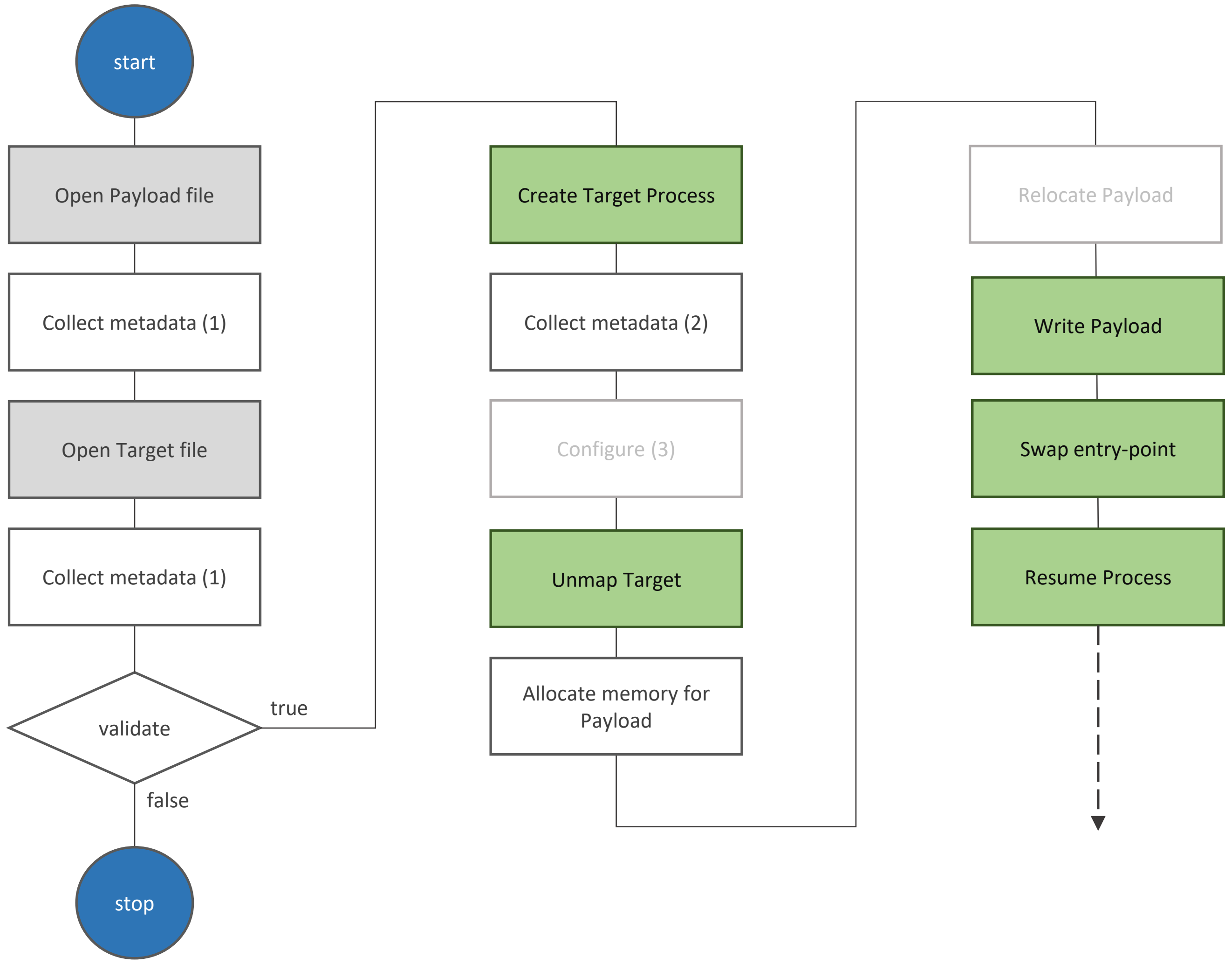
Windows Process Hollowing

- Actors > Scenario



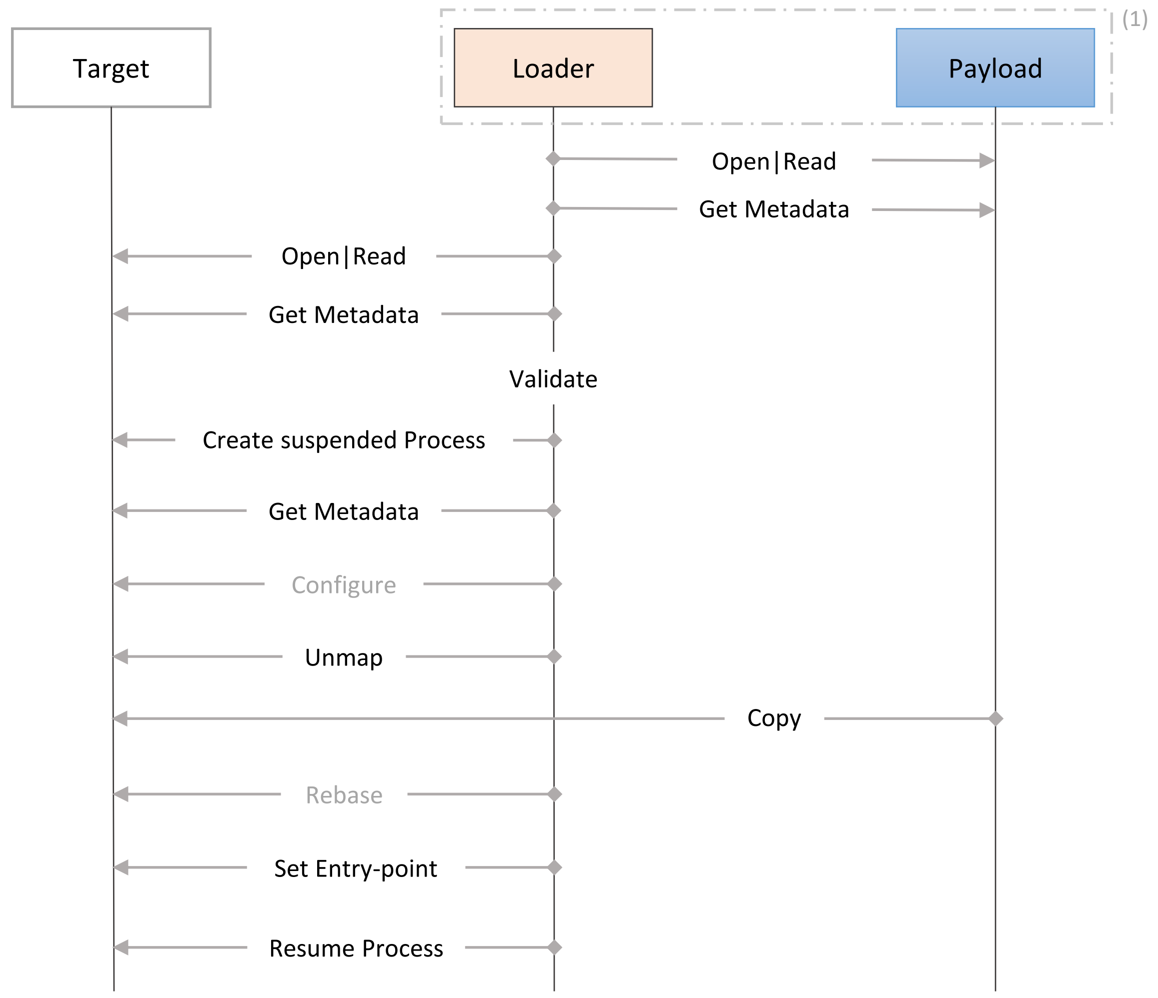
Windows Process Hollowing

- Steps



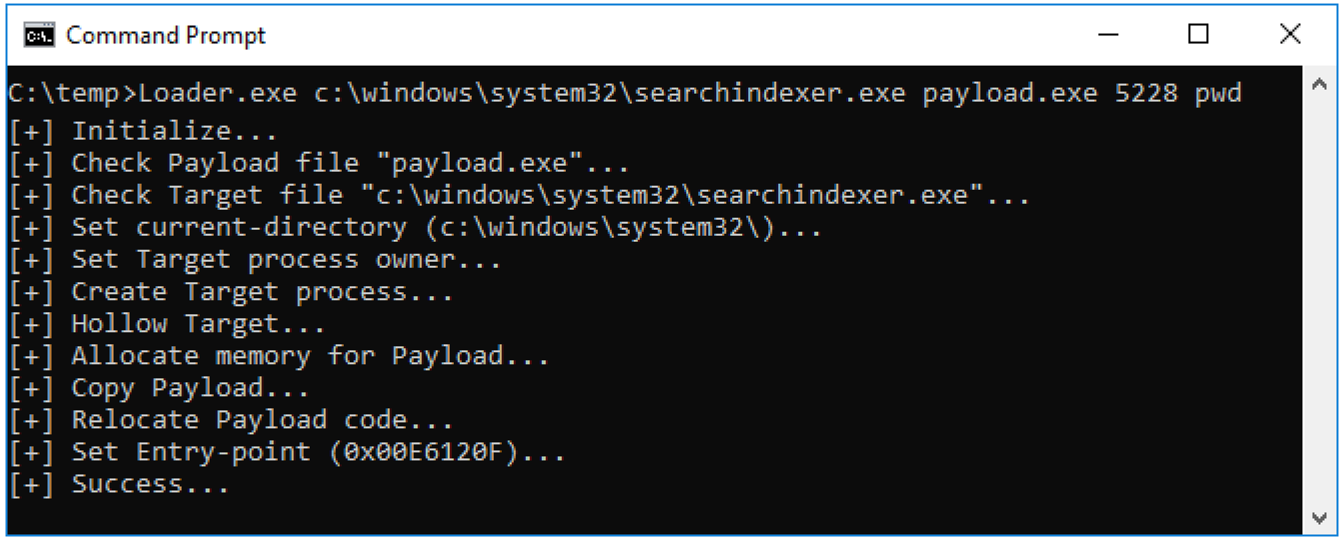
Windows Process Hollowing

- Sequences



Windows Process Hollowing

- Demo



```
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...
```

Windows Process Hollowing

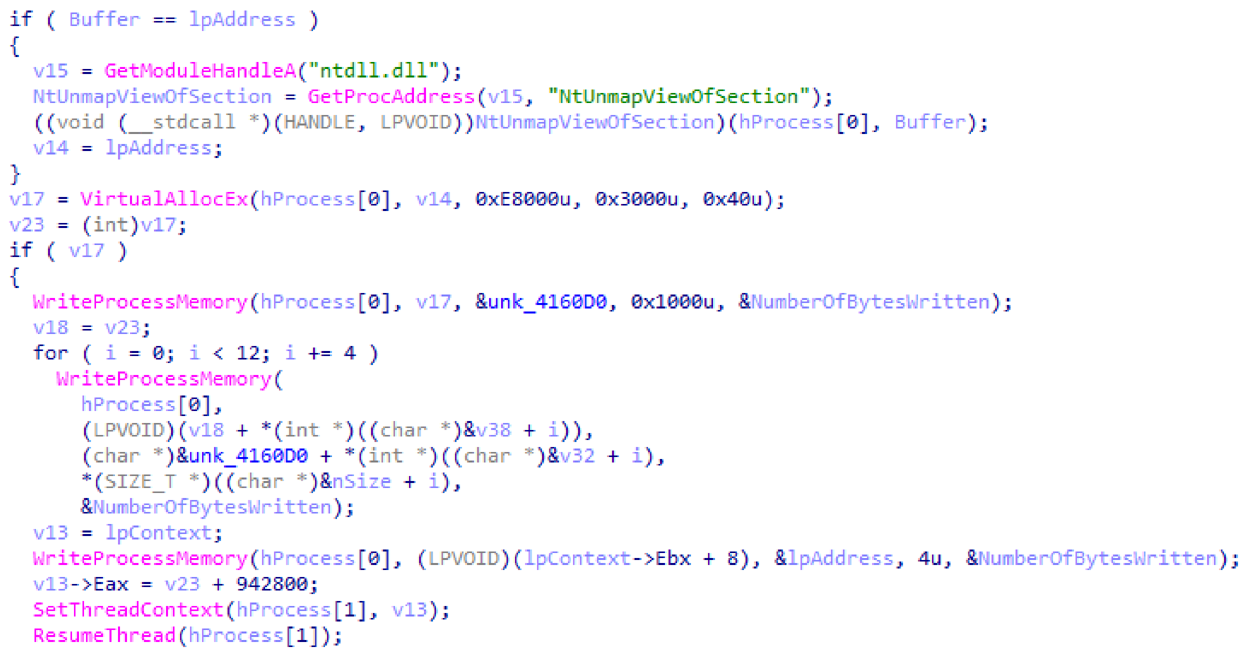
- Prerequisites
  - CPU width
  - Subsystem
  - Relocation Support
  - Integrity Level

	NATIVE	GUI	CUI
NATIVE	-	-	-
GUI	-	**x**	-
CUI	-	**x**	**x**

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

Windows Process Hollowing

- Indicators



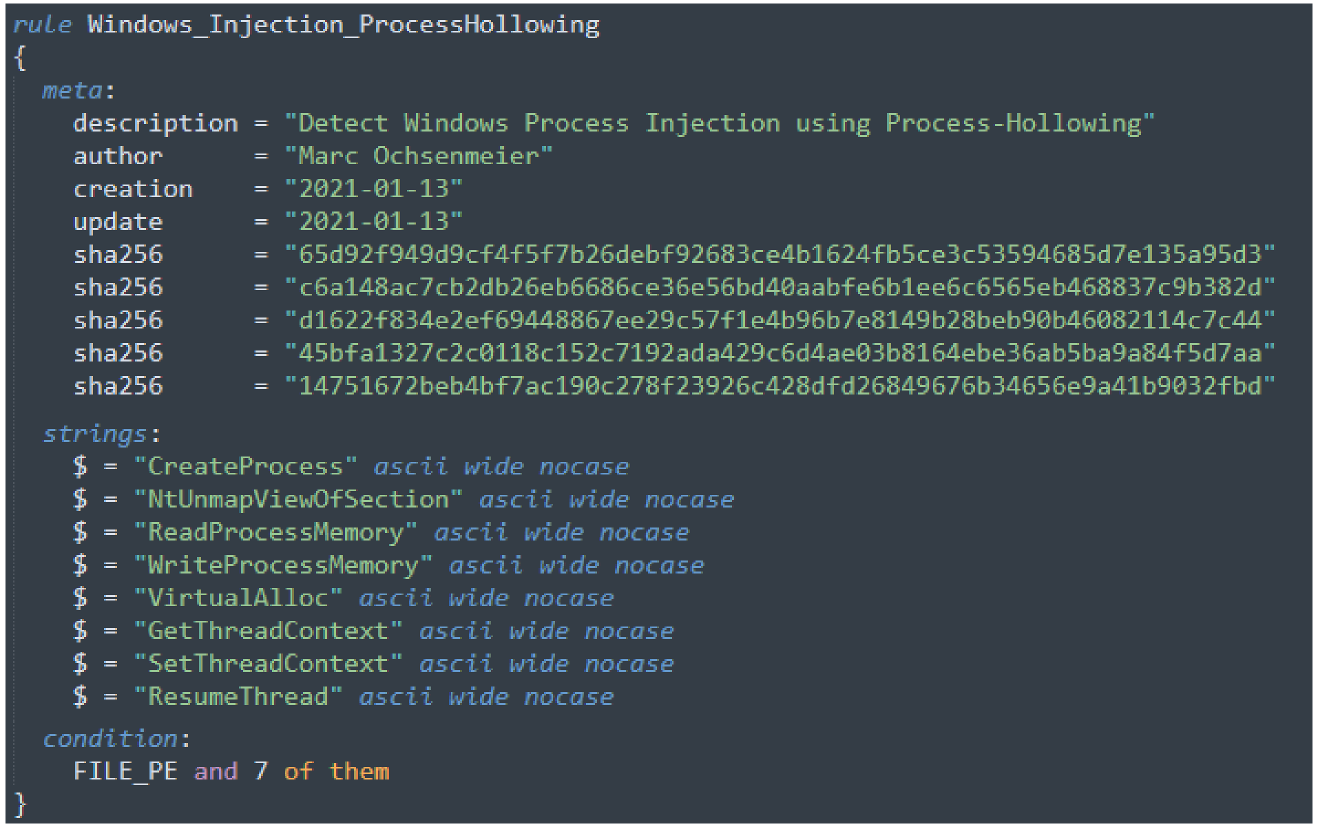
```
if ( Buffer == lpAddress )
{
  v15 = GetModuleHandleA("ntdll.dll");
  NtUnmapViewOfSection = GetProcAddress(v15, "NtUnmapViewOfSection");
  ((void (__stdcall *)(HANDLE, LPVOID))NtUnmapViewOfSection)(hProcess[0], Buffer);
  v14 = lpAddress;
}
v17 = VirtualAllocEx(hProcess[0], v14, 0xE8000u, 0x3000u, 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]);
```

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

md5,0580896027E9B92E00887E57202E27A8

Windows Process Hollowing

- Hunt > YARA



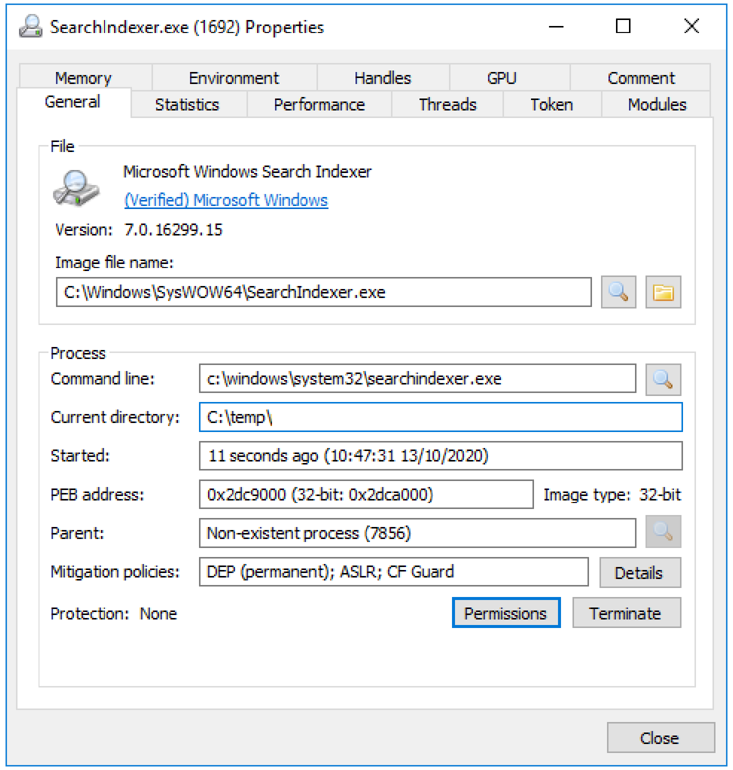
```
rule Windows_Injection_ProcessHollowing
{
  meta:
    description = "Detect Windows Process Injection using Process-Hollowing"
    author      = "Marc Ochsenmeier"
    creation    = "2021-01-13"
    update      = "2021-01-13"
    sha256      = "65d92f949d9cf4f5f7b26debf92683ce4b1624fb5ce3c53594685d7e135a95d3"
    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
}
```

Windows Process Hollowing

- Characteristics



File

Microsoft Windows Search Indexer
(Verified) Microsoft Windows

Version: 7.0.16299.15

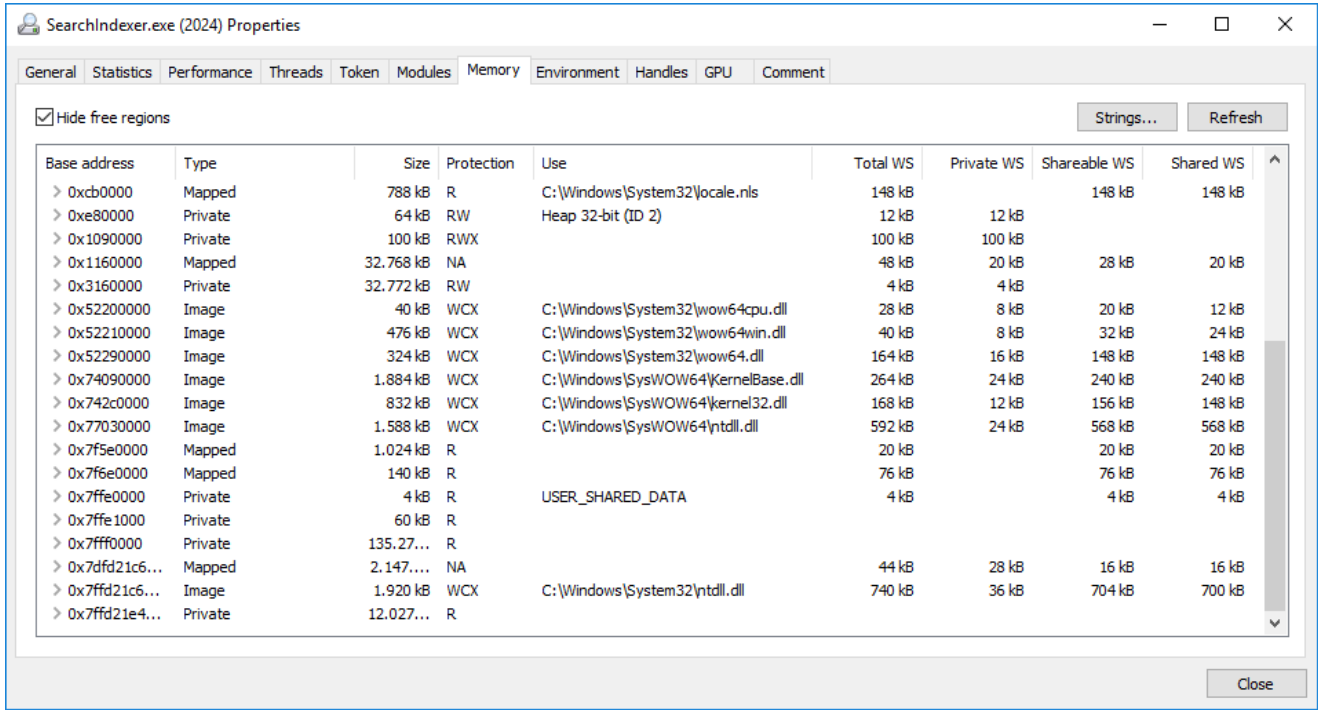
Image file name: C:\Windows\SysWOW64\SearchIndexer.exe

Process

Command line:	c:\windows\system32\searchindexer.exe
Current directory:	C:\temp\
Started:	11 seconds ago (10:47:31 13/10/2020)
PEB address:	0x2dc9000 (32-bit: 0x2dca000) Image type: 32-bit
Parent:	Non-existent process (7856)
Mitigation policies:	DEP (permanent); ASLR; CF Guard
Protection:	None

Windows Process Hollowing

- Characteristics

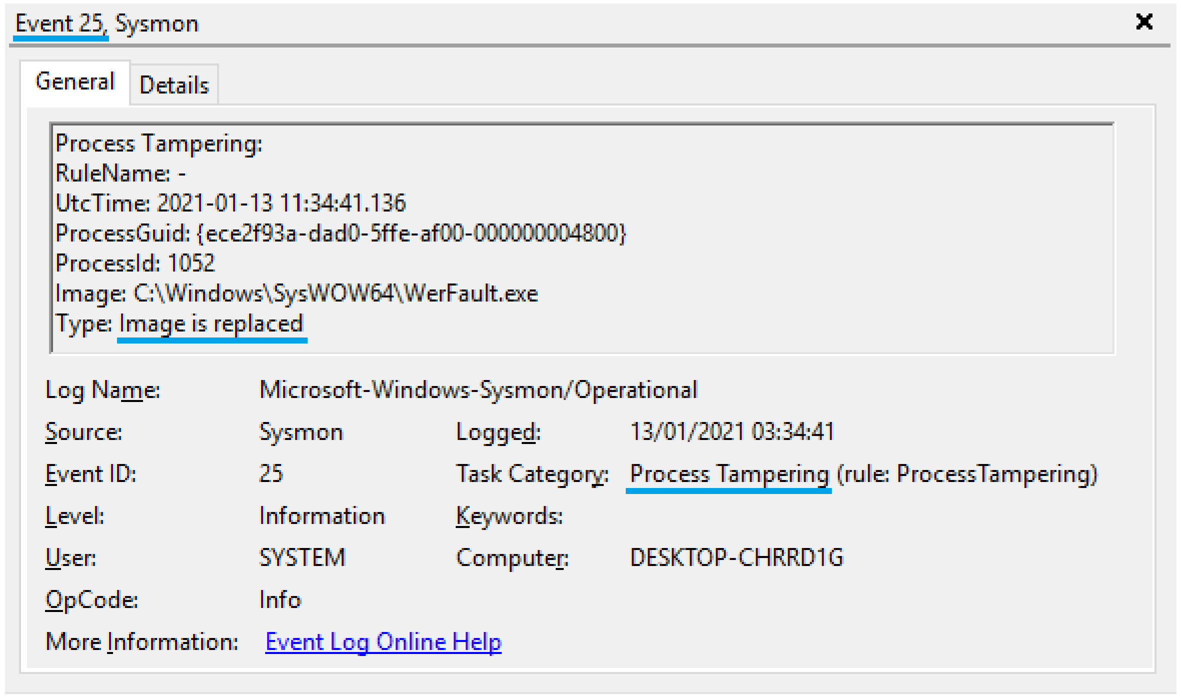


☑ Hide free regions

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					

Windows Process Hollowing

- Detection



Event 25, Sysmon

General | Details

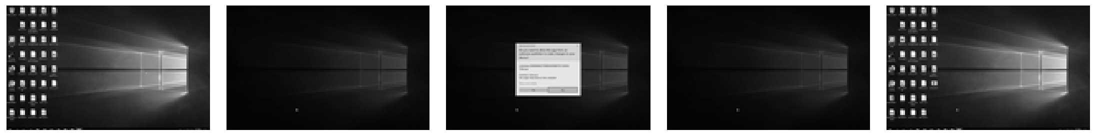
```
Process Tampering:
RuleName: -
UtcTime: 2021-01-13 11:34:41.136
ProcessGuid: {ece2f93a-dad0-5ffe-af00-000000004800}
ProcessId: 1052
Image: C:\Windows\SysWOW64\WerFault.exe
Type: Image is replaced
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	13/01/2021 03:34:41
Event ID:	25	Task Category:	Process Tampering (rule: ProcessTampering)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DESKTOP-CHRRD1G
OpCode:	Info		
More Information:	Event Log Online Help		

Windows Process Hollowing

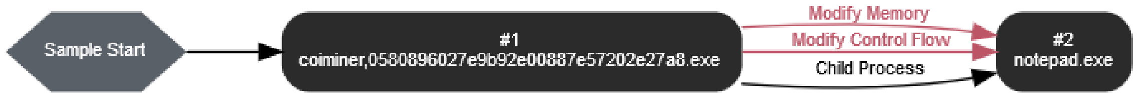
- Analysis

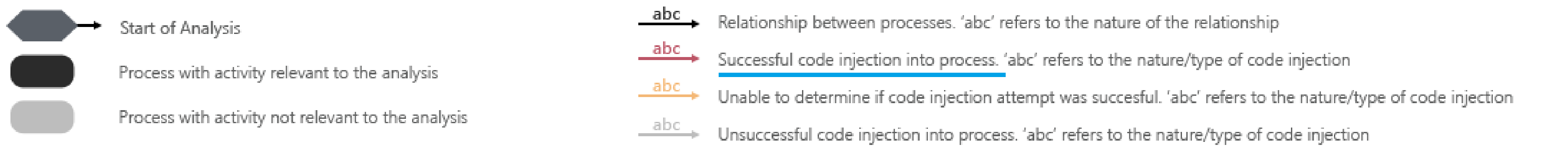
Screenshots



(VMRay)

Monitored Processes





⬣ →	Start of Analysis
⬛	Process with activity relevant to the analysis
⬜	Process with activity not relevant to the analysis

abc →	Relationship between processes. 'abc' refers to the nature of the relationship
abc →	Successful code injection into process. 'abc' refers to the nature/type of code injection
abc →	Unable to determine if code injection attempt was succesful. 'abc' refers to the nature/type of code injection
abc →	Unsuccessful code injection into process. 'abc' refers to the nature/type of code injection

Windows Process Hollowing

- 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

Windows Process Hollowing

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