Windows Process Injection - Process Hollowing

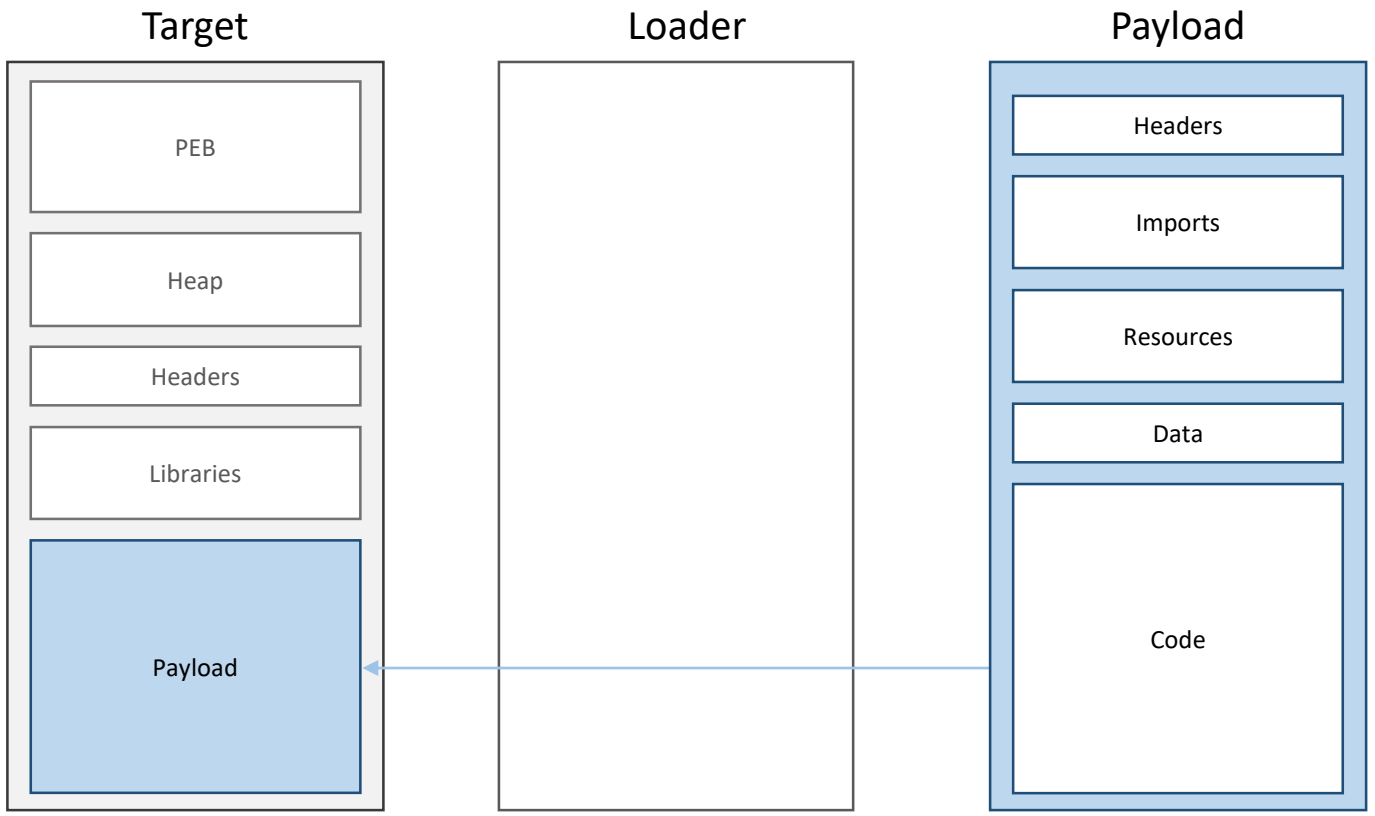
January, 2021

Marc Ochsenmeier

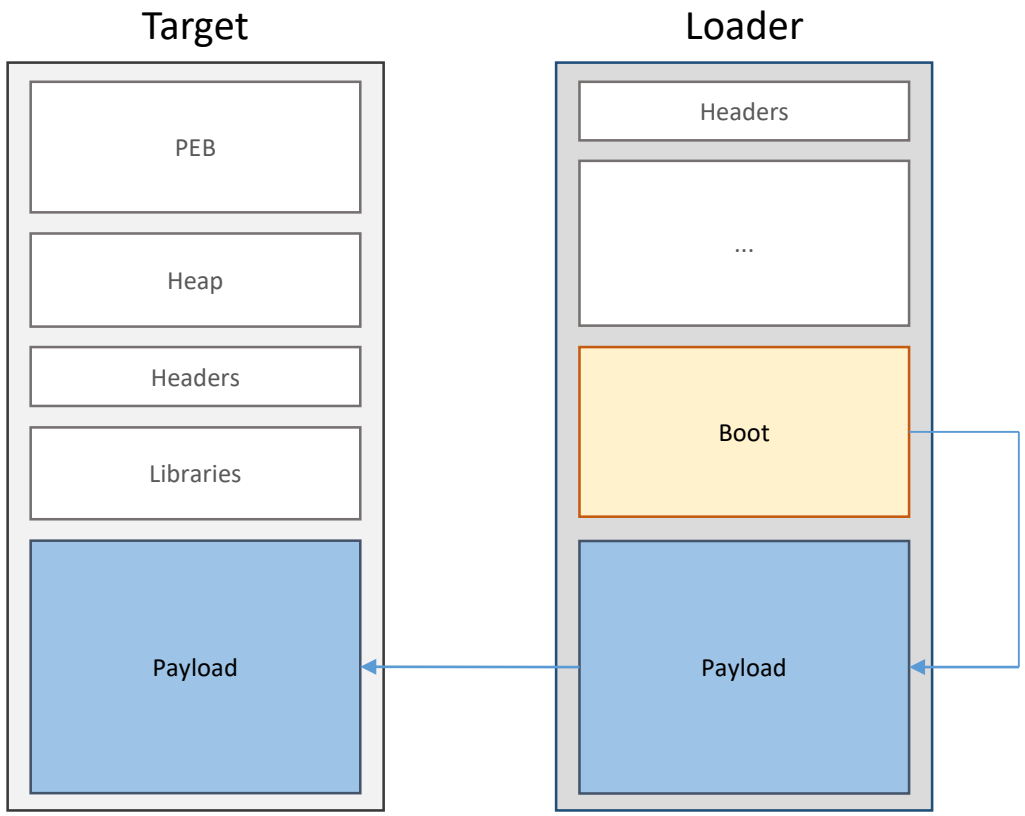
@ochsenmeier

www.winitor.com

- Actors

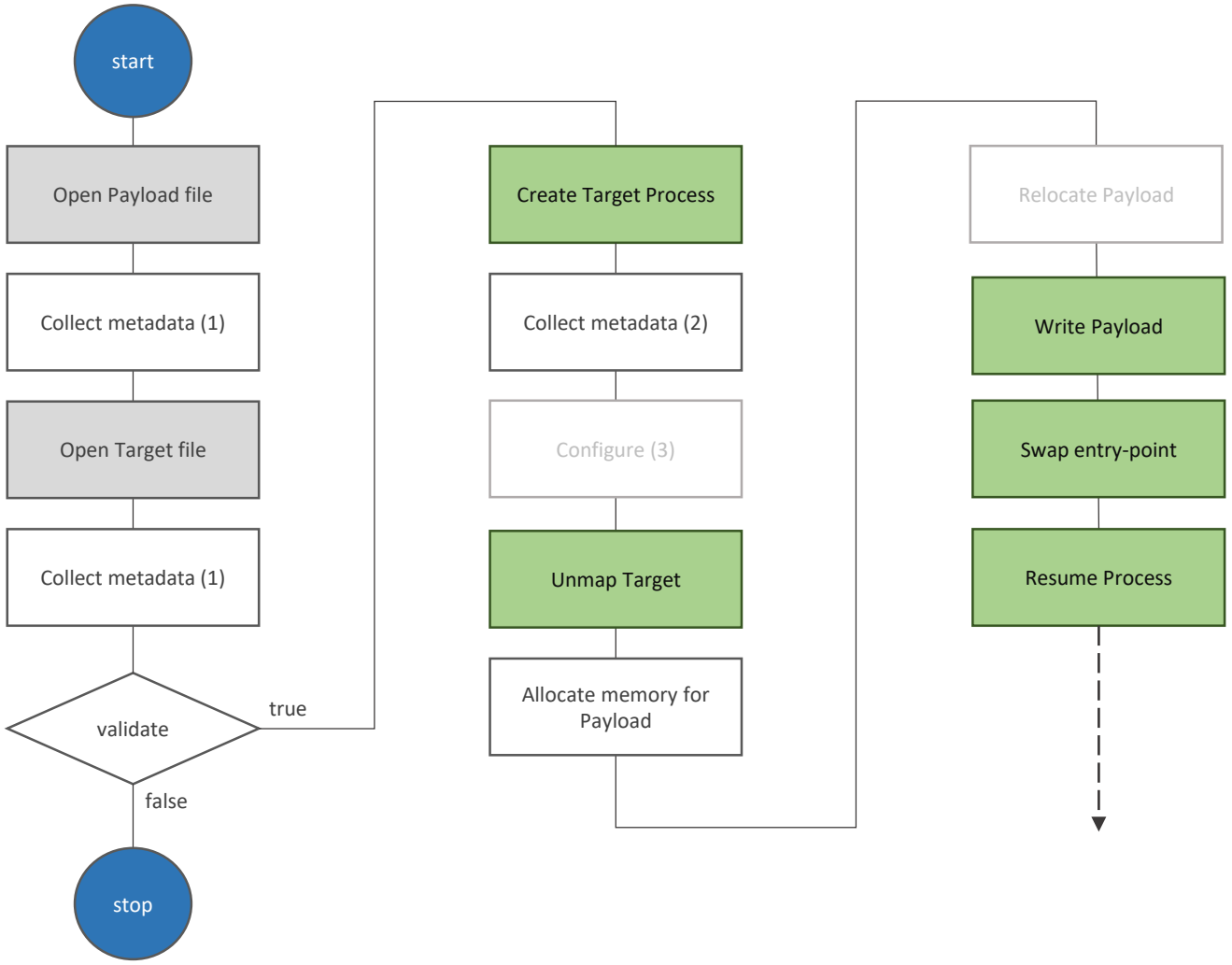


- Actors



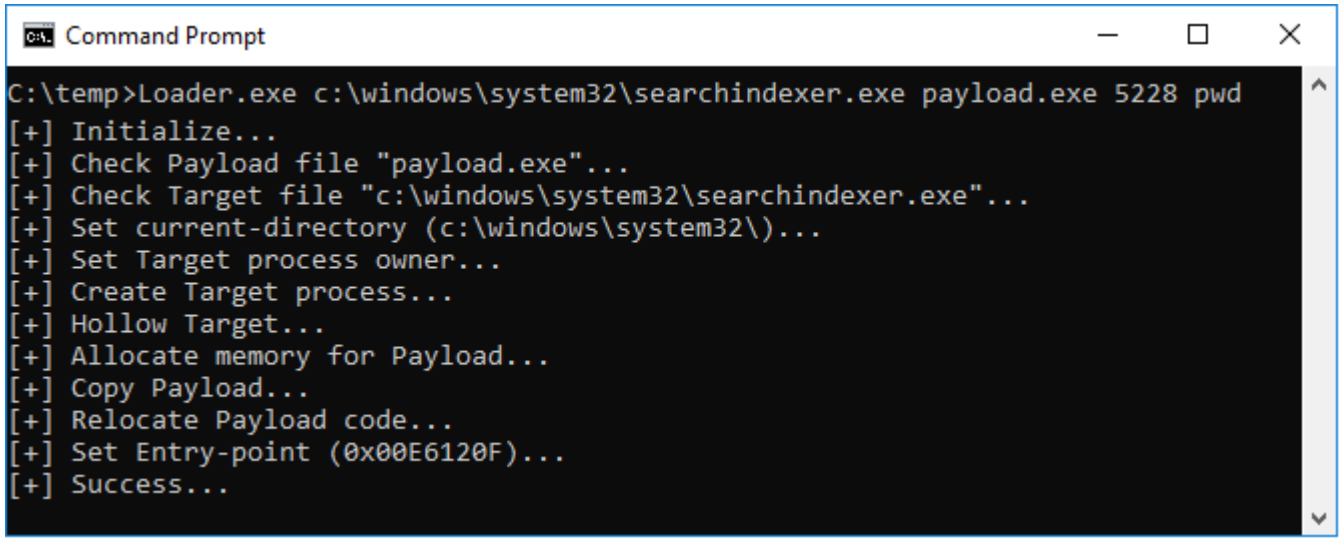
Windows Process Hollowing

- Logical Steps



Windows Process Hollowing

- Demo

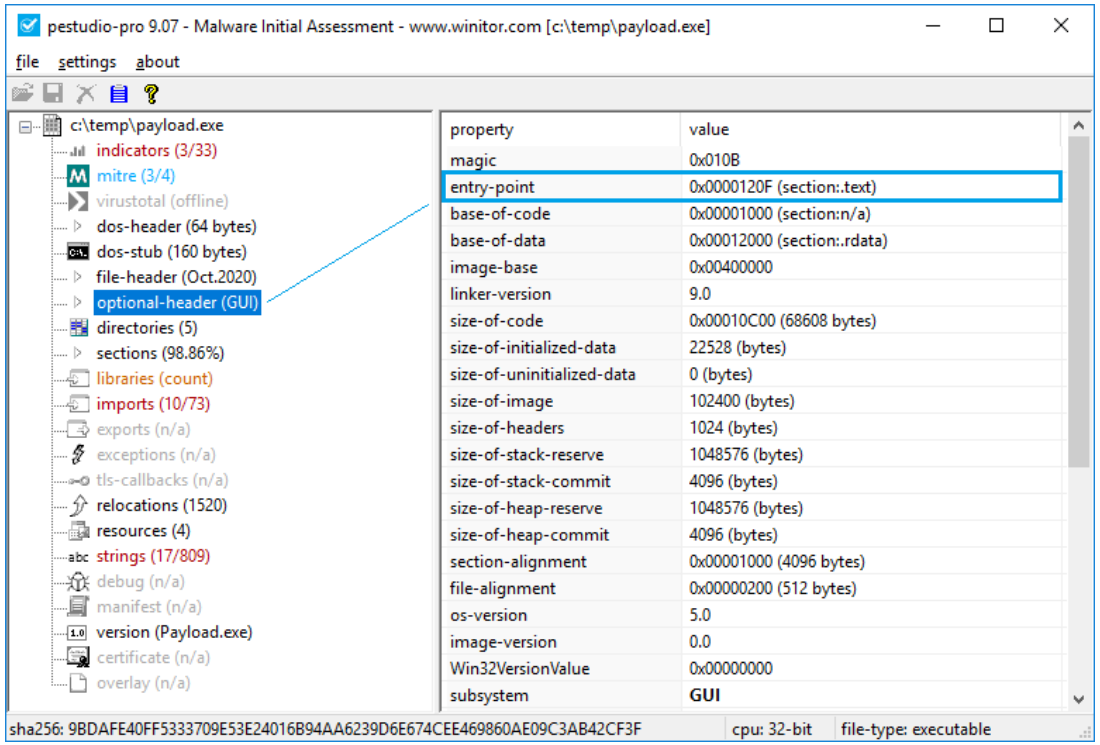


- Prerequisites > Environment
  - CPU width
  - Subsystem
  - Relocation Support
  - Integrity Level

	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



- 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]);
```

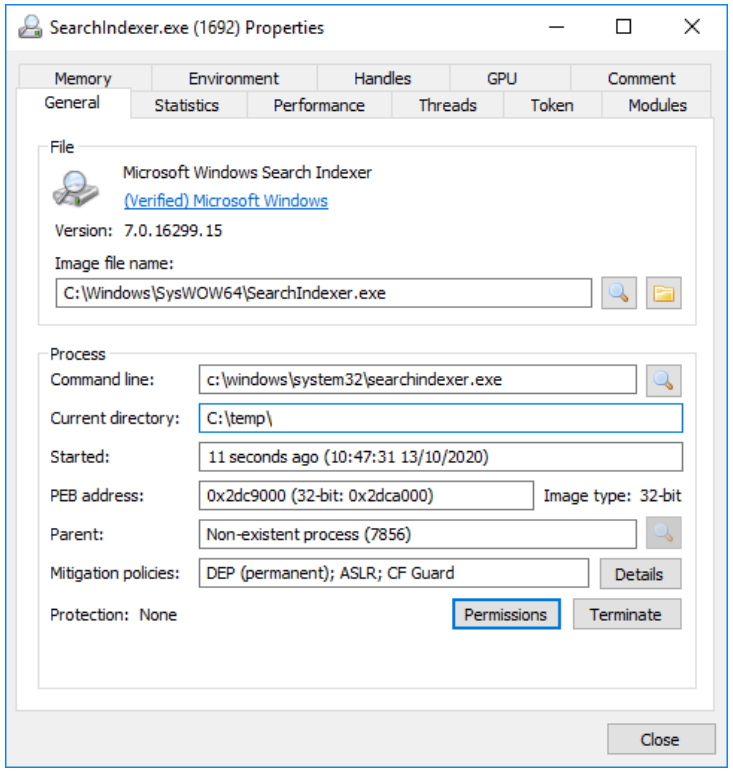
md5,0580896027E9B92E00887E57202E27A8

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

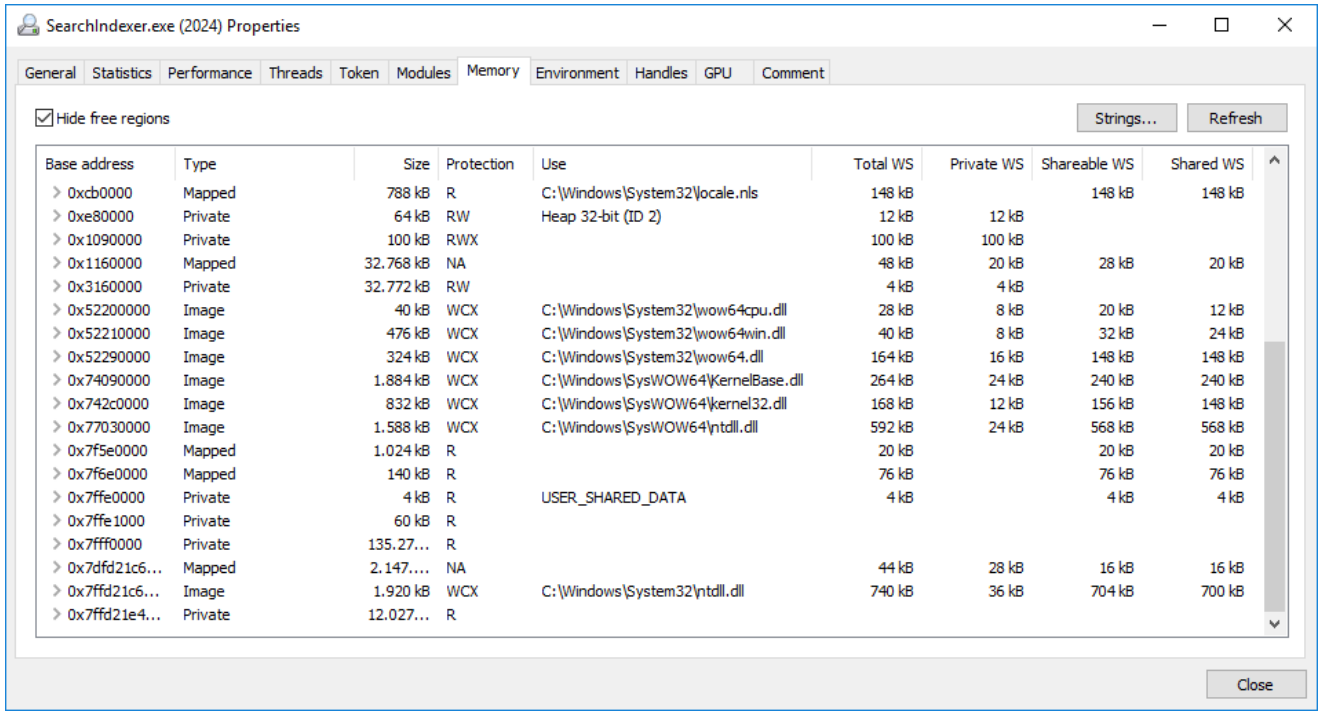
- Hunting > YARA

```
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      = "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
}
```

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

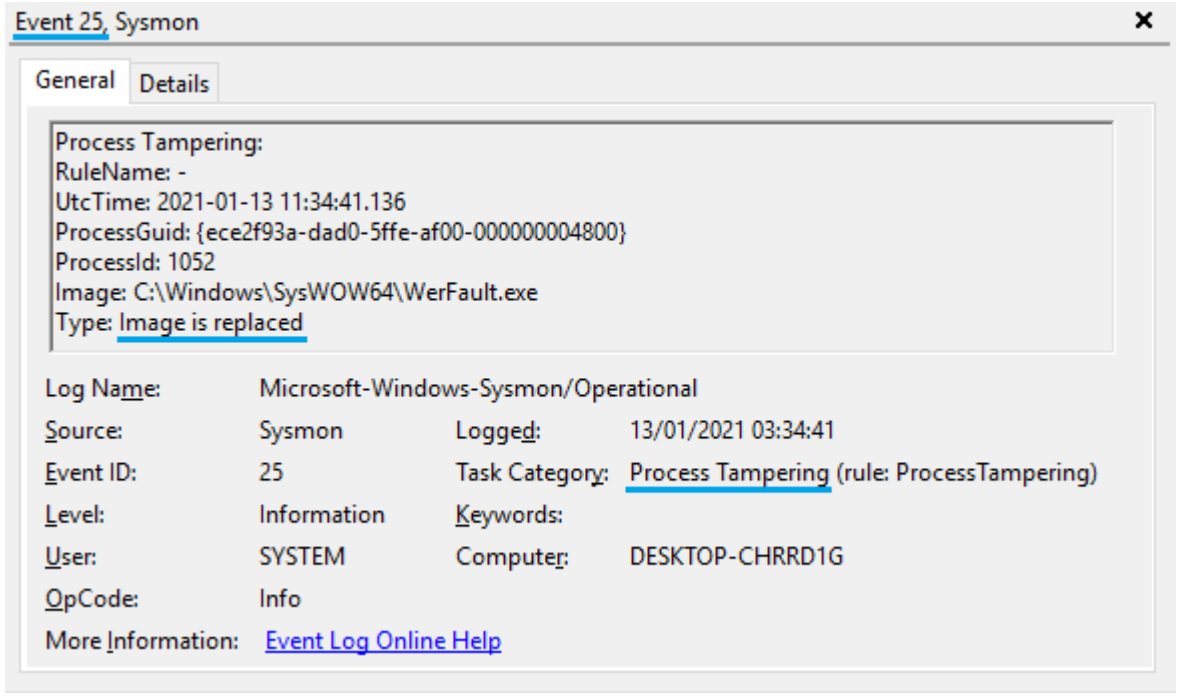


- Characteristics > Memory regions



Windows Process Hollowing

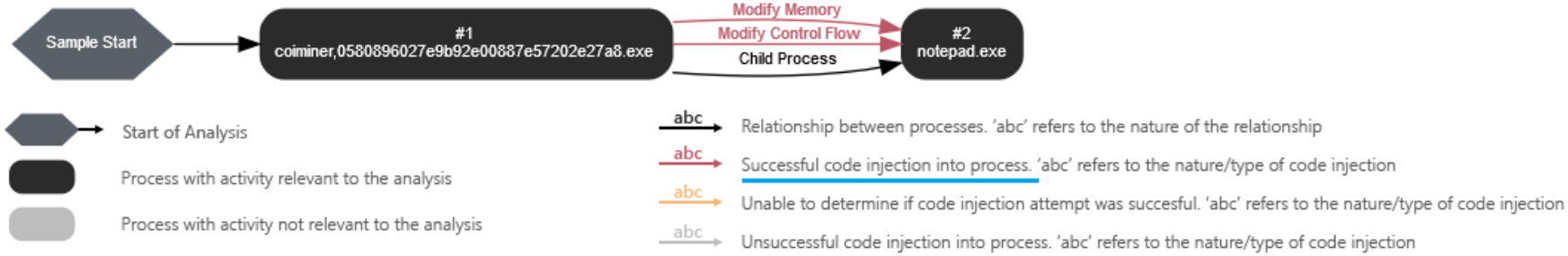
- Detection > Tools > Sysmon



- 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